PTO/AIA/01 (06-12)
Approved for use through 01/31/2014 OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Method and apparatus for emulating multiple cards in mobile devices

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____
  filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Xiangzhen Xie Date (Optional): 3/1/2013

Signature: Xie Xiangzhen

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Method and apparatus for emulating multiple cards in mobile devices

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Liang Seng Koh Date (Optional) 2/27/2013

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Method and apparatus for emulating multiple cards in mobile devices

As the below named inventor, I hereby declare that:

This declaration is directed to:

[■] The attached application, or

[ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

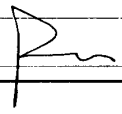
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Hsin Pan Date (Optional): 2/27/2013

Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office: U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

☒ Practitioners associated with Customer Number: 26797

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☐ The address associated with Customer Number:

OR

☐	Firm or Individual Name		
	Address		
	City	State	Zip
	Country		
	Telephone	Email	

Assignee Name and Address: RFCyber Corporation, 4160 Technology Drive, Suite A, Fremont, CA 94538

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	02/27/2013
Name	Hsin Pan	Telephone	(408)777-8873
Title	General Manager		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: RFCyber Corporation

Application No./Patent No.: Unassigned Filed/Issue Date: herewith

Titled: Method and apparatus for emulating multiple cards in mobile devices

RFCyber Corporation, a California corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/ joe zheng /	03/01/2013
Signature	Date
Joe Zheng	39,450
Printed or Typed Name	Title or Registration Number

ASSIGNMENT OF PATENT APPLICATION

Whereas I, an undersigned inventor, have invented certain new and useful improvements as set forth in the patent application entitled:

Method and apparatus for emulating multiple cards in mobile devices

(Docket No. RFID-084), (check one)

☑ for which I have executed a U.S. patent application on even date herewith. (Accompanying)
☐ which bears U.S. application No. . (Not accompanying)
☐ which is a U.S. provisional application. (Accompanying)

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I, an undersigned inventor, hereby:

1) Sell, assign and transfer to RFCyber Corp., a corporation in the State of California having a principal place of business at 4160 Technology Drive, Suite A, Fremont, CA 94538, USA ("ASSIGNEE"), the entire right, title and interest in any and all improvements and inventions disclosed in, applications based upon, and patents (including foreign patents and the right to claim priority) granted upon, the above-referenced application.

2) Authorize and request the Commissioner of Patents to issue any and all Letters Patents resulting from said application or any division, continuation, substitute, renewal, re-examination or reissue thereof to the ASSIGNEE.

3) Agree to execute all papers and documents and, entirely at the ASSIGNEE's expense, perform any acts which are reasonably necessary in connection with the prosecution of said application, as well as any derivative applications thereof, foreign applications based thereon, and/or the enforcement of patents resulting from such applications.

4) Agree that the terms, covenants and conditions of this assignment shall inure to the benefit of the ASSIGNEE, its successors, assigns and other legal representative, and shall be binding upon the inventor, as well as the inventor's heirs, legal representatives and assigns.

5) Warrant and represent that I have not entered, and will not enter into any assignment, contract, or understanding that conflicts with this assignment.

6) Authorize and request my representative to insert above the application No. in order to assist with recordal of this assignment.

Signed on the date indicated beside my signature.

1. Inventor Signature: Xie Xiangzhen — Date: 3/1/2013
Xiangzhen Xie

2. Inventor Signature: _____ Date: _____
Liang Seng Koh

3. Inventor Signature: _____ Date: 2/27/2013
Hsin Pan

ASSIGNMENT OF PATENT APPLICATION

Whereas I, an undersigned inventor, have invented certain new and useful improvements as set forth in the patent application entitled:

Method and apparatus for emulating multiple cards in mobile devices

(Docket No. RFID-084), (check one)

☒ for which I have executed a U.S. patent application on even date herewith. (Accompanying)
☐ which bears U.S. application No. . (Not accompanying)
☐ which is a U.S. provisional application. (Accompanying)

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I, an undersigned inventor, hereby:

1) Sell, assign and transfer to RFCyber Corp., a corporation in the State of California having a principal place of business at 4160 Technology Drive, Suite A, Fremont, CA 94538, USA ("ASSIGNEE"), the entire right, title and interest in any and all improvements and inventions disclosed in, applications based upon, and patents (including foreign patents and the right to claim priority) granted upon, the above-referenced application.

2) Authorize and request the Commissioner of Patents to issue any and all Letters Patents resulting from said application or any division, continuation, substitute, renewal, re-examination or reissue thereof to the ASSIGNEE.

3) Agree to execute all papers and documents and, entirely at the ASSIGNEE's expense, perform any acts which are reasonably necessary in connection with the prosecution of said application, as well as any derivative applications thereof, foreign applications based thereon, and/or the enforcement of patents resulting from such applications.

4) Agree that the terms, covenants and conditions of this assignment shall inure to the benefit of the ASSIGNEE, its successors, assigns and other legal representative, and shall be binding upon the inventor, as well as the inventor's heirs, legal representatives and assigns.

5) Warrant and represent that I have not entered, and will not enter into any assignment, contract, or understanding that conflicts with this assignment.

6) Authorize and request my representative to insert above the application No. in order to assist with recordal of this assignment.

Signed on the date indicated beside my signature.

1. Inventor Signature: _____ Date: _____
Xiangzhen Xie

2. Inventor Signature: _____ Date: 2/27/2013
Liang Seng Koh

3. Inventor Signature: _____ Date: _____
Hsin Pan

Samsung Ex. 1016, Page 8 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Filer:	Joe Zheng
Attorney Docket Number:	RFID-084

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	98	98
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**533**

Electronic Acknowledgement Receipt	
EFS ID:	15098638
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	01-MAR-2013
Filing Date:	
Time Stamp:	18:29:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$533
RAM confirmation Number	6386
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Specification	PatentAsFiled.pdf	236720 32ad80c1263ec1e99ae1dcb5b83ee0370fc4e521	no	59
Warnings:					
Information:					
2	Drawings-only black and white line drawings	Drawings.pdf	1125222 9291819fc69bb737620ed0c6a9126de0f6a975a3	no	35
Warnings:					
Information:					
3	Application Data Sheet	ADS.pdf	1433533 2cbb460a0564d000781dfefbe15ce6987cacae2b	no	7
Warnings:					
Information:					
4	Oath or Declaration filed	SignedDeclaration.pdf	1381715 465c223c4e781395399fc0f974ef96edd6d3dd50	no	3
Warnings:					
Information:					
5	Power of Attorney	SignedPOA.pdf	1257763 7bf878df96738843bd662754f1f3cf434ef1d6d9	no	5
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	32572 35388d395f265fbf92618ea4f4419ba3fca70271	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	5467525		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: RFID-084

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT APPLICATION

FOR

Method and apparatus for emulating multiple cards in mobile devices

Inventor(s): Xiangzhen Xie
C505, Long Tai Xuan, Nanguang Village
Nanshang District
Shenzhen, Guangdong Province, 518051, China
Citizenship: P. R. China

Liang Seng Koh
41291 Carmen Street
Fremont, CA 94539, USA
Citizenship: USA.

Hsin Pan
2374 Olive Avenue
Fremont, CA 94539, USA
Citizenship: USA.

Express Mail Label # E-filing Date of Deposit: March 1, 2013
I hereby certify that this paper or fee is being deposited with the United States Postal Service using "Express Mail Post Office To Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to "Mail Stop: New Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313"

Signed: / joe zheng /
Joe Zheng

Samsung Ex. 1016, Page 14 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Method and apparatus for emulating multiple cards in mobile devices

Xiangzhen Xie
Liang Seng Koh
Hsin Pan

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention is generally related to the area of electronic commerce. Particularly, the present invention is related to a mobile device configured to support multiple cards (e.g., Mifare) or applications of similar type.

The Background of Related Art

[0002] A contactless smart card is a pocket-sized card with embedded integrated circuits that can process and store data, and communicate with a terminal via radio waves. Contactless smart cards do not contain an ordinary read-only RFID, but they do contain a re-writeable smart card microchip that can be transcribed via radio waves. Contactless smart cards can be used for identification, authentication, and data storage. They provide a means of effecting business transactions in a flexible, secure, standard way with minimal human intervention.

[0003] MIFARE is one of the most popular contactless cards used in many daily applications such as building door access, car park entrance, and transit e-purse. MIFARE or Mifare is the NXP Semiconductors-owned trademark of a series of chips widely used in contactless smart cards or proximity cards. A Mifare classic card is fundamentally just a memory storage device, where the memory is divided into segments and blocks with simple security mechanisms for access control. Many people may have more than one Mifare cards in their wallets, for example, one for transit use, one for meals, and one for admission. As mobile devices with near field communication (NFC) capability (thus NFC devices) are being advanced to replace

Samsung Ex. 1016, Page 15 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

the wallets, it is important for these NFC devices to support more than one Mifare cards. However, a current NFC device is loaded with only one emulator and could be designed to function as one contactless card, such as a Mifare card for transportation, there is a need for solutions to make an NFC device with an emulator to support or function as many Mifare cards as possible.

SUMMARY OF THE INVENTION

[0004] This section is for the purpose of summarizing some aspects of the present invention and to briefly introduce some preferred embodiments. Simplifications or omissions may be made to avoid obscuring the purpose of the section. Such simplifications or omissions are not intended to limit the scope of the present invention.

[0005] The present invention is related to techniques for mobile devices configured to support or function as multiple contactless cards, such as Mifare contactless card commonly used. According to one aspect of the present invention, a mobile device embedded with an emulator is loaded with a plurality of software modules or applications, each emulating or simulating one card or one type of contactless cards. An emulator is implemented in a secure element that is personalized for a user of the mobile device while the applications are respectively provisioned via their respective providers per the personalized secure element. When the mobile device is to be used as a contactless card to perform a set of monetary functions, a corresponding application is loaded into and executed in the emulator. When the mobile device is to be used to perform another set of monetary functions, a corresponding application is loaded into the emulator to replace the previous application entirely or partially in the emulator. As a result, the mobile device can be used as a monetary device in lieu of multiple contactless cards.

[0006] According to still another aspect of the present invention, the mobile device is a near field communication (NFC) device and being part of a mobile payment ecosystem in which various parties are work with each other in order for the mobile payment ecosystem successful. Via a server (e.g., implemented as a manager)

Samsung Ex. 1016, Page 16 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

configured to provide what is referred to herein as Trusted Service Management (TSM), the secure element in the mobile device can be remotely personalized and the applications can be downloaded, updated, managed or replaced after they are respectively provisioned via the Trusted Service Manager (i.e., the TSM server).

[0007] According to still another aspect of the present invention, for supporting the Mifare contactless cards, a module (implemented as a manager) providing Trusted Mifare Service Management (TMSM) is provided to manage the provisioned applications in the mobile device to emulate the mobile device as multiple contactless cards. A card proxy manager implemented in the mobile device to facilitate communication between the TSM server and the TMSM module in the secure element. Additional applications are also implemented in the mobile devices to provide specific functions to read only specific data from one of the applications simulating a contactless card or write transactional activities into the application.

[0008] According to still another aspect of the present invention, when an application (e.g., a Mifare contactless card or an e-purse supporting the Mifare contactless card) is being provisioned, security keys (either symmetric or asymmetric) are personalized within a three-tier security model so as to be able to perform secured transaction with a payment server. An example of the three-tier security model includes a physical security, an e-purse security and an SE security, concentrically encapsulating one with another. In one embodiment, the essential data to be personalized into the e-purse include one or more operation keys (e.g., a load or top-up key and a purchase key), default personal identification numbers (PINs), administration keys (e.g., an unblock PIN key and a reload PIN key), and passwords (e.g., from a service provider such as Mifare). During a transaction, the security keys are used to establish a secured channel between a provisioned e-purse and a Security Authentication Module (SAM) or backend server in a financial institute (e.g., bank, credit union, credit clearing bureau, etc.).

[0009] According to yet another aspect of the present invention, a portable device is configured to conduct e-commerce and/or m-commerce as an electronic mobile seller (e.g., mobile POS). E-commerce and m-commerce operations (i.e.,

Samsung Ex. 1016, Page 17 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

offline payment, online payment, real time top-up, virtual top-up, batch transactions upload, and various queries of balances and transactions) can be conducted using the portable device with a POS application (e.g., a manager) and a POS SAM installed therein.

[0010] One important features, advantages and benefits in the present invention is to enable a mobile device to support multiple contactless cards. The present invention may be implemented as a single device, a server, a system or a part of system. It is believed that various implementations may lead to results that may not be achieved conventionally.

[0011] According to one embodiment, the present invention is a mobile device comprising: an emulator; a near field communication (NFC) interface to facilitate data exchange between a reader and an application being loaded and executed in the emulator, wherein the application in the emulator being one of the applications is replaceable in entirety or in part by another one of the applications; and a storage device configured to store the multiple applications, anyone of the applications being loadable into the emulator when selectively activated and subsequently replacing the application in the emulator, wherein the mobile device changes functions offered by the application to functions offered by another application newly loaded and executed in the emulator, wherein each of the applications has been remotely provisioned by a server configured to provide trusted service management (TSM).

[0012] In the embodiment, the emulator is implemented in the secure element, that is enclosed in the mobile device or in a detachable card to the mobile device. Each of the applications simulating functions of one of contactless cards is provided respectively to perform a function related to monetary, the mobile device is able to be used for all of the contactless cards when the applications are respectively loaded into and executed in the emulator.

[0013] According to another embodiment, the present invention is a method for a mobile device to support multiple applications, the method comprises: installing the applications respectively in the mobile device, each of the applications pertaining to a

Samsung Ex. 1016, Page 18 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

physical contactless card, so that the mobile device is to be used in lieu of multiple physical contactless cards.

[0014] Other objects, features, and advantages of the present invention will become apparent upon examining the following detailed description of an embodiment thereof, taken in conjunction with the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

[0016] FIG. 1A shows a simplified system in which two exemplary computing devices and 104 being respectively configured to support multiple contactless cards according to one embodiment of the present invention;

[0017] FIG. 1B shows two different models of security channel supports that may be used for an on-board trusted service manager in the mobile device;

[0018] FIG. 1C shows a block diagram of a simplified architecture of an NFC-enabled mobile device with a secure element (SE) that may be used in FIG. 1A;

[0019] FIG. 1D shows a flowchart or process of personalizing an SE according to one embodiment of the present invention;

[0020] FIG. 1E shows relationships among an SE manufacturer, a TSM admin and the TSM system for both offline and online modes;

[0021] FIG. 1F illustrates data flows among a user for an NFC device (e.g., an NFC mobile phone), the NFC device itself, a TSM server, a corresponding SE manufacturer and an SE issuer;

[0022] FIG. 1G shows a data flowchart or process of personalizing data flow among three entities: a land-based SAM or a network e-purse server, an e-purse acting as a gatekeeper, and a single function tag, according to one embodiment;

Samsung Ex. 1016, Page 19 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0023] FIG. 2A shows a mobile payment ecosystem in which related parties are shown in order for the mobile payment ecosystem successful;

[0024] FIG. 2B shows a flowchart or process of provisioning one or more applications according to one embodiment;

[0025] FIG. 2C shows a data flow illustrating various interactions among different parties when an application is being provisioned in one embodiment;

[0026] FIG. 2D shows a data flow among different entities when preparing the application data in provisioning an application;

[0027] FIG. 2E shows a flowchart or process for locking or disabling an installed application;

[0028] FIG. 2F shows an exemplary architecture diagram of a portable device enabled as an e-purse conducting e-commerce and m-commerce, according to one embodiment of the present invention;

[0029] FIG. 3A is a block diagram of related modules interacting with each other to achieve what is referred to herein as e-purse personalization by an authorized personnel (a.k.a., personalizing a mobile device or a secure element therein while provisioning an application);

[0030] FIG. 3B shows a block diagram of related modules interacting with each other to achieve what is referred to herein as e-purse personalization by a user of the e-purse;

[0031] FIG. 3C shows a flowchart or process of personalizing an e-purse according to one embodiment of the present invention;

[0032] FIG. 4A and FIG. 4B show together a flowchart or process of financing, funding, load or top-up an e-purse according to one embodiment of the present invention;

[0033] FIG. 4C shows an exemplary block diagram of related blocks interacting with each other to achieve the process FIG. 4A and FIG. 4B;

Samsung Ex. 1016, Page 20 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0034] FIG. 5A is a diagram showing a first exemplary architecture of a portable device for enabling e-commerce and m-commerce functionalities over a cellular communications network (i.e., 3G, LTE or GPRS network), according an embodiment of the present invention;

[0035] FIG. 5B is a diagram showing a second exemplary architecture of a portable device for enabling e-commerce and m-commerce functionalities over a wired and/or wireless data network (e.g., Internet), according another embodiment of the present invention;

[0036] FIG. 5C is a flowchart illustrating an exemplary process of enabling the portable device of FIG. 5A for services/applications provided by one or more service providers in accordance with one embodiment of the present invention;

[0037] FIG. 6A is a diagram showing an exemplary architecture, in which a portable device is enabled as a mobile POS conducting e-commerce and m-commerce, according to one embodiment of the present invention;

[0038] FIG. 6B is a diagram showing an exemplary architecture, in which a portable device is enabled as a mobile POS conducting a transaction upload operation over a network, according to an embodiment of the present invention;

[0039] FIG. 6C is a flowchart illustrating an exemplary process of conducting m-commerce using the portable device enabled as a mobile POS with an e-token enabled device as a single functional card in accordance with one embodiment of the present invention;

[0040] FIG. 6D is a flowchart illustrating an exemplary process of conducting m-commerce using the portable device enabled as a mobile POS against a an e-token enabled device as a multi-functional card;

[0041] FIG. 7 is a diagram depicting an exemplary configuration in which a portable device used for an e-ticking application;

[0042] FIG. 8A shows a diagram of multiple parties involved in a TSM operated and orchestrated by a business;

Samsung Ex. 1016, Page 21 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0043] FIG. 8B shows relevant operations among the parties in the TSM according to one embodiment;

[0044] FIG. 8C shows a work flow among multiple parties to establish mutually agreed arrangement in an exemplary TSM;

[0045] FIG. 8D shows a data flow for an ISD mapping between an SE issuer and a TSM;

[0046] FIG. 8E shows a corresponding data flow among a server provider, an SE issuer and a TSM;

[0047] FIG. 8F shows a data flow for the approval of an application by an SE issuer;

[0048] FIG. 8G shows a process of replacing an SE; and

[0049] FIG. 9 shows an exemplary snapshot of a screen display for a personalized SE in an account.

DETAILED DESCRIPTION OF THE INVENTION

[0050] In the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. The present invention may be practiced without these specific details. The description and representation herein are the means used by those experienced or skilled in the art to effectively convey the substance of their work to others skilled in the art. In other instances, well-known methods, procedures, components, and circuitry have not been described in detail since they are already well understood and to avoid unnecessarily obscuring aspects of the present invention.

[0051] Reference herein to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one implementation of the invention. The appearances of the phrase “in one embodiment” or “in the embodiment” in various places in the specification are not necessarily all referring to the same embodiment,

Samsung Ex. 1016, Page 22 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

nor are separate or alternative embodiments mutually exclusive of other embodiments. Further, the order of blocks in process, flowcharts or functional diagrams representing one or more embodiments do not inherently indicate any particular order nor imply limitations in the invention. As used in this specification and the appended claims, the singular forms "a," "an," and "the" include plural referents unless the context clearly dictates otherwise. It should also be noted that the term "or" is generally employed in its sense including "and/or" unless the context clearly dictates otherwise.

[0052] Embodiments of the present invention are discussed herein with reference to FIGS. 1A-9. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes only as the invention extends beyond these limited embodiments.

[0053] Near Field Communication (NFC) presents significant business opportunities when used in mobile devices for applications such as payment, transport ticketing, loyalty, physical access control, and other exciting new services. To support this fast evolving business environment, various NFC-enabled mobile phones or devices are being advanced to support various contactless smart cards that are popularly used in various applications.

[0054] According to one embodiment of the present invention, FIG. 1A shows a simplified system 100 in which two exemplary computing devices 102 and 104 are being configured to support multiple contactless cards or used in lieu of multiple contactless cards. Instead of brining a number of cards, each for one purpose, one embodiment of the current invention allows a user to bring only one mobile device for all uses for the cards. Unless otherwise explicitly indicated, the term of “computing device”, “mobile device”, “smart phone”, “portable device” or “handset” will be interchangeably used herein, but those skilled in the art will understand the description herein shall be equally applicable to other devices such as a smart phone, a tablet, a laptop computer, and other portable device with the capability of near field communication.

[0055] As it is well known, Mifare is one of the most popular contactless cards used in many daily applications, where Mifare is the NXP Semiconductors-owned

Samsung Ex. 1016, Page 23 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

trademark of a series of chips widely used in contactless smart cards or proximity cards. To facilitate the understanding of the present invention, the description herein is based on the Mifare cards. Those skilled in the art shall understand that the description herein is equally applicable to cards other than the Mifare cards.

[0056] To support multiple cards, in one embodiment, an on-card Trusted Mifare Service Manager 106 (implemented as a module or an applet) is provided in a secure element (SE) 108. As further described below, depending on implementation, the SE 108 may be embedded in an NFC device 102 or 104 or a detachable card (e.g., a SD card or a microSDHC card) to a device. The NFC device 102 may be a mobile device embedded with the SE 108 while the NFC device 104 may be a smart card or a device upgradable with a detachable card embedded with the SE 108. In one embodiment, the NFC device 104 communicates with the SE 108 via a reader 110. In any case, it is assumed that either one of the NFC devices 102 and 104 is equipped with a secure element (e.g., the SE 108) that is personalized before a function requiring security can be performed with the NFC devices 102 or 104. The details of personalizing the SE 108 will be further provided herein when it deems necessary.

[0057] According to one embodiment of the present invention, the NFC device 102 or 104 includes a card manager proxy 112 that facilitates the communication between a Trusted Service Manager (i.e., TSM server) 114 and the TMSM 106, a set of readonly wallet user interface (UI) applications 116 and transaction wallet applications 118. The card manager proxy 112 is a software module configured to execute commands (e.g., application protocol data unit commands or APDU commands) embedded in network messages on behave of the TSM 114 against the applets in the SE, and send network messages including APDU responses from the applets in the SE to the TSM 114. The readonly wallet UI 116 provides an interface to query one or more Mifare applications on information that can be accessed by well-known read sector keys or default keys, but will not modify the information in the underlying Mifare cards being supported. For example, an application can be written to display balances from many existing transit purses in different cities in China. The transaction wallet UI 118 is provided for conducting operations that will modify one or

Samsung Ex. 1016, Page 24 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

more Mifare sectors. Different write keys will be needed for altering the various sectors.

[0058] In one embodiment, the operations of the transaction wallet UI 118 includes:

1. top up balance of a transit purse after transferring money from a linking account;
2. deduct balance from a transit purse when make a payment for goods or services;
3. add a loyalty point to a partner company of a transit operator.

These operations need to modify certain sectors in a supported card or an application simulating the card to keep track of the purse balance, transaction log and/or loyalty point in an underlying Mifare card.

[0059] According to one embodiment, each pair of the readonly wallet UI applications 116 and transaction wallet applications 118 are provided by one of corresponding application/service providers 120. As will be further described below, these applications may be downloaded from a portal or provided via the TSM 114 and subsequently provisioned for a user.

[0060] Further, the TMSM 106 is a component or applet configured to be responsible for installing and personalizing the applications, and swapping one or another application into or out an emulator 122 as long as one the applications remains activated. As used herein, an emulator means a hardware device or a program that pretends to be another particular device or program that other components expect to interact with. In one embodiment, the emulator 122 emulates the Mifare classic operating system by providing the exact same hardware and/or software functionality. Once the emulator 122 (implemented in hardware or software) is installed, it responds exactly like a native Mifare chip to an interface (e.g., a reader) transmitting Mifare commands. According to one embodiment, the TMSM 106 is configured to provide the following functionalities:

1. providing a set of APIs so that a wallet application (e.g., simulating a Mifare card), when instructed by an user, can be caused to swap (i.e., activate on an emulator) an application in and out the Mifare emulator 122 so that the NFC device 102 or 104 is able to support more than one Mifare cards or applications

Samsung Ex. 1016, Page 25 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

of similar type. Depending on implementation, the APIs may replace one application in the Mifare emulator 122 with an activated application in entirety or only a portion of the original application to keep those to be used by the newly activating application. It shall be noted that an application herein does not mean that there is only one file for the application. In general, there are a number of data sets and files for one application. Therefore, when an application in the emulator is being replaced by the activated application, some data sets may be retained for use with the activated application loaded into the emulator.

2. providing a set of APIs to read off a wallet application (e.g., to read out balance or transaction history).
3. enabling the TSM 114 to remotely personalize/provision multiple Mifare applications, which includes installing application keys and application data to the TMSM 106 and later on swapping an activated one to the emulator 122.
4. enabling the TSM 114 to manage provisioned Mifare applications. This includes locking and unlocking of a Mifare application so that it cannot be swapped into the emulator 122.
5. providing a trusted environment such that an application provider can only modify its application and meta data thereof that is owned by the application provider.
6. providing a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards (e.g., in lieu of multiple physical Mifare cards) swapped out from the emulator 122 to the TMSM 106, partly for solving the issue of limited memory in the emulator 122.

[0061] In one embodiment, the TMSM 106 is implemented by enhancing the Mifare4Mobile technology. Mifare4Mobile was initially developed by NXP and may support only a few of the functionalities listed above but not all. The current design of the Mifare4Mobile technology was based upon the assumption that all service providers trust a TSM (e.g., the TSM 114) and each other. A Mifare4Mobile service manager (a software module) does not have a mean to differentiate application ownerships. With an established secured channel to a Mifare4Mobile service manager, a service provider can access to all Mifare service objects (i.e., Mifare

Samsung Ex. 1016, Page 26 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

applications) installed in that manager. As a result, an application provider could easily overwrite the content of another application that is not owned by application provider.

[0062] According to one embodiment, the implementation of FIG. 1A is able to overcome the deficiency of the Mifare4Mobile technology. Besides interacting with a GlobalPlatform card manager (not shown), the card manager proxy 118 is configured to interact with the TMSM 106 for installing corresponding Mifare service objects of a Mifare application. FIG. 1B shows two different models of security channel supports that may be used for the TMSM 106. Model 1 of FIG. 1B is to make use of a security channel mechanism supported by GlobalPlatform, where GlobalPlatform is an independent, not-for-profit organization concerned with a standardized infrastructure for development and management of smart cards. Model 2 of FIG. 1B is to have a mechanism of security channel support built into a TMSM.

[0063] There are at least two types of applications/services that can be supported in the configuration of FIG. 1A; read only and transaction-based. For the read only applications, an operation can use the RETRIEVE DATA APDU to retrieve application data (e.g., balance) from the TMSM 106. PIN validation might be needed by the applications before the data can be retrieved. For the transaction-based applications, the UI application can interact with a dedicated application applet to perform a transaction. A transaction might involve more than one APDU. The respective UI applications also act as proxy to the backend server of an application provider.

[0064] As shown in FIG. 1A, the TMSM 106 includes a set of service objects and corresponding key indexes. Each logical Mifare card in the TMSM 106 is called a service object. Each application can be associated with a key set index (also called key version number) of the installed SSD (Supplementary Secured Domain) key. Currently, each SSD can support a maximum of 127 different keysets. Thus it is possible to install more than one key set on the SSD. There are many ways to assign these key sets. In an extreme case, each application has its own key set. Another way is that each application provider has its own key set and all applications from the same application providers share the same key set. In one embodiment, the

Samsung Ex. 1016, Page 27 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Mifare4Mobile service manager is enhanced to apply access rules to the requested APDU commands based on this key association. This enhancement does not require any modification to the APDU format of the Mifare4Mobile specification v1.0.1. The extension is as follows:

1. Define a new optional tag to the proprietary content for the private meta data of a Mifare service object. This tag is used to store the key set index and establish an association between a key set and an application.
2. Add new logic to the Mifare4Mobile service manager to enforce this association when a requested APDU command is targeted to a Mifare application (i.e. service object in the TMSM 106).
3. Reserve 15 key set indices from 0x01 to 0x10 to TSM for TSM operations. For any service object that does not have associated key set index, any of this installed TSM key set indices can be used to work with the service object.

[0065] A new proprietary tag 0x8C is defined for the private meta data of a service object in the following:

Value Name	Type	Presence	Tag	Length (bytes)	Value
Proprietary Content – SSD Key Set Index	Private Data	Optional	8C	1	1 to 127

If an application is assigned a dedicated key set index, this tag must be set to the index of that key set. For example, if an application is assigned a key set index 5, the private meta of that service object has a tag 8C with value 5.

[0066] This enhancement does not require any modification to the APDU format of the Mifare4Mobile specification v1.0.1. A specified key index set for a service object does not have to be pre-installed in its residing Mifare4Mobile service manager. The manager does not check the existence of the specified key set index. However, the key index set has to be put (via PUT KEY command) into the manager before the service object is activated, otherwise, no modification can be done to that service object.

Samsung Ex. 1016, Page 28 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0067] When performing operations on a service object, the TSM 114 or a service provider 120 has to establish a SSD secure channel using a key set index. The key set index is specified in the INITIAL UPDATE command when sending to the Mifare4Mobile Service Manager. After the secured channel is successfully established, the Mifare4Mobile Service manager is configured to store this index. During this secured session, the Mifare4Mobile service manager enforces the following access rules to requested commands:

Command against a service object (SO)	Allowed Key Set Index
DELETE	TSM
UPDATE DATA against application data	TSM or SO
UPDATE DATA against all data (meta and application)	TSM
GET DATA	No SSD
RETRIEVE DATA	No SSD
ACITIVATE	No SSD

[0068] Each row defines an access rule of a command. The first column is a requested APDU command. The second column indicates what the key indices are allowed to perform the command. The TSM 114 denotes a set of key indices assigned to the TSM 114. SO indicates a key index associated with that Mifare service object. It shall be noted that it is not any service object key set index but the associated key set index for the Mifare service object specified in the 8C tag.

[0069] For supporting locking and unlocking a Mifare application, two APDUs are added to the Mifare4Mobile Service Manager. These two APDUs are TSM based API. A TSM security channel must be established between the TSM 114 via the card manager proxy 112 to the TMSM 106 before the commands can be issued against a Mifare application. Upon receiving the commands, the TMSM 106 sets the corresponding Mifare service object to an appropriate status. It is noted that the Mifare4Mobile service manager is extended with an additional lock state. If a Mifare application is locked, a wallet application is not able to swap (i.e., activate) that Mifare application. The TSM 114 will have to unlock that application before the Mifare application can be swapped into the emulator 122.

Samsung Ex. 1016, Page 29 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0070] As the memory, especially in a smartcard, is very limited, one implementation is to allow the service objects to be swapped to the baseband persistent storage from the TMSM 106. The baseband persistent storage (not shown) maintains a mapping table. Each row of the table contains information about a service object. At least the following information is kept; the service object ID (SOID) of a service object, and a service object in an encrypted format. The TMSM 106 will encrypt a service object before it is swapped out therefrom.

[0071] According to one embodiment, the TMSM 104 has a new swapping counter. Upon a successful swapping, the counter is incremented by 1. The TMSM 104 maintains a swapping table to keep track of the SOs that are currently swapped out. This table shall maintain two columns: the SOID and a value of the swap counter when the SO was swapped. When an SO is swapped, the encryption of the following information is returned to the baseband for storage: value of the swap counter and the service object. In the embodiment, the encryption key can be the mifare4mobile DEK key or a new key personalized into the TMSM applet 106 specifically for this purpose. The encryption is recommended to be 3DES with CBC mode using all zeros for initial vector.

[0072] In addition, each service object is enhanced with a new attribute to indicate whether the service object is allowed to be swapped to the baseband storage. This indicator is set when the service object is installed. In one embodiment, the Mifare4Mobile APDU command set for the TMSM is enhanced as follows:

1. a new APDUs for swapping a service object to the baseband storage.
2. the applet behavior is modified when receiving the Mifrae4Mobile ACTIVATE or INSTALL command.

[0073] According to one embodiment, the details of the modification are as follows:

1. Swap command: ask the applet to find and mark a service object that can be swapped to the baseband. This service object must be swappable and has the oldest access time stamp. This requests that an APDU request shall have the following characteristics:

Samsung Ex. 1016, Page 30 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

a. The command option P1 has a value to indicate it is swappable for activation or swappable for installation.
b. The request data contains one or two pieces of information:
    i. the service object ID to be swapped to the applet (e.g., emulator).
    ii. the encrypted service object to be swapped if it is swappable for activation. This encrypted service object is retrieved from the baseband, wherein there is a mapping table based on the given SOID.

Upon receiving the request, the TMSM 106 first performs validation to ensure the APDU is proper. In addition, if the SOID has already in the applet, then an error code is returned to indicate that the SOID is in the applet. If the request includes an encrypted service object, the TMSM 106 has to recover the service object and the swapped counter from the encrypted data. The TMSM 106 is then configured to verify the counter against the swapping table. If both counters are not matched, it returns an error message to indicate the data has been corrupted. This decrypted SO is kept and used in the next ACTIVATE command. On the other hand, upon successful execution, the APDU response contains two pieces of information: the ID of the SO that will be swapped out of the Applet, and the encryption of this SO and a swap counter. If the next immediate command that the TMSM 106 receives is neither ACTIVATE nor INSTALL, it will unmark the service object.

2. Activate or Install for Install commands: These two commands are modified with the following behavior. Upon receiving one of these two commands, the TMSM 106 checks to see whether there is a marked swapped SO. If not, the subsequent behavior shall be the same as the original commands. Otherwise, it checks to ensure that APDU matches the purpose for swapping in the previous Swap command. The request is rejected if it is not matched. If the APDU passes the test, the marked swapped SO will be deleted. For the case of ACTIVATE, the previously encrypted data will be used to update the SO table. After that, the subsequent behavior will be the same as the original commands.

Samsung Ex. 1016, Page 31 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0074] According to one embodiment, a layer of SDK is provided for the baseband so that when activating or installing a SO,

1. For activate command, it will check to see the mapping table maintained in the baseband whether the service object is in the baseband. If it is not, it simply issues the original activate command to the applet. Otherwise, it jumps to step 3 below.
2. For install, it bypasses the above checking and jumps to step 3.
3. The swapping steps are as follow:
    a. it issues a swap command to the TMSM applet. The SDK retrieves the SO based on the SOID from the mapping table to prepare the swap APDU command.
    b. If the response contains encrypted data and its SOID, the SDK will use the information in the response to update the mapping table.
    c. It then issues the original ACTIVATE or INSTALL command.

[0075] Referring now to FIG. 1C, that shows a block diagram of an exemplary computing (mobile) device 130 that may be used in FIG. 1A. The computing device 130 includes a near field communication (NFC) controller 131 that enables the device 130 to interact with another device wirelessly to exchange data with. For example, a user may use the mobile device 130 as an e-purse or a wallet to pay for a purchase or an admission. In operation, the e-purse is controlled by a secure element (SE) 132. Essentially, the SE 132 enables such a mobile device 130 to perform a financial transaction, transport ticketing, loyalty, physical access control, and other exciting new services in a secured manner. To offer such services, the SE 132 is configured to support various applets, applications or modules (by way of example, only two exemplary applications 134 and 136 are shown in FIG. 1B). Depending on implementation, these applications or modules may be hardware modules embedded or inserted thereon, or software modules downloadable from one or more servers via a data network.

[0076] When a mobile device is first purchased by or delivered to a customer, the SE 132 in the mobile device is installed with a set of default keys (e.g., an Issuer

Samsung Ex. 1016, Page 32 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Security Domain (ISD) key set by the SE manufacturer). In one embodiment, the SE 132 is a tamper-proof chip capable to embed smart card-grade applications (e.g., payment, transport …) with the required level of security and features. In FIG. 1B, the SE 132 is embedded or associated with various applications (e.g., NFC-related) and is connected to the NFC controller 131 to act as the contactless front end. Typically, a standard-compliant SE comes with one issuer security domain (ISD) and an option for one or more supplemental security domains (SSD). Each of these domains includes a set of keys. In one embodiment, the SE 132 is a chip embedded in the mobile device 130 or in a miniature card inserted into the mobile device 130 via a card interface 139. In another embodiment, the SE 132 is or includes a software module loaded in a secured memory space 137 in the mobile device 130. The software module may be updated by downloading updating components from a designated server using a network interface 133 (e.g., a 3G network or an LTE network) in the mobile device 130.

[0077] The SE 132 needs to go through a personalization process before it can be used. In one embodiment, the personalization process is to load the SE 132 with or update a key set with a derived personalized key set of a chosen card issuer (i.e., a so-called SE issuer). Depending on situation, an SE issuer and an SE manufacturer may be two separate entities and a single entity. To facilitate the description of the present invention, the SE issuer and the SE manufacturer will be described herein as if they are two separate entities. Further, a personalization process may be also referred to as a provisioning process. According to one embodiment, the SE provisioning process is performed over the air (OTA) to cause the SE to be personalized while installing an application or enabling a service (i.e., application installation and personalization). The personalization of an SE is only done once the SE is associated with an SE issuer. The application installation and provisioning shall be done for each application when a user subscribes or installs an application.

[0078] In one embodiment, when updating or upgrading the SE 132, only one or some components pertaining to the SE 132 are replaced by newer updates to avoid personalizing the SE 132 from beginning. Depending on implementation, such newer updates may be automatically or manually obtained to be loaded into the mobile

Samsung Ex. 1016, Page 33 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

device 130. In one embodiment, applications are available for an NFC-enabled mobile device for downloading from a server or a TSM portal depending on the corresponding SE issuer and the TSM thereof.

[0079] TSM, standing also for Trusted Service Management, is a collection of services. One main role envisaged for the TSM is to help service providers securely distribute and manage contactless services for their customers using the networks of mobile operators. The TSM or its server(s) does not necessarily participate in actual contactless transactions involving the NFC devices. These transactions are processed normally in whatever system the service provider and its merchant partners have already put in place. Another role of the TSM is to accelerate the successful deployment and ramp-up of mobile NFC applications by acting as a commercial intermediary that facilitates contractual arrangements and other aspects of ongoing business relationships among different parties that make the commerce via the mobile networks possible.

[0080] The personalization process can be done either physically in a service center or remotely via a web portal by a TSM server. In the first scenario, the customer may physically go to a service center to let a service representative to personalize the SE in a mobile device. With a computer connected to an NFC reader at a designated place (e.g., a service center), a provisioning manager can be either an installed application or a web-based application connecting to a backend TSM. The provisioning manager is configured to communicate with the SE of the mobile device (e.g., via a reader). Such a personalization process is referred to as a process Over the Internet (OTI).

[0081] In the second scenario, the customer registers his/her mobile phone via a server (often a TSM web portal). The TSM server is configured to push a universal resource identifier (URI) of a provisioning manager to the registered mobile phone. Depending on a type of the device, the push can be either an SMS (Short Message Service) Push or a Google Android Push. The customer can download the provisioning manager into the mobile device and start the personalization process. Such a personalization process is referred to as a process Over the Air (OTA).

Samsung Ex. 1016, Page 34 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0082] In either one of the scenarios, the provisioning manager acts as a proxy between the SE in the mobile device and the TSM server. Referring now to FIG. 1D, it shows a flowchart or process 150 of personalizing an SE according to one embodiment of the present invention. Depending on implementation, the process 150 may be implemented in software or a combination of software and hardware. When a user receives a new NFC device (e.g., a part of a mobile device), the SE therein needs to be personalized.

[0083] At 152, the new NFC device is determined if it is a genuine NFC device. One example is to check a serial number associated with the NFC device. The serial number may be verified with a database associated with a TSM server. In the example of an NFC mobile device, the device serial number of the mobile device may be used for verification. It is now assumed that the NFC device is a genuine device (recognizable by a mobile operator). The process 150 goes to 154 to have the NFC device communicated with a dedicated server. In one embodiment, the server is a part of the Trusted Service Management (TSM) system and accessible via a wireless network, the Internet or a combination of wireless and wired networks (herein referred to as a data network or simply a network).

[0084] At 156, the NFC device is registered with the server. Once the NFC device becomes part of the system, various services or data may be communicated to the device via the network. As part of the personalization process, the server requests device information of the SE at 158. In one embodiment, the server is configured to send a data request (e.g., a WAP PUSH) to the device. In responding to the request, the device sends back CPLC (card product life cycle) information retrieved from the SE. The CPLC includes the SE product information (e.g., the smart card ID, manufacturer information and a batch number and etc.). Based on the CPLC info, the server is able to retrieve corresponding default Issuer Security Domain (ISD) information of this SE from its manufacturer, its issuer, an authorized distributor or a service provider. Depending on implementation, there are two ways that the server may communicate with an SE distributor or manufacturer, which will be fully discussed herein late when deemed appropriate.

Samsung Ex. 1016, Page 35 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0085] At 160, it is up to the manufacturer whether to update the device information. In general, when an SE is shipped from the manufacturer, the SE is embedded with some default device information. If it is decided that the default information such as the CPLC data is to be updated with the manufacturer, the process 150 goes to 162, where the manufacturer uploads corresponding updated device information to the server. The updated device information is transported to the device and stored in the SE at 164. If it is decided that the default information in the SE is not to be updated with the manufacturer, the process 150 goes to 164 to store the retrieved default device information in a database with the TSM server. In one embodiment, the server is configured to include an interface to retrieve a derived SE key set from the mobile device. According to one embodiment, the derived key set is generated with the device information (e.g., ISD) of the SE. When the derived ISD key set is successfully installed on the SE, the corresponding SE issuer is notified of the use of the derived ISD key set.

[0086] According to one embodiment, the device information (default or updated) is used to facilitate the generation of a set of keys at 166. In operation, the server is configured to establish a secured channel using the default ISD between its hardware security module (HSM) and the SE. The server is also configured to compute a derived key set for the SE. Depending on a business agreement, a master ISD key of an issuer for the SE may be housed in a hardware security module (HSM) associated with the server or in a local HSM of the SE issuer. An HSM is a type of secure crypto-processor provided for managing digital keys, accelerating crypto-processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications. If it is housed in the HSM of the server, the server is configured to instruct the HSM to compute the derived key set. Then, the server prepares a mechanism (e.g., PUT KEY APDU) and uses the default channel to replace the default key set originally in the SE with the derived key set. If the master ISD key of the SE issuer is in a local HSM of the SE issuer, the server is configured to interact with the remote HSM to retrieve the keys.

[0087] At 168, the set of keys is securely delivered to the SE. The set of keys is thus personalized to the SE and will be used for various secured subsequent operations or services with the NFC device. The server at 130 is configured to synchronize the SE

Samsung Ex. 1016, Page 36 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

with the issuer or provider (e.g., sending a notification thereto about the status of the SE). After the personalization, the SE can only be accessed using the personalized ISD key of the SE issuer. Depending on the security requirement of each service provider, the TSM can create additional SSDs for the various providers to personalize their respective applications (e.g., the modules 134 or 136 of FIG. 1C).

[0088] As mentioned above, there are two ways that may be used to retrieve the corresponding default Issuer Security Domain (ISD) information from the SE in interfacing with the manufacturer thereof. Depending on the infrastructure, a manufacturer can choose to use a real-time approach or a batch approach.

[0089] In the real-time approach, the server is configured to communicate with the manufacturer (i.e., its server thereof) when an SE by the manufacturer is being personalized by the TSM server. The default key set is, thus, retrieved on demand from the server of the manufacturer. In one embodiment, the TSM server includes a plugin module for each of the manufacturers to communicate therewith.

[0090] In the batch approach, it can be done either offline mode or online mode. In the offline mode, the SE manufacturer delivers the default ISD information for all SEs being supported via an encrypted physical media. An administrator for the TSM may or a computing device may be configured to import the information in a media to a computing device. The default ISDs are then decrypted and retrieved, and stored in a database. In the online mode, the SE manufacturer uploads the default ISD information for the SEs it supports via a network. The default ISDs are then decrypted and retrieved, and stored in a database. Afterwards, the TSM only needs to access its own HSM o the database during an SE personalization process. FIG. 1E shows respective relationships among the SE manufacturer, the TSM admin and the TSM system for both offline and online modes. FIG. 1F illustrates data flows among a user for an NFC device (e.g., an NFC mobile phone), the NFC device itself, a TSM server, a corresponding SE manufacturer and an SE issuer according to one embodiment.

[0091] In one perspective, the SE 132 of FIG. 1C may be perceived as a preload operating system in a smart card, providing a platform for PIN management and security channels (security domains) for card personalization. The SE 132

Samsung Ex. 1016, Page 37 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple applications running in the smart cards. As an example, one module 134 referred to as an e-purse security defines a set of protocols that enable micro payment transactions to be carried out over a data network. With an electronic purse (a.k.a., e-purse application) stored on a smart card, a set of keys (either symmetric or asymmetric) is personalized into the e-purse after the e-purse is issued. During a transaction, the e-purse uses a set of respective keys for encryption and MAC computation in order to secure the message channel between the e-purse and an SAM (Security Authentication Module) or backend servers. For a single functional card, the e-purse security 134 is configured to act as gates to protect actual operations performed on a single functional card. During personalization, the single functional card access keys (or its transformation) are personalized into the e-purse with the e-purse transaction keys.

[0092] As an example, it is assumed that an installed application, e-purse or a Mifare card, has been provisioned with the SE. FIG. 1G shows a flowchart or process 190 of data flow among three entities: a land-based SAM or a network e-purse server 192, an e-purse 194 acting as a gatekeeper, and a single function tag 196. Communications between the land-based SAM or the network e-purse server 192 and the e-purse 194 are conducted in sequence of a type of commands (e.g., APDU) while communications between the e-purse 194 and the single function tag 196 are conducted in sequence of another type of commands, wherein the e-purse 194 acts as the gate keeper to ensure only secured and authorized data transactions could happen.

[0093] In one embodiment, the physical security for the e-purse is realized in an emulator. As used herein, an emulator means a hardware device or a software module that pretends to be another particular device or program that other components expect to interact with. The e-purse security is realized between one or more applets configured to provide e-purse functioning and communicate with a payment server. An SE supporting the e-purse is responsible for updating security keys to establish appropriate channels for interactions between a payment server and the applets,

Samsung Ex. 1016, Page 38 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

wherein the e-purse applet(s) acts as a gatekeeper to regulate or control the data exchange.

[0094] Referring now to FIG. 2A, it shows a mobile payment ecosystem 200 in which related parties are involved in order for the mobile payment ecosystem successful. According to one embodiment, an NFC device is allowed to install or download one or more applications from respective designated servers 202 (i.e., application management providers), where the applications are originally developed by developers 204 and distributed by service providers 210, application management providers 202 or others. It is assumed that the secure element 206 provided by a secure element provider 208 has already been personalized via a TSM or a trusted third party (e.g., a financial institution 212).

[0095] Once an application is installed in an NFC device, the next step is to provision the application with the secure element. An application provisioning process can be started in several ways. One of the ways is that an SE holder selects an application from a TSM portal on the mobile device and initiates the provisioning process. Another one is that the SE holder receives an application provisioning notification on the mobile device from the TSM on behalf of an application (service) provider.

[0096] The TSM or application providers can publish their applications on a TSM portal to be downloaded to a mobile device with the SE and/or subscribed at a request of a user (a.k.a., an SE holder). In one embodiment, the TSM is a cloud service to serve many SE issuers. Thus, many applications from various service providers are available on the TSM portal. However, when getting onto the TSM portal, SE holders can only see those applications approved by its own SE issuer. Depending on the arrangement between an SE and a service provider, an application can either be downloaded/installed/personalized using the ISD keyset of the SE or a specific SSD keyset of the service provider. If a SSD keyset has not been installed on the SE, it can be installed during an application installation.

[0097] The TSM is designed to know the memory state or status of an SE for various SSDs. Based on the state of the SE and the memory allocation policy of the

Samsung Ex. 1016, Page 39 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

SSDs, the available applications for the various SSD in the application store may be marked with different indicators, for example, “OK to install”, or “Insufficient memory to install”. This will prevent unnecessary failure for users.

[0098] Once an application is installed on an NFC device, the application initiates a provisioning process by itself, or the TSM can push a provisioning notification to the NFC device via a cellular network or a wireless data network. Depending on the type of the devices, there are many different types of push messages to cause the NFC device to initial the provision process. An example of the push methods includes an SMS push or an Android Google Push. Once a user accepts the notification, the provisioning process starts. The details of the provisioning process will be described below whenever deemed appropriate.

[0099] As part of the application provisioning, a TSM server implements some protective mechanism. One is to prevent an SE from being accidentally locked. Another is to disable application download if there is no sufficient memory on SE. In some cases, an SE may permanently lock itself if there are too many failed mutual authentications during secure channel establishment. In order to prevent the SE from being accidentally locked, the TSM keeps the track of the number of failed authentications between an SE and the TSM when establishing a secured channel between the two entities. In one embodiment, the TSM is configured to reject any further request if a preset limit is reached. The TSM can continue to process the SE request if the SE is reset at the service center manually.

[00100] The TSM also keeps track of the memory usage of each SE. The TSM decides whether an application can be installed on an SE based on the memory allocation assigned by the SE issuer to each service provider. According one embodiment, there are three types of policies:

- pre-assigned fixed memory to guarantee a space of fixed capacity.
- pre-assigned minimum memory to guarantee a space of a minimum capacity (implying that the capacity may be expanded under some conditions).

Samsung Ex. 1016, Page 40 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

- best efforts (e.g., a contractual provision which requires the SE issuer to use its highest efforts to perform its obligations and to maximize the benefits to be received by the user).

[00101] According to one embodiment, an SE issuer uses a TSM web portal to make this assignment.

1. For a batch of SE, the SE issuer can pre-assign a memory policy for a service provider to install its applications via the TSM web portal;
2. The TSM server verifies whether the space of the respective service provider conforms to its policy when a mobile device requests to install one of its applications. If not conformed, this request is rejected, otherwise, the TSM server will proceed to handle the provisioning request;
3. If the provisioning succeeds, the TSM will accumulate the memory size of this application service.

[00102] When a mobile user subscribes to a mobile application (assuming it has been installed), the application has to be provisioned with the SE in the mobile device before it can be used. According to one embodiment, the provisioning process includes four major stages:

- to create an supplemental security domain (SSD) on the SE, if needed;
- to download and install an application cap on the SE;
- to personalize the application on the SE; and
- to download a UI component on mobile phone.

[00103] FIG. 2B shows a flowchart or process 220 of provisioning one or more applications according to one embodiment. The process 220 may be implemented in software or a combination of software and hardware. In one embodiment, the application provisioning process 220 needs to go through a provisioning manager (i.e., proxy) on the mobile phone to interact with the SE therein.

[00104] As shown in FIG. 2B, at 222, the application provisioning process 220 may be started manually or automatically. For example, a user may initiate the process 220 by selecting an installed application to subscribe related services or the installed application, when activated, initiates the provisioning process, provided it has

Samsung Ex. 1016, Page 41 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

not been provisioned. In another embodiment, a provider of an application pushes a message (e.g., SMS) to the mobile phone to initiate the provisioning process.

[00105] In any case, the process 220 goes to 224 to establish a communication with a dedicated server (e.g., a TSM server or a server operated by an application distributor) after the device information (e.g., CPLC) is retrieved from the SE in the mobile device. The device information along with an identifier identifying the application is transmitted to the server at 226. Based on the device information, the server identifies the issuer for the SE first at 228 to determine if the SE has been personalized at 230. If the SE has not been personalized, the process 220 goes to 232 to personalize the SE, where one embodiment of the function 232 may be implemented in accordance with the process 150 of FIG. 1B.

[00106] It is now assumed that the SE in the mobile device has been personalized. The process 220 now goes to 234 to establish a secure channel with the SE using the derived ISD. Depending on who houses the HSM (TSM or SE issuer) for the ISD, the server will contact the HSM to compute the derived ISD for the SE and establish a secure channel with the SE using this derived ISD. The server is then configured to check to see whether there is an SSD associated with this application at 236. If there is not an SSD associated with the application, the server is configured to check a database to see whether it has been installed with this SE. If the SSD installation is needed, then the process 220 goes to install the SSD. In one embodiment, the user is alerted of the installation of the SSD (keys). Should the user refuse to install the SSD at 238, the process 220 stops and goes to 222 to restart the provisioning process 220.

[00107] It is now assumed that the process of installing the SSD proceeds at 240. Installing the SSD is similar to installing the ISD. The TSM server is configured to contact the HSM that houses the SSD master key to compute the derived SSD key set for the SE. The master SSD key set can be either in the TSM or with the service provider or the SE issuer, largely depending on how the arrangement is made with all parties involved.

Samsung Ex. 1016, Page 42 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[00108] To download/install the application to the SE, the server is configured to establish a secure channel with the SE using this derived SSD at 242. In one embodiment, this is similar to how the ISD-based secure channel is established. At 244, the data for the application is prepared, the detail of which will be further discussed below. According to one embodiment, the server is configured to contact the service provider to prepare asset of APDUs, such as STORE DATA APDUs, where ADPU stands for Application Protocol Data Unit. Depending on an application installed in a mobile device, the server may be caused to repeatedly issue STORE DATA to personalize the application with the SE. Additional data including an appropriate interface (e.g., a user interface of the application per the mobile device) may be downloaded provided that the provisioning process is successfully done. At 246, the server will notify the application provider the status of the application that has been provisioned. According to one embodiment and the above description, FIG. 2C shows a data flow 250 illustrating various interactions among different parties when an application is being provisioned in one embodiment.

[00109] As shown in 244 of FIG. 2B, one of the important functions in provisioning an application is to prepare customized application data for the targeted SE. For example, for an e-purse application, the personalized data for the application includes various personalized transaction keys generated based on the device information (e.g., CPLC info) of the SE. For transit e-purse, part of the personalized data includes the Mifare access keys derived from an identifier (ID) of the Mifare card, the server is configured to personalize both Java Card applications and Mifare4Mobile service objects. In general, there are at least two different ways to prepare the data to facilitate subsequent transactions.

[00110] For data preparation, one embodiment of the present invention supports two operation modes to interact with service providers for computing the personalized application data. For the first mode, a TSM server does not have direct access to the HSM associated with a service provider. The service provider may have a server interacting with its HSM to generate the application keys (e.g., Transit, e-purse, or Mifare Key). The TSM data preparation implementation is to make use of application program interfaces (API) or a protocol provided by the server to request for

Samsung Ex. 1016, Page 43 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

derived application keys. The second mode is that data preparation implementation can directly access the HSM associated with the service provider to generate the application keys.

[00111] According to one embodiment, FIG. 2D shows a data flow 255 among different entities when preparing the application data in provisioning an application. FIG. 2D is provided to show the first mode in which a TSM server does not have direct access to the HSM associated with a service provide. The second mode has a similar flow except that the application data preparation implementation will interact directly with the HSM of a service provider.

[00112] Besides supporting a provisioning process, one embodiment of the present invention also supports the life cycle management of an SE. The life cycle management includes, but may not be limited to, SE lock, SE unlock, Application Delete (disabling). The initiation of these activities may be through a TSM push notification. In actual use of mobile devices, FIG. 2E shows a flowchart or process 260 of locking an installed application. An NFC device may have been installed with a number of applications in connection with or running on top of the secured element therein. For some reason (e.g., no activity for a prolonged period or expiration), an application needs to be disabled or locked by its distributor or provider.

[00113] FIG. 2E shows an operation or process 260 to disable an installed application. The process 260 is initiated at 262. In one embodiment, the process 260 is initiated by an operator manually via a TSM web portal. In another embodiment, the process 260 is automatically initiated by a service provider internal workflow (e.g., using TSM web service API). Once the process 260 is initiated, a message is pushed to an NFC device (e.g., within a mobile device) in which an application is to be disabled. Depending on application, such a message may come in different forms. In one embodiment, the message is a PUSH command. In another embodiment, the message is a TCP/IP request delivered to the device via a network. The message may be sent from a server (e.g., a TSM server) at 264. Depending on implementation, such a message may include an identifier identifying an application to be locked or disabled. Upon receiving such a message, a card manager proxy on the device is caused to

Samsung Ex. 1016, Page 44 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

verify whether such a message is indeed from its original distributor or provider by returning a message at 266. According to one embodiment, the message is sent to the TSM server for verification. If the verification fails, namely there is no acknowledgement to such an inquiry, the process 260 is abandoned.

[00114] It is now assumed that the verification is successful, namely the inquiry from the device to a provider of the application returns an acknowledgement that the original request is authenticated. In general, such an acknowledgement includes an identifier confirming the application to be locked at 268. The TSM server is configured to establish a secure channel with the SE as described previously. Then, the TSM server is to prepare appropriate APDUs (such as SET STATUS, or/and DELETE) for the SE for execution via the card manager proxy.

[00115] In any case, in responding to the command, the SE proceeds by locking the application at 272. According to one embodiment, the SE is caused to disassociate with the application, thus making the installed application no longer usable with the SE. At 274, the SE is configured to send out an acknowledgement to notify related parties that this application is no longer operating in the device. In one embodiment, the acknowledgement is sent over to the TSM server where there is a database recording what applications have been installed in what device, and a corresponding status of each. The database is updated with the acknowledgement from the SE.

[00116] FIG. 2E shows a flowchart or process for disabling or locking an installed application. It is known to those skilled in the art that other operations, such as unlocking or enabling an installed application, extending expiration of an installed application, are similar to the one shown in FIG. 2E, and thus the flowcharts thereof are not provided herein.

[00117] Referring now to FIG. 2F, there shows an exemplary architecture diagram 280 of a portable device enabled as an electronic wallet or e-purse to facilitate e-commerce and m-commerce, according to one embodiment of the present invention. The diagram 280 includes a cell phone 282 embedded with a smart card module. An example of such a cell phone is a near field communication (NFC) enabled

Samsung Ex. 1016, Page 45 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

cellphone that includes a Smart MX (SMX) module. Not separately shown, there is an SE that has already personalized according to the process discussed above. An application to enable the device as e-purse has also been installed. Unless explicitly stated, the following description will not call out which part is performing the function of a secure element and which part is performing as an application. Those skilled in the art shall appreciate the proper parts or functions being performed given the detailed description herein.

[00118] The SMX is pre-loaded with a Mifare emulator 288 (which is a single functional card) for storing values. The portable phone is equipped with a contactless interface (e.g., ISO 14443 RFID) that allows the portable phone to act as a tag. In one embodiment, the SMX is a JavaCard that can run Java applets. The e-purse application is configured to be able to access the Mifare data structures with appropriate transformed passwords based on the access keys created when the SE is personalized.

[00119] In the portable phone 282, an e-purse manager MIDlet 204 is provided. For m-commerce, the MIDlet 284 acts as an agent to facilitate communications between an e-purse applet 286 and one or more payment network and servers 290 to conduct transactions therebetween. As used herein, a MIDlet is a software component suitable for being executed on a portable device. The e-purse manager MIDlet 284 is implemented as a “MIDlet” on a Java cell phone, or an “executable application” on a PDA device. One of the functions of the e-purse manager MIDlet 284 is to connect to a wireless network and communicate with an e-purse applet which can reside on either the same device or an external smart card. In addition, it is configured to provide administrative functions such as changing a PIN, viewing an e-purse balance and a transaction history log. In one application in which a card issuer provides a SAM 292 that is used to enable and authenticate any transactions between a card and a corresponding server (also referred to as a payment server). As shown in FIG. 2F, APDU commands are constructed by the servers 290 having access to a SAM 292, where the APDU is a communication unit between a reader and a card. The structure of an APDU is defined by the ISO 7816

Samsung Ex. 1016, Page 46 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

standards in one embodiment. Typically, an APDU command is embedded in network messages and delivered to the server 290 or the e-purse applet 286 for processing.

[00120] For e-commerce, a web agent 294 on a computer (not shown) is responsible for interacting with a contactless reader (e.g., an ISO 14443 RFID reader) and the network server 290. In operation, the agent 294 sends the APDU commands or receives responses thereto through the contactless reader 296 to/from the e-purse applet 286 residing in the cell phone 282. On the other hand, the agent 294 composes network requests (such as HTTP) and receives responses thereto from the payment server 280.

[00121] To personalize or provision the portable phone 282, FIG. 3A shows a block diagram 300 of related modules interacting with each other to achieve what is referred to herein as e-purse personalization (or provisioning) by an authorized person. FIG. 3B shows a block diagram 320 of related modules interacting with each other to achieve what is referred to herein as e-purse personalization by a user of the e-purse as shown in FIG. 2F.

[0100] FIG. 3C shows a flowchart or process 350 of personalizing an e-purse applet according to one embodiment of the present invention. FIG. 3C is suggested to be understood in conjunction with FIG. 3A and FIG. 3B. The process 350 may be implemented in software, hardware or a combination of both.

[0101] As described above, an e-purse manager is built on top of the already-personalized SE to provide a security mechanism necessary to personalize the e-purse applet designed therefor. In operation, a security domain is used for establishing a secured channel between a personalization application server and the e-purse applet. According to one embodiment, the essential data to be personalized into the e-purse applet include one or more operation keys (e.g., a load or top-up key and a purchase key), default PINs, administration keys (e.g., an unblock PIN key and a reload PIN key), and passwords (e.g., from Mifare).

[0102] It is assumed that a user desires to personalize an e-purse applet embedded in a portable device (e.g., a cell phone). At 352 of FIG. 3C, a personalization process is initiated. Depending on implementation, the personalization process may be

Samsung Ex. 1016, Page 47 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

implemented in a module in the portable device and activated manually or automatically, or a physical process initiated by an authorized person (typically associated with a card issuer). As shown in FIG. 3A, an authorized personal initiates a personalization process 304 to personalize the e-purse applet for a user thereof via an existing new e-purse SAM 306 and an existing SAM 308 with the contactless reader 310 as the interface. The card manager 311 performs at least two functions: 1) establishing a security channel, via a security domain, to install and personalize an external application (e.g., e-purse applet) in the card personalization; and 2) creating security means (e.g., PINs) to protect the application during subsequent operations. As a result of the personalization process using the personalization application server 304, the e-purse applet 312 and the emulator 314 are personalized.

[0103] Similarly, as shown in FIG. 3B, a user of an e-purse desires to initiate a personalization process to personalize the e-purse applet wirelessly (e.g., via the m-commerce path of FIG. 2). Different from FIG. 3A, FIG. 3B allows the personalization process to be activated manually or automatically. For example, there is a mechanism on a cell phone that, if pressed, activates the personalization process. Alternatively, a status of “non-personalized” may prompt to the user to start the personalization process. As described above, a MIDlet 322 (i.e., a provisioning manager or a service manager) in a portable device acts as an agent to facilitate the communication between a payment server 324 and the e-purse applet 312 as well as the emulator 314, wherein the payment server 324 has the access to the existing new e-purse SAM 306 and an existing SAM 308. As a result of the personalization process, the e-purse applet 312 and the emulator 314 are personalized.

[0104] Referring now back to FIG. 3C, after the personalization process is started, in view of FIG. 3A, the contactless reader 310 is activated to read the tag ID (i.e., RFID tag ID) and essential data from a smart card in the device at 354. With an application security domain (e.g., a default security setting by a card issuer), a security channel is then established at 356 between a new e-purse SAM (e.g., the SAM 306 of FIG. 3A) and an e-purse applet (e.g., the e-purse applet 312 of FIG. 3A) in the portable device.

Samsung Ex. 1016, Page 48 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0105] Each application security domain key set includes at least three (3) DES keys. For example:

Key1: 255/1/DES-ECB/404142434445464748494a4b4c4d4e4f

Key2: 255/2/DES-ECB/404142434445464748494a4b4c4d4e4f

Key3: 255/3/DES-ECB/404142434445464748494a4b4c4d4e4f

A security domain is used to generate session keys for a secured session between two entities, such as the card manager applet and a host application, in which case the host application may be either a desktop personalization application or a networked personalization service provided by a backend server.

[0106] A default application domain can be installed by a card issuer and assigned to various application/service providers. The respective application owner can change the value of the key sets before the personalization process (or at the initial of the process). Then the application can use the new set to create a security channel for performing the personalization process.

[0107] With the security channel is established using the application provider's application security domain, the first set of data can be personalized to the e-purse applet. The second set of data can also be personalized with the same channel, too. However, if the data are in separate SAM, then a new security channel with the same key set (or different key sets) can be used to personalize the second set of data.

[0108] Via the new e-purse SAM 306, a set of e-purse operation keys and PINs are generated for data transactions between the new e-purse SAM and the e-purse applet to essentially personalize the e-purse applet at 358.

[0109] A second security channel is then established at 360 between an existing SAM (e.g., the SAM 308 of FIG, 3A) and the e-purse applet (e.g., the e-purse applet 312 of FIG, 3A) in the portable device. At 362, a set of transformed keys is generated using the existing SAM and the tag ID. The generated keys are stored in the emulator for subsequent data access authentication. At 358, a set of MF passwords is generated using the existing SAM and the tag ID, then is stored into the e-purse applet for future data access authentication. After it is done, the e-purse

Samsung Ex. 1016, Page 49 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

including the e-purse applet and the corresponding emulator is set to a state of "personalized".

[0110] FIG. 4A and FIG. 4B show together a flowchart or process 400 of financing or funding an e-purse according to one embodiment of the present invention. The process 400 is conducted via the m-commerce path of FIG. 2. To better understand the process 400, FIG. 4C shows an exemplary block diagram 450 of related blocks interacting with each other to achieve the process 400. Depending on an actual application of the present invention, the process 400 may be implemented in software, hardware or a combination of both.

[0111] A user is assumed to have obtained a portable device (e.g., a cell phone) that is configured to include an e-purse. The user desires to fund the e-purse from an account associated with a bank. At 402, the user enters a set of personal identification numbers (PIN). Assuming the PIN is valid, an e-purse manger in the portable device is activated and initiates a request (also referred to an over-the-air (OTA) top-up request) at 404. The MIDlet in the portable device sends a request to the e-purse applet at 406, which is illustrated in FIG. 4C where the e-purse manager MIDlet 434 communicates with the e-purse applet 436.

[0112] At 408, the e-purse applet composes a response in responding to the request from the MIDlet. Upon receiving the response, the MIDlet sends the response to a payment network and server over a cellular communications network. As shown in FIG. 4C, the e-purse manager MIDlet 434 communicates with the e-purse applet 436 for a response that is then sent to the payment network and server 440. At 410, the process 400 needs to verify the validity of the response. If the response cannot be verified, the process 400 stops. If the response can be verified, the process 400 moves to 412 where a corresponding account at a bank is verified. If the account does exist, a fund transfer request is initiated. At 414, the bank receives the request and responds to the request by returning a response. In general, the messages exchanged between the payment network and server and the bank are compliant with a network protocol (e.g., HTTP for the Internet).

Samsung Ex. 1016, Page 50 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0113] At 416, the response from the bank is transported to the payment network and server. The MIDlet strips and extracts the APDU commands from the response and forwards the commands to the e-purse applet at 418. The e-purse applet verifies the commands at 420 and, provided they are authorized, sends the commands to the emulator at 420 and, meanwhile updating a transaction log. At 422, a ticket is generated to formulate a response (e.g., in APDU format) for the payment server. As a result, the payment server is updated with a successful status message for the MIDlet, where the APDU response is retained for subsequent verification at 424.

[0114] As shown in FIG. 4C, the payment network and server 440 receives a response from the e-purse manager MIDlet 434 and verifies that the response is from an authorized e-purse applet 436 originally issued therefrom with a SAM 444. After the response is verified, the payment network and server 440 sends a request to the financing bank 442 with which the user 432 is assumed to maintain an account. The bank will verify the request, authorize the request, and return an authorization number in some pre-arranged message format. Upon receiving the response from the bank 442, the payment server 440 will either reject the request or accept the request by forming a network response sent to the MIDlet 434.

[0115] The e-purse manager 434 verifies the authenticity (e.g., in APDU format) and sends commands to the emulator 438 and updates the transaction logs. By now, the e-purse applet 436 finishes the necessary steps and returns a response to the MIDlet 434 that forwards an (APDU) response in a network request to the payment server 440.

[0116] Although the process 400 is described as funding the e-purse. Those skilled in the art can appreciate that the process of making purchasing over a network with the e-purse is substantially similar to the process 400, accordingly no separate discussion on the process of making purchasing is provided.

[0117] Referring to FIG. 5A, there is shown a first exemplary architecture 500 of enabling a portable device 530 for e-commerce and m-commerce over a cellular communications network 520 (e.g., a GPRS network) in accordance with one

Samsung Ex. 1016, Page 51 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

embodiment of the present invention. The portable device 530 comprises a baseband 524 and a secured element 529 (e.g., a smart card). One example of such portable device is a Near Field Communication (NFC) enabled portable device (e.g., a cell mobile phone or a PDA). The baseband 524 provides an electronic platform or environment (e.g., a Java Micro Edition (JME), or Mobile Information Device Profile (MIDP)), on which an application MIDlet 523 and a service manager 522 can be executed or run. The secured element 529 contains a global platform (GP) card manager 526, an emulator 528 and other components such as PIN manager (not shown), wherein the global platform is an independent, not-for-profit organization concerned with a standardized infrastructure for development, deployment and management of smart cards.

[0118] To enable the portable device 530 to conduct e-commerce and m-commerce, one or more services/applications need to be pre-installed and pre-configured thereon. An instance of a service manager 522 (e.g., a MIDlet with GUI) needs to be activated. In one embodiment, the service manager 522 is downloaded and installed. In another embodiment, the service manager 522 is preloaded. In any case, once the service manager 522 is activated, a list of directories for various services is shown. The items in the list may be related to the subscription by a user, and may also include items in promotion independent of the subscription by the user. The directory list may be received from a directory repository 502 of a directory server 512. The directory server 512 acts as a central hub (i.e., yellow page functions) for different service providers (e.g., an installation server, a personalization server) that may choose to offer products and/or services to subscribers. The yellow page functions of the directory server 512 may include service plan information (e.g., service charge, start date, end date, etc.), installation, personalization and/or MIDlet download locations (e.g., Internet addresses). The installation and personalization may be provided by two different business entities. For example, the installation is provided by an issuer of a secured element 529, while the personalization may be provided by a service provider who holds application transaction keys for a particular application.

[0119] According to one embodiment, the service manager 522 is configured to connect to one or more servers 514 (e.g., a TSM server) from a service provider(s)

Samsung Ex. 1016, Page 52 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

over the cellular communications network 520. It is assumed that the user has chosen one of the applications from the displayed directory. A secured channel 518 is established between the one or more servers 514 and the GP manager 526 to install/download an application applet 527 selected by the user and then to personalize the application applet 527 and optionally emulator 528, and finally to download an application MIDlet 523. The applet repository 504 and MIDlet repository 506 are the sources of generic application applets and application MIDlets, respectively. GP SAM 516 and application SAM 517 are used for creating the secured channel 518 for the personalization operations.

[0120] FIG. 5B is a diagram showing a second exemplary architecture 540 of enabling a portable device 530 for e-commerce and m-commerce over a public network 521, according to another embodiment of the present invention. Most of the components of the second architecture 540 are substantially similar to those of the first architecture 500 of FIG. 5A. While the first architecture 500 is based on operations over a cellular communications network 520, the public network 521 (e.g., Internet) is used in the second architecture 540. The public network 521 may include a local area network (LAN), a wide area network (WAN), a Wi-Fi (IEEE 802.11) wireless link, a Wi-Max (IEEE 802.16) wireless link, etc. In order to conduct service operations over the public network 521, an instance of the service manager 532 (i.e., same or similar functionality of the service manager MIDlet 522) is installed on a computer 538, which is coupled to the public network 521. The computer 538 may be a desktop personal computer (PC), a laptop PC, or other computing devices that can execute the instance of the service manager 532 and be connected to the public network 521. The connection between the computer 538 and the portable device 530 is through a contactless reader 534. The service manager 532 acts as an agent to facilitate the installation and personalization between one or more servers 514 of a service provider and a GP card manager 526 via a secured channel 519.

[0121] FIG. 5C is a flowchart illustrating a process 550 of enabling a portable device for e-commerce and m-commerce functionalities in accordance with one embodiment of the present invention. The process 550 may be implemented in software, hardware or a combination of both depending on implementation. To better

Samsung Ex. 1016, Page 53 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

understand the process 500, previous figures especially FIG. 5A and FIG. 5B are referred to in the following description.

[0122] Before the process 550 starts, an instance of a service manager 522 or 532 has been downloaded or pre-installed on either the portable device 530 or a computer 538. At 552, the service manager is activated and sends a service request to the server 514 at a service provider. Next after the authentication of a user and the portable device has been verified, at 554, the process 550 provides a directory list of services/applications based on subscription of the user of the portable device 530. For example, the list may contain a mobile POS application, an e-purse application, an e-ticketing application, and other commercially offered services. Then one of the services/applications is chosen from the directory list. For example, an e-purse or a mobile-POS may be chosen to configure the portable device 530. Responding to the user selection, the process 550 downloads and installs the selected services/applications at 556. For example, e-purse applet (i.e., application applet 527) is downloaded from the applet repository 504 and installed onto a secured element 529. The path for downloading or installation may be either via a secured channel 518 or 519. At 558, the process 550 personalizes the downloaded application applet and the emulator 528 if needed. Some of the downloaded application applets do not need to be personalized and some do. In one embodiment, a mobile POS application applet ("POS SAM") needs to be personalized, and the following information or data array has to be provided:

a unique SAM ID based on the unique identifier of the underlying secured element;

a set of debit master keys;

a transformed message encryption key;

a transformed message authentication key;

a maximum length of remark for each offline transaction;

a transformed batch transaction key; and

a GP PIN.

[0123] In another embodiment, personalization of an e-purse applet for a single functional card not only needs to configure specific data (i.e., PINs, transformed keys,

Samsung Ex. 1016, Page 54 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

start date, end date, etc.) onto the e-purse, but also needs to configure the emulator to be operable in an open system. Finally, at 560, the process 550 downloads and optionally launches the application MIDlet 523. Some of the personalized data from the application applet may be accessed and displayed or provided from the user. The process 550 ends when all of the components of services/applications have been installed, personalized and downloaded.

[0124] According to one embodiment, an exemplary process of enabling a portable device 530 as a mobile POS is listed as follows:

connecting to an installation server (i.e., one of the service provider server 514) to request the server to establish a first security channel (e.g., the secured channel 518) from an issuer domain (i.e., applet repository 504) to the GP card manager 526 residing in a secured element 529;

receiving one or more network messages including APDU requests that envelop a POS SAM applet (e.g., a Java Cap file from the applet repository 504);

extracting the APDU requests from the received network messages;

sending the extracted APDU requests to the GP card manager 526 in a correct order for installation of the POS SAM (i.e., application applet 527) onto the secured element 529;

connecting to a personalization server (i.e., one of the service provider servers 514) for a second security channel (may or may not be the secured channel 518 depending on the server and/or the path) between the personalization server and the newly downloaded applet (i.e., POS SAM);

receiving one or more network messages for one or more separated 'STORE DATA APDU'; and

extracting and sending the 'STORE DATA APDU' to personalize POS SAM; and

downloading and launching POS manager (i.e., application MIDlet 523).

[0125] Referring to FIG. 6A, there is shown an exemplary architecture 600, in which a portable device 630 is enabled as a mobile POS to conduct e-commerce and m-commerce, according to one embodiment of the present invention. The portable device 630 comprises a baseband 624 and a secured element 629. A POS manager 623 is downloaded and installed in the baseband 623 and a POS SAM 628 is installed

Samsung Ex. 1016, Page 55 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

and personalized in the secured element 629 to enable the portable device 630 to act as a mobile POS. Then a real time transaction 639 can be conducted between the mobile POS enabled portable device 630 and an e-token enabled device 636 (e.g., a single functional card or a portable device enabled with an e-purse). The e-token may represent e-money, e-coupon, e-ticket, e-voucher or any other forms of payment tokens in a device.

[0126] The real time transaction 639 can be conducted offline (i.e., without the portable device connecting to a backend POS transaction server 613). However, the portable device 630 may connect to the backend POS transaction servers 613 over the cellular network 520 in certain instances, for example, the amount of the transaction is over a pre-defined threshold or limit, the e-token enabled device 636 needs a top-up or virtual top-up, transactional upload (single or in batch).

[0127] Records of accumulated offline transactions need to be uploaded to the backend POS transaction server 613 for settlement. The upload operations are conducted with the portable device 630 connecting to the POS transaction server 613 via a secured channel 618. Similar to the installation and personalization procedures, the upload operations can be conducted in two different routes: the cellular communications network 520; or the public network 521. The first route has been described and illustrated in FIG. 6A.

[0128] The second route is illustrated in FIG. 6B showing an exemplary architecture 640, in which a portable device 630 is enabled as a mobile POS conducting a transaction upload in batch operation over a public network 521, according to an embodiment of the present invention. Records of offline transactions in the mobile POS are generally kept and accumulated in a transaction log in the POS SAM 628. The transaction log are read by a contactless reader 634 into a POS agent 633 installed on a computer 638. The POS agent 633 then connects to a POS transaction server 613 over the public network 521 via a secured channel 619. Each of the upload operations is marked as a different batch, which includes one or more transaction records. Data communication between the POS SAM 628, the contactless reader 634 and the POS agent 632 in APDU containing the transaction records.

Samsung Ex. 1016, Page 56 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Network messages that envelop the APDU (e.g., HTTP) are used between the POS agent 632 and the POS transaction server 613.

[0129] In one embodiment, an exemplary batch upload process from the POS manager 623 or the POS agent 633 includes:

sending a request to the POS SAM 628 to initiate a batch upload operation;

retrieving accumulated transaction records in form of APDU commands from a marked "batch" or "group" in the POS SAM 628 when the POS SAM 628 accepts the batch upload request;

forming one or more network messages containing the retrieved APDU commands;

sending the one or more network messages to the POS transaction server 613 via a secured channel 619;

receiving a acknowledgement signature from the POS transaction server 613;

forwarding the acknowledgement signature in form APDU to the POS SAM 628 for verification and then deletion of the confirmed uploaded transaction records; and

repeating the step b) to step f) if there are additional un-uploaded transaction records still in the same "batch" or "group".

[0130] Referring to FIG. 6C, there is shown a flowchart illustrating a process 650 of conducting m-commerce using the portable device 630 enabled to act as a mobile POS with an e-token enabled device 636 as a single functional card in accordance with one embodiment of the present invention. The process 650, which is preferably understood in conjunction with the previous figures especially FIG. 6A and FIG. 6B, may be implemented in software, hardware or a combination of both.

[0131] The process 650 (e.g., a process performed by the POS manager 623 of FIG. 6A) starts when a holder of an e-token enabled device (e.g., a Mifare card or an e-purse enabled cell phone emulating single functional card) desires to make a purchase or order a service with the mobile POS (i.e., the portable device 630). At 652, the portable device 630 retrieving an e-token (e.g., tag ID of Mifare card) by reading the e-token enabled device. Next, the process 650 verifies whether the retrieved e-token is valid at 654. If the e-token enabled device 636 of FIG. 6A is a

Samsung Ex. 1016, Page 57 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

single functional card (e.g., Mifare), the verification procedure performed by the POS manager 623 includes: i) reading the card identity (ID) of the card stored on an area that is unprotected or protected by a well-known key; ii) sending an APDU request containing the card ID to the POS SAM 628; iii) and receiving one or more transformed keys (e.g., for transaction counter, an issuer data, etc.) generated by the POS SAM 628. If the one or more received transformed keys are not valid, that is, the retrieved e-token being not valid, then the process 650 ends. Otherwise, the process 650 following the "yes" branch to 656, in which it is determined whether there is enough balance in the retrieved e-token to cover the cost of the current transaction. If the result is "no" at 656, the process 650 may optionally offer the holder to top-up (i.e., load, fund, finance) the e-token at 657. If "no", the process 650 ends. Otherwise if the holder agrees to a real time top-up of the e-token enabled device, the process 650 performs either a top-up or a virtual top-up operation at 658. Then the process 650 goes back to 656. Whereas there is enough balance in the e-token, the process 650 deducts or debits the purchase amount from the e-token of the e-token enabled device 636 at 660. In the single functional card case, the one or more transformed keys are used to authorize the deduction. Finally at 662, records of one or more offline transactions accumulated in the POS SAM 628 are uploaded to the POS transaction server 613 for settlement. The upload operations may be conducted for each transaction or in batch over either the cellular communications network 520 or the public domain network 521.

[0132] The top-up operations have been described and shown in the process 400 of FIG. 4A. A virtual top-up operation is a special operation of the top-up operation and typically is used to credit an e-token by a sponsor or donor. To enable a virtual top-up operation, the sponsor needs to set up an account that ties to an e-token enabled device (e.g., a single functional card, a multi-functional card, an e-token enable cell phone, etc.). For example, an online account is offered by a commercial entity (e.g., business, bank, etc.). Once the sponsor has funded the e-token to the online account, the holder of the e-token enabled device is able to receive an e-token from the online account when connecting to the mobile POS. Various security measures are implemented to ensure the virtual top-up operation is secure and

Samsung Ex. 1016, Page 58 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

reliable. One exemplary usage of the virtual top-up is that a parent (i.e., a sponsor) can fund an e-token via an online account, which is linked to a cell phone (i.e., an e-token enabled device) of a child (i.e., the holder), such that the child may receive the funded e-token while the child makes a purchase at a mobile POS. In addition to various e-commerce and m-commerce functionalities described herein, the POS manager 623 is configured to provide various query operations, for example, a) checking the un-batched (i.e., not uploaded) balance accumulated in the POS SAM, b) listing the un-batched transaction log in the POS SAM, c) viewing details of a particular transaction stored in the POS SAM, d) checking the current balance of an e-token enabled device, e) listing a transaction log of the e-token enabled device, and f) viewing details of a particular transaction of the e-token enabled device.

[0133] Referring to FIG. 6D, there is shown a flowchart illustrating an exemplary process 670 of conducting m-commerce using the portable device 630 enabled to act as a mobile POS with an e-token enabled device 636 as a multi-functional card in accordance with one embodiment of the present invention. The process 670, which is preferably understood in conjunction with the previous figures especially FIG. 6A and FIG. 6B, may be implemented in software, hardware or a combination of both.

[0134] The process 670 (e.g., a process performed by the POS manager 623 of FIG. 6A) starts when a holder of an e-token enabled device 636 (e.g., a multi-functional card or an e-purse enabled cell phone emulating a multi-functional card) desires to make a purchase or order a service with the mobile POS (i.e., the portable device 630). At 672, the process 670 sends an initial purchase request to the e-token enabled device 636. The purchase amount is sent along with the initial request (e.g., APDU commands). Next the process 670 moves to decision 674. When there is not enough balance in the e-token enabled device 636. The initial purchase request will be turned down as a return message received at the POS manager 623. As a result, the process 670 ends with the purchase request being denied. If there is enough balance in the e-token enabled device 636, the result of the decision 674 is “yes” and the process 670 follows the “yes” branch to 676. The received response (e.g., APDU commands) from the e-token enabled device 636 is forwarded to the POS SAM 628. The response comprises information such as the version of the e-token key and a

Samsung Ex. 1016, Page 59 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

random number to be used for establishing a secured channel between the applet (e.g., e-purse applet) resided on the e-token enabled device 636 and the POS SAM 628 installed on the portable device 630. Then, at 678, the process 670 receives a debit request (e.g., APDU commands) generated by the POS SAM 628 in response to the forwarded response (i.e., the response at 676). The debit request contains a Message Authentication Code (MAC) for the applet (i.e., e-purse applet) to verify the upcoming debit operation, which is performed in response to the debit request sent at 680. The process 670 moves to 682 in which a confirmation message for the debit operation is received. In the confirmation message, there are additional MACs, which are used for verification and settlement by the POS SAM 628 and the POS transaction server 613, respectively. Next at 684, the debit confirmation message is forwarded to the POS SAM 628 for verification. Once the MAC is verified and the purchase transaction is recorded in the POS SAM 628, the recorded transaction is displayed at 686 before the process 670 ends. It is noted that the e-commerce transaction described may be carried out offline or online with the POS transaction server 613. Also when there is not enough balance in the e-token enabled device, a top-up or funding operation may be performed using the process 400 illustrated in FIG. 4A and FIG. 4B.

[0135] FIG. 7 shows an exemplary configuration in which a portable device is used for an e-ticketing application. A portable device 730 is configured to include an e-purse 724. When an owner or holder of the portable device 730 desires to purchase a ticket for a particular event (e.g., a concert ticket, a ballgame ticket, etc.), the owner can use e-purse 724 to purchase a ticket through an e-ticket service provider 720. The e-ticket service provider 720 may contact a traditional box office reservation system 716 or an online ticketing application 710 for ticket reservation and purchase. Then e-token (e.g., e-money) is deducted from the e-purse 724 of the portable device 730 to pay the ticket purchase to a credit/debit system 714 (e.g., a financial institute, a bank). A SAM 718 is connected to the e-ticket service provider 720 so that the authentication of e-purse 724 in the portable device 730 can be assured. Upon a confirmation of the payment is received, the e-ticket is delivered to the portable device 730 over the air (e.g., a cellular communications network) and stored onto a secured

Samsung Ex. 1016, Page 60 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

element 726 electronically, for example, an e-ticket code or key or password. Later on, when the owner of the portable device 730, the ticket holder, attends the particular event, the owner needs only to let a gate check-in reader 734 to read the stored e-ticket code or key in the portable device 730. In one embodiment, the gate check-in reader 734 is a contactless reader (e.g., an ISO 14443 complied proximity coupling device). The portable device 730 is a NFC capable mobile phone.

[0136] Referring now to FIG. 8A, it shows a diagram of multiple parties involved in a TSM operated and orchestrated by a business according to one embodiment. A TSM operation team 802 includes an administration responsible for managing accounts for users that have personalized their SEs via the TSM and other tasks. In one embodiment, the TSM operation team 802 includes someone for managing the accounts and someone for managing system resources, such as managing HSM, creating HSM indices and GP keyset mapping. In addition, the team is responsible for offline importing default ISD info from one or more SE manufacturers. The team may also include someone referred to as a certification engineer responsible to collaborate with service providers and the SE issuers on application approval process. The TSM sales team 804, also referred to as business account manager, is responsible for sales and account management for the vendors of the TSM. Some of the team 804 may only work with the SE manufacturers, some may only work with SE Issuers while other may work with more than one type of vendors. The TSM partner service team 806, also referred to as support engineers, is responsible for providing technical support to the vendors of the TSM, such as the SE issuers and the service providers. The TSM partner service team 806, does not deal directly with mobile users but helps partners analyze audit logs. The vendors 808 include one or more of the SE Issuers, the SE manufacturers, and the service providers. An SE issuer holds the responsibilities for the issuance of SEs and owns the ISD of the SEs. Working with the TSM teams, it can install additional SSD for service providers if needed. An SE manufacturer as the name suggests is responsible for manufacturing the SEs and installing a default ISD in the SEs. It also works with the TSM teams to provide these default ISD key sets. The service provider is responsible for developing NFC mobile applications. Exemplary applications from the service providers include, but may not be limited to, transit

Samsung Ex. 1016, Page 61 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

purses, bank's e-purses and credit cards. Smaller service providers may be those to provide applications used as room keys.

[0137] FIG. 8B shows relevant operations among the parties in the TSM according to one embodiment. The description of the operations is not to be described in detail herein to avoid obscuring the important aspect of the embodiment of the present invention. FIG. 8C shows a work flow among multiple parties to establish mutually agreed arrangement in an exemplary TSM. An SE issuer or a service provider asks the TSM to house its GP keyset. For the SE issuer. In one embodiment, this GP keyset is most likely to be used as ISD. For the service provider, this keyset will be used as SSD. The process of creating the keyset involves creating the keys in the HSM and creates a mapping in TSM system as indicated in FIG. 8C. The effective range of the mapping will be set to a contract expiring date. In general, an HSM key index cannot be active for more than one mapping at the same time.

[0138] When the keyset is about to expire, a renewal may be made. The renewal flow is similar to the creation process shown in FIG. 8C. According to one embodiment, the TSM will send a notification to the keyset owner periodically a few months before the keyset expires. The notification stops once the keyset owner renews the contract. The keyset owner can start the renewal process by creating a work request or item. A responsible TSM business account manager approves/rejects the work item. Upon receiving the approved work item, the TSM administration updates the keyset expiring date according to the renewal contract.

[0139] Similarly, the keyset can be expired earlier or terminated. The terminate flow is similar to the creation process shown in FIG. 8C. The keyset owner can request to stop the keyset at a future date. The responsible TSM business account manager will verify and approve/reject the request immediately. The TSM administration sets the expiring date of the mapping to the specified date. The HSM key indices can be reused by the TSM for other vendors. An audit log is maintained to keep track of the transactions.

[0140] FIG. 8D shows a data flow for an ISD mapping between an SE issuer and the TSM. In general, the ISD mappings are managed by each SE Issuer directly.

Samsung Ex. 1016, Page 62 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

An SE Issuer can create a mapping to bind an external or internal keyset to an ISD key index. External keysets are keysets not residing in an HSM associated with aTSM while the internal keysets are those residing in the HSM. Normally, the SE issuer should not need to specify the default ISD as the default ISD comes from the SE manufacturer. However, an SE Issuer has an option to overwrite this default ISD if needed.

[0141] According to FIG. 8D, the SE Issuer creates an ISD mapping for a card OS to bind a keyset and an ISD key index (e.g., ranging from 1 to 127). If the keyset is not external, the TSM will ensure that the keyset mapping with its HSM exists. In operation, the SE issuer can directly modify or delete the ISD mapping. As described above, an SE Manufacturer has the default ISD information for the SEs that it produces. The TSM provides both batch and real-time approaches for the SE manufacturer to share this information. Depending on the agreement with TSM, the manufacturer can use either the batch or real-time approach, which has been described above.

[0142] For security reasons, a service provider (SP) may want to have its own SSD for personalizing its applications. The SSD mapping is created by an SE issuer to bind a key index it assigns to the service provider to the SP keyset. FIG. 8E shows a corresponding data flow among a server provider, an SE issuer and the TSM. Similar to the SSD creation, a service provider may request the SE issuer to delete a SSD mapping. The workflow is substantially similar to the SSD creation.

[0143] As described above, applications are provided by service providers to the users. An application needs to be approved and published before it is available for mobile users to subscribe and download. For example, a service provider needs to submit an application to SE issuer and TSM for approval. In operation, a service provider needs to submit an application to the SE issuer and TSM for approval. FIG. 8F shows a data flow for the approval of an application by an SE issuer. If a dedicated SSD is needed, the service provider can request a SSD beforehand as described in Section 6, or can indicate in the request. If a dedicated SSD is needed, the service provider can request a SSD beforehand as above or can indicate in the request.

Samsung Ex. 1016, Page 63 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Before an approved application is available to general public yet, either the service provider or the SE issuer can initiate the publishing process. Both parties must agree before the application is published in the TSM for the users. Then the vendors are notified of the date and availability of the application.

[0144] In some cases, an SE needs to be replaced. The SE replacement could happen at a request of either a mobile user or its SE issuer. Mostly, it is to upgrade a SE for a bigger memory for more services. The following three points should be noted:

- For those applications need to migrate their application states from the old SE, the old SE

need to be still accessible by the applications (via TSM).

- For those applications requiring no state migration, the TSM needs simply just reinstall and personalize the applications.
- However, if any applications that have states in the SE but do not support state migration, the TSM is not able to migrate their states. For these applications, they will be treated as the second case (namely, the applications must be reinstalled and personalized).

[0145] FIG. 8G shows a process of replacing an SE and involves the following stages. An SE issuer informs a TSM about

- SE issuer informs TSM about SE replacement request;
- TSM collaborates with service providers to prepare APDU commands for collecting states of applications on the old SE;
- For each application, TSM executes the command(s) to retrieve application states and lock the application;
- TSM informs mobile user to physically change the new SE. Mobile user may change his/her mind to rollback the replacement request. No rollback is possible after this step;
- TSM will update the default ISD if it has not been done; and
- Collaborating with Service Providers, TSM will install and personalize or provision each application. If needed, TSM will install the SSD for service providers. The personalization data will be prepared based on the static data in the service provider and the dynamic application states.

Samsung Ex. 1016, Page 64 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

[0146] Referring now to FIG. 9, it shows a snapshot of a screen display of an account for a personalized SE. As shown in the menu 902, the account maintains detailed information 904 about the SE that has been personalized. In addition, the account includes a list of provisioned applications as well as security keys. Other information such as application owners (who developed the applications), the responsible contact at the TSM, an SE log as well as an applications log may be maintained.

[0147] The invention is preferably implemented by software, but can also be implemented in hardware or a combination of hardware and software. The invention can also be embodied as computer readable code on a computer readable medium. The computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves. The computer readable medium can also be distributed over network-coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

[0148] The present invention has been described in sufficient details with a certain degree of particularity. It is understood to those skilled in the art that the present disclosure of embodiments has been made by way of examples only and that numerous changes in the arrangement and combination of parts may be resorted without departing from the spirit and scope of the invention as claimed. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description of embodiment.

Samsung Ex. 1016, Page 65 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Claims

We claim:

1. A mobile device supporting multiple applications, the mobile device comprising:
   an emulator;
   a near field communication (NFC) interface to facilitate data exchange between a reader and an application being loaded and executed in the emulator, wherein the application in the emulator being one of the applications is replaceable in entirety or in part by another one of the applications; and
   a storage device configured to store the multiple applications, anyone of the applications being loadable into the emulator when selectively activated and subsequently replacing the application in the emulator, wherein the mobile device changes functions offered by the application to functions offered by another application newly loaded and executed in the emulator, wherein each of the applications has been remotely provisioned by a server configured to provide trusted service management (TSM).

2. The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:
   initiating data communication between the mobile device and the server;
   receiving device information of the secure element from the mobile device in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and
   sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider.

Samsung Ex. 1016, Page 66 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

3. The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of contactless cards provided respectively to perform a function related to monetary, the mobile device is able to be used for all of the contactless cards when one of the applications is loaded into and executed in the emulator.

5. The mobile device as recited in claim 4, wherein each of the contactless cards is a Mifare contactless card.

6. The mobile device as recited in claim 5, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. The mobile device as recited in claim 6, wherein mobile device further includes a card manager proxy configured to facilitate communication between the TSM server and the TMSM module in the secure element, a readonly user interface (UI) application provided to query one or more of the applications on information stored therein but will not modify the information, and a transaction UI application for conducting operations that will modify one or more sectors in one or more of the applications.

8. The mobile device as recited in claim 6, wherein the TMSM module is configured to:

Samsung Ex. 1016, Page 67 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module and later on swapping another one of the applications to the emulator;

enable the TSM server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. The mobile device as recited in claim 2, wherein the mobile device is a smartphone, a portable computer and a smart card.

11. The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

Samsung Ex. 1016, Page 68 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

12. A method for a mobile device to support multiple applications, the method comprising:

installing the applications respectively in the mobile device, each of the applications pertaining to a physical contactless card, so that the mobile device is to be used in lieu of multiple physical contactless cards, wherein the mobile device comprises:

an emulator;

a near field communication (NFC) interface to facilitate data exchange between a reader and an application being loaded and executed in the emulator, wherein the application in the emulator being one of the applications is replaceable in entirety or in part by another one of the applications; and

a storage device configured to store the multiple applications, anyone of the applications being loadable into the emulator when selectively activated and subsequently replacing the application in the emulator, wherein the mobile device changes functions offered by the application to functions offered by another application newly loaded and executed in the emulator, wherein each of the applications has been remotely provisioned by a server configured to provide trusted service management (TSM).

13. The method as recited in claim 12, wherein the mobile device is associated with a secure element, the method further comprises:

initiating data communication between the mobile device and the server;

receiving device information of the secure element from the mobile device in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the

Samsung Ex. 1016, Page 69 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

request is a command causing the mobile device to retrieve the device information from the secure element therein; and

sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider.

14. The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. The method as recited in claim 14, wherein each of the physical contactless cards is loaded with a Mifare emulator, the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. The mobile device as recited in claim 15, wherein mobile device further includes a card manager proxy configured to facilitate communication between the TSM server and the TMSM module in the secure element, a readonly user interface (UI) application provided to query one or more of the applications on information stored therein but will not modify the information, and a transaction UI application for conducting operations that will modify one or more sectors in one or more of the applications.

17. The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

Samsung Ex. 1016, Page 70 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

18. The method as recited in claim 12, wherein the mobile device is a smartphone, a portable computer and a smart card.

19. The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

Samsung Ex. 1016, Page 71 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Method and apparatus for emulating multiple cards in mobile devices

Abstract

Techniques for mobile devices configured to support or function as multiple contactless cards, such as Mifare contactless cards, are disclosed. According to one embodiment, a mobile device embedded with an emulator is loaded with a plurality of software modules or applications, each emulating one card or one type of contactless cards. An emulator is implemented in a secure element that is personalized for a user of the mobile device while the applications are respectively provisioned via their respective providers per the personalized secure element. When the mobile device is to be used as a contactless card to perform a monetary function, a corresponding application is loaded into and executed in the emulator. When the mobile device is to be used to perform another monetary function, a corresponding application is loaded into the emulator to replace the previous application entirely or partially in the emulator. As a result, the mobile device can be used as a monetary device in lieu of multiple contactless cards.

Samsung Ex. 1016, Page 72 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

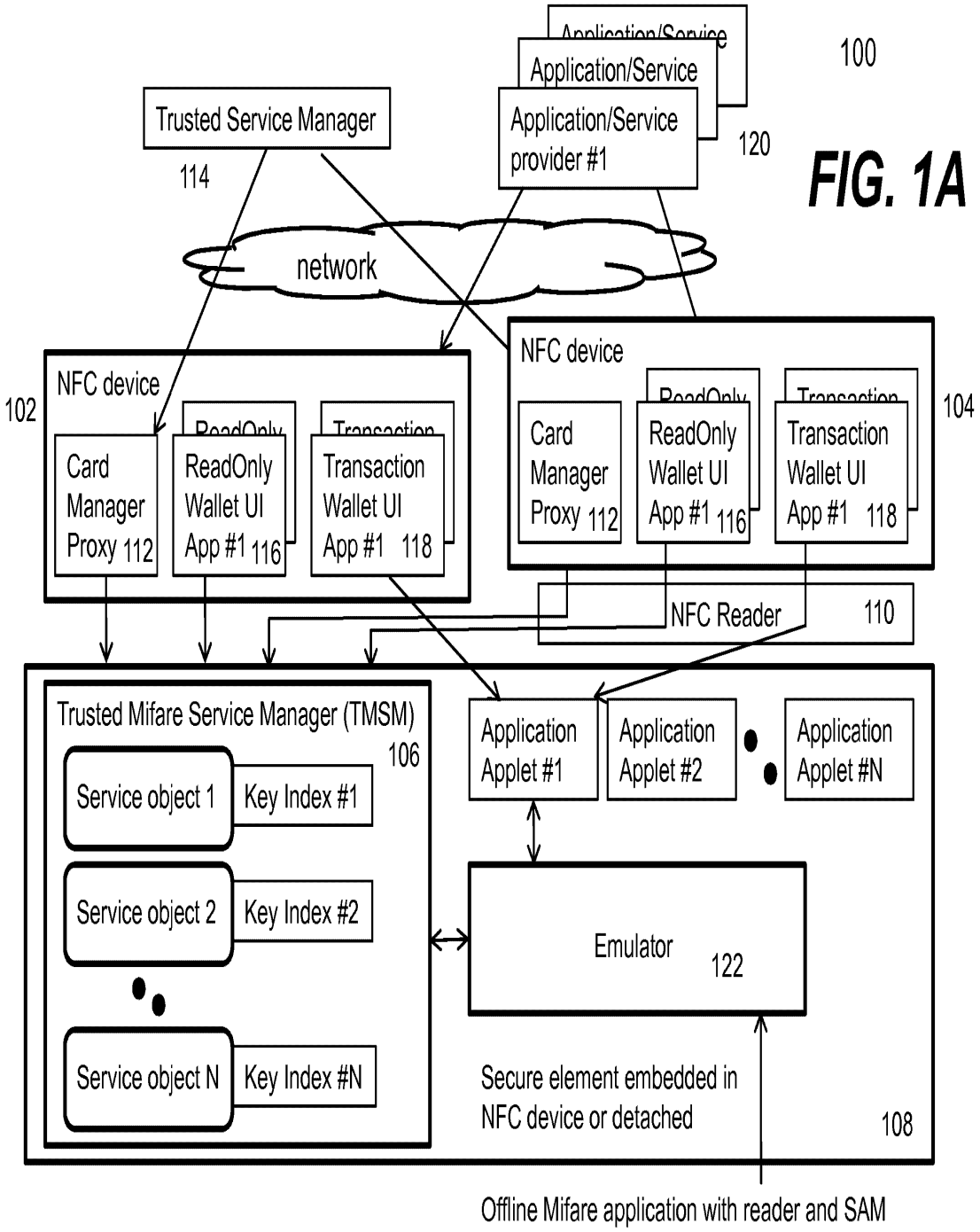

100
Application/Service
Application/Service
Application/Service provider #1
120
Trusted Service Manager
114
network
NFC device
102
Card Manager Proxy 112
ReadOnly Wallet UI App #1 116
Transaction Wallet UI App #1 118
NFC device
104
Card Manager Proxy 112
ReadOnly Wallet UI App #1 116
Transaction Wallet UI App #1 118
NFC Reader 110
Trusted Mifare Service Manager (TMSM)
106
Service object 1
Key Index #1
Service object 2
Key Index #2
Service object N
Key Index #N
Application Applet #1
Application Applet #2
Application Applet #N
Emulator 122
Secure element embedded in NFC device or detached
108
Offline Mifare application with reader and SAM

FIG. 1A

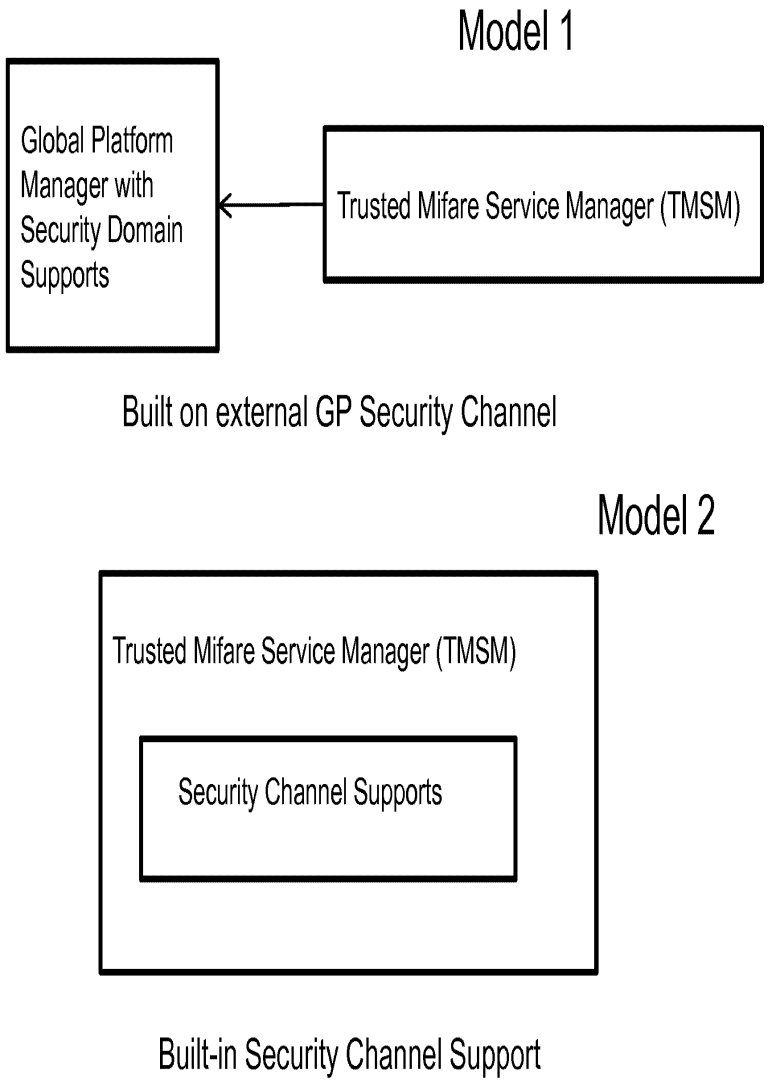

Model 1
Global Platform Manager with Security Domain Supports
Trusted Mifare Service Manager (TMSM)
Built on external GP Security Channel
Model 2
Trusted Mifare Service Manager (TMSM)
Security Channel Supports
Built-in Security Channel Support

FIG. 1B

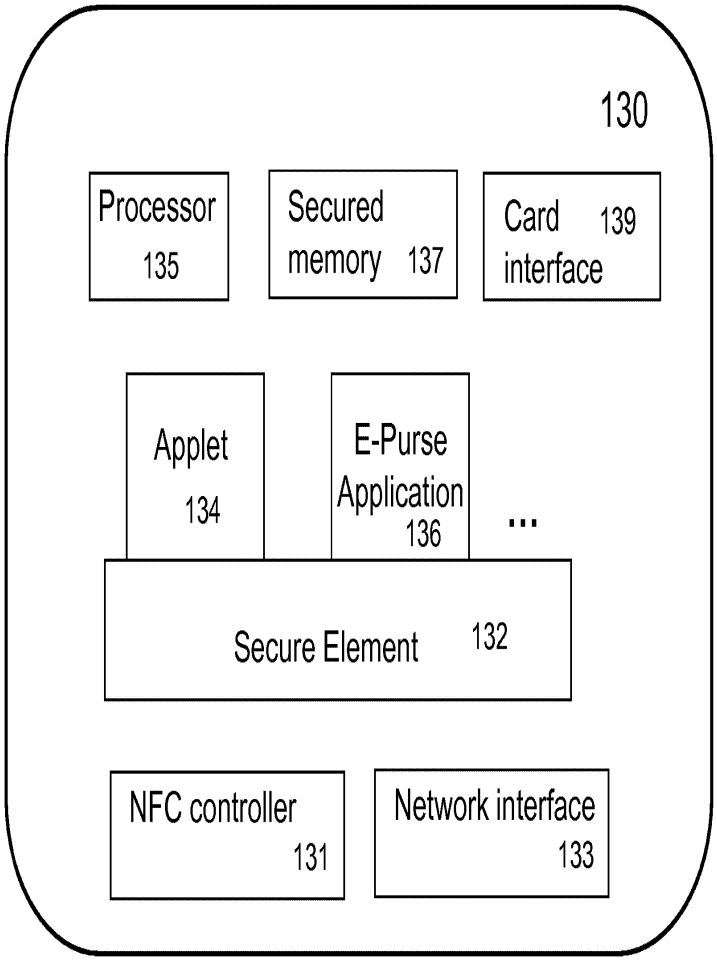

130
Processor
135
Secured
memory 137
Card 139
interface
Applet
134
E-Purse
Application
136
...
Secure Element 132
NFC controller
131
Network interface
133

FIG. 1C

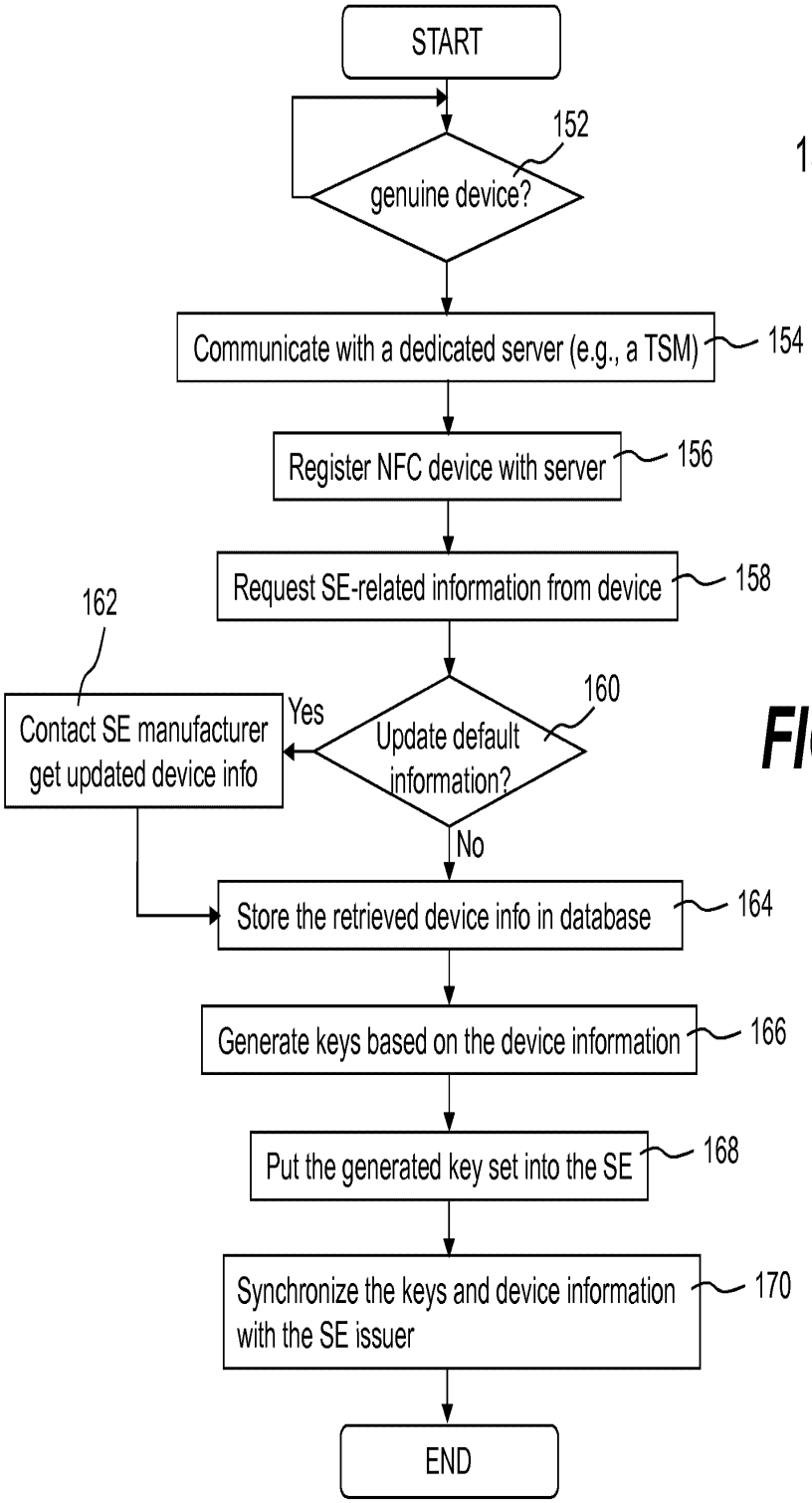
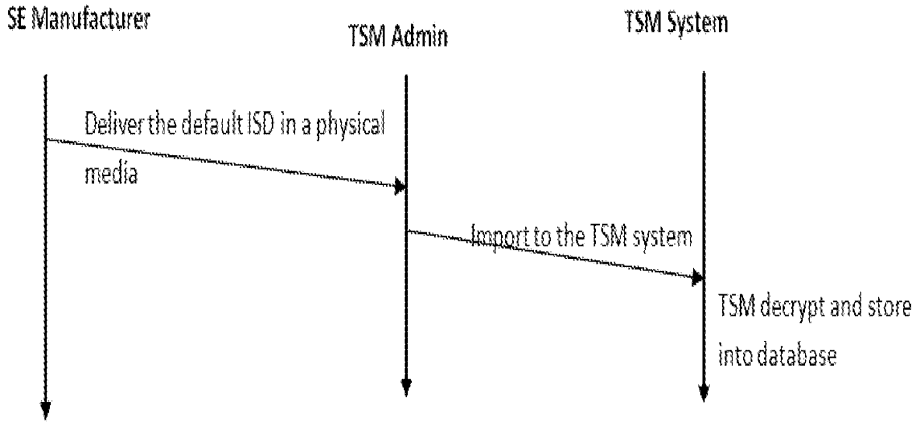
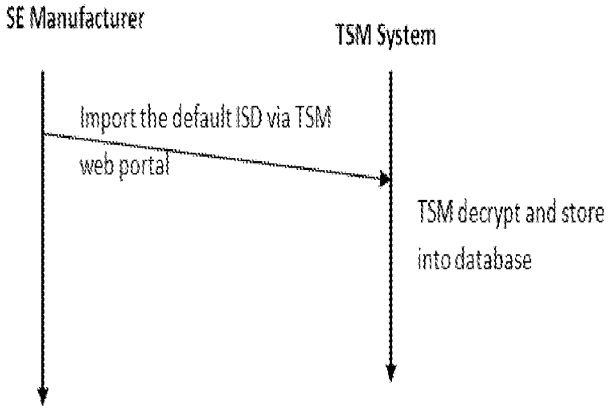

START
152
genuine device?
150
Communicate with a dedicated server (e.g., a TSM)
154
Register NFC device with server
156
Request SE-related information from device
158
162
Contact SE manufacturer get updated device info
Yes
160
Update default information?
No
Store the retrieved device info in database
164
Generate keys based on the device information
166
Put the generated key set into the SE
168
Synchronize the keys and device information with the SE issuer
170
END

FIG. 1D



Offline Batch Approach for Default ISD Update



Online Batch Approach for Default ISD Update

FIG. 1E

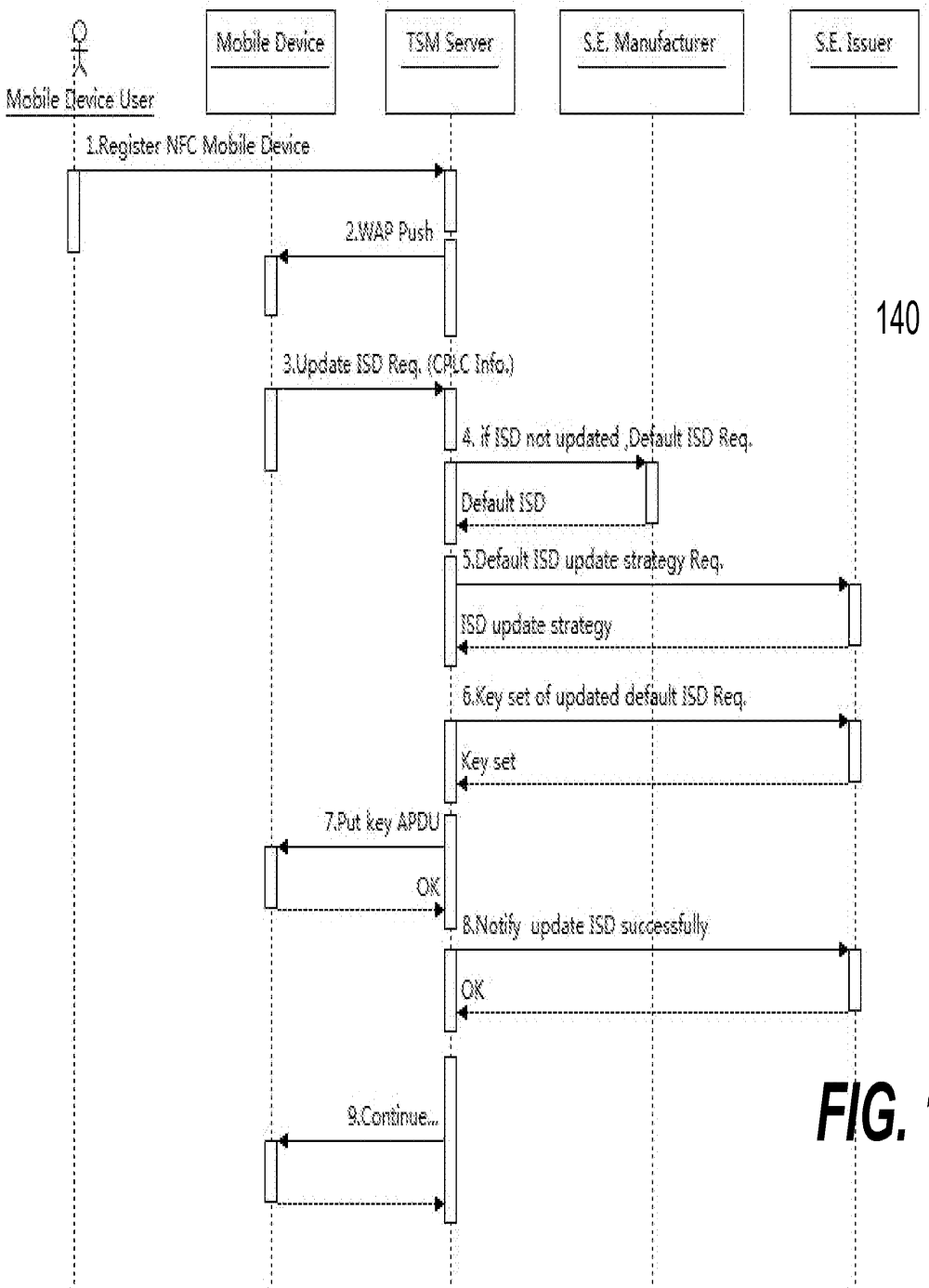

Mobile Device User
Mobile Device
TSM Server
S.E. Manufacturer
S.E. Issuer
1.Register NFC Mobile Device
2.WAP Push
140
3.Update ISD Req. (CPLC Info.)
4. if ISD not updated ,Default ISD Req.
Default ISD
5.Default ISD update strategy Req.
ISD update strategy
6.Key set of updated default ISD Req.
Key set
7.Put key APDU
OK
8.Notify update ISD successfully
OK
9.Continue...

FIG. 1F

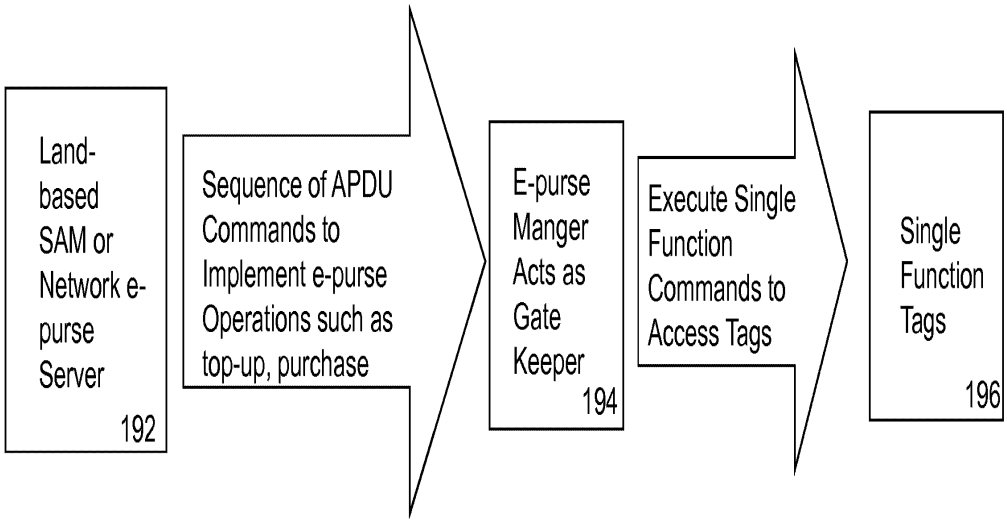

190
Land-based SAM or Network e-purse Server
192
Sequence of APDU Commands to Implement e-purse Operations such as top-up, purchase
E-purse Manger Acts as Gate Keeper
194
Execute Single Function Commands to Access Tags
Single Function Tags
196

FIG. 1G

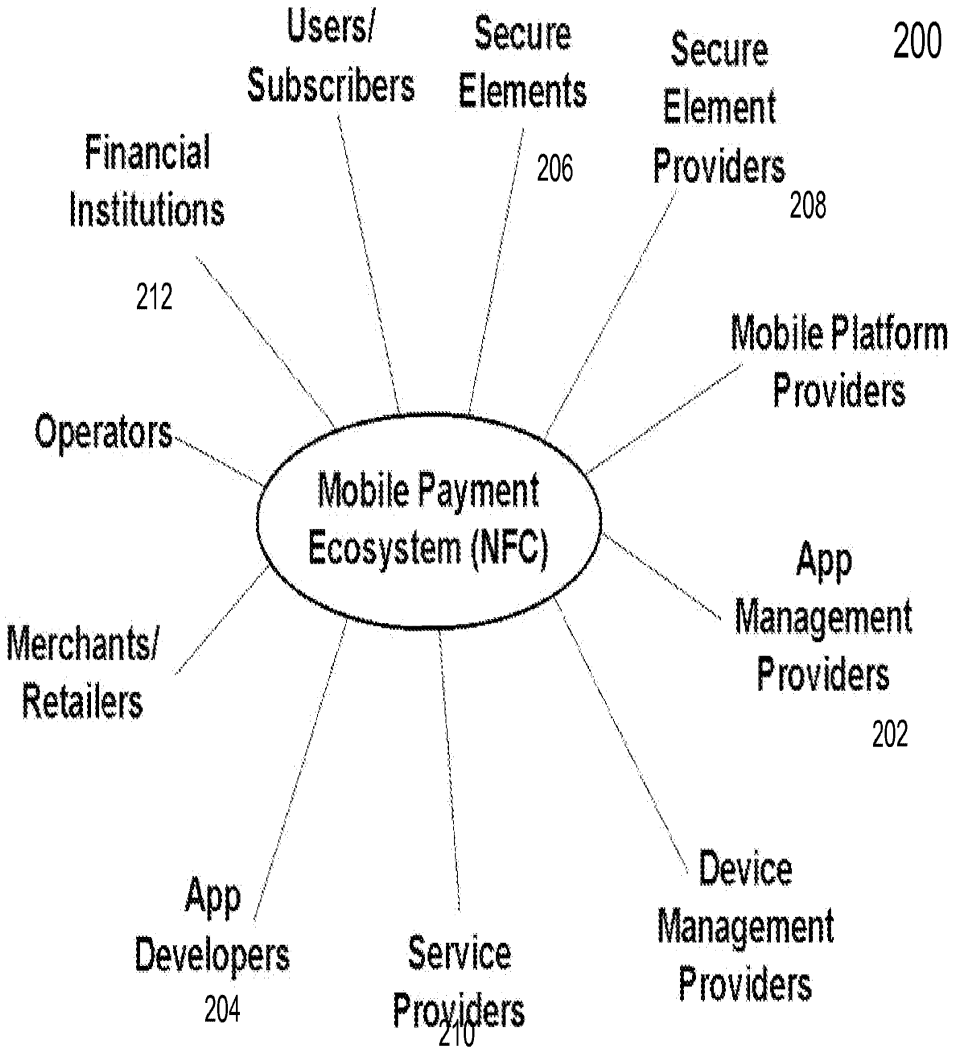

200
Users/
Subscribers
Secure
Elements
206
Secure
Element
Providers
208
Financial
Institutions
212
Mobile Platform
Providers
Operators
Mobile Payment
Ecosystem (NFC)
App
Management
Providers
202
Merchants/
Retailers
App
Developers
204
Service
Providers
210
Device
Management
Providers

FIG. 2A

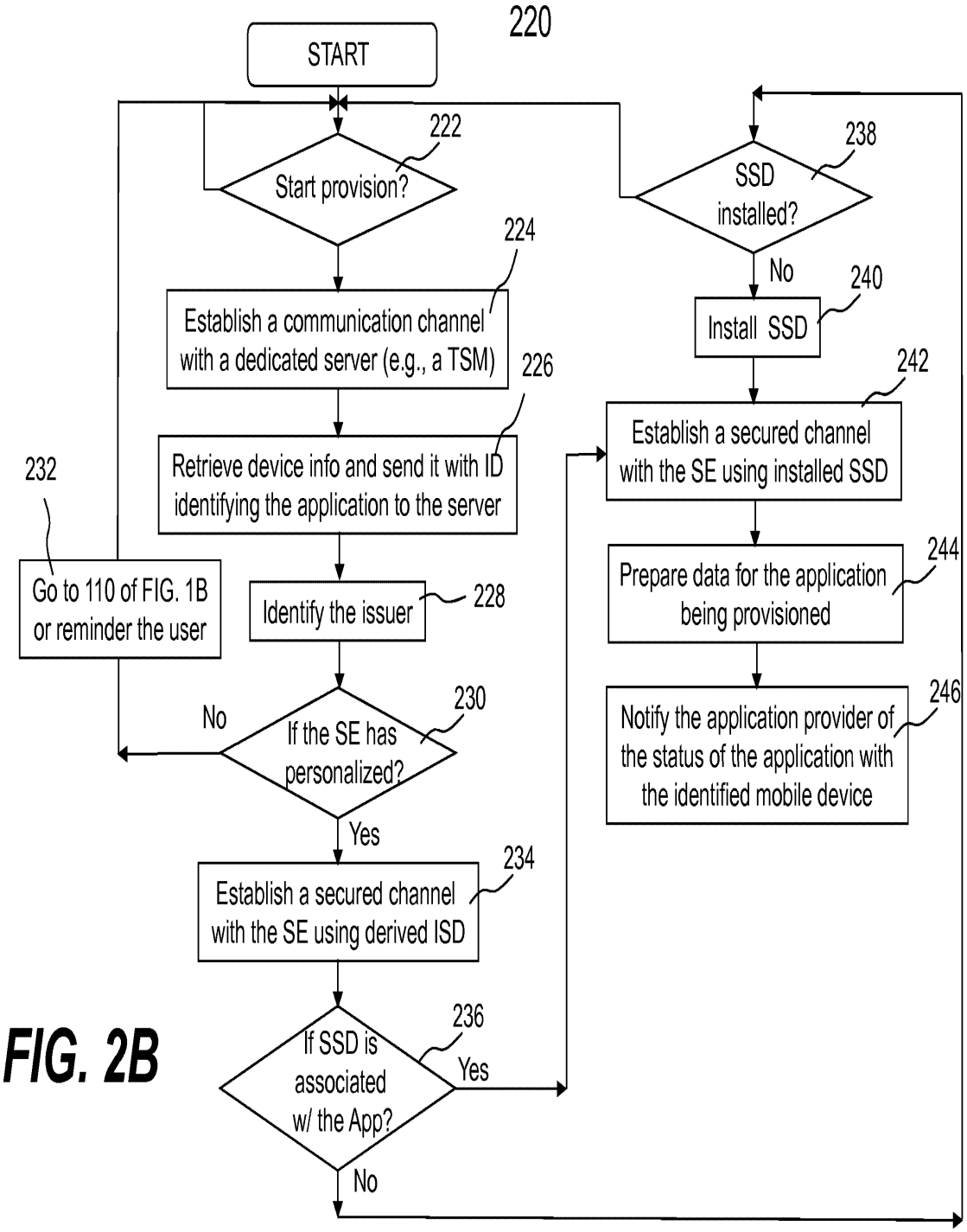

220
START
222
Start provision?
224
Establish a communication channel with a dedicated server (e.g., a TSM)
226
Retrieve device info and send it with ID identifying the application to the server
228
Identify the issuer
230
If the SE has personalized?
No
232
Go to 110 of FIG. 1B or reminder the user
Yes
234
Establish a secured channel with the SE using derived ISD
236
If SSD is associated w/ the App?
Yes
No
238
SSD installed?
No
240
Install SSD
242
Establish a secured channel with the SE using installed SSD
244
Prepare data for the application being provisioned
246
Notify the application provider of the status of the application with the identified mobile device

FIG. 2B

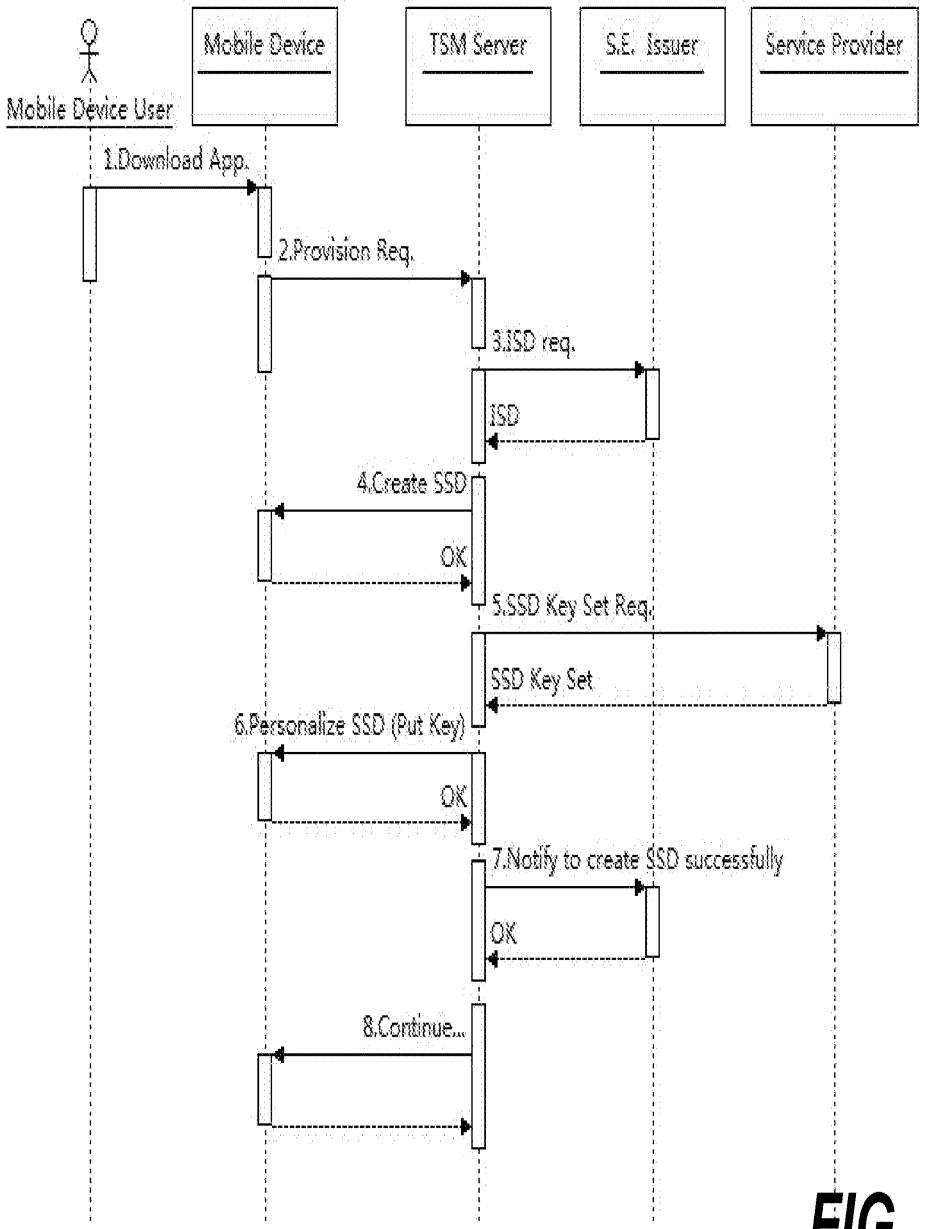
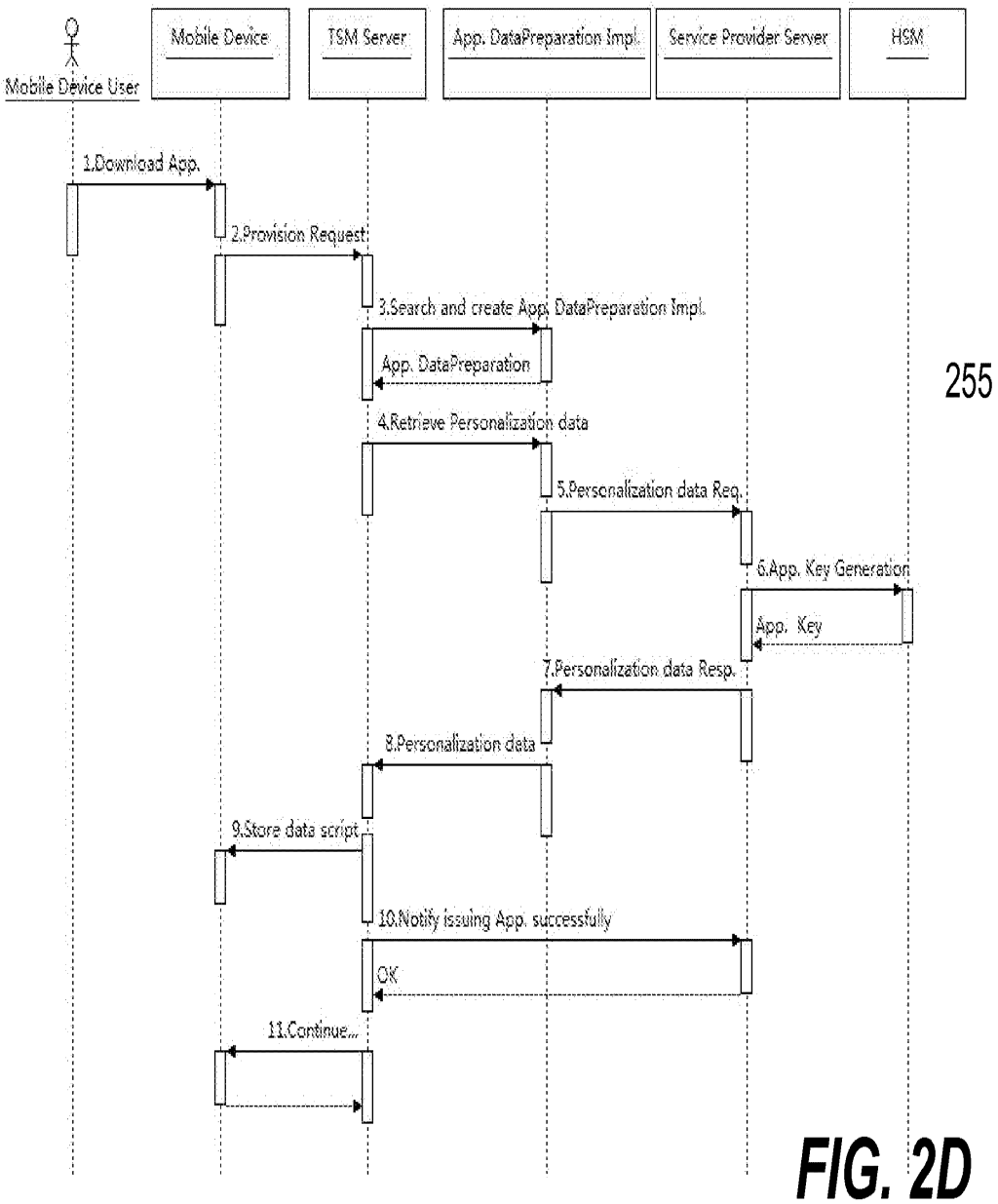

Mobile Device User
Mobile Device
TSM Server
S.E. Issuer
Service Provider
250
1.Download App.
2.Provision Req.
3.ISD req.
ISD
4.Create SSD
OK
5.SSD Key Set Req.
SSD Key Set
6.Personalize SSD (Put Key)
OK
7.Notify to create SSD successfully
OK
8.Continue...

FIG. 2C


Mobile Device User
Mobile Device
TSM Server
App. DataPreparation Impl.
Service Provider Server
HSM
1.Download App.
2.Provision Request
3.Search and create App. DataPreparation Impl.
App. DataPreparation
4.Retrieve Personalization data
5.Personalization data Req.
6.App. Key Generation
App. Key
7.Personalization data Resp.
8.Personalization data
9.Store data script
10.Notify issuing App. successfully
OK
11.Continue...

255

FIG. 2D

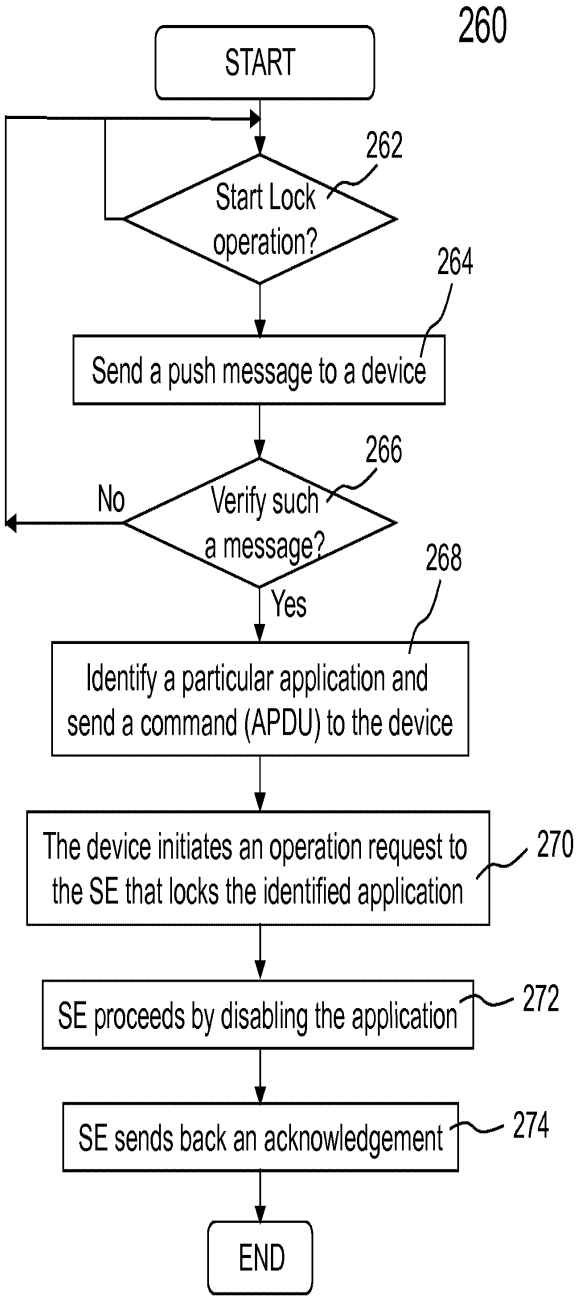

260
START
262
Start Lock operation?
264
Send a push message to a device
266
No
Verify such a message?
Yes
268
Identify a particular application and send a command (APDU) to the device
The device initiates an operation request to the SE that locks the identified application
270
SE proceeds by disabling the application
272
SE sends back an acknowledgement
274
END

FIG. 2E

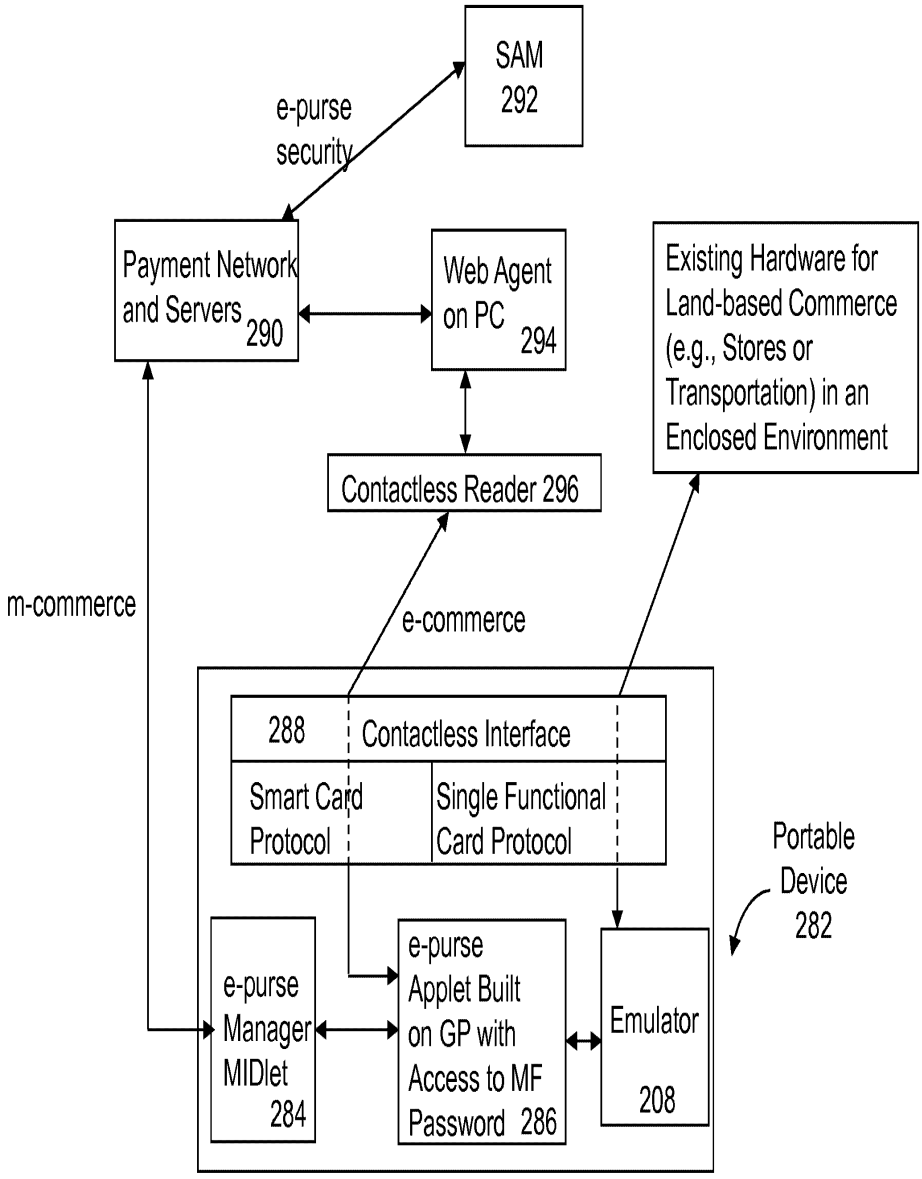

280
SAM
292
e-purse
security
Payment Network
and Servers
290
Web Agent
on PC
294
Existing Hardware for
Land-based Commerce
(e.g., Stores or
Transportation) in an
Enclosed Environment
Contactless Reader 296
m-commerce
e-commerce
288
Contactless Interface
Smart Card
Protocol
Single Functional
Card Protocol
Portable
Device
282
e-purse
Manager
MIDlet
284
e-purse
Applet Built
on GP with
Access to MF
Password 286
Emulator
208

FIG. 2F

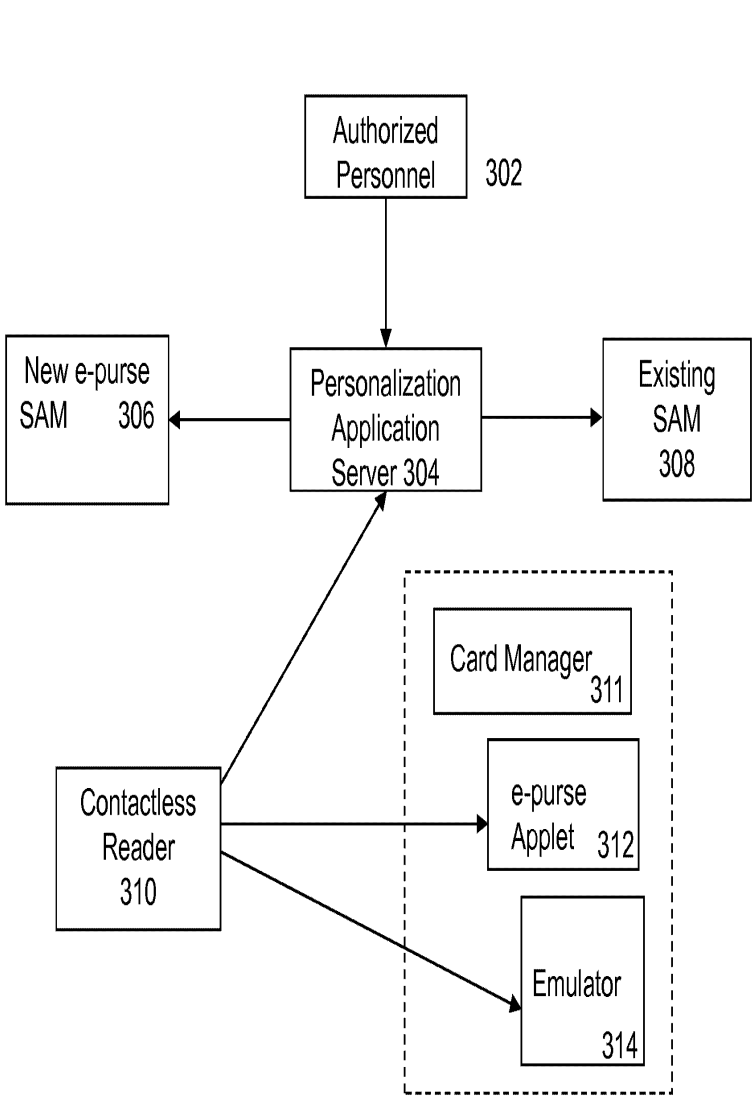

300
Authorized Personnel
302
New e-purse SAM
306
Personalization Application Server 304
Existing SAM
308
Card Manager
311
Contactless Reader
310
e-purse Applet
312
Emulator
314

FIG. 3A

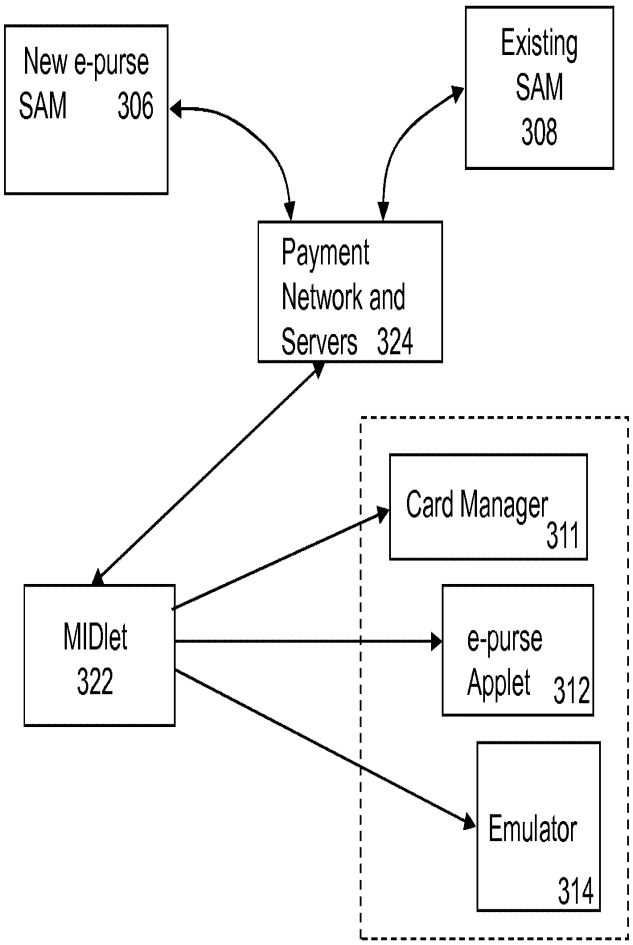

320
New e-purse SAM 306
Existing SAM 308
Payment Network and Servers 324
Card Manager 311
MIDlet 322
e-purse Applet 312
Emulator 314

FIG. 3B

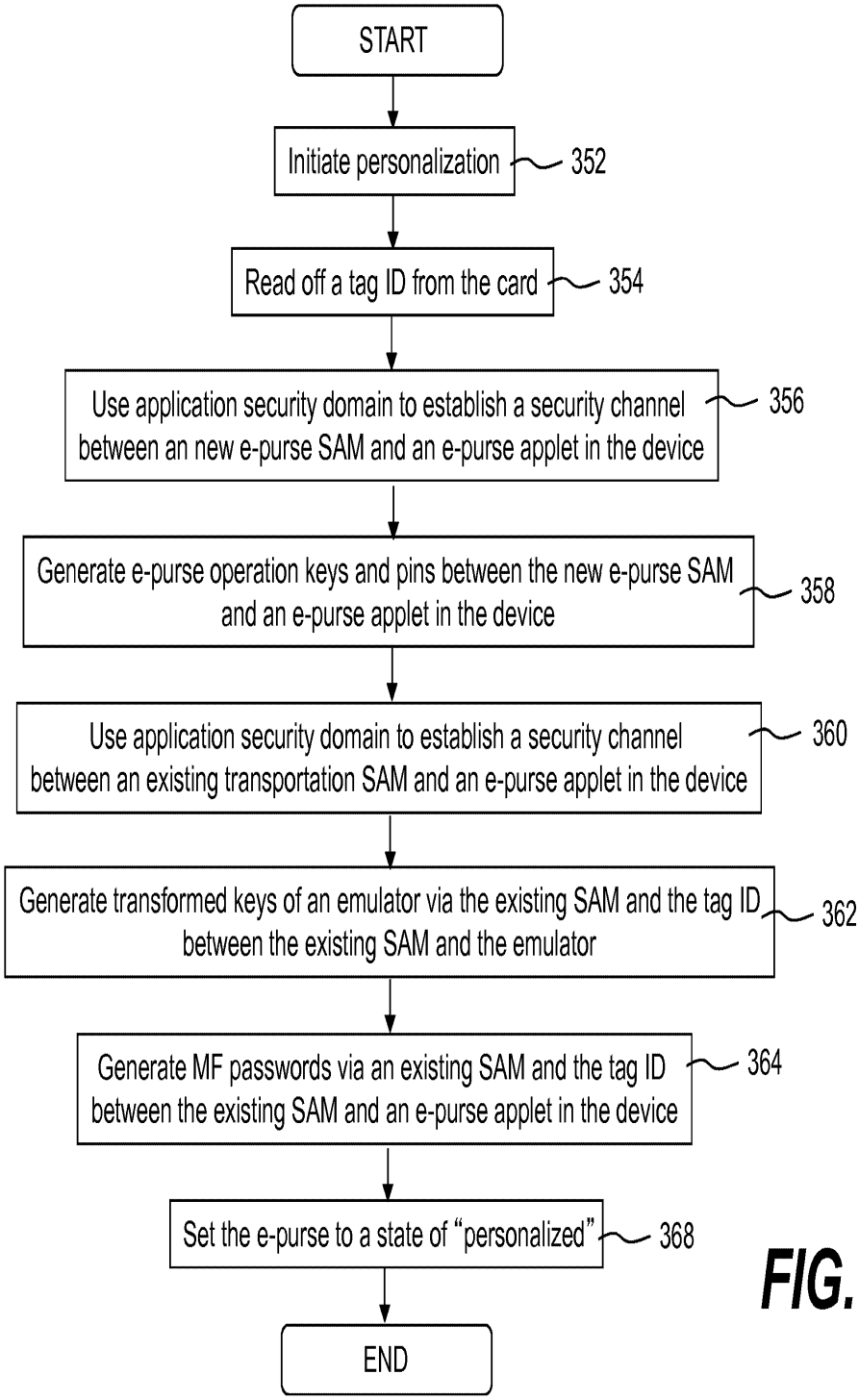

START
350
Initiate personalization
352
Read off a tag ID from the card
354
Use application security domain to establish a security channel between an new e-purse SAM and an e-purse applet in the device
356
Generate e-purse operation keys and pins between the new e-purse SAM and an e-purse applet in the device
358
Use application security domain to establish a security channel between an existing transportation SAM and an e-purse applet in the device
360
Generate transformed keys of an emulator via the existing SAM and the tag ID between the existing SAM and the emulator
362
Generate MF passwords via an existing SAM and the tag ID between the existing SAM and an e-purse applet in the device
364
Set the e-purse to a state of "personalized"
368
END

FIG. 3C

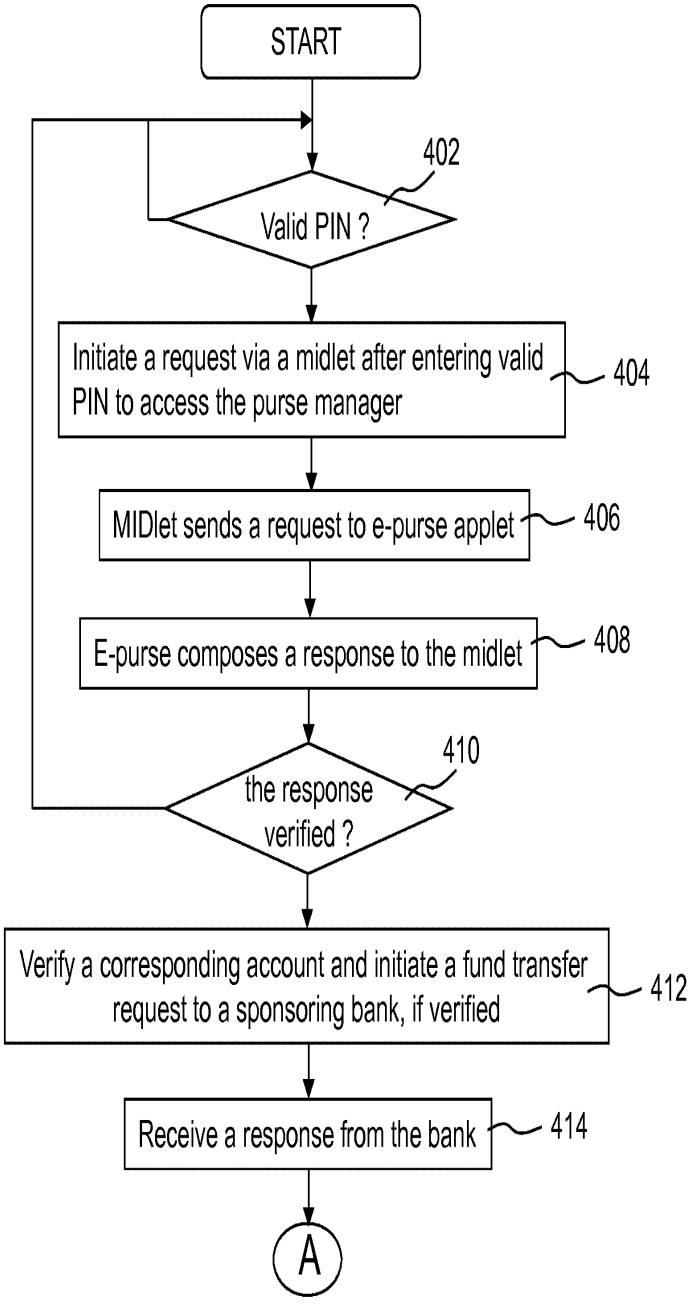

START
400
402
Valid PIN ?
Initiate a request via a midlet after entering valid PIN to access the purse manager
404
MIDlet sends a request to e-purse applet
406
E-purse composes a response to the midlet
408
410
the response verified ?
Verify a corresponding account and initiate a fund transfer request to a sponsoring bank, if verified
412
Receive a response from the bank
414
A

FIG. 4A

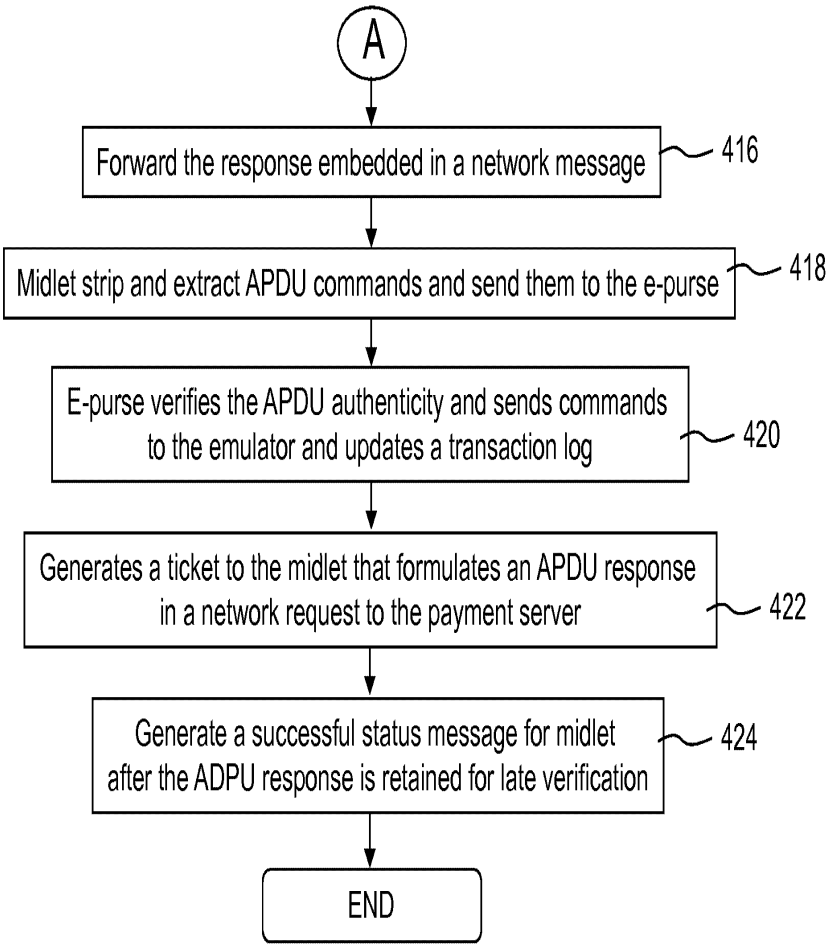

A
Forward the response embedded in a network message
416
Midlet strip and extract APDU commands and send them to the e-purse
418
E-purse verifies the APDU authenticity and sends commands to the emulator and updates a transaction log
420
Generates a ticket to the midlet that formulates an APDU response in a network request to the payment server
422
Generate a successful status message for midlet after the ADPU response is retained for late verification
424
END

FIG. 4B

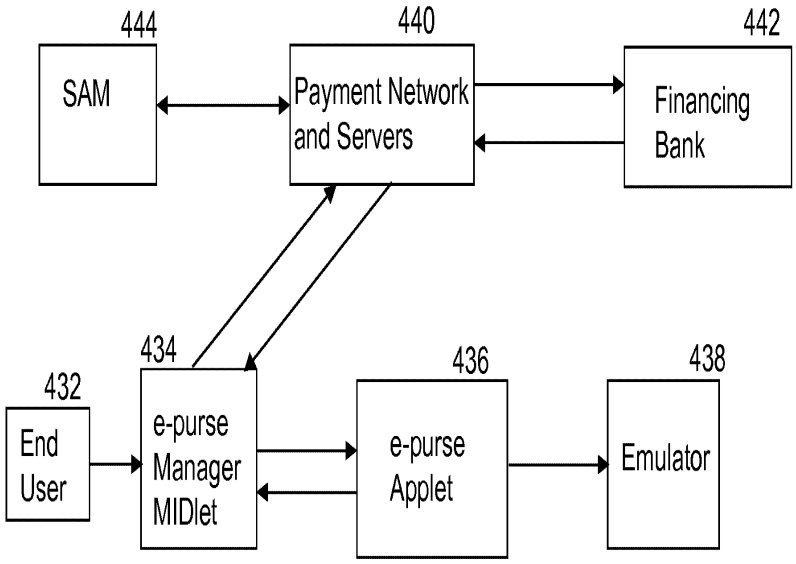

444
SAM
440
Payment Network and Servers
442
Financing Bank
434
432
End User
e-purse Manager MIDlet
436
e-purse Applet
438
Emulator

FIG. 4C

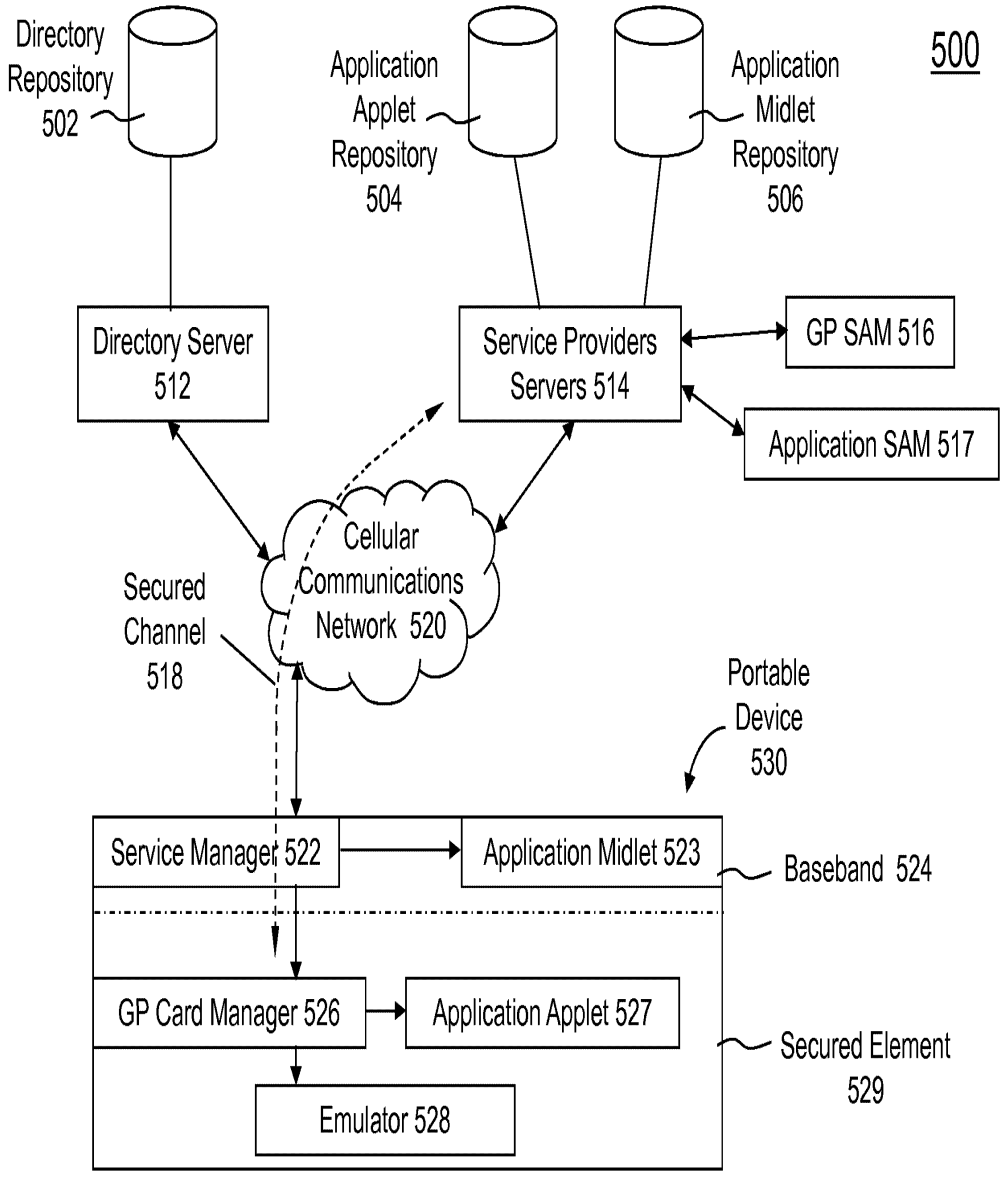

500
Directory Repository 502
Application Applet Repository 504
Application Midlet Repository 506
Directory Server 512
Service Providers Servers 514
GP SAM 516
Application SAM 517
Cellular Communications Network 520
Secured Channel 518
Portable Device 530
Service Manager 522
Application Midlet 523
Baseband 524
GP Card Manager 526
Application Applet 527
Secured Element 529
Emulator 528

FIG. 5A

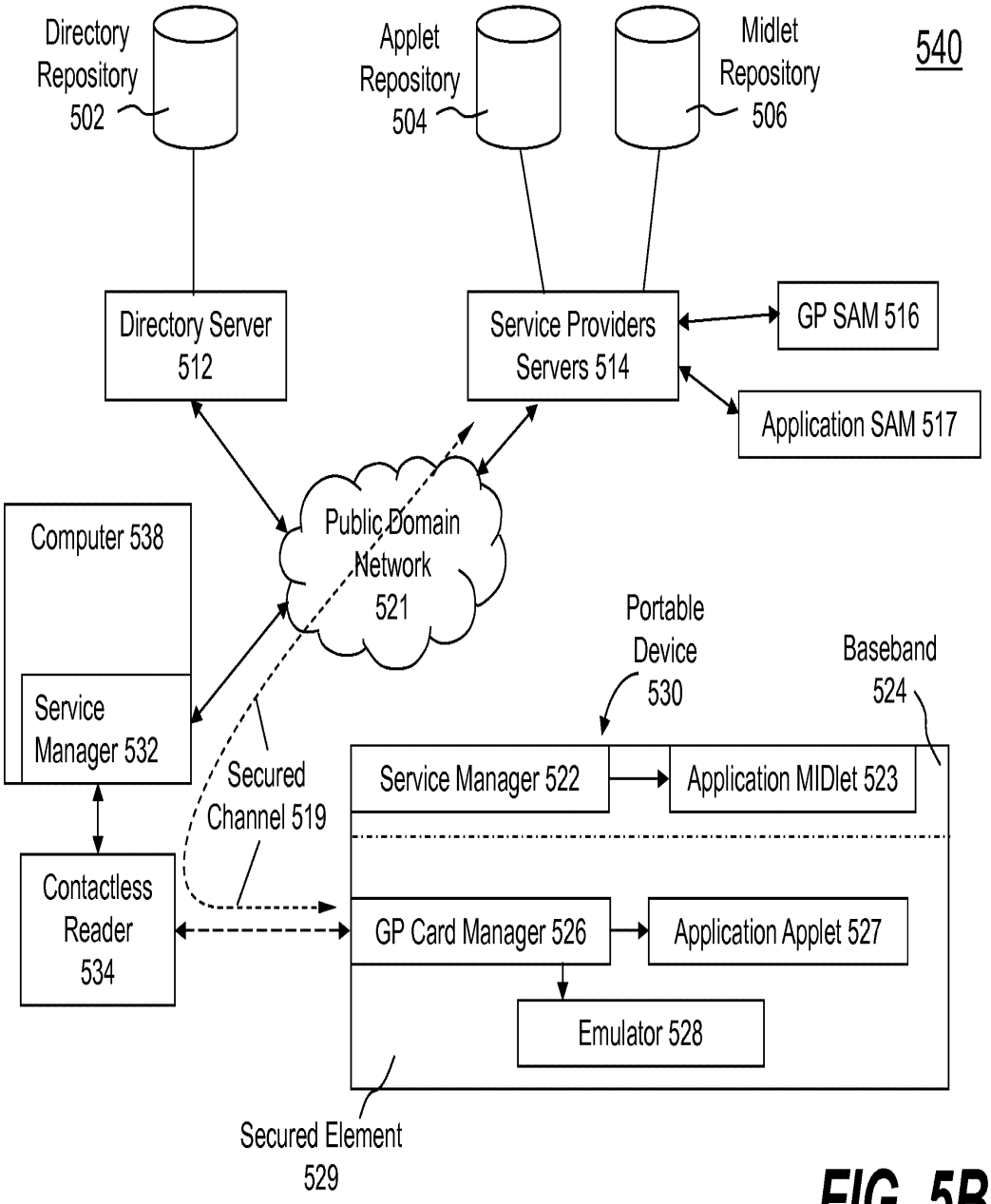
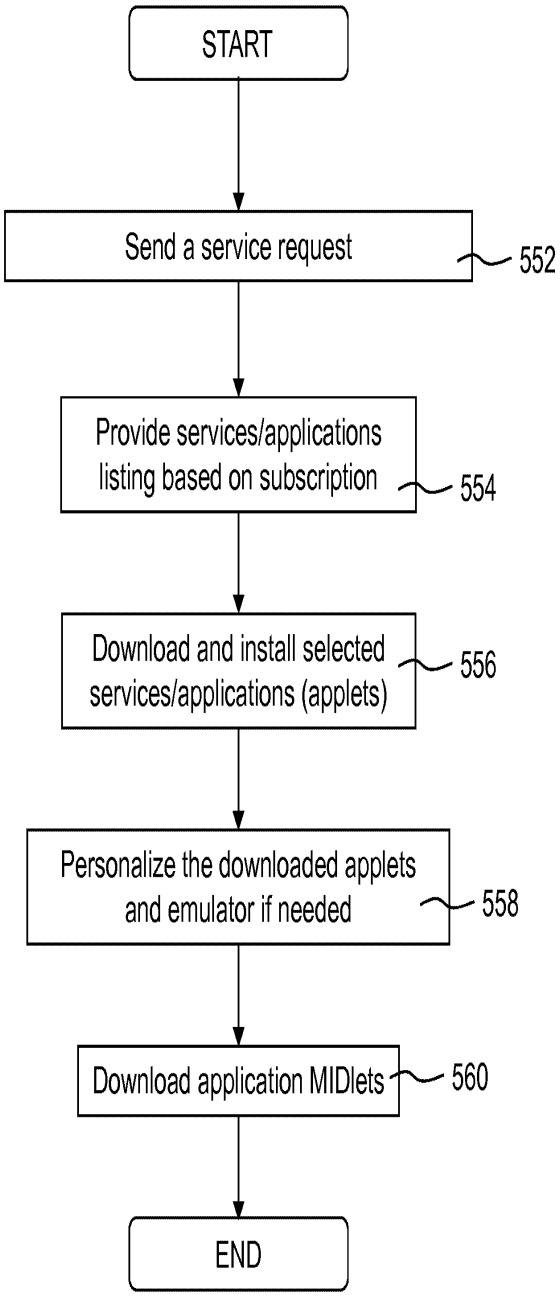

Directory Repository 502
Applet Repository 504
Midlet Repository 506
540
Directory Server 512
Service Providers Servers 514
GP SAM 516
Application SAM 517
Public Domain Network 521
Computer 538
Service Manager 532
Portable Device 530
Baseband 524
Secured Channel 519
Service Manager 522
Application MIDlet 523
Contactless Reader 534
GP Card Manager 526
Application Applet 527
Emulator 528
Secured Element 529

FIG. 5B


START
Send a service request
552
Provide services/applications listing based on subscription
554
Download and install selected services/applications (applets)
556
Personalize the downloaded applets and emulator if needed
558
Download application MIDlets
560
END

550

FIG. 5C

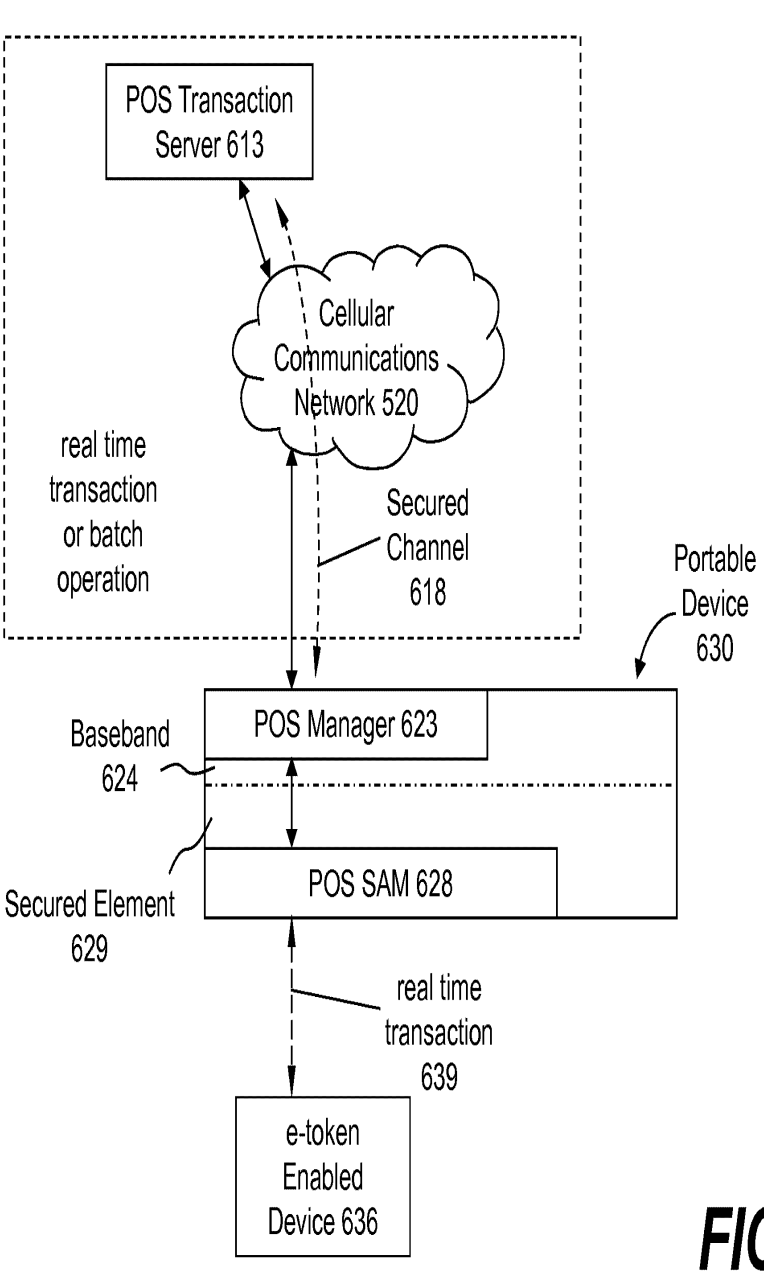

600
POS Transaction Server 613
Cellular Communications Network 520
real time transaction or batch operation
Secured Channel 618
Portable Device 630
Baseband 624
POS Manager 623
POS SAM 628
Secured Element 629
real time transaction 639
e-token Enabled Device 636

FIG. 6A

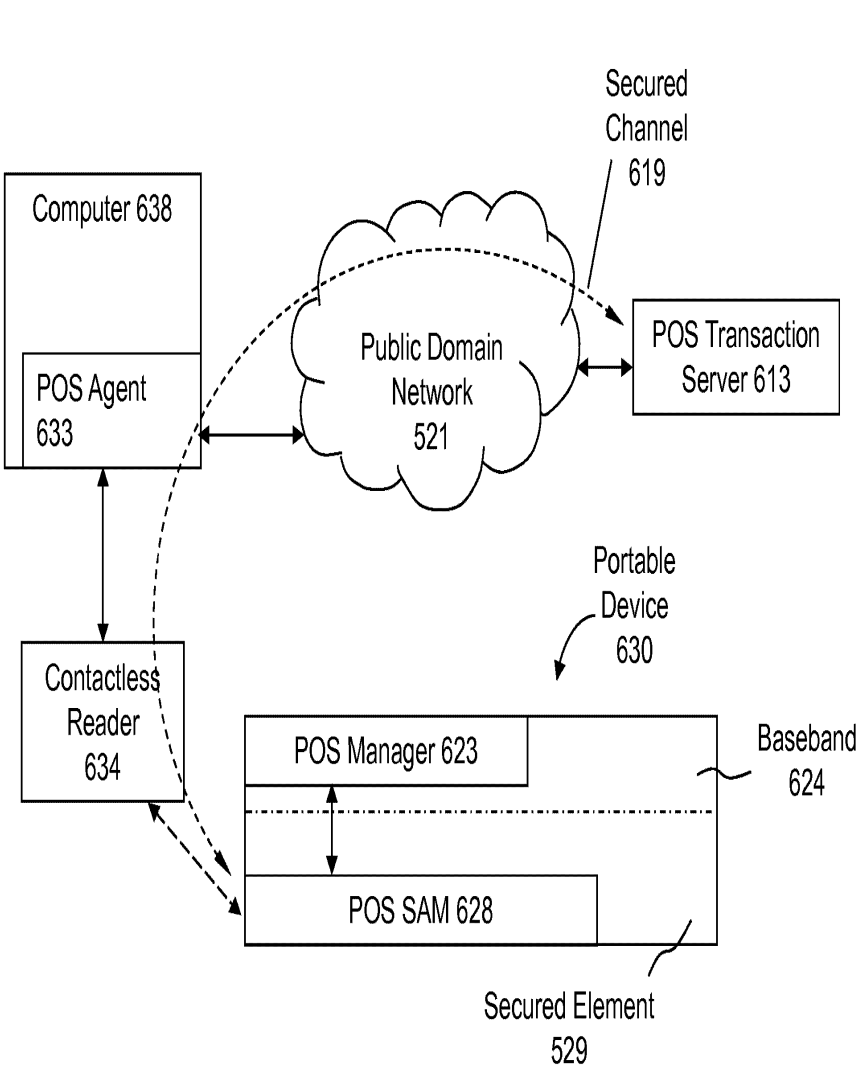

640
Secured
Channel
619
Computer 638
POS Agent
633
Public Domain
Network
521
POS Transaction
Server 613
Portable
Device
630
Contactless
Reader
634
POS Manager 623
Baseband
624
POS SAM 628
Secured Element
529

FIG. 6B

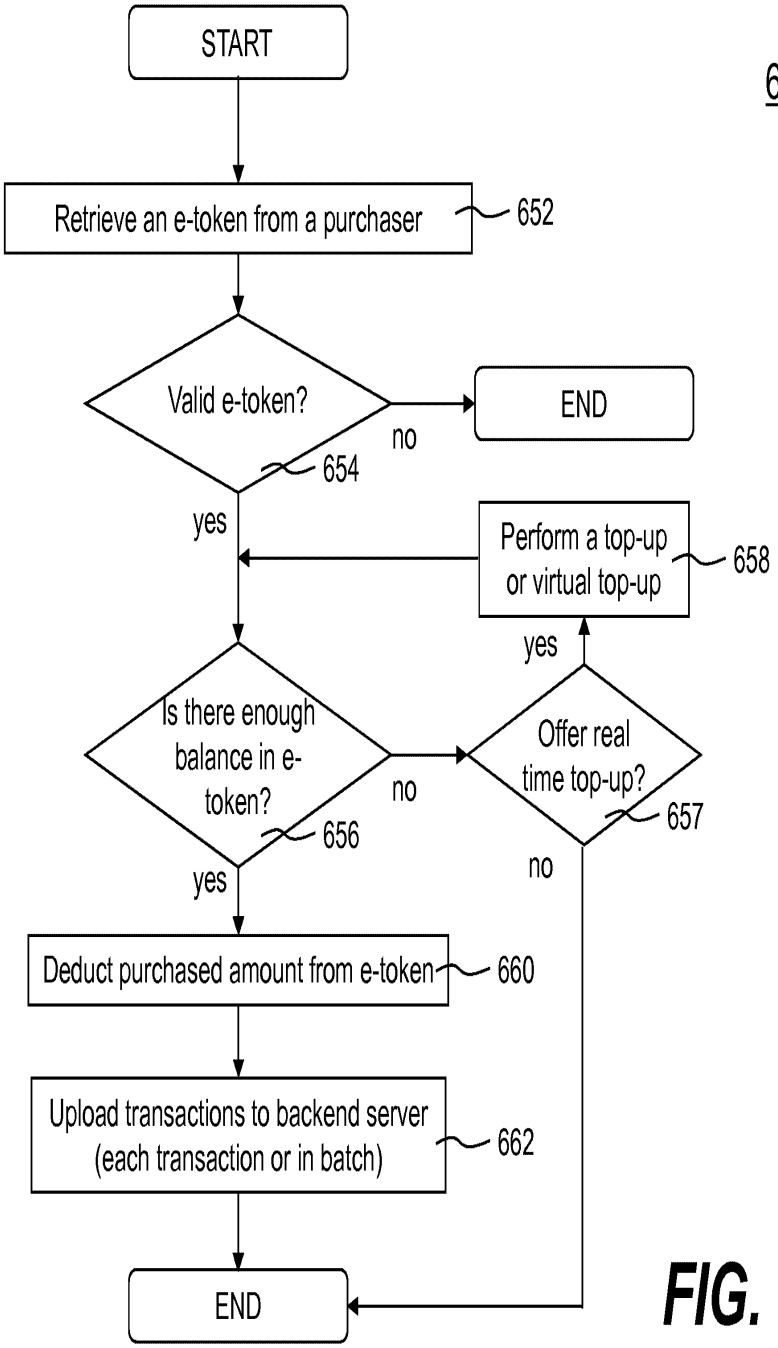

650
START
Retrieve an e-token from a purchaser
652
Valid e-token?
654
no
END
yes
Perform a top-up or virtual top-up
658
yes
Is there enough balance in e-token?
656
no
Offer real time top-up?
657
yes
no
Deduct purchased amount from e-token
660
Upload transactions to backend server (each transaction or in batch)
662
END

FIG. 6C

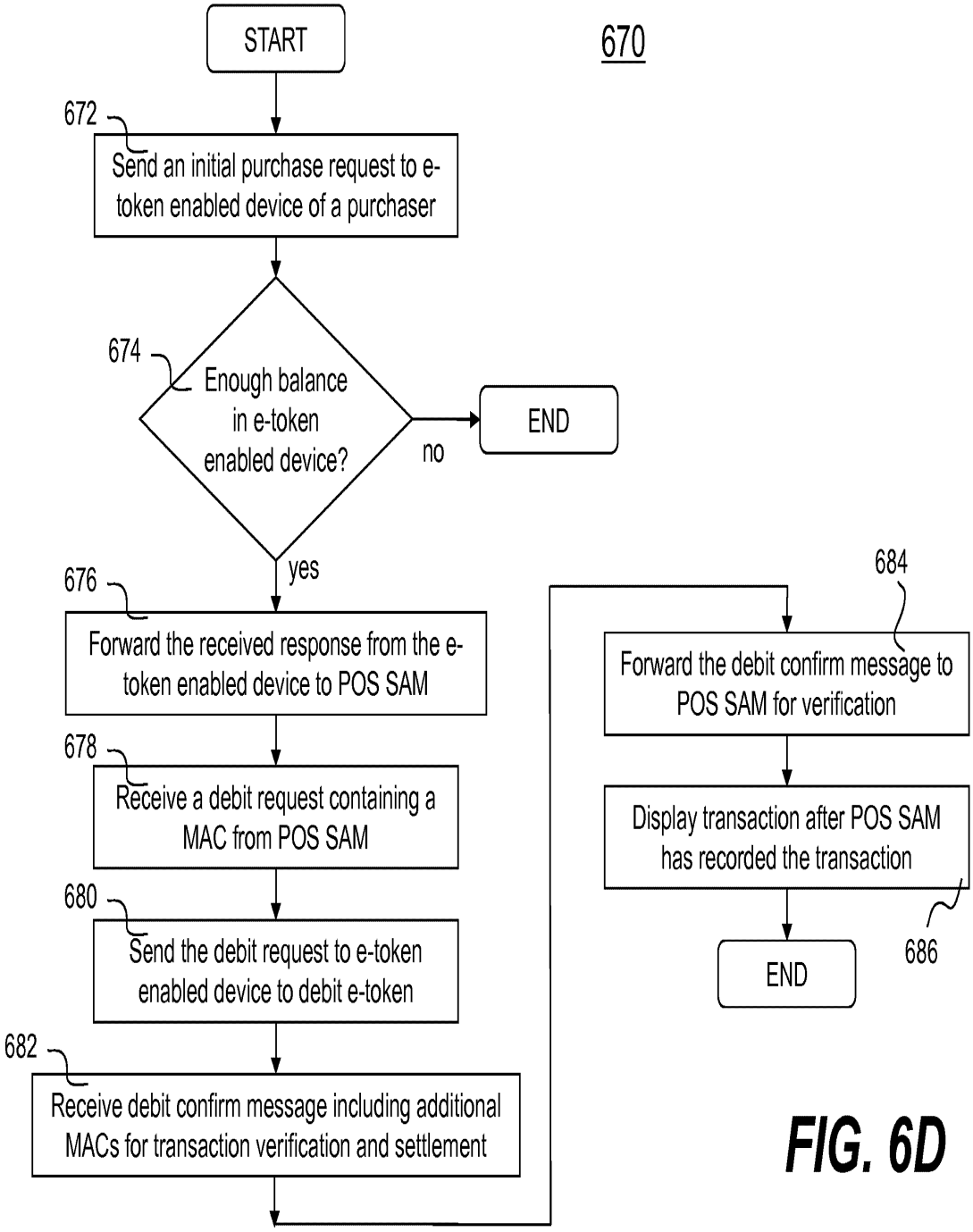

START
670
672
Send an initial purchase request to e-token enabled device of a purchaser
674
Enough balance in e-token enabled device?
no
END
yes
676
Forward the received response from the e-token enabled device to POS SAM
678
Receive a debit request containing a MAC from POS SAM
680
Send the debit request to e-token enabled device to debit e-token
682
Receive debit confirm message including additional MACs for transaction verification and settlement
684
Forward the debit confirm message to POS SAM for verification
Display transaction after POS SAM has recorded the transaction
686
END

FIG. 6D

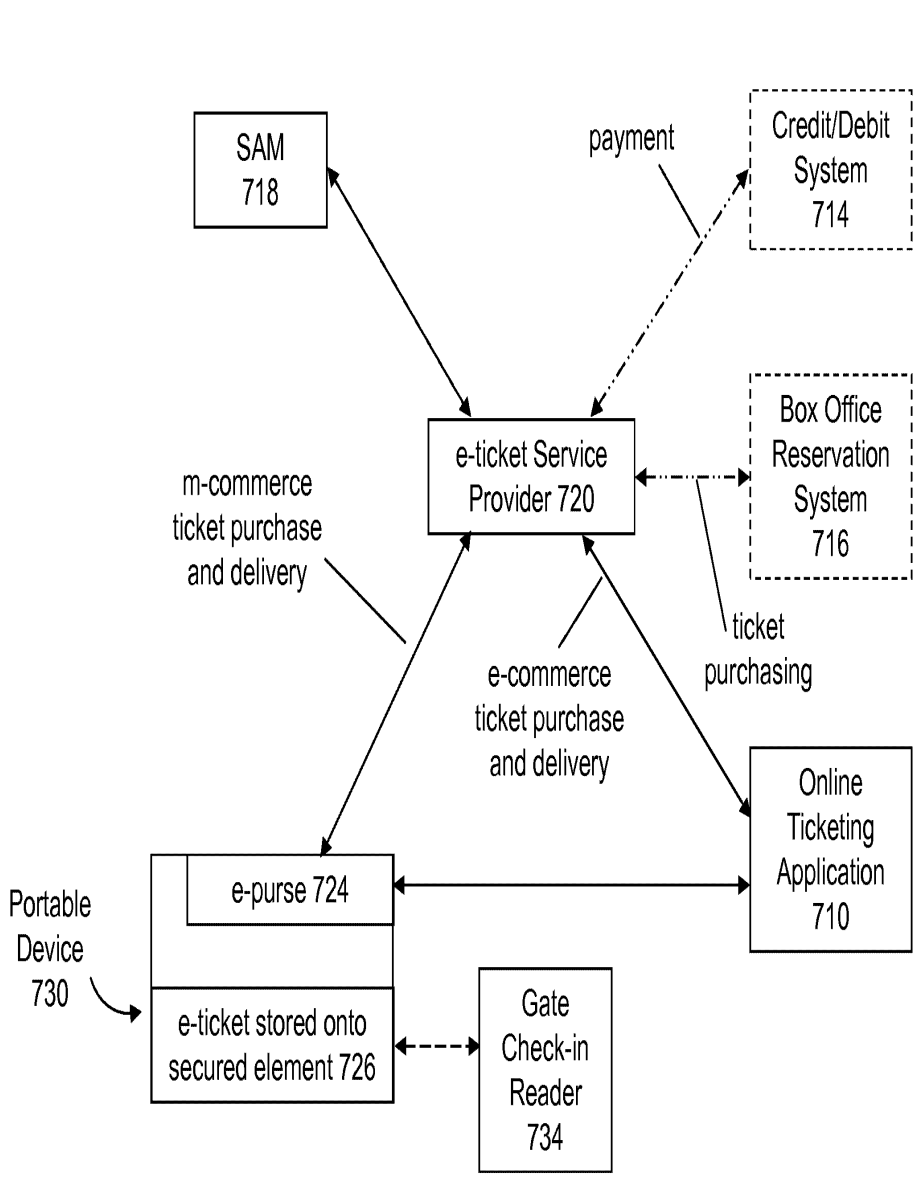

700
SAM
718
payment
Credit/Debit
System
714
e-ticket Service
Provider 720
Box Office
Reservation
System
716
m-commerce
ticket purchase
and delivery
ticket
purchasing
e-commerce
ticket purchase
and delivery
Online
Ticketing
Application
710
e-purse 724
Portable
Device
730
e-ticket stored onto
secured element 726
Gate
Check-in
Reader
734

FIG. 7

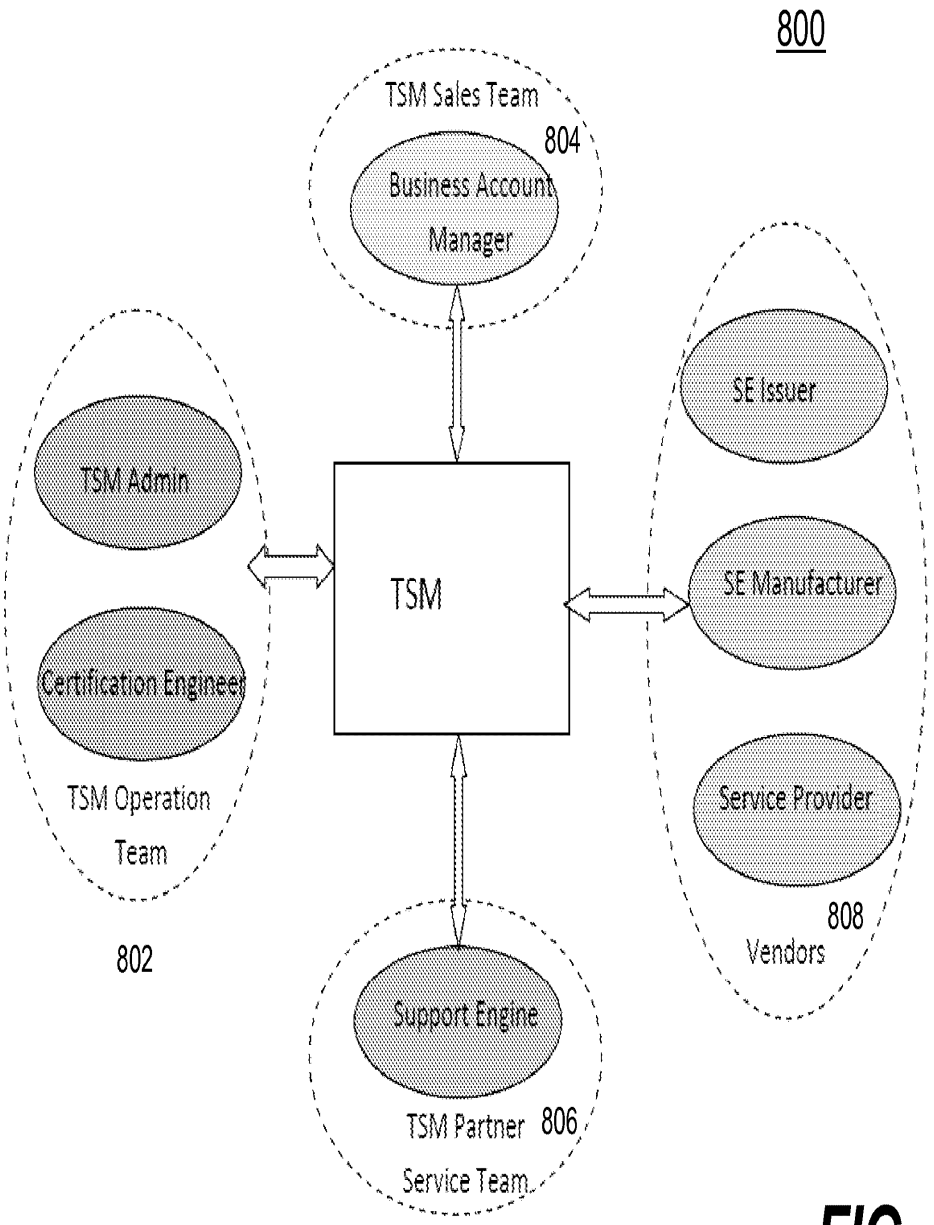

800
TSM Sales Team
804
Business Account Manager
TSM Admin
Certification Engineer
TSM Operation Team
802
TSM
SE Issuer
SE Manufacturer
Service Provider
808
Vendors
Support Engine
TSM Partner Service Team
806

FIG. 8A

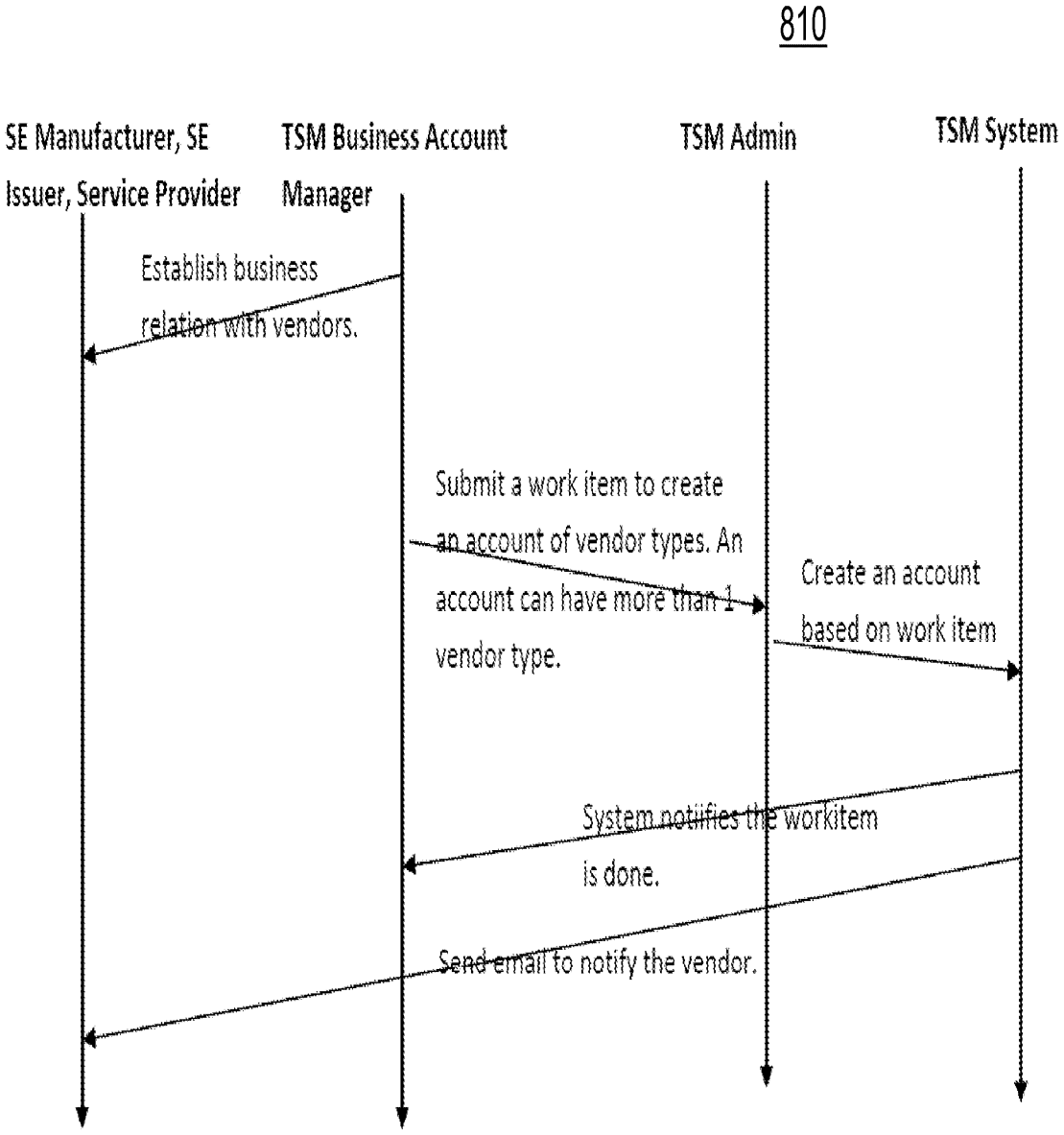

810
SE Manufacturer, SE Issuer, Service Provider
TSM Business Account Manager
TSM Admin
TSM System
Establish business relation with vendors.
Submit a work item to create an account of vendor types. An account can have more than 1 vendor type.
Create an account based on work item
System notifies the workitem is done.
Send email to notify the vendor.

FIG. 8B

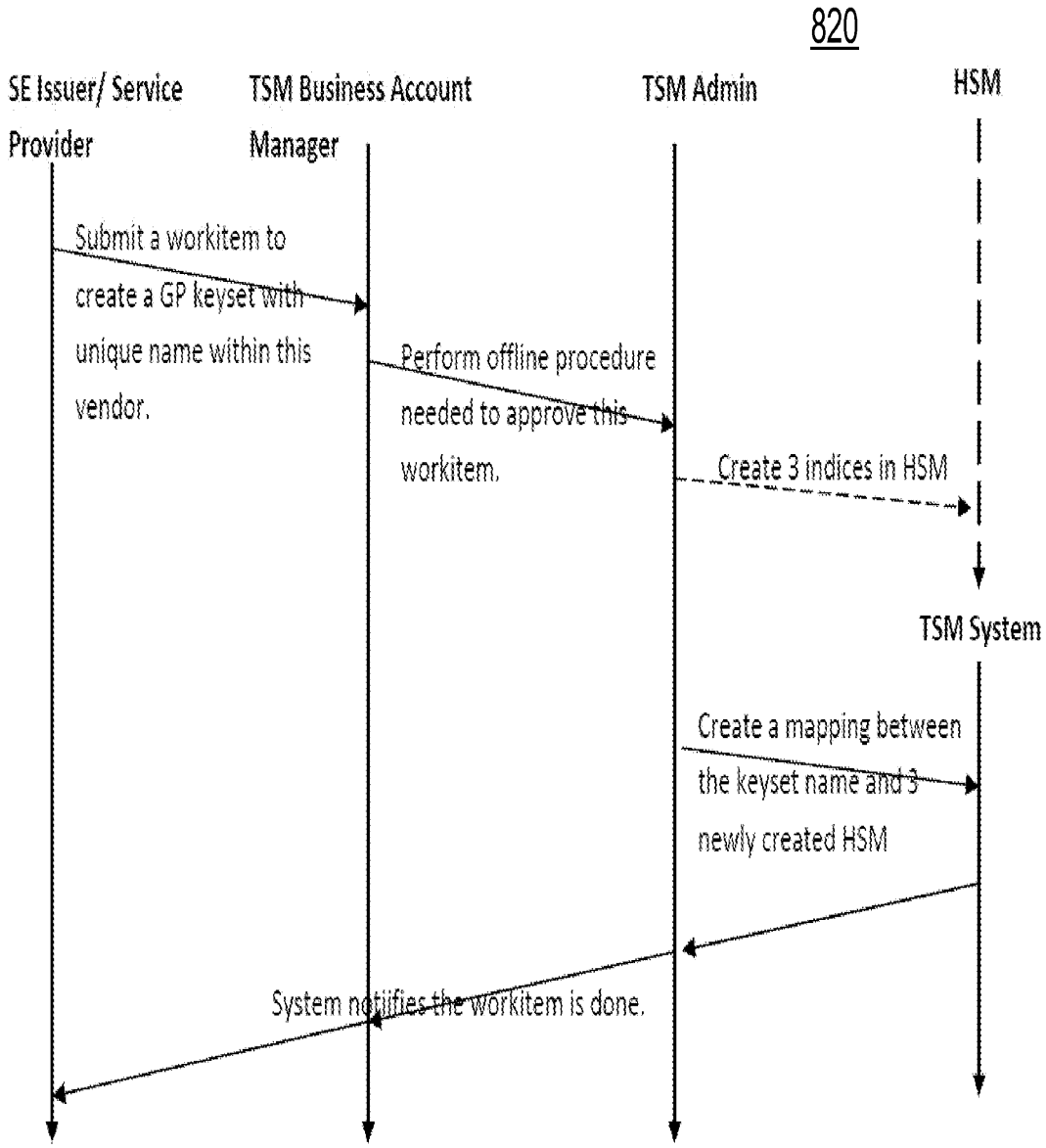

820
SE Issuer/ Service Provider
TSM Business Account Manager
TSM Admin
HSM
Submit a workitem to create a GP keyset with unique name within this vendor.
Perform offline procedure needed to approve this workitem.
Create 3 indices in HSM
TSM System
Create a mapping between the keyset name and 3 newly created HSM
System notifies the workitem is done.

FIG. 8C

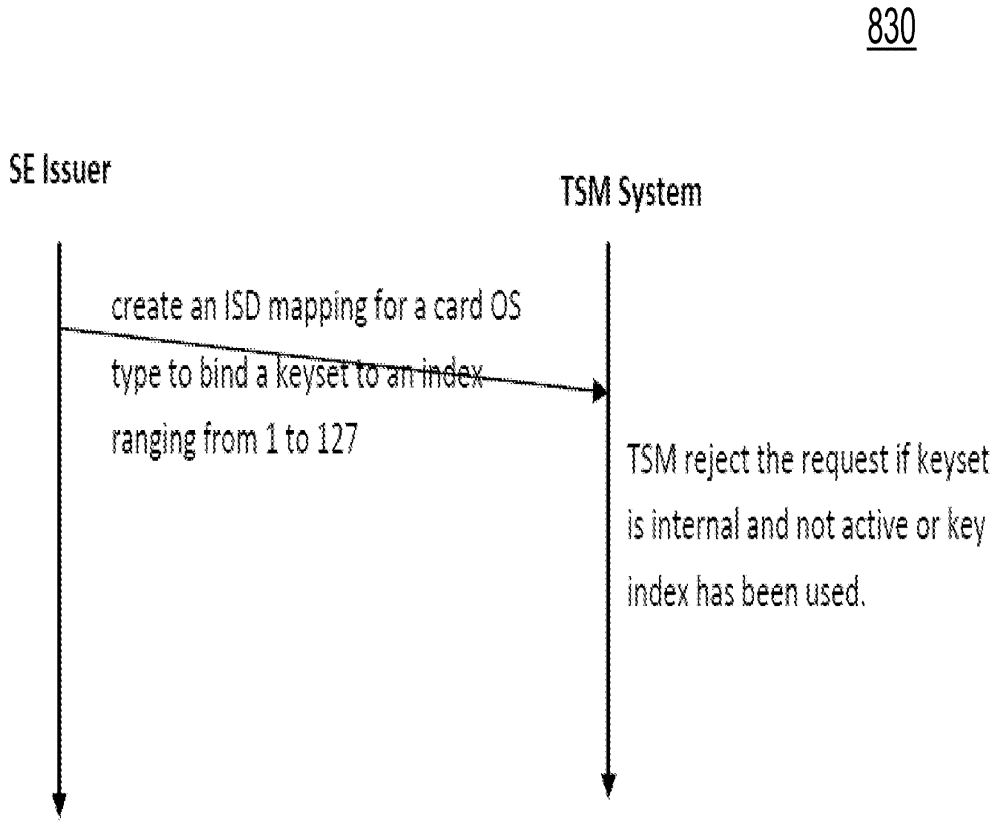

830
SE Issuer
TSM System
create an ISD mapping for a card OS type to bind a keyset to an index ranging from 1 to 127
TSM reject the request if keyset is internal and not active or key index has been used.

FIG. 8D

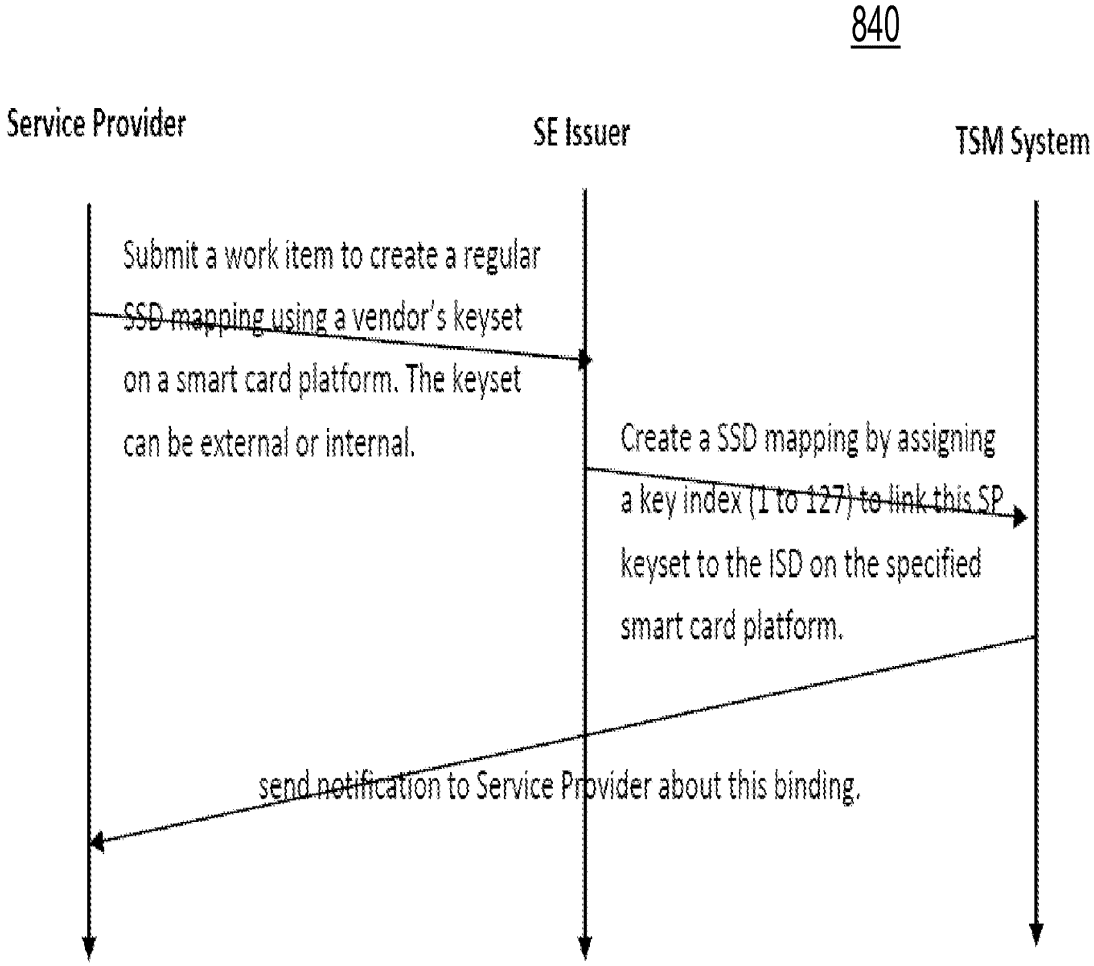

840
Service Provider
SE Issuer
TSM System
Submit a work item to create a regular SSD mapping using a vendor's keyset on a smart card platform. The keyset can be external or internal.
Create a SSD mapping by assigning a key index (1 to 127) to link this SP keyset to the ISD on the specified smart card platform.
send notification to Service Provider about this binding.

FIG. 8E

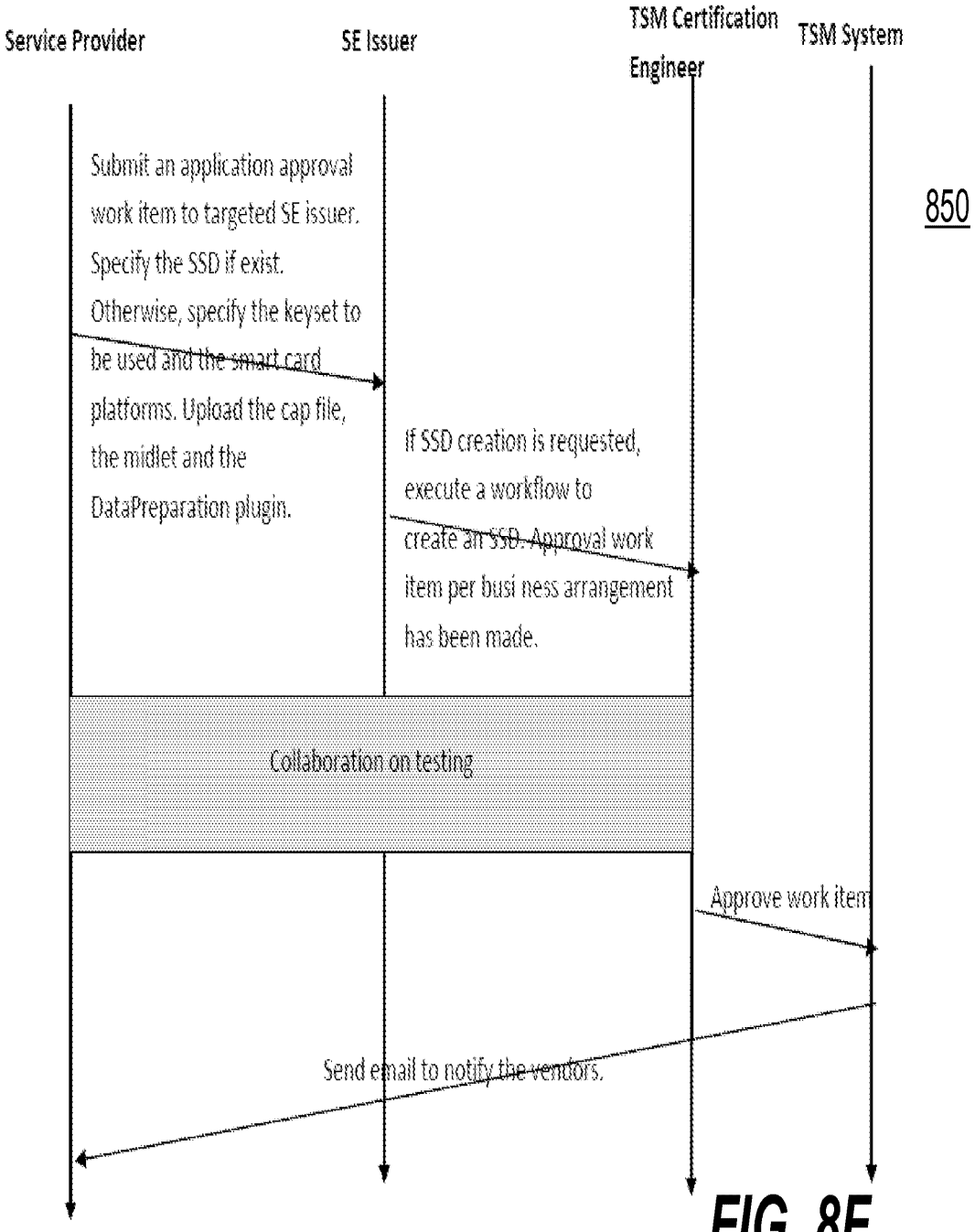

Service Provider
SE Issuer
TSM Certification Engineer
TSM System
Submit an application approval work item to targeted SE issuer. Specify the SSD if exist. Otherwise, specify the keyset to be used and the smart card platforms. Upload the cap file, the midlet and the DataPreparation plugin.
If SSD creation is requested, execute a workflow to create an SSD. Approval work item per business arrangement has been made.
Collaboration on testing
Approve work item
Send email to notify the vendors.
850

FIG. 8F

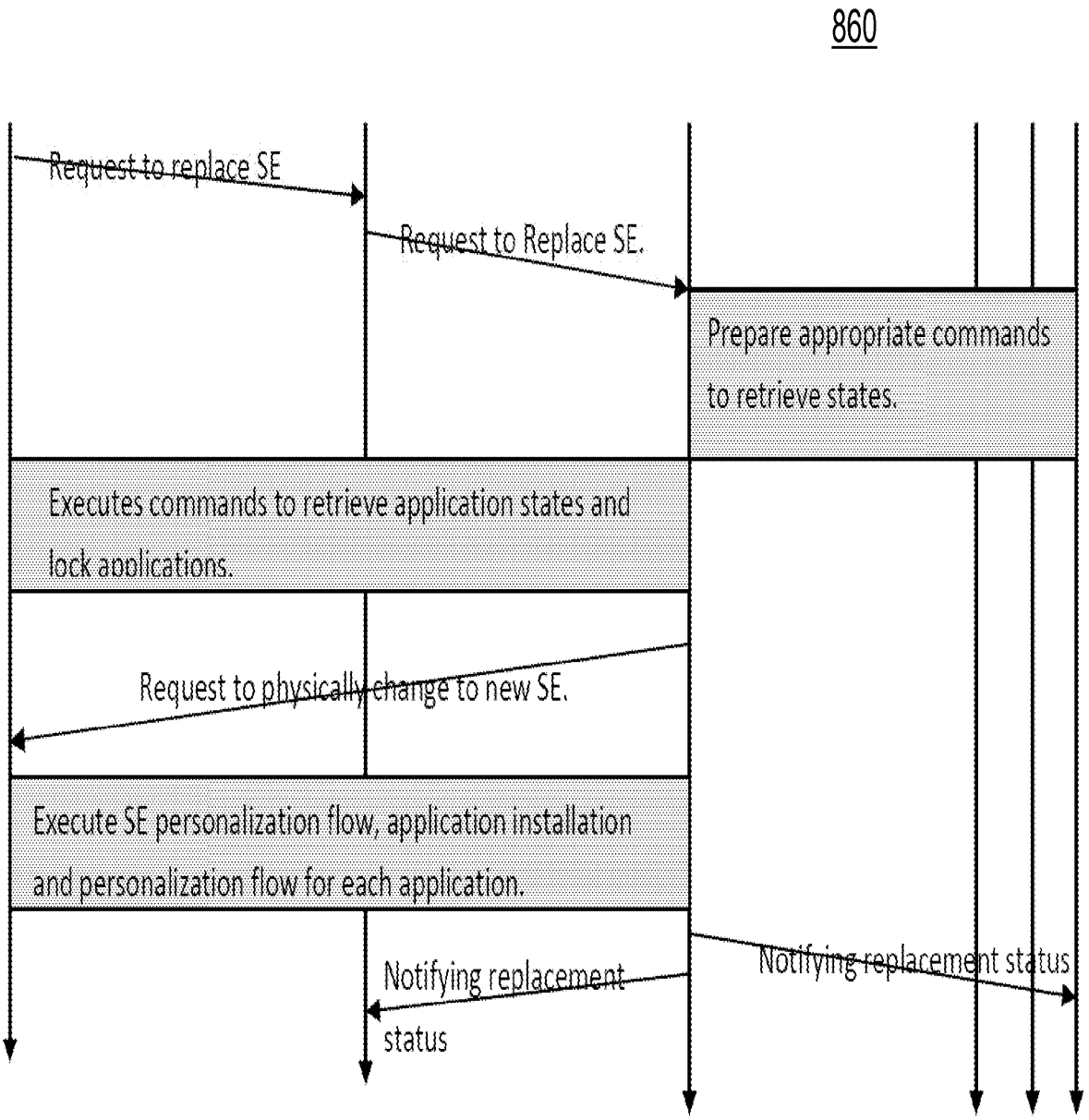
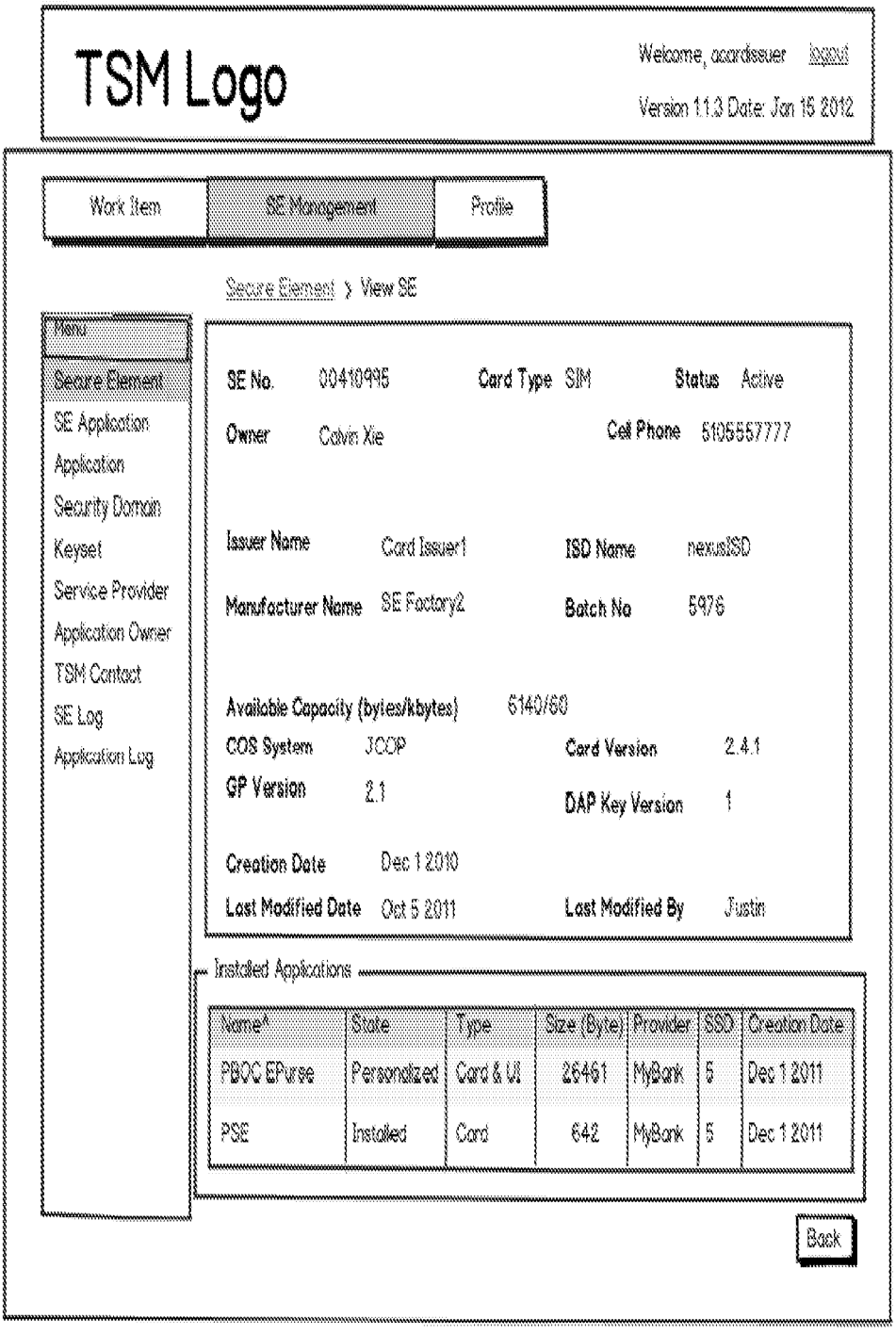

860
Request to replace SE
Request to Replace SE.
Prepare appropriate commands to retrieve states.
Executes commands to retrieve application states and lock applications.
Request to physically change to new SE.
Execute SE personalization flow, application installation and personalization flow for each application.
Notifying replacement status
Notifying replacement status

FIG. 8G


TSM Logo
Welcome, ocardissuer logout
Version 1.1.3 Date: Jan 15 2012
Work Item
SE Management
Profile
Secure Element > View SE
Menu
Secure Element
SE Application
Application
Security Domain
Keyset
Service Provider
Application Owner
TSM Contact
SE Log
Application Log
SE No. 00410995
Card Type SIM
Status Active
Owner Calvin Xie
Cell Phone 5105557777
Issuer Name Card Issuer1
ISD Name nexusISD
Manufacturer Name SE Factory2
Batch No 5976
Available Capacity (bytes/kbytes) 6140/60
COS System JCOP
Card Version 2.4.1
GP Version 2.1
DAP Key Version 1
Creation Date Dec 1 2010
Last Modified Date Oct 5 2011
Last Modified By Justin
Installed Applications
Name* State Type Size (Byte) Provider SSD Creation Date
PBOC EPurse Personalized Card & UI 26461 MyBank 5 Dec 1 2011
PSE Installed Card 642 MyBank 5 Dec 1 2011
Back

900

FIG. 9

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RFID-084
	Application Number	
Title of Invention	Method and apparatus for emulating multiple cards in mobile devices	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	Xiangzhen		Xie	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Shenzhen	Country of Residence	CN

Mailing Address of Inventor:

Address 1	C505, Long Tai Xuan, Nanguang Village		
Address 2	Nanshang District		
City	Shenzhen	**State/Province**	GD
Postal Code	518051	**Country**	CN

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	Liang Seng		Koh	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Fremont	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	41291 Carmen Street		
Address 2			
City	Fremont	**State/Province**	CA
Postal Code	94539	**Country**	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	Hsin		Pan	

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RFID-084
	Application Number	
Title of Invention	Method and apparatus for emulating multiple cards in mobile devices	

Residence Information (Select One)	◉ US Residency	○ Non US Residency	○ Active US Military Service

City	Fremont	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	2374 Olive Avenue		
Address 2			
City	Fremont	State/Province	CA
Postal Code	94539	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	26797		
Email Address	uspatents@sbcglobal.net	Add Email	Remove Email

Application Information:

Title of the Invention	Method and apparatus for emulating multiple cards in mobile devices		
Attorney Docket Number	RFID-084	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	35	Suggested Figure for Publication (if any)	1A

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RFID-084
	Application Number	
Title of Invention	Method and apparatus for emulating multiple cards in mobile devices	

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	26797		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61606451	2012-03-04
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	13350832	2012-01-16
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13350832	Continuation in part of	11534653	2006-09-24
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RFID-084
	Application Number	
Title of Invention	Method and apparatus for emulating multiple cards in mobile devices	

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	RFCyber Corporation

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RFID-084
	Application Number	
Title of Invention	Method and apparatus for emulating multiple cards in mobile devices	

Mailing Address Information:			
Address 1	4160 Technology Drive, Suite A		
Address 2			
City	Fremont	**State/Province**	CA
Country [i]	US	Postal Code	94538
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section only if non-applicant assignee information is desired to be included on the patent application publication in accordance with 37 CFR 1.215(b). Do not include in this section an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest), as the patent application publication will include the name of the applicant(s).

Remove

If the Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RFID-084
	Application Number	
Title of Invention	Method and apparatus for emulating multiple cards in mobile devices	

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/ joe zheng /			Date (YYYY-MM-DD)	2013-03-28
First Name	Joe	Last Name	Zheng	Registration Number	39450
Additional Signature may be generated within this form by selecting the Add button. Add					

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Samsung Ex. 1016, Page 114 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 13782948 Document Date: 03/01/2013

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/782,948

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	19 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/782,948	03/01/2013	2876	533	RFID-084	19	2

CONFIRMATION NO. 5348

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

FILING RECEIPT

OC000000060045907

Date Mailed: 04/03/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Xiangzhen Xie, Shenzhen, CHINA;
Liang Seng Koh, Fremont, CA;
Hsin Pan, Fremont, CA;

Applicant(s)

RFCyber Corporation, Fremont, CA

Assignment For Published Patent Application

RFCYBER CORPORATION, Fremont, CA

Power of Attorney: The patent practitioners associated with Customer Number 26797

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/606,451 03/04/2012
and is a CIP of 13/350,832 01/16/2012
which is a CIP of 11/534,653 09/24/2006 PAT 8118218 *
(*)Data provided by applicant is not consistent with PTO records.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 03/22/2013
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/782,948**
Projected Publication Date: 07/11/2013

Samsung Ex. 1016, Page 117 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Method and apparatus for emulating multiple cards in mobile devices

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

Samsung Ex. 1016, Page 118 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Samsung Ex. 1016, Page 119 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084

CONFIRMATION NO. 5348

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

POA ACCEPTANCE LETTER

OC000000060045927

Date Mailed: 04/03/2013

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/01/2013.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/eruga/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Samsung Ex. 1016, Page 120 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084

CONFIRMATION NO. 5348

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

PUBLICATION NOTICE

OC000000062503601

Title: Method and apparatus for emulating multiple cards in mobile devices

Publication No.US-2013-0178159-A1
Publication Date:07/11/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Samsung Ex. 1016, Page 121 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 02/19/2016

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
ILUONAKHAMHE, ISIDORA	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
02/19/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Office Action Summary	Application No. 13/782,948	Applicant(s) XIE ET AL.	
	Examiner ISIDORA ILUONAKHAMHE	Art Unit 3685	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/01/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-19* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-19* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 03/01/2013.

2. Claims 1-19 are pending.

3. Claims 1-19 have been examined.

Notice of Pre-AIA or AIA Status

4. The present application is being examined under the pre-AIA first to invent provisions.

Specification

5. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

6. Claim 4 is objected to because of the following informalities: “related to monetary,”. Appropriate correction is required.

Examiner’s Comments

7. Regarding claim 1, with respect to claim language “configured to provide…", claims 2 and 13, “device to retrieve…”, “device to receive…”, claim 4, “provided

respectively to perform…", "device is able to be used for all…", claims 7 and 16, "operations that will modify…", claim 8, "server to remotely provision…", "server to manage…", claims 9 and 17, "that is determined to be updates…", claim 11, "a request to provision…", "the application to be provisioned…", claim 12, "device is to be used…", "interface to facilitate…", "device configured to store…", "server configured to provide…", claim 13, "instruction to cause…", claim 15, "Module configured to provide… to store", claim 16, "Card manager proxy configured to facilitate", "user interface application provided to query", "UI application for conducting" and claim 19, "request to provision…", "application to be provisioned…", "(SSD) to be associated…" recites intended use and therefore does not have patentable weight. See MPEP 2114.

8. Regarding claim 1, the language "storage device configured to", "server configured to", recites functional language, and therefore does not have patentable weight. See MPEP 2111, 2114, 2181.

9. Regarding claims 2 and 13, "information is a sequence…", "request is a command…", claims 11 and 19, "the data includes…", claim 13, "information is a sequence…", and claim 15, "secure element further includes…" are nonfunctional descriptive material and therefore do not have patentable weight. See *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai,* 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01. MPEP 2111.05 III.

10. Regarding claim 12, the language "so that the mobile device …" is a result and therefore has not patentable weight (*Minton v. Nat'l Ass'n of Securities Dealers, Inc.,* 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a "'whereby clause

in a method claim is not given weight when it simply expresses the intended result of a process step positively recited.'" See MPEP 2111.04.

11. Regarding claim 12, the language "wherein the mobile device comprises…", claim 14, "wherein the emulator…the secure element is enclosed…", and claim 15, "the secure element further includes…" is a structural limitation in a method claim and has no patentable weight. *Ex parte Pfeiffer*, 135 USPQ 31 (Bd. App. 1961).

12. Regarding claim 12, the language "application being loaded and executed...", "device changes functions offered…", "application has been remotely provisioned…", claim 13, "the server determines….", "keys are generated…", "secure element facilitates...", claim 14, "emulator is implemented…", "secure element is enclosed...", claim 15, "cards is loaded...", claim 16, "proxy configured to facilitate…", "application provided to query…", "information stored…", claim 17, "element is preloaded…" and claim 19, the language "application has been remotely…", "application installed…", "element is distributed…" does not disclose a positively recited step and therefore does not patentable weight. See MPEP 2111.04.

13. Regarding claim 12, "application is replaceable…", "application being loadable…", "the emulator when selectively activated…" is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I) (c).

Claim Rejections - 35 USC § 101

14. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

15. Claims 12-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

16. The claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. The claim(s) does/do not include additional elements that are sufficient to amount to significantly more than the judicial exception because claim(s) 12 is directed to an abstract idea of installing information. Viewed as a whole, these additional claim element(s) "installing…" does not provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself. Therefore, the claim(s) are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Claims 13-19 are also rejected.

Claim Rejections - 35 USC § 112

17. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

18. Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly

claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

19. Claim 1 is a product claim of “the mobile device comprising…”, but the claim adopts circular reasoning in the explanation of not what the device comprises but what it does, "wherein the mobile device changes...." Dependent claims 2-11 are rejected.

20. Claims 1 and 12 recite “wherein each of the applications has been remotely provisioned by a server configured to provide trusted service management (TSM). The scope of the claims are unclear as to whether the server is part of the claimed mobile device or the claimed method for a mobile device. Similarly, claims 2 and 13 recite “after the server determines that the secure element…,” claim 8 recites “enable the TSM server to remotely provision…” and “enable the TSM server to manage…”, and claims 11 and 19 recite "applications has been remotely provisioned by the TSM server with operations of: receiving… establishing... preparing... notifying..." The scope of the claims are unclear as to whether the server or the TSM server are part of the claimed mobile device or the claimed method for a mobile device. Dependent claims 2-11 and 13-19 are rejected.

21. Claims 1 and 12 recite “anyone of the applications being loadable into the emulator when selectively activated and subsequently replacing the application in the emulator”, it is unclear whether the applications are only loadable when activated and subsequently replace a previous application or whether they are loadable and then activated to subsequently replace another application. Dependent claims 2-11 and 13-19 are rejected.

22. As per claims 1, 2, 6, 7, 8 the claims recite the following means plus functions limitations:

a. interface to facilitate…(claim 1)

b. configured to store…(claim 1)

c. instruction to cause… (claim 2)

d. Module configured to provide… to store (claim 6)

e. Card manager proxy configured to facilitate (claim 7)

f. user interface application provided to query (claim 7)

g. UI application for conducting (claim 7)

h. Interfaces…to read (claim 8)

i. TMSM module is configured to (claim 8)

j. Applications… is caused to swap (claim 8)

k. Mechanism to make …for storing (claim 8)

This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites the phrase “means for” or “step for” (or appellant identifies the limitation as a means (or step) plus function limitation in the appeal brief) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. Also see *Altiris Inc. v. Semantec Corp.*, 318 F.3d 1363, 1375 (Fed. Cir. 2003). 35 USC § 112, ¶ 6, requires such claim to be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof. “If one employs means plus function language in a claim, one must set forth in the specification an adequate

disclosure showing what is meant by that language. If an applicant fails to set forth an adequate disclosure, the applicant has in effect failed to particularly point out and distinctly claim the invention as required by the second paragraph of section § 112." *In re Donaldson Co.*, 16 F.3d 1189, 1195, 29 USPQ 1845, 1850 (Fed. Cir. 1994) (in banc.). For a computer-implemented means-plus-function claim limitation that invokes 35 USC § 112, ¶ 6, the corresponding structure is required to be more than simply a general purpose computer. *Aristocrat Technologies, Inc. v. International Game Technology*, 521 F.3d 1328, 1333, 86 USPQ2d 1235, 1239-40 (Fed. Cir. 2008). The corresponding structure for a computer-implemented function must include the algorithm as well as the general purpose computer. *WMS Gaming, Inc. v. International Game Technology*, 184 F.3d 1339, 51 USPQ2d 1385 (Fed. Cir. 1999). The written description must at least disclose the algorithm that transforms the general purpose microprocessor to a special purpose computer programmed to perform the claimed function. *Aristocrat*, 521 F.3d at 1338, 86 USPQ2d at 1242.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56, 57, 60, 61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56, 57, 61, 75, 76 describe the module

interchangeable with software modules, applications and applets but there is no indication of what structure is used. ¶ 61 describes “a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards” but there is no indication of what structure is used. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-11 are rejected.

23. Claims 2, 11, 13 and 19 recite the limitation "the portable device". Similarly, claims 7, 8 and 16 recite the limitation “the TSM server” and "the TMSM module". There is insufficient antecedent basis for this limitation in the claim.

24. Claim 2 recites “a set of keys from a designated place", the claim is unclear as to where this designated place is or why there should ambiguity as to where the keys come from, thereby rendering the claim indefinite. Similarly, claim 8 recites “to read certain data therefrom”, the claim language creates ambiguity, making the claim unclear and rendering the claim indefinite.

25. Regarding claim 8, the claim recites “provide…., when instructed by a user” However, claim 1, from which claim 8 depends, is directed to a mobile device. The claim is a hybrid claim as the cited language is not directed to the mobile device but to external use of claimed structural elements. Therefore, it would be unclear whether infringement of claim 8 occurs based on possession of the mobile device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

26. Claim 13 recites “after the server determines…,” it is unclear how the mobile device receives notice to monitor how the server functions.

Claim Rejections - 35 USC § 102

27. The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

28. Claims 12-19 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Wentker et al. (6,481,632) (“Wentker”).

29. Regarding claims 1 and 12, Wentker teaches installing the applications respectively in the mobile device, each of the applications pertaining to a physical contactless card, so that the mobile device is to be used in lieu of multiple physical contactless cards, wherein the mobile device comprises (column 9, line 1-11, column 14, line 51-65, column 16, 49-67). The remaining limitations are structural limitations in a method claim and have no patentable weight. *Ex parte Pfeiffer*, 135 USPQ 31 (Bd. App. 1961). Dependent claims 13-19 are rejected.

Claim Rejections - 35 USC § 103

30. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker et al. (6,481,632) ("Wentker"), and further in view of Huomo et al. (8,005,426) ("Huomo").

32. Regarding claims 1 and 12, Wentker teaches installing the applications respectively in the mobile device, each of the applications pertaining to a physical contactless card, so that the mobile device is to be used in lieu of multiple physical contactless cards, wherein the mobile device comprises (column 9, line 1-11, column 14, line 51-65, column 16, 49-67): an emulator (claim 1, 4); and a storage device configured to store the multiple applications, anyone of the applications being loadable into the emulator when selectively activated and subsequently replacing the application in the emulator, wherein the mobile device changes functions offered by the application to functions offered by another application newly loaded and executed in the emulator, wherein each of the applications has been remotely provisioned by a server configured to provide trusted service management (TSM) (column 6, line 13-30, 47-67, column 8, line column 9, line 1-8, column 10, line 8-14, column 15, line 1-19, column 16, line 25-35, 49-67, column 17, line 21-35). wherein the application in the emulator being one of the applications is replaceable in entirety or in part by another one of the applications;

Wentker does not teach a near field communication (NFC) interface to facilitate data exchange between a reader and an application being loaded and executed in the

emulator. Huomo a near field communication (NFC) interface to facilitate data exchange between a reader and an application being loaded and executed in the emulator (column 7, line 9-60, column 10, line 49-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wentker and Huomo in order to provide a user with controlling means for using smart cards and contactless cards (Huomo; column 2, line 53-62).

33. Regarding claims 3 and 14, Huomo teaches wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device (column 8, line 3-23).

34. Regarding claim 4, Huomo teaches wherein each of the applications emulating functions of one of contactless cards provided respectively to perform a function related to monetary, the mobile device is able to be used for all of the contactless cards when one of the applications is loaded into and executed in the emulator (column 7, line 8-19, column 9, line 4-21, column 10, line 49-67).

35. Regarding claim 5, Huomo teaches wherein each of the contactless cards is a Mifare contactless card (column 2, line 27-61, column 8, line 3-37).

36. Regarding claims 6 and 15, Wentker teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications (column 9, line 1-33, column 13, line 11-39, column 14, line 24-43, column 21, line 17-31).

37. Regarding claims 7 and 16, Wentker teaches wherein mobile device further includes a card manager proxy configured to facilitate communication between the TSM server and the TMSM module in the secure element, interface application provided to query one or more of the applications on information stored therein but will not modify the information (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and a transaction UI application for conducting operations that will modify one or more sectors in one or more of the applications (column 10, line 8-56). Wentker does not teach a readonly user interface (UI). Huomo teaches a readonly user interface (UI) (column 6, line 61-67, column 8, line 54-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wentker and Huomo in order to provide a user with controlling means for using smart cards and contactless cards (Huomo; column 2, line 53-62).

38. Regarding claims 9 and 17, Wentker teaches wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element (column 7, line 38-56, column 13, line 11-39, column 19, line 1-8).

39. Regarding claims 10 and 18, Huomo teaches wherein the mobile device is a smartphone, a portable computer and a smart card (column 16, line 26-36, 43-67, column 17, line 1-5).

40. Regarding claims 11 and 19, Wentker teaches receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned

with the secure element is distributed by an application provider (column 7, line 15-37, column 8, line 1-10, column 14, line 24-43, column 15, line 1-19, column 16, line 25-35, 49-67, column 17, line 21-35); establishing a secured channel with the secure element using a set of keys (column 7, line 15-37, column 10, line 15-23, column 13, line 11-39, column 15, line 52-67, preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67); and notifying the application provider of a status of the application with the portable device (column 12, line 58-67, column 13, line 1-10, column 17, line 4-20, column 18, line 62-67, column 19, line 44-46).

41. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker et al. (6,481,632) ("Wentker"), in view of Huomo et al. (8,005,426) ("Huomo") and further in view of De Groot (2006/0141987) ("Groot").

42. Regarding claims 2 and 13, Groot teaches initiating data communication between the mobile device and the server (¶ 36, 40, 44); receiving device information of the secure element from the mobile device in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (¶ 30, 34, 36, 37, 39, 40, 43, 47, 48, 53); and sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated

in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider (Figure 1, element M1-3; ¶ 30, 31, 34, 40-45, 47-49, 53). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wentker, Huomo and Groot in order to provide secure transmissions with a terminal and a server using an identifier (Groot; ¶ 1-7).

43. Claim 8 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker et al. (6,481,632) ("Wentker"), in view of Huomo et al. (8,005,426) ("Huomo") and further in view of Vayssiere (2006/0065741) ("Vayssiere").

44. Regarding claim 8, Wentker teaches provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator (column 6, line 36-55, column 7, line 1-7, column 8, line 17-32); provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom (column 6, line 36-55, column 8, line 17-32); enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module (column 7, line 15-37, column 16, line 3-23, column 17, line 21-35, column 22, line 17-31) enable the TSM server to manage each of the applications by locking or unlocking one of the applications (column 7, line 1-7, column 9, line 34-44, column 10, line 24-44); provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and provide a mechanism to make baseband storage as an extension for storing some or all of the applications

swapped out from the emulator to the TMSM module (column 22, line 51-67, column 23, line 1-24).

Neither Wentker and Huomo and later on swapping another one of the applications to the emulator. Vayssiere and later on swapping another one of the applications to the emulator (¶ 35). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wentker, Huomo and Vayssiere in order to provide a smartcard to perform multiple functions (Vayssiere; ¶ 3).

Conclusion

45. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA ILUONAKHAMHE whose telephone number is (571)272-9862. The examiner can normally be reached on Monday-Thursday 7:30am-5pm EDT.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. I./
Examiner, Art Unit 3685

/CALVIN L HEWITT II/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination XIE ET AL.	
	Examiner ISIDORA ILUONAKHAMHE	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6,481,632 B2	11-2002	Wentker; David C.	G06F8/60	235/376
*	B	US-2006/0065741 A1	03-2006	Vayssiere; Julien JP.	G06K19/07703	235/492
*	C	US-2006/0141987 A1	06-2006	De Groot; Max	H04L63/0414	455/411
*	D	US-8,005,426 B2	08-2011	Huomo; Heikki	G06Q20/20	235/441
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 5348

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/782,948	03/01/2013	705	3685	RFID-084

APPLICANTS

RFCYBER CORPORATION, Fremont, CA

INVENTORS

Xiangzhen Xie, Shenzhen, CHINA;
Liang Seng Koh, Fremont, CA;
Hsin Pan, Fremont, CA;

**** CONTINUING DATA **************************

This appln claims benefit of 61/606,451 03/04/2012
and is a CIP of 13/350,832 01/16/2012
which is a CIP of 11/534,653 09/24/2006 PAT 8118218 *
(*)Data provided by applicant is not consistent with PTO records.

**** FOREIGN APPLICATIONS **************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
03/22/2013

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged / / Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CHINA	35	19	2

ADDRESS

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015
UNITED STATES

TITLE

Method and apparatus for emulating multiple cards in mobile devices

FILING FEE RECEIVED		
533	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13782948	XIE ET AL.
	Examiner	**Art Unit**
	ISIDORA ILUONAKHAMHE	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								

Samsung Ex. 1016, Page 142 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	(("6481632") or ("20060065741")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	OFF	2016/02/01 17:42
S1	26	(trusted adj service adj management)	US-PGPUB; USPAT	OR	ON	2014/05/28 14:29
S2	548	(Bank or issuer or (financial adj institution) or institution or entit$3 or bank or compan$3 or credit adj union or banc or business$4 or brokerage or financial adj service or savings adj2 loan or clearing adj house or clearinghouse) near4 (wire or wiring or issue or issuing or forwardwire or route or routing or transfer or relay$3 or send$3 or sent or transmi$3 or dispatch$3) near4 ((pass adj word) or (pass$1word) or key or keys or signature or rsa or token or code or coding or certificate or pki or pks or id or ids or pin or pins or number or digit) near4 ((E adj wallet) or e-wallet or (electronic adj wallet) or chargecard or creditcard or debitcard or bankcard or checkcard or cashcard or debit or (stored adj2 value) or (open adj loop) or purse or smart or ic or (integrated adj circuit) or chip)	US-PGPUB; USPAT	OR	ON	2014/05/28 16:11
S3	1539	((E adj wallet) or e-wallet or (electronic adj wallet) or chargecard or creditcard or debitcard or bankcard or checkcard or cashcard or debit or (stored adj2 value) or (open adj loop) or purse or smart or ic or (integrated adj circuit) or chip) with (nfc near4 device)	US-PGPUB; USPAT	OR	ON	2014/05/28 16:12
S4	0	S2 same S3	US-PGPUB; USPAT	OR	ON	2014/05/28 16:13
S5	3	S2 and S3	US-PGPUB; USPAT	OR	ON	2014/05/28 16:13
S6	31	(Bank or issuer or (financial adj institution) or institution or entit$3 or bank or compan$3 or credit adj union or banc or business$4 or brokerage or financial adj service or savings adj2 loan or clearing adj house or clearinghouse) near4 (wire or wiring or issue or issuing	US-PGPUB; USPAT	OR	ON	2014/05/28 16:13

		or forwardwire or route or routing or transfer or relay$3 or send$3 or sent or transmi$3 or dispatch$3) near4 ((pass adj word) or (pass$1word) or key or keys or signature or rsa or token or code or coding or certificate or pki or pks or id or ids or pin or pins or number or digit) near4 (smart adj card)				
S7	2	S6 and nfc	US-PGPUB; USPAT	OR	ON	2014/05/28 16:14
S8	7	S3 and @pd<="20060924"	US-PGPUB; USPAT	OR	ON	2014/05/28 16:15
S9	1	("6327578").PN.	US-PGPUB; USPAT	OR	OFF	2014/05/29 07:22
S11	4758	(Bank or issuer or (financial adj institution) or institution or entit$3 or bank or compan$3 or credit adj union or banc or business$4 or brokerage or financial adj service or savings adj2 loan or clearing adj house or clearinghouse) near4 ((pass adj word) or (pass$1word) or key or keys or signature or rsa or token or code or coding or certificate or pki or pks or id or ids or pin or pins or number or digit) near4 ((E adj wallet) or e-wallet or (electronic adj wallet) or chargecard or creditcard or debitcard or bankcard or checkcard or cashcard or debit or (stored adj2 value) or (open adj loop) or purse or smart or ic or (integrated adj circuit) or chip or (secure adj element))	US-PGPUB; USPAT	OR	ON	2014/05/29 10:02
S17	891	(nfc or (field adj communication)) near4 ((pass adj word) or (pass$1word) or key or keys or signature or rsa or token or code or coding or certificate or pki or pks or id or ids or pin or pins or number or digit) near4 (pda or (personal adj digital adj assistant) or smartphone or cell adj phone or cellphone or pager or handset or laptop or device or (mobile adj device))	US-PGPUB; USPAT	OR	ON	2014/05/29 10:06
S48	106413	personal$4 with ((E adj wallet) or e-wallet or (electronic adj wallet) or chargecard or creditcard or debitcard or bankcard or checkcard or cashcard or debit or (stored adj2 value) or (open adj loop) or purse or smart or ic or (integrated adj circuit) or chip or (secure adj element))	US-PGPUB; USPAT	OR	ON	2014/05/29 14:30
S51	1801	((smart adj card) or ic or (integrated adj circuit) or smart) with ((mobile adj device) or device or phone) with nfc	US-PGPUB; USPAT	OR	ON	2014/05/29 14:52

2/1/2016 5:43:48 PM
C:\Users\iiluonakhamhe\Documents\EAST\Workspaces\13350832.wsp

Samsung Ex. 1016, Page 145 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13782948	XIE ET AL.
	Examiner	Art Unit
	ISIDORA ILUONAKHAMHE	3685

CPC- SEARCHED		
Symbol	Date	Examiner
G06Q	2/1/2016	II

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705			

SEARCH NOTES		
Search Notes	Date	Examiner
See attached notes	2/1/2016	II

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/I.I./ Examiner.Art Unit 3685	

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

Courtesy Reminder for
Application Serial No: 13/782,948

Attorney Docket No: RFID-084
Customer Number: 26797
Date of Electronic Notification: 02/19/2016

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
uspatents@sbcglobal.net

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

June 17, 2016

Mail Stop: No-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to First OA

Dear Sir:

In response to Office Action dated 02/19/2016, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begins on page 2 of this Response.

REMARKS/ARGUMENTS begin on page 9 of this Response.

Samsung Ex. 1016, Page 148 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

June 17, 2016

Mail Stop: No-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to First OA

Dear Sir:

In response to Office Action dated 02/19/2016, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begins on page 2 of this Response.

REMARKS/ARGUMENTS begin on page 9 of this Response.

Samsung Ex. 1016, Page 149 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

Please amend Claims 1-2, 4-7, 9, 12-13 and 15-16 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards ~~supporting multiple applications~~, the mobile device comprising:

   a storage device for storing a plurality of applications, each corresponding to one of the cards;

   an emulator, coupled to the storage, for receiving one of the applications, wherein each of the applications corresponds to one of the cards;

   a ~~near field~~ communication ~~(NFC)~~ interface to facilitate data exchange between a reader and ~~an~~ the one of the applications being ~~loaded and~~ executed in the emulator, wherein the one of the applications in the emulator ~~being one of the applications~~ is replaceable in entirety or in part by another one of the applications; and

   a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications, wherein

   ~~a storage device configured to store the multiple applications, anyone of the applications being loadable into the emulator when selectively activated and subsequently replacing the application in the emulator, wherein the mobile device changes~~ functions of the mobile device related to one of the cards offered by the application are changed to functions offered by the another one of the applications related to another one of the cards when the another one of the applications is activated and ~~newly loaded and~~ executed in the emulator, ~~wherein each of the applications has been remotely provisioned by a server configured to provide trusted service management (TSM).~~

2. (*Currently amended*) The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:

Samsung Ex. 1016, Page 150 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

initiating data communication between the mobile device and ~~the~~ a designated server providing trusted service management (TSM);

receiving device information of the secure element ~~from the mobile device~~ in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Currently amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of ~~contactless~~ the cards provided respectively to perform a function related to a monetary transaction, the mobile device is ~~able to be~~ used ~~for~~ to emulate each all of the ~~contactless~~ cards when one of the applications is loaded into and executed in the emulator.

5. (*Currently amended*) The mobile device as recited in claim 4, wherein ~~each~~ at least one of the ~~contactless~~ cards is a Mifare contactless card.

6. (*Currently amended*) The mobile device as recited in claim ~~5~~3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along

Samsung Ex. 1016, Page 151 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Currently amended*) The mobile device as recited in claim 6, wherein each of the applications has been remotely provisioned by the server configured to provide trusted service management (TSM), and the mobile device further includes:

a card manager proxy ~~configured to~~for facilitating communication between the TSM server and the TMSM module in the secure element,

a ~~readonly~~ user interface (UI) application provided to query one or more of the applications on information stored therein but ~~will~~ not to modify the information;, and

a transaction UI application for conducting operations that ~~will~~ modify one or more sectors in one or more of the applications.

8. (*Original*) The mobile device as recited in claim 6, wherein the TMSM module is configured to:

provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module and later on swapping another one of the applications to the emulator;

enable the TSM server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

Samsung Ex. 1016, Page 152 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Currently amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information ~~that is~~ determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Original*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone, a portable computer and a smart card.

11. (*Original*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards~~support multiple applications~~, the method comprising:

installing ~~the~~ a plurality of applications ~~respectively~~ in a storage device of the mobile device, each of the applications pertaining to ~~a physical contactless~~one of the cards, ~~so that~~ wherein the mobile device is ~~to be~~ used

Samsung Ex. 1016, Page 153 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

in lieu of ~~multiple physical contactless~~ the cards; ~~wherein the mobile device comprises:~~

providing an emulator in the mobile device to receive a first application;

~~a near field communication (NFC) interface to~~ facilitating data exchange between a reader and ~~an~~ the first application being ~~loaded and~~ executed in the emulator, wherein the first application in the emulator ~~being one of the applications~~ is replaceable in entirety or in part by ~~another one of the~~ a second application~~s~~; ~~and~~

causing the second application to replace the first application being loaded and executed in the emulator, wherein ~~a storage device configured to store the multiple applications, anyone of the applications being loadable into the emulator when selectively activated and subsequently replacing the application in the emulator, wherein~~ functions of the mobile device related to one of the cards offered by the first application are changed to ~~the mobile device changes~~ functions offered by the application to functions offered by ~~another~~the second application related to another one of the cards when the second application is activated ~~newly loaded~~ and executed in the emulator~~, wherein each of the applications has been remotely provisioned by a server configured to provide trusted service management (TSM)~~.

13. (*Currently amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication between the mobile device and ~~the~~ a designated server providing trusted service management (TSM);

receiving device information of the secure element ~~from the mobile device~~ in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

Samsung Ex. 1016, Page 154 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Currently amended*) The method as recited in claim 14, wherein ~~each of the physical contactless cards is loaded with a Mifare emulator,~~ the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Currently amended*) The mobile device as recited in claim 15, ~~wherein mobile device~~ further comprising~~includes~~
~~a card manager proxy configured to~~ facilitating communication between the TSM server and the TMSM module in the secure element;
~~a readonly user interface (UI) application provided to~~ querying via a user interface (UI) one or more of the applications in detail; ~~on information stored therein but will not modify the information,~~ and
~~a transaction UI application for~~ conducting operations that ~~will~~ modify one or more sectors in one or more of the applications.

17. (*Original*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

Samsung Ex. 1016, Page 155 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

18. (*Original*) The method as recited in claim 12, wherein the mobile device is a smartphone, a portable computer and a smart card.

19. (*Original*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

Samsung Ex. 1016, Page 156 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

REMARKS

Claims 1 - 19 were submitted for examination. In the Office Action dated 02/19/2016, Claims 12-19 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Wentker et al. (US Pat. No.: 6,481,632, "Wentker"), and Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker, and further in view of Huomo et al. (US Pat. No.: 8,005,426, "Huomo"), Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Huomo and further in view of De Groot (US Pub. No.: 2006/0141987, "Groot"), and Claim 8 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Huomo and further in view of Vayssiere (US Pub. No.: 2006/00657 41, "Vayssiere").

The Applicants appreciate the Examiner for providing detailed comments in the Office Action. In the foregoing amendments, Claims 1-2, 4-7, 9, 12-13 and 15-16 have been amended to further distinguish from the cited references. No new matters have been introduced. Reconsideration of pending claims is respectfully requested.

Re: Examiner's Comments

On page 2, Section 7, the Examiner alleges that the phrases "configured to provide ... ", "device to retrieve ... ", "device to receive ... ", etc. recites intended use and therefore are not given patentable weight. Applicant respectfully submits that this interpretation is improper.

It is well established that a claim term is to be accorded “the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention” (see *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005)). *Phillips* also indicated that evidence for the meaning of a term may be derived from “the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art” (see *Id.* at 1314).

Samsung Ex. 1016, Page 157 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

The Applicant respectfully submits that the present specification supports an interpretation where one of the identified phrases denotes an actual state of configuration that fundamentally ties the phrase to the physical characteristics of the feature preceding the phrase. For example, the phrase "device to retrieve" is not adequate to judge whether it shall be given patentable weight or not. Per MPEP 2181, the examiner must carefully consider the term in light of the specification and the commonly accepted meaning in the technological art. Every application will turn on its own facts. The context of the phrase "the request is a command causing the *mobile device to retrieve the device information* from the secure element therein" recited in Claim 2 is a special instruction to which the mobile device is designed to react. In other words, the mobile device does not react to anything else to retrieve the device information or the mobile device is not a regular mobile device that would retrieve the device information upon any command.

As a result, the claim language reaches well beyond merely describing an intended use since the claims actively recite an actual state of configuration. The Office Action presents no evidence or reasoning why one of ordinary skill in the art would interpret the phrase as merely denoting an intended use. Similarly, the Applicant found no evidence or reasoning supporting this position in the claims, specification, prosecution history and extrinsic evidence. Accordingly, the Applicant respectfully asserts, that "no patentable weight" given by the Examiner is improper. Nevertheless, the Applicant has tried to amend the claims to minimize the use of the similar structure that may be misunderstood.

On page 3, Section 8, the Examiner alleges that the language "storage device configured to", "server configured to", recites functional language, and therefore does not have patentable weight. Applicant respectfully submits that this interpretation is improper.

The present specification supports an interpretation where one of these identified phrases denotes an actual function performed by an actual element (e.g., a storage device or a server) in an apparatus claim. For example, "storage device configured to" (now amended to "storage for storing") is an actual device uniquely

Samsung Ex. 1016, Page 158 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

designed for what it does. Any device that can keep a signal may be called storage, but not any storage can be used to store an application that works with an emulator. To facilitate the understanding, it is a lot clear to recite a name for what it is.

The Office Action presents no evidence or reasoning why one of ordinary skill in the art would interpret the language as merely denoting a function. Similarly, the Applicant found no evidence or reasoning supporting this position in the claims, specification, prosecution history and extrinsic evidence. Accordingly, the Applicant respectfully asserts, that "no patentable weight" given by the Examiner is improper. Nevertheless, the Applicant has tried to amend the claims to minimize the use of the similar structure that may be misunderstood.

On page 3, Section 9, the Examiner alleges that the phrases, "information is a sequence ... ", "request is a command ... " in claims 2 and 13, "the data includes ... " claims 11 and 19, "information is a sequence ... " in claim 13, and "secure element further includes ... " in claim 15 are nonfunctional and therefore do not have patentable weight. Applicant respectfully submits that this interpretation is improper.

The Examiner seems to be inconsistent in the claim interpretation. In Section 8, the Examiner alleges that a further description of an element is a functional language, therefore no patentable weight. In this section, each of these phrases precisely further describes what an element in the apparatus claim does, but the Examiner alleges that a further description of the element is nonfunctional and therefore do not have patentable weight.

As properly described in the Specification, a term, such as "device information", "a request", "secure element", followed by a description is to specify what the term is, what unique features it has from other similarly named item, and/or what configuration or physical relationship it has with other components. It should be given proper patentable weight in examining the corresponding claim.

Many issues mentioned respectively in Sections 10-13 by the Examiner are related to the issues similar to those stated in Sections 7-9. Without repeating the same, the Applicant wishes to apply the above reasons or through foregoing amendments to argue against these issues. In any case, the Applicant welcomes

Samsung Ex. 1016, Page 159 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Examiner to provide any suggestions that may advance the prosecution of this instant application.

Claim Rejections - 35 USC§ 101

On Page 5, Section 15, of this Office Action, Claims 12-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter under 35 U.S.C. 101. The Examiner alleges that the claim(s) does/do not include additional elements that are sufficient to amount to significantly more than the judicial exception because claim(s) 12 is directed to an abstract idea of installing information.

The Applicant respectfully disagrees with the Examiner on the ground of rejection on Claims 12-19 under 35 USC 101 and submits the invention as claimed does not involve an abstract idea and the claims amount to significantly more than the abstract idea itself for the following reasons.

In the Office Rejection, Claims 12-19 were rejected under 35 U.S.C. §101 as being directed to an abstract idea. The Applicant respectfully reminds the Examiner that the Examiner "*bears the initial burden ... of presenting a prima facie case of unpatentability.*" *In re Oetiker,* 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992) and MPEP 2106(III). A proper *prima facie* case of unpatentability requires that the Examiner provide "*clear rationale supporting the determination that an abstract idea has been claimed.*" MPEP 2106(II)(B)(2). In other words, in making a rejection under § 101, the Examiner "*should specifically point out the factors that are relied upon in making the determination.*" *Id.* By specifically identifying the factors used in the analysis, it will allow "*the Applicant to make specific arguments in response to the rejection if the Applicant believes that the conclusion that the claim is directed to an abstract idea is in error.*" *Id.*

With regard to the present application, the Applicant respectfully submits that the rejection of the claims under 35 USC 101 is defective in view of the USPTO's MEMORANDUM dated May 19, 2016, for the reason that the Office Action: 1) fails to compare the claim to claims already found to be directed to an abstract idea in a previous court decision when determining whether a claim is directed to an abstract

Samsung Ex. 1016, Page 160 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

idea, 2) fails to apply a filter to the claims, when interpreted in view of the specification, based on whether their character as a whole is directed to a patent ineligible concept, 3) interprets or describes a claim at a high level of abstraction untethered from the language of the claim when determining the focus of the claimed invention, and 4) fail to realize the fact that an invention's ability to run on a general purpose computer does not automatically doom the claim.

Accordingly, the Applicant respectfully requests the Examiner to withdraw the rejection of Claims 12-19 under 35 USC 101 in view of the amendments thereto.

Claim Rejections - 35 USC § 112

On Page 5, Section 18, of this Office Action, Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

In the foregoing amendments, Claims 1-2, 4-7, 9, 12-13 and 15-16 have been amended. It is believed that most of the claim rejection under 35 U.S.C. 112 shall have been overcome.

On Page 7, Section 22, of this Office Action, the Examiner alleges claims 1, 2, 6, 7, 8 recite means plus functions thus invokes 35 USC§ 112, Paragraph 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites the phrase "means for" or "step for" (or appellant identifies the limitation as a means (or step) plus function limitation in the appeal brief) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. Applicants respectfully traverse the rejection as follows.

Before an Examiner can assert that each of the phrases listed on Page 7 of the Office Action (i.e., terms a - k) is a single means, the Examiner must determine whether the claim limitation invokes the sixth paragraph of 35 U.S.C. § 112. MPEP § 2181(I) states that a claim feature will be presumed to invoke the sixth paragraph of 35 U.S.C. § 112 if the feature meets the following 3-prong analysis:

Samsung Ex. 1016, Page 161 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

(A) the claim limitations must use the phrase "means for" or "step for";

(B) the "means for" or "step for" must be modified by functional language; and

(C) the phrase "means for" or "step for" must not be modified by sufficient structure, material, or acts for achieving the specified function.

In the instant application, none of Claims 1, 2, 6, 7, 8 includes the recitation “means for” or “step for” and, therefore, cannot be considered to invoke the sixth paragraph of 35 U.S.C. § 112. In addition, the claim features are not written as a function to be performed, but instead recited as sufficient structure to preclude application of the sixth paragraph of 35 U.S.C. § 112. Because neither of the terms can be interpreted to invoke the sixth paragraph of 35 U.S.C. § 112, the Applicant respectfully submits that each of Claims 1, 2, 6, 7, 8 does not recite a single means, as alleged by the Office Action. Accordingly, withdrawal of the rejection is respectfully requested.

Claim Rejections - 35 USC § 102

On Page 10, Section 28, of this Office Action, Claims 12-19 are rejected under pre-AIA 35 U.S.C. 102(a) as being anticipated by Wentker. The Applicant respectfully traverses the rejections of Claims 12-19 under 35 USC 102. A cited prior art reference anticipates a claimed invention under 35 USC 102 only if every element of the claimed invention is identically shown in the single reference, arranged as they are in the claim. MPEP 2131; in re Bond, 910 F.2d 831, 832, 15 USPQ2d 1566, 1567 (Fed. Cir. 1990). Each and every limitation of the claimed invention is significant and must be found in the single cited prior reference. In re Donohue, 766 F2.d 531, 534, 266 USPQ 619, 621 (Feb. Cir. 1985). As set forth more fully below, Wentker neither discloses nor suggests each and every element of the claimed invention.

As amended, Claim 12 now recites:

A method for a mobile device to <u>emulate a plurality of cards</u>, the method comprising:

Samsung Ex. 1016, Page 162 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

installing a plurality of applications in a storage device of the mobile device, each of the applications pertaining to one of the cards, wherein the mobile device is used in lieu of the cards;

providing an emulator in the mobile device to receive a first application;

facilitating data exchange between a reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application;

causing the second application to replace the first application being loaded and executed in the emulator, wherein functions of the mobile device related to one of the cards offered by the first application are changed to functions offered by the application to functions offered by the second application related to another one of the cards when the second application is activated and executed in the emulator.

(*emphasis added*)

One of the purposes in the instant application is to emulate multiple cards in a mobile device, where a card is fundamentally a memory storage device. In reality, different companies may issue different cards, using a mobile device to emulate any one of these cards would make life simple, otherwise one would have to carry many cards. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality applications, each pertaining to one of cards. When a card is needed, a user can cause the mobile application (via an interface) to load in a corresponding application into an emulator that turns the mobile device to function as the card.

In contrast, Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. Wentker neither teaches nor suggests a mobile device to emulate a plurality of cards. To emulate a number of different cards, an emulator is needed. Wentker is completely silent about an emulator. In a perspective, Wentker teaches away from Claim 12 by managing only one card via the provided APIs. Accordingly, the Applicant submits Claim 12 as amended shall be allowable over Wentker. Reconsideration of Claims 12-19 is kindly requested.

Samsung Ex. 1016, Page 163 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Claim Rejections - 35 USC § 103

On Page 11, Section 31, of this Office Action, Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker Wentker and further in view of Huomo.

As amended, Claim 1 now recites:

A mobile device for emulating a plurality of cards, the mobile device comprising:
a storage device for storing a plurality of applications, each corresponding to one of the cards;
an emulator, coupled to the storage, for receiving one of the applications, wherein each of the applications corresponds to one of the cards;
a communication interface to facilitate data exchange between a reader and the one of the applications being executed in the emulator, wherein the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications; and
a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications, wherein functions of the mobile device related to one of the cards offered by the application are changed to functions offered by the another one of the applications related to another one of the cards when the another one of the applications is activated and executed in the emulator.

(*Emphasis added*)

As described above, one of the purposes in the instant application is to emulate multiple cards in a mobile device, where a card is fundamentally a memory storage device. In reality, different companies may issue different cards, using a mobile device to emulate any one of these cards would make life simple, otherwise one would have to carry many cards. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality applications, each pertaining to one of cards. When a card is needed, a user can cause the mobile application (via an interface) to load in a corresponding application into an emulator that turns the mobile device to function as the card.

Samsung Ex. 1016, Page 164 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

In contrast, Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. The functions of the smart card CANNOT be replaced by another application so that the smart card would function as a different card. To emulate a number of different cards, an emulator is needed. Wentker is completely silent about an emulator. In other words, Wentker neither teaches nor suggests a mobile device to emulate a plurality of cards. In a perspective, Wentker teaches away from Claim 1 by managing only one card via the provided APIs. Accordingly, the Applicant submits Claim 1 as amended shall be allowable over Wentker.

The Examiner admits Wentker does not teach a near field communication (NFC) interface to facilitate data exchange between a reader and an application being loaded and executed in the emulator. Huomo is then cited to suggest the teaching.

The Applicant respectfully contests the combination of Wentker and Huomo as it is believed that there is no motivation to combine these two references in the manner proposed by the Examiner. In order to establish a *prima facie* case of obviousness under 35 USC 103, *Graham v. John Deer Co. of Kansas City*, 383 US 1 (1966) requires determining, respectively, the scope and content of the prior art, the difference between the prior art and the claims at issue, and the level of ordinary skilled in the art. Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning, to support the legal conclusion of obviousness. *KSR v. Teleflex*, No. 04-1350 (US Apr. 30, 2007) (citing In re Kahn, 441 F. 3d 977, 988 (Canada Fed. 2006)). The suggestion to make the claim combination must be found in the prior art, not in the Applicant's disclosure. In re Vaek, 20 USPQ2d 1438 (Fed. Cir. 1991). Moreover, in accordance with MPEP 2142.02, each prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L.Gore & Associates Inc. v. Garlock, Inc.* 220 USPQ 303 (Fed. Cir. 1993). A third essential requirement for establishing a *prima facie* case, set forth in MPEP 2143.01 is that the proposed modification cannot render the prior art unsatisfactory for its intended purpose.

Samsung Ex. 1016, Page 165 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Huomo teaches about an IC card in a mobile device but is silent about changing the function of the card to make the mobile device to act as another card. Given the deficiency in the Wentker as set forth above, the Applicant submits there are not any technical ways to modify Wentker with Huomo to make up the stated deficiency in the Wentker in view of Claim 1 as amended. Accordingly, the Applicant submits Claim 1 as amended shall be allowable over Wentker and Huomo, viewed alone or in combination. Reconsideration of Claims 1-11 is kindly requested.

The patentability of the independent claims has been argued specifically as set forth above and thus the Applicant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, Applicant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

In view of the above amendments and remark, the Applicant believes that Claims 1-19 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", June 17, 2016. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng
Reg.: No. 39,450

Samsung Ex. 1016, Page 166 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Electronic Patent Application Fee Transmittal

Application Number:	13782948
Filing Date:	01-Mar-2013
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Filer:	Joe Zheng
Attorney Docket Number:	RFID-084

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	2251	1	100	100
Miscellaneous:				
		Total in USD ($)		**100**

Electronic Acknowledgement Receipt	
EFS ID:	26098507
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	17-JUN-2016
Filing Date:	01-MAR-2013
Time Stamp:	13:43:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$100
RAM confirmation Number	061716INTEFSW00010475502436
Deposit Account	502436
Authorized User	Joe Zheng
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ResponseTo1stOA.pdf	181567 f1f56dee8e9e918784e3903b809ac196dbd1b944	no	18
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30321 69c121f5f14578f9e1940516b7cc6b7b473d1ca2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	211888		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/782,948	Filing Date 03/01/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☒ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	**195**
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	**195**

APPLICATION AS AMENDED – PART II

AMENDMENT		(Column 1)		(Column 2)	(Column 3)		
	06/17/2016	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 19	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

AMENDMENT		(Column 1)		(Column 2)	(Column 3)		
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/GLORIA J. TRAMMELL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 09/27/2016

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
09/27/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Office Action Summary	Application No. 13/782,948	Applicant(s) XIE ET AL.	
	Examiner ISIDORA IMMANUEL	Art Unit 3685	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06/17/2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-19* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-19* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 06/17/2016.

2. Claims 1, 2, 4-7, 9, 12, 13, 15 and 16 amended.

3. Claims 1-19 are pending.

4. Claims 1-19 have been examined.

Notice of Pre-AIA or AIA Status

5. The present application is being examined under the pre-AIA first to invent provisions.

Specification

6. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Response to Arguments

7. Applicant's arguments filed 06/17/2016 have been fully considered but they are not persuasive.

8. 101

9. In the instant case, claim 1 is directed to a device and claim 12 is directed to a method.

10. The newly amended claims recite the steps of "installing a plurality of applications…providing an emulator in the mobile device to receive a first application…, causing the second application to replace the first application..." The claim is directed towards a receiving and processing information which is similar to Alice which dealt with receiving, processing, and storing data and Bancorp which dealt with automating mental tasks (*Bancorp Services LLC v. Sun Life Assurance Co. of Canada (U.S.)*. Therefore, based on case law precedent, the claims are claiming subject matter similar to concepts already identified by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)). Claim 1 is directed towards the generic computer used to implement the method of claim 12 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving information in your device, processing selections for switching between tasks, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas.

11. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Similar to Using a processor or software for receiving, sending and processing data, and automating switching, for example, from a calculator function to a note taking function, are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

12. 112

13. Applicant argues "the claim limitations must use the phrase 'means for' or 'step for'". It appears Applicant might not be referencing the most recent version of the MPEP 2181. Additionally, courts have argued that "Our consideration of this case has led us to conclude that such a heightened burden is unjustified and that we should abandon characterizing as "strong" the presumption that a limitation lacking the word "means" is not subject to § 112, para. 6. That characterization is unwarranted, is uncertain in meaning and application, and has the inappropriate practical effect of placing a thumb on what should otherwise be a balanced analytical scale. It has shifted the balance struck by Congress in passing § 112, para. 6 and has resulted in a proliferation of functional claiming untethered to § 112, para. 6 and free of the strictures set forth in the statute. Henceforth, we will apply the presumption as we have done prior to *Lighting World,* without requiring any heightened evidentiary showing and expressly overrule the characterization of that presumption as "strong." We also overrule the strict requirement of "a showing that the limitation essentially is devoid of anything that can be construed as structure." *Williamson v. Citrix Online, LLC,* 115 USPQ2d 1105 (Fed. Cir. 2015).

14. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112(f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112,paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for,"

"apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f)or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d 1344, 1354,80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206, 1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

15. 103

16. Applicant argues Wentker does not teach an emulator. By Applicant's own explanation of an emulator, "an emulator, coupled to the storage, for receiving one of the applications…", to be "executed in the emulator". Wentker teaches " card manager **104** loads issuer application **112** and performs related card content management on behalf of the card issuer while also managing the loading, installation and deletion of applications provided by application providers…. card manager **104**, acting as the default application, is ready to receive, execute and respond to external APDU commands" (column 6, line 63-67, column 7, line 1-14, column 8, line 6-16, column 9, line 1-9). Next, Applicant argues there is no motivation to combine Huomo and Wentker. First, In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior

art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). Secondly, the arguments made do not appear to be based on the office action sent to Applicant, for example, Applicant argues “the suggestion to make the claim combination must be found in the prior art, not in the Applicant's disclosure...." A glance at the combination of the prior art will alert Applicant to the prior art and the citation for where the suggestion was found, with the format (Prior art; citation), located at the end of the combination claim. Furthermore, if applicant garnered from the combination suggestion that the motivation might have come from "Applicant’s disclosure", it is not because it came from the Applicant but rather because all three applications are very similar in scope and content, as can be gleamed from their field and background of the invention.

Examiner’s Comments

17. Regarding claim 1, with respect to claim language “device for storing…", “applications to be loaded into the emulator to replace…”, claims 2 and 13, “device to retrieve…”, “device to receive…”, claim 4, “provided respectively to perform…”, claims 7 and 16, “server configured to provide…”, claim 8, “server to remotely provision…”, “server to manage…”, claims 9 and 17, “that is determined to be updates…”, claim 11, “a request to provision…”, “the application to be provisioned…”, claim 12, “device to

receive…", "application to replace…", claim 13, "instruction to cause…", claim 15, "Module configured to provide… to store", claim 16, "Card manager proxy configured to facilitate", "user interface application provided to query", "UI application for conducting" and claim 19, "request to provision…", "application to be provisioned…", "(SSD) to be associated…" recites intended use and therefore does not have patentable weight. See MPEP 2114.

18. Regarding claim 1, the language "storage device for storing…", "processor,…, causing…", recites functional language, and therefore does not have patentable weight. See MPEP 2111, 2114, 2181.

19. Regarding claims 2 and 13, "information is a sequence…", "request is a command…", claims 11 and 19, "the data includes…", claim 13, "information is a sequence…", and claim 15, "secure element further includes…" are nonfunctional descriptive material and therefore do not have patentable weight. See *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai,* 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01. MPEP 2111.05 III.

20. Regarding claim 14, "wherein the emulator…the secure element is enclosed…", and claim 15, "the secure element further includes…" is a structural limitation in a method claim and has no patentable weight. *Ex parte Pfeiffer*, 135 USPQ 31 (Bd. App. 1961).

21. Regarding claim 12, the language "wherein the mobile device is used…", "application being executed...", "application are changed to functions offered… to functions offered", "the second application is activated…", claim 13, "the server

determines….", "keys are generated…", "secure element facilitates...", claim 14, "emulator is implemented…", "secure element is enclosed...", claim 15, "cards is loaded...", claim 16, "proxy configured to facilitate…", "application provided to query…", "information stored…", claim 17, "element is preloaded…" and claim 19, the language "application has been remotely…", "application installed…", "element is distributed…" does not disclose a positively recited step and therefore does not patentable weight. See MPEP 2111.04.

22. Regarding claim 12, "application is replaceable…" is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I) (c).

23. Regarding claim 12, the language "application are changed to functions offered… when the second application is activated…" is a result and therefore has not patentable weight (*Minton v. Nat'l Ass'n of Securities Dealers, Inc.,* 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a "'whereby clause in a method claim is not given weight when it simply expresses the intended result of a process step positively recited.'" See MPEP 2111.04.

Claim Rejections - 35 USC § 101

24. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

25. Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Subject Matter Eligibility Standard

26. When considering subject matter eligibility under 35 U.S.C. 101, it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and abstract idea), and if so, it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. (*Alice Corporation Pty. Ltd. v. CLS Bank International, et al. US Supreme Court, No. 13-298, June 19, 2014*).

Analysis

27. In the instant case, claim 1 is directed to a device and claim 12 is directed to a method.

28. The newly amended claims recite the steps of "installing a plurality of applications…providing an emulator in the mobile device to receive a first application…, causing the second application to replace the first application..." The claim is directed towards a receiving and processing information which is similar to Alice which dealt with receiving, processing, and storing data and Bancorp which dealt with automating mental tasks (*Bancorp Services LLC v. Sun Life Assurance Co. of Canada (U.S.)*. Therefore,

based on case law precedent, the claims are claiming subject matter similar to concepts already identified by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)). Claim 1 is directed towards the generic computer used to implement the method of claim 12 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving information in your device, processing selections for switching between tasks, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas.

29. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Similar to Using a processor or software for receiving, sending and processing data, and automating switching, for example, from a calculator function to a note taking function, are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

30. The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional elements are still drawn to receiving, sending and processing data, (Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), electronic recordkeeping (Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), automating mental tasks (Bancorp Services LLC v. Sun Life Assurance Co. of Canada (U.S.), 103 USPQ2d 1425 (Fed. Cir. 2012), (Cybersource Corp. v. Retail Decisions, Inc., 654 F.3d 1366, 1372 (Fed. Cir. 2011)) and receiving or transmitting data over a network, e.g.,

using the Internet to gather data (Ultramercial, Inc. v. Hulu, LLC, 772 F.3d 709, 714-15 (Fed. Cir. 2014), (buySAFE, Inc. v. Google, Inc., 765 F.3d 1350, 1355 (Fed. Cir. 2014), (Cyberfone Systems, LLC v. CNN Interactive Group, Inc., 558 Fed. Appx. 988, 993 (Fed. Cir. 2014)).

31. Viewed as a whole, instructions/method claims simply recite the concept of receiving, sending and automating data processing, as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of receiving, and processing data using some unspecified, generic computer. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2360.

32. The use of a processor implementing the abstract idea does not render the claim patent eligible because it does not provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment and requires no more than a generic computer to perform generic computer functions.

Conclusion

33. The claim as a whole, does not amount to significantly more than the abstract idea itself. This is because the claim does not affect an improvement to another technology or technical filed; the claim does not amount to an improvement to the functioning of a computer system itself; and the claim does not move beyond a general link of the use of an abstract idea to a particular technological environment.

34. Accordingly, the Examiner concludes that there are no meaningful limitations in the claim that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

35. Dependent claims do not resolve the deficiency of independent claims and accordingly stand rejected under 35 USC 101 based on the same rationale.

36. Dependent claims 2-11 and 13-19 are also rejected.

37. Claims 1 and 12 recite “a storage device…" which, in this case, is directed to a signal. The specification (¶ 239), says “the computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves,” explaining that the storage device can be a carrier wave. A signal is a carrier wave or other propagation media, according to MPEP 2106 II IV, however, there are four categories of invention: process, machine, article of manufacture or composition of matter, therefore, as a "signal" is not a category of invention nor a subset of one of the categories, it does not represent patent eligible subject matter. See *In re Nuijten*, 84 U.S.P.Q.2d 1495 (Fed. Cir. 2007), *Gottschalk v. Benson, 409 U.S. at 72, 175 USPQ at 676-77*. Dependent claims 2-11 and 13-19 are also rejected.

Claim Rejections - 35 USC § 112

38. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it

> is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

39. Claims 1-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

40. Claim 1 recites “causing the another one of the applications to be loaded into the emulator...”, similarly, claim 12 recites “causing the second application to replace….” The specification (¶ 62-69) explains that “when instructed by an user, can be caused to swap (ie. Activate on an emulator) an application in and out the Mifare emulator….” The specification provides support for a user command being the catalyst for the application replacement. The specification does not provide for an algorithm that gives “a processor”, or non-human entity the ability or operation to cause an application “to be loaded into the emulator to replace the one of the applications...” without user instruction, as directed by the specification. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

41. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.
>
> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

42. Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

43. Claim 1 recites “a storage device for storing…”, similarly, claim 12 recites “installing a plurality of applications in a storage device….” It is unclear whether the device refers to a secure element that stores the applications, as described by the specification (¶ 133-138), a secure element in the mobile device that could be software and without structure (¶ 58, 101), or whether the device refers to the secured memory space of the mobile device (Figure 1C, element 137; ¶ 101) or whether the storage device refers to the computer readable medium that could also be software and without structure (¶ 239), which says “the computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves,” explaining that the storage device can be a carrier wave. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

44. Claim 1 recites “the one of the applications being executed in the emulator, wherein the one of the applications in the emulator…”, similarly, claim 12 recites “ facilitating data exchange between a reader and the first application being executed in the emulator, wherein the first application in the emulator….” It is unclear how applications exist in the emulator to be executed when no applications are located nor have been received in or by the emulator. As explained by Applicant’s limitation, the applications are located in the “storage device”, not the emulator, and while “an emulator in the mobile device” can receive an application, one has not yet been received. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

45. As per claims 1, 2, 6, 7, 8 the claims recite the following means plus functions limitations:

a. interface to facilitate…(claim 1)

b. instruction to cause… (claim 2)

c. Module configured to provide… to store (claim 6)

d. Card manager proxy for facilitating (claim 7)

e. user interface application provided to query (claim 7)

f. UI application for conducting (claim 7)

g. Interfaces…to read (claim 8)

h. TMSM module is configured to (claim 8)

i. Applications… is caused to swap (claim 8)

j. Mechanism to make …for storing (claim 8)

46. This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112(f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112,paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for," "apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f)or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d 1344, 1354,80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206, 1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56, 57, 59-61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56, 57, 61, 75, 76 describe the module interchangeable with software modules, applications and applets but there is no indication of what structure is used. ¶ 59 describes the “card manager proxy” as a “software module”. ¶ 61 describes “a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards” but there is no indication of what structure is used. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-11 are rejected.

47. Claims 2, 11, 13 and 19 recite the limitation "the portable device". Similarly, claims 7, 8 and 16 recite the limitation “the TSM server” and "the TMSM module". There is insufficient antecedent basis for this limitation in the claim.

48. Claims 2 and 13 recite “after the server determines that the secure element…,” claim 8 recites “enable the TSM server to remotely provision…” and “enable the TSM server to manage…”, and claims 11 and 19 recite "applications has been remotely provisioned by the TSM server with operations of: receiving… establishing... preparing...

notifying..." The scope of the claims are unclear as to whether the server or the TSM server are part of the claimed mobile device or the claimed method for a mobile device.

49. Claim 2 recites “a set of keys from a designated place", the claim is unclear as to where this designated place is or why there should ambiguity as to where the keys come from, thereby rendering the claim indefinite. Similarly, claim 8 recites “to read certain data therefrom”, the claim language creates ambiguity, making the claim unclear and rendering the claim indefinite.

50. Regarding claim 8, the claim recites “provide…., when instructed by a user” However, claim 1, from which claim 8 depends, is directed to a mobile device. The claim is a hybrid claim as the cited language is not directed to the mobile device but to external use of claimed structural elements. Therefore, it would be unclear whether infringement of claim 8 occurs based on possession of the mobile device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

51. Claim 12 recites “causing the second application to replace… when the second application is activated....” since “causing” cannot occur without the activation of the second application activating. The claims are missing an essential step. Dependent claims 13-19 are rejected as each depends on rejected claim 12.

52. Claim 13 recites “after the server determines…,” it is unclear how the mobile device receives notice to monitor how the server functions.

53. Claim 16 recites “querying via a user interface (UI) one or more of the applications in detail…” the claim is unclear as to the scope or extent of “in detail”.

Claim Rejections - 35 USC § 103

54. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

55. Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo et al. (8,005,426) (“Huomo”), and in view of Wentker et al. (6,481,632) (“Wentker”).

56. Regarding claims 1 and 12, Huomo teaches a storage device for storing a plurality of applications, each corresponding to one of the cards (column 8, line 3-12, 42-47, column 14, line 54-67); an emulator, coupled to the storage, for receiving one of the applications, wherein each of the applications corresponds to one of the cards (column 8, line 42-47, column 12, line 28-43); a communication interface to facilitate data exchange between a reader and the one of the applications being executed in the emulator, wherein the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications (column 7, line 8-60, column 8, line 24-37, column 15, line 27-67); and a processor, in communication with the emulator and the storage device (column 14, line 54-67), wherein functions of the mobile device related to

one of the cards offered by the application are changed to functions offered by the another one of the applications related to another one of the cards when the another one of the applications is activated and executed in the emulator (column 9, line 30-46, column 10, line 49-67, column 11, line 1-3, column 12, line 28-43).

Huomo does not teach causing the another one of the application to be loaded into the emulator to replace the one of the applications. Wentker teaches causing the another one of the application to be loaded into the emulator to replace the one of the applications (column 6, line 63-67, column 7, line 1-14, column 8, line 6-16, column 9, line 1-9). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Huomo and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

57. Regarding claims 3 and 14, Huomo teaches wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device (column 8, line 3-23).

58. Regarding claim 4, Huomo teaches wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when one of the applications is loaded into and executed in the emulator (column 7, line 8-19, column 9, line 4-46, column 10, line 49-67, column 11, line 1-13, column 12, line 28-43).

59. Regarding claim 5, Huomo teaches wherein at least one of the cards is a Mifare contactless card (column 2, line 27-61, column 8, line 3-37).

60. Regarding claims 6 and 15, Wentker teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications (column 9, line 1-33, column 13, line 11-39, column 14, line 24-43, column 21, line 17-31).

61. Regarding claims 7 and 16, Huomo teaches a user interface (UI) (column 6, line 61-67, column 8, line 54-67). Wentker teaches wherein each of the applications has been remotely provisioned by the server configured to provide trusted service management(TSM) (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and the mobile device further includes a card manager proxy for facilitating communication between the TSM server and the TMSM module in the secure element, interface application provided to query one or more of the applications on information stored therein but not to modify the information (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications (column 10, line 8-56). Wentker does not teach a user interface (UI). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Huomo and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

62. Regarding claims 9 and 17, Wentker teaches wherein the secure element is preloaded with default Issuer Security Domain (ISD) information determined to be updated entirely or partially subject to retrieved corresponding default ISD information

from a party originating the secure element (column 7, line 38-56, column 13, line 11-39, column 19, line 1-8).

63. Regarding claims 10 and 18, Huomo teaches wherein the mobile device is a smartphone, a portable computer and a smart card (column 16, line 26-36, 43-67, column 17, line 1-5).

64. Regarding claims 11 and 19, Wentker teaches receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider (column 7, line 15-37, column 8, line 1-10, column 14, line 24-43, column 15, line 1-19, column 16, line 25-35, 49-67, column 17, line 21-35); establishing a secured channel with the secure element using a set of keys (column 7, line 15-37, column 10, line 15-23, column 13, line 11-39, column 15, line 52-67, preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67); and notifying the application provider of a status of the application with the portable device (column 12, line 58-67, column 13, line 1-10, column 17, line 4-20, column 18, line 62-67, column 19, line 44-46).

65. Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo et al. (8,005,426) (“Huomo”), in view of Wentker et al. (6,481,632) (“Wentker”) and further in view of De Groot (2006/0141987) (“Groot”).

66. Regarding claims 2 and 13, Wentker teaches and a designated server providing trusted service management (TSM) (column 6, line 13-67, column 8, line 17-32, column

21, line 1-31). Groot teaches initiating data communication between the mobile device (¶ 36, 40, 44); receiving device information of the secure element from the mobile device in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (¶ 30, 34, 36, 37, 39, 40, 43, 47, 48, 53); and sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider (Figure 1, element M1-3; ¶ 30, 31, 34, 40-45, 47-49, 53). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Huomo, Wentker, and Groot in order to provide secure transmissions with a terminal and a server using an identifier (Groot; ¶ 1-7).

67. Claim 8 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo et al. (8,005,426) (“Huomo”), in view of Wentker et al. (6,481,632) (“Wentker”) and further in view of Vayssiere (2006/0065741) (“Vayssiere”).

68. Regarding claim 8, Wentker teaches provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator (column 6, line 36-55, column 7, line 1-7, column 8, line 17-32); provide a set of Application Programming Interfaces to one of the

applications to read certain data therefrom (column 6, line 36-55, column 8, line 17-32); enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module (column 7, line 15-37, column 16, line 3-23, column 17, line 21-35, column 22, line 17-31) enable the TSM server to manage each of the applications by locking or unlocking one of the applications (column 7, line 1-7, column 9, line 34-44, column 10, line 24-44); provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module (column 22, line 51-67, column 23, line 1-24).

Neither Huomo and Wentker teach and later on swapping another one of the applications to the emulator. Vayssiere and later on swapping another one of the applications to the emulator (¶ 35). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Huomo, Wentker, and Vayssiere in order to provide a smartcard to perform multiple functions (Vayssiere; ¶ 3).

Conclusion

69. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

70. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA IMMANUEL whose telephone number is (571)272-9862. The examiner can normally be reached on Monday-Thursday 7:30am-5pm EDT.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. I./
Examiner, Art Unit 3685

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13782948	XIE ET AL.
	Examiner	Art Unit
	ISIDORA IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							

Samsung Ex. 1016, Page 199 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

Courtesy Reminder for
Application Serial No: 13/782,948

Attorney Docket No: RFID-084
Customer Number: 26797
Date of Electronic Notification: 09/27/2016

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
uspatents@sbcglobal.net

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

RECEIVED
CENTRAL FAX CENTER

FEB 27 2017

Doc Code: AP.PRE.REQ

PTO/AIA/33 (03-13)
Approved for use through 07/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): RFID-084

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]
on 2/27/2017

Signature / joe zheng /

Typed or printed name Joe Zheng

Application Number	Filed
13/782,948	03/01/2013

First Named Inventor: Xiangzhen Xie

Art Unit	Examiner
3685	Isidora I. Immanuel

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 39,450

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/ joe zheng /
Signature

Joe Zheng
Typed or printed name

(408)777-8873
Telephone number

2/27/2017
Date

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of One forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED
CENTRAL FAX CENTER

FEB 27 2017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

Mail Stop: AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Pre-Appeal Brief Request for Review

Dear Sir:

Claims 1-19 are currently pending. In the final Office Action dated 09/27/2016,

A. Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter;
B. Claims 1-9 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement;
C. Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo et al. (8,005,426) ("Huomo"), and in view of Wentker et al. (6,481,632) ("Wentker").

The Appellant respectfully disagrees with the Examiner on these rejections.

1. **Arguments with respect to Issue A**:

The Appellant noticed in Sections 11 and 29 of the Office Action that the Examiner only looked at the gerund or verbal nouns in each of the clauses or elements in Claim 1, even though only Claim 12 recites these elements, such as (see Section 28) "installing a plurality of applications ... providing an emulator in the mobile device to receive a first application ... , causing the second application to replace the first application ... " and

PAGE 4/8 * RCVD AT 2/27/2017 10:38:22 PM [Eastern Standard Time] * SVR:W-PTOFAX-001/2 * DNIS:2738300 * CSID:12067706341 * DURATION (mm-ss):07-20

Samsung Ex. 1016, Page 202 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

concluded that the claim is directed towards receiving and processing information which is similar to Alice which dealt with receiving, processing, and storing data and Bancorp which dealt with automating mental tasks.

The Appellant submits that Claim 1, being an apparatus claim, does not recite "receiving and processing information", neither does Claim 12, as alleged by the Examiner. Further Claim 1 or Claim 12, as a whole, is not simply related to receiving and processing information, and there is no any similarity to the case of Alice. Specifically, Claim 1 is related to a mobile device for emulating a plurality of cards, where each of the cards is supported by an application. When a card (e.g., a Visa card) is chosen, a corresponding application is loaded and executed in an emulator of the mobile device to cause the mobile device to function as a Visa card for transaction. When another card (e.g., a Master card) is chosen, a corresponding application is loaded to replace the originally loaded application and executed in the emulator to cause the mobile device to function as a Master card for transaction. It is believed that the Examiner fails to understand what is being claimed without examining the specific limitations collectively recited in Claim 1 or Claim 12.

On Page 10, Section 29 of the Final Office Action, the Examiner states "Taking the claim elements separately, the functions performed by the machine *at each step of the process are purely conventional*". Given the fact that Claim 1 is an apparatus claim, the Appellant respectfully challenges the Examiner to show which elements in Claim 1 or Claim 12 that could be interpreted as "receiving and processing information" similar to Alice.

On Page 10, Section 28 of the Final Office Action, the Examiner alleges that "Claim 1 is directed towards the generic computer used to implement the method of claim 12 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving information in your device, processing selections for switching between tasks, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas."

The Appellant respectfully disagrees with the allegation. First of all, Alice case is not related to switching tasks implemented on a device. Second, the Examiner provides no such citation but merely proffers an abstract idea by itself. Further MPEP 2103 I(C) states "*Diamond v. Diehr, 450 U.S. 175, 188-89, 209 USPQ 1, 9 (1981) ("In determining the eligibility of respondents' claimed process for patent protection under §101, their claims*

PAGE 5/8 * RCVD AT 2/27/2017 10:38:22 PM [Eastern Standard Time] * SVR:W-PTOFAX-001/2 * DNIS:2738300 * CSID:12067706341 * DURATION (mm-ss):07-20

must be considered as a whole. It is inappropriate to dissect the claims into old and new elements and then to ignore the presence of the old elements in the analysis. This is particularly true in a process claim because a new combination of steps in a process may be patentable even though all the constituents of the combination were well known and in common use before the combination was made." (see https://www.uspto.gov/web/offices/pac/mpep/s2103.html). Accordingly, it is concluded that the Examiner is erroneous in making the rejections based on "taking the claim elements separately" without considering specific limiations/steps recited in Claims 1 and 12. The Appellant respectfully submits that the rejection of Claims 1-19 under 35 USC 101 in the Office Action dated 09/27/2016 is defective and should be hereby reversed.

2. **Arguments with respect to Issue B**:

On Page 13, Section 40, the Examiner states "The specification does not provide for an algorithm that gives "a processor", or non-human entity the ability or operation to cause an application "to be loaded into the emulator to replace the one of the applications ... " without user instruction, as directed by the specification". The Appellant *does not* disagree with the Examiner. The application is indeed switched in part or full only at a command of a user of the mobile device. Claim 1 explicitly recites "*a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications* ". The Appellant is wondering why the Examiner believes there is an algorithm and interprets Claim 1 beyond the original intent by calling out something that is not recited in the claim. The Appellant respectfully submits that the Examiner is erroneous in making the rejections under 35 USC 112(a), alleging no support of the limitation "an algorithm" because there is no algorithm or an intention recited in the claim. Accordingly, the rejection of Claims 1-19 under 35 USC 112(a) in the Office Action dated 09/27/2016 should be hereby reversed.

Further, on Page 14, Section 43, the Examiner states "It is unclear whether the (storage) device refers to a secure element that stores the applications". Claim 1 is directed to the structures within a mobile device while Claim 12 recites steps being executed by a mobile device. It is irrelevant what the storage device is as long as it is in the mobile device, but it cannot be CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier

PAGE 6/8 * RCVD AT 2/27/2017 10:38:22 PM [Eastern Standard Time] * SVR:W-PTOFAX-001/2 * DNIS:2738300 * CSID:12067706341 * DURATION (mm-ss):07-20

waves given the context of the invention. The Appellant respectfully submits that the Examiner is erroneous in making the rejections under 35 USC 112(b) by interpreting an element beyond the limitation explicitly recited in the claim. Accordingly, the rejection of Claims 1-19 under 35 USC 112(b) in the Office Action dated 09/27/2016 should be hereby reversed.

3. **Arguments with respect to Issue C**:

As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality applications, each pertaining to one of the cards. An emulator is used in a secure element to load in and execute only one application at a time to emulate a corresponding card. When another card is selected (e.g., by a user), the previously loaded application must be partially or fully replaced with another application corresponding to the newly chosen card. In other words, the mobile device can only function as one type of cards.

Huomo does teach about an IC card in a mobile device supporting multiple application. As shown in FIG. 2a and FIG. 2b and further described in corresponding paragraphs of these two figures, applications in the secure module 200 are automatically started depending on the environment. Further shown in FIG. 4a, the applications can be respectively activated. But Huomo neither teaches nor suggests of loading a new application from a storage device (corresponding to the storage 530 in Huomo) to replace a previously loaded application, implying that the emulator can activate only one application at a time. In a perspective, Huomo teaches away "*a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications*" by explicitly teaching that multiple applications are respectively activated. On Page 20, the Examiner also admits Huomo does not teach causing the another one of the application to be loaded into the emulator to replace the one of the applications.

The Examiner then cites Wentker to show the teaching in combination with Huomo. However, Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. As described in Col. 7, lines 9-14, the card manager 104 manages the loading of an application into an IC card, but it is assumed it is a new IC card.

PAGE 7/8 * RCVD AT 2/27/2017 10:38:22 PM [Eastern Standard Time] * SVR:W-PTOFAX-001/2 * DNIS:2738300 * CSID:12067706341 * DURATION (mm-ss):07-20

In other words, Wentker is silent about replacing partially or in full a previously loaded application in an IC card when a new application is selected. The modification of Huomo with Wentker does not fundamentally cure the deficiency of Huomo that "Huomo does not teach causing the another one of the application to be loaded into the emulator to replace the one of the applications" stated by the Examiner. It is believed that the Examiner made the rejections on obviousness grounds without some articulated reasoning to support the legal conclusion of obviousness. *KSR v. Teleflex*, No. 04-1350 (US Apr. 30, 2007) (citing In re Kahn, 441 F. 3d 977, 988 (Canada Fed. 2006)).

The Appellant submits the combination of Huomo and Wentker fails to suggest "*a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications*" recited in Claim 1. The similar limitation is also recited in Claim 12. Accordingly, Claims 1 and 12 shall be allowable over Huomo and Wentker, viewed alone or in combination. The rejection of Claims 1-19 under 35 USC 103 in the Office Action dated 09/27/2016 should be hereby reversed

The patentability of the independent claims has been argued specifically as set forth above and thus Appellant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, the Appellant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

The undersigned can be reached at (408)777-8873 if there is a need to respond to any inquiry from the Panel.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", on January 27, 2017

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Reg. No.: 39,450

PAGE 8/8 * RCVD AT 2/27/2017 10:38:22 PM [Eastern Standard Time] * SVR:W-PTOFAX-001/2 * DNIS:2738300 * CSID:12067706341 * DURATION (mm-ss):07-20

RECEIVED
CENTRAL FAX CENTER
FEB 27 2017

PTO/AIA/31 (03-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD

Docket Number (Optional): RFID-084

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, on Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on 02/27/2017.

Signature: /joe zheng/

Typed or printed name: Joe Zheng

In re Application of: Xiangzhen Xie et al

Application Number	Filed
13/782,948	03/01/2013

For: Method and apparatus for emulating multiple cards in mobile devices

Art Unit	Examiner
3685	Isidora I. Iuonakhamhe

Applicant hereby appeals to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

☑ Applicant asserts small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by 50%, and the resulting fee is: $ 400.00

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Therefore, the fee shown above is reduced by 75%, and the resulting fee is: $ _____
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☑ Payment by credit card. Form PTO-2038 is attached.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 502436.

☐ Payment made via EFS-Web.

☑ A petition for an extension of time under 37 CFR 1.136(a) (PTO/AIA/22 or equivalent) is enclosed.
For extensions of time in reexamination proceedings, see 37 CFR 1.550.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant ☑ attorney or agent of record Registration number 39,450 ☐ attorney or agent acting under 37 CFR 1.34 Registration number _____

Signature: /joe zheng/

Typed or printed name: Joe Zheng

Telephone Number: (408)777-9873

Date: 02/27/2017

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.20(b)(1) and 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

02/28/2017 JVONG1 00000010 13782948
01 FC:2401 400.00 OP

RECEIVED
CENTRAL FAX CENTER
FEB 27 2017

PTO-2038 (02-2015)
Approved for use through 01/31/2018. OMB 0651-0043
United States Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Credit Card Payment Form

(Do not submit this form electronically via EFS-Web)

Please Read Instructions before Completing this Form

02/28/2017 JVONG1 00000010 13782948

02 FC:2252 300.00 OP
03 FC:1999 100.00 OP

Payment Amount (US Dollars): $800	
Cardholder Signature:	Date (mm/dd/yyyy): 2/27/2017

The USPTO does not accept an s-signature (37 CFR 1.4(e)) on credit card payment forms.
Refund Policy: The USPTO may refund a fee paid by mistake or in excess of that required. A change of purpose after the payment of a fee will not entitle a party to a refund of such fee. The USPTO will not refund amounts of $25.00 or less unless a refund is specifically requested and will not notify the payor of such amounts (37 CFR 1.26). Refund of a fee paid by credit card will be issued as a credit to the credit card account to which the fee was charged.
Maximum Daily Limit: There is a $24,999.99 daily limit per credit card account effective June 1, 2015. There is no daily limit for debit cards.

Credit Card Billing Address

Street Address 1: 7394 Wildflower Way	
Street Address 2:	
City: Cupertino	
State/Province: CA	Zip/Postal Code: 95014
Country: US	
Daytime Phone #: (408)891-9468	Fax #:

Request and Payment Information

Description of Request and Payment Information:
Fees for Notice of Appeal and 2-month ext

☒ Patent Fee	☐ Patent Maintenance Fee	☐ Trademark Fee	☐ Other Fee
Application No.: 13/782,948	Application No.	Application No.	IDON Customer No.
Patent No.	Patent No.	Registration No.	
Attorney Docket No.: RFID-084		Identify or Describe Mark	

If the cardholder includes a credit card number on any form or document other than the Credit Card Payment Form or submits this form electronically via EFS-Web, the United States Patent and Trademark Office will not be liable in the event that the credit card number becomes public knowledge.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 04/25/2017

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
04/25/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Notice of Panel Decision from Pre-Appeal Brief Review	Application No.	Applicant(s)
	13/782,948	XIE ET AL.
	Examiner	Art Unit
	ISIDORA IMMANUEL	3685

This is in response to the Pre-Appeal Brief Request for Review filed 27 February, 2017.

1. ☐ **Improper Request** – The Request is improper and a conference will not be held for the following reason(s):

☐ The Notice of Appeal has not been filed concurrent with the Pre-Appeal Brief Request.
☐ The request does not include reasons why a review is appropriate.
☐ A proposed amendment is included with the Pre-Appeal Brief request.
☐ Other: .

The time period for filing a response continues to run from the receipt date of the Notice of Appeal or from the mail date of the last Office communication, if no Notice of Appeal has been received.

2. ☒ **Proceed to Board of Patent Appeals and Interferences** – A Pre-Appeal Brief conference has been held. The application remains under appeal because there is at least one actual issue for appeal. Applicant is required to submit an appeal brief in accordance with 37 CFR 41.37. The time period for filing an appeal brief will be reset to be one month from mailing this decision, or the balance of the two-month time period running from the receipt of the notice of appeal, whichever is greater. Further, the time period for filing of the appeal brief is extendible under 37 CFR 1.136 based upon the mail date of this decision or the receipt date of the notice of appeal, as applicable.

☒ The panel has determined the status of the claim(s) is as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: *1-19*.
Claim(s) withdrawn from consideration: _____.

3. ☐ **Allowable application** – A conference has been held. The rejection is withdrawn and a Notice of Allowance will be mailed. Prosecution on the merits remains closed. No further action is required by applicant at this time.

4. ☐ **Reopen Prosecution** – A conference has been held. The rejection is withdrawn and a new Office action will be mailed. No further action is required by applicant at this time.

All participants:	
(1) */ISIDORA IMMANUEL/*.	(3)*/CALVIN LOYD HEWITT II/*.
(2) */JAMES DANIEL NIGH/*.	(4)_____.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EX PARTE

US Patent Application Number 13/782,948

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

APPEAL BRIEF

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service via USPTO electronic filing system addressed to: Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: May 19, 2017

Signed: / joe zheng /
Joe Zheng

Samsung Ex. 1016, Page 211 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

TABLE OF CONTENTS

		Page No.
I.	REAL PARTY IN INTEREST	1
II.	RELATED APPEALS AND INTERFERENCES	2
III.	STATUS OF CLAIMS	3
IV.	STATUS OF AMENDMENTS	4
V.	SUMMARY OF CLAIMED SUBJECT MATTER	5
VI.	GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	7
VII.	ARGUMENT	8
VIII.	CLAIMS APPENDIX	14
IX.	EVIDENCE APPENDIX	20
X.	RELATED PROCEEDINGS APPENDIX	21
XI.	SUMMARY	22

Samsung Ex. 1016, Page 212 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

I. REAL PARTY IN INTEREST

Rfcyber Corporation
41291 Carmen Street
Fremont, CA 94539

Samsung Ex. 1016, Page 213 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

II. RELATED APPEALS AND INTERFERENCES

None

Samsung Ex. 1016, Page 214 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

III. STATUS OF THE CLAIMS

Claims 1 - 19 are pending. On 02/27/2017, the Applicant appealed from the rejections, dated 09/27/2016, of Claims 1 - 19 that are rejected under 35 U.S.C. 101, 35 U.S.C. 112(b) and under 35 USC 103(a).

A. Total number of claims in Application

The claims in the application are: 1 - 19

B. Status of all the claims in Application

Claims 1-19 were initially filed
Claims cancelled: 0
Claims pending: 1 - 19
Claims allowed: None
Claims rejected: 1 - 19
Claims objected to: None

C. Claims on Appeal

Claims 1 - 19

Samsung Ex. 1016, Page 215 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

IV. STATUS OF AMENDMENTS

Claims 1-19 on appeal herein are as amended in the Response dated June 17, 2016 to the Office Action dated February 19, 2017.

Samsung Ex. 1016, Page 216 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

V. SUMMARY OF CLAIMED SUBJECT MATTER

The instant application is related to emulating multiple cards in a mobile device. In reality, different companies may issue different cards (e.g., library card, Costco membership card, Visa and Master Card), using a mobile device to emulate any one of these cards would make life simple, otherwise one would have to carry many cards. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality applications, each pertaining to one of the cards. When a card is needed, a user can cause the mobile device (via an interface) to load in a corresponding application into an emulator that causes the mobile device to function as the card. When another card is needed, the user can cause the mobile device to load in another corresponding application into the emulator that causes the mobile device to function as the other card. As clearly shown in FIG. 1C and described in the specification, a mobile device must have a microcontroller (MCU) or a processor on its own while an emulator in the context of this instant invention is neither a MCU nor a processor. The emulator is a special piece of hardware or software provided in the mobile device to enable the mobile device (called the *host*) to behave like another computing device (called the *guest*), see Wikipedia (https://en.wikipedia.org/wiki/Emulator). Conceptually, a mobile device works fine without an emulator but delivers something unique when equipped with such an emulator as described in the instant application.

In accordance with 37 CFR 41.37 (c)(1)(v) "A concise explanation of the subject matter defined in each of the independent claims involved in the appeal, which must refer to the specification by page and line number, and to the drawing, if any, by reference characters." All page and line numbers and the drawing are in italic and inserted directly in the independent claims below.

Claim 1: A mobile device for emulating a plurality of cards, the mobile device comprising:

a storage device for storing a plurality of applications, each corresponding to one of the cards; (*FIG. 1A* and *Para [0054]*)

Samsung Ex. 1016, Page 217 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

an emulator, coupled to the storage, for receiving one of the applications, wherein each of the applications corresponds to one of the cards; (*FIG. 1A* and *Para [0054]*)

a communication interface to facilitate data exchange between a reader and the one of the applications being executed in the emulator, (*FIG. 1C* and *Para [0056]*) wherein the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications; (*Para [0005], [0011], [0060]*) and

a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications, (*FIG. 1C* and *Para [0056]*) wherein

functions of the mobile device related to one of the cards offered by the application are changed to functions offered by the another one of the applications related to another one of the cards when the another one of the applications is activated and executed in the emulator. (FIG. 1A, *Para [0005], [0011]*)

Claim 12: A method for a mobile device to emulate a plurality of cards, the method comprising:

installing a plurality of applications in a storage device of the mobile device, each of the applications pertaining to one of the cards, wherein the mobile device is used in lieu of the cards; (*FIG. 1A* and *Para [0054]*)

providing an emulator in the mobile device to receive a first application; (*FIG. 1A* and *Para [0054]*)

facilitating data exchange between a reader and the first application being executed in the emulator, (*FIG. 1C* and *Para [0056]*) wherein the first application in the emulator is replaceable in entirety or in part by a second application; (*Para [0005], [0011], [0060]*)

causing the second application to replace the first application being loaded and executed in the emulator, (*Para [0005], [0011], [0060]*) wherein functions of the mobile device related to one of the cards offered by the first application are changed to functions offered by the application to functions offered by the

Samsung Ex. 1016, Page 218 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

second application related to another one of the cards when the second application is activated and executed in the emulator. (FIG. 1A, *Para [0005], [0011]*)

Samsung Ex. 1016, Page 219 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection which the Appellant believes to be most pertinent to the present appeal include the following issues:

A. Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter;

B. Claims 1-9 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement;

C. Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo et al. (8,005,426) ("Huomo"), and in view of Wentker et al. (6,481,632) ("Wentker"); and

D. Claim 8 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo in view of Wentker and further in view of Vayssiere (2006/00657 41) ("Vayssiere").

Samsung Ex. 1016, Page 220 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

VII. ARGUMENT

1. Arguments with respect to Issue A:

On Page 8, Section 25, of the Final Office Action dated

Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter 09/27/2016, Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The Appellant respectfully disagrees with the Examiner.

Sections 10 and 28 of the Office Action demonstrate that the Examiner only looked at the gerund or verbal nouns in each of the clauses or elements in Claim 1, even though only Claim 12 recites these elements, such as (see Section 28) "installing a plurality of applications ... providing an emulator in the mobile device to receive a first application ... , causing the second application to replace the first application ... ", and concluded that the claims are directed towards receiving and processing information which is similar to Alice which dealt with receiving, processing, and storing data and Bancorp which dealt with automating mental tasks.

The Appellant submits that Claim 1, being an apparatus claim, does not recite "receiving and processing information", neither does Claim 12, as alleged by the Examiner. Further Claim 1 or Claim 12, as a whole, is not simply related to receiving and processing information, and there is no any similarity of these claims to the case of Alice. Specifically, Claim 1 is related to a mobile device for emulating a plurality of cards, where each of the cards is supported by an application executing in an emulator at a time. When a card (e.g., a Visa card) is chosen, a corresponding application is loaded and executed in an emulator of the mobile device to cause the mobile device to function as a card (e.g. Visa for transaction). When another card (e.g., a Costco membership card) is chosen, a corresponding application is loaded to replace the originally loaded application and executed in the emulator to cause the mobile device to function as an extrance card to enter Costco. It is believed that the Examiner fails to understand what is being claimed without examining the specific limitations collectively recited in Claim 1 or Claim 12.

Samsung Ex. 1016, Page 221 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

On Page 10, Section 29 of the Final Office Action, the Examiner states "Taking the claim elements separately, the functions performed by the machine *at each step of the process are purely conventional*". Given the fact that Claim 1 is an apparatus claim, the Appellant respectfully challenges the Examiner to show which elements in Claim 1 or Claim 12 that could be interpreted as "receiving and processing information" similar to Alice.

On Page 10, Section 28 of the Final Office Action, the Examiner alleges that "Claim 1 is directed towards the generic computer used to implement the method of claim 12 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving information in your device, processing selections for switching between tasks, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas".

The Appellant respectfully disagrees with the allegation. First of all, Alice case is not related to switching tasks implemented on a device. Second, the Examiner provides no such citation but merely proffers an abstract idea by itself. Further MPEP 2103 I(C) states "Diamond v. Diehr, 450 U.S. 175, 188-89, 209 USPQ 1, 9 (1981) ("In determining the eligibility of respondents' claimed process for patent protection under §101, their claims must be considered as a whole. It is inappropriate to dissect the claims into old and new elements and then to ignore the presence of the old elements in the analysis. This is particularly true in a process claim because a new combination of steps in a process may be patentable even though all the constituents of the combination were well known and in common use before the combination was made". Accordingly, it is concluded that the Examiner is erroneous in making the rejections based on "taking the claim elements separately" without considering specific limitations/steps recited in Claims 1 and 12. The Appellant respectfully submits that the rejection of Claims 1-19 under 35 USC 101 in the Office Action dated 09/27/2016 is defective and should be hereby reversed.

2. Arguments with respect to Issue B:

On Page 13, Section 40, the Examiner states "The specification does not provide for an algorithm that gives "a processor", or non-human entity the ability or operation to cause an application "to be loaded into the emulator to replace the one

Samsung Ex. 1016, Page 222 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

of the applications ... " without user instruction, as directed by the specification". The Appellant wishes to point out that pending claims per se have never recited a requirement for such an algorithm. An application for simulating a card is switched in part or full only at a command of a user of the mobile device, not an algorithm. Claim 1 explicitly recites "*a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications*". The Appellant respectfully challenges the Examiner why there is an algorithm required for the processor to switch an application already in the emulator with another application and submits that Examiner seems to have interpreted Claim 1 beyond the original intent by calling out something that is not recited in the claim.

The Appellant respectfully submits that the Examiner is erroneous in making the rejections under 35 USC 112(a), alleging no support of the limitation "an algorithm" because there is no algorithm or an intention thereof recited in the claim. Accordingly, the rejection of Claims 1-19 under 35 USC 112(a) in the Office Action dated 09/27/2016 should be hereby reversed.

Further, on Page 14, Section 43, the Examiner states "It is unclear whether the (storage) device refers to a secure element that stores the applications". Claim 1 is directed to the structures within a mobile device while Claim 12 recites steps being executed by a mobile device. It is irrelevant what the storage device is as long as it is in the mobile device, but technically there is no way that such storage could be something like CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves given the context of the invention. The Appellant asserts that the Examiner interprets the claim beyond the original intent, and respectfully submits that the Examiner is erroneous in making the rejections under 35 USC 112(b) by interpreting an element beyond the limitation explicitly recited in the claim. Accordingly, the rejection of Claims 1-19 under 35 USC 112(b) in the Office Action dated 09/27/2016 should be hereby reversed.

3. Arguments with respect to Issue C:

On Page 19, Section 55, Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo and in view of Wentker.

Samsung Ex. 1016, Page 223 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

The Appellant respectfully disagrees with the Examiner and asserts that the Examiner interprets the cited references beyond the reasonable interpretation.

As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality applications, each pertaining to one of the cards. An emulator is used in a secure element to load in and execute only one application at a time to emulate a corresponding card. When another card is selected (e.g., by a user), the previously loaded application must be partially or fully replaced with another application corresponding to the newly chosen card. In other words, the mobile device can only function as one type of cards. It shall be also noted that an emulator is not a general processor. A common definition of "emulator" can be found on Wikipedia (https://en.wikipedia.org/wiki/Emulator) while emulation refers to the ability of a computer program in an electronic device to emulate (or imitate) another program or device.

Huomo does teach about an IC card in a mobile device supporting multiple applications. As shown in FIG. 2a and FIG. 2b and further described in corresponding paragraphs of these two figures, all applications in the secure module 200 are automatically started depending on the environment. Further shown in FIG. 4a, the applications can be respectively activated. But Huomo neither teaches nor suggests of loading a new application from a storage device (corresponding to the storage 530 in Huomo) to replace a previously loaded application, implying that the emulator can activate only one application at a time. In a perspective, Huomo teaches away "*a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications*" by explicitly teaching that multiple applications are respectively activated. On Page 20, the Examiner also admits Huomo does not teach causing the another one of the application to be loaded into the emulator to replace the one of the applications.

The Examiner then cites Wentker to show the teaching in combination with Huomo. However, Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. As described in Col. 7, lines 9-14, the card manager 104 manages the loading of an application into an IC card, but it is

Samsung Ex. 1016, Page 224 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

assumed it is a new IC card. In other words, Wentker is silent about replacing partially or in full a previously loaded application in an IC card when a new application is selected. The modification of Huomo with Wentker does not fundamentally cure the deficiency of Huomo that "*Huomo does not teach causing the another one of the application to be loaded into the emulator to replace the one of the applications*" stated by the Examiner and affirmed again on Page 24 of the Office Action. It is believed that the Examiner made the rejections on obviousness grounds without some articulated reasoning to support the legal conclusion of obviousness. *KSR v. Teleflex*, No. 04-1350 (US Apr. 30, 2007) (citing In re Kahn, 441 F. 3d 977, 988 (Canada Fed. 2006)).

The Appellant submits the combination of Huomo and Wentker fails to suggest "*a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications*" recited in Claim 1. The similar limitation is also recited in Claim 12. Accordingly, Claims 1 and 12 shall be allowable over Huomo and Wentker, viewed alone or in combination. The rejection of Claims 1-19 under 35 USC 103 in the Office Action dated 09/27/2016 should be hereby reversed.

4. Arguments with respect to Issue D:

On Page 23, Section 67, Claim 8 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Huomo in view of Wentker and further in view of Vayssiere. The Examiner admits on Page 24 of the Office Action that "none of [neither] Huomo and Wentker teach and later on swapping another one of the applications to the emulator" and then cites Vayssiere to show the teaching in combination.

As shown described in paragraph [0023], Vayssiere uses a microprocessor in an IC card. It is well-known that many microprocessors can perform multi-tasks, which is exactly Vayssiere needs. What Vayssiere emphasizes is the dynamic display portion switched from a first display to a second display in response to an application use of the smartcard while the microprocessor in the IC card is still executing multiple applications.

Samsung Ex. 1016, Page 225 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Claim 1 of the instant application recites both a processor and an emulator. The Appellant challenges the Examiner to show technically which role of the processor in Vayssiere plays in view of the processor and the emulator recited in Claim 1.

The Appellant respectfully points out that the combination of Huomo, Wentker and Vayssiere is not proper as it is believed that there is no motivation to combine these three references in the manner proposed by the Examiner. Accordingly, Claim 8 shall be allowable over Huomo, Wentker and Vayssiere in view of the limitations recited in Claims 6, 3, 2 and 1. The rejection of Claim 8 under 35 USC 103 in the Office Action dated 09/27/2016 should be hereby reversed.

Samsung Ex. 1016, Page 226 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

VIII. CLAIMS APPENDIX

1. (*Previously amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a storage device for storing a plurality of applications, each corresponding to one of the cards;

an emulator, coupled to the storage, for receiving one of the applications, wherein each of the applications corresponds to one of the cards;

a communication interface to facilitate data exchange between a reader and the one of the applications being executed in the emulator, wherein the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications; and

a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications, wherein

functions of the mobile device related to one of the cards offered by the application are changed to functions offered by the another one of the applications related to another one of the cards when the another one of the applications is activated and executed in the emulator.

2. (*Previously amended*) The mobile device as recited in claim 1, further comprising

a secure element that has been personalized by operations of:

initiating data communication between the mobile device and a designated server providing trusted service management (TSM);

receiving device information of the secure element in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are

Samsung Ex. 1016, Page 227 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when one of the applications is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a Mifare contactless card.

6. (*Previously amended*) The mobile device as recited in claim 3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Previously amended*) The mobile device as recited in claim 6, wherein each of the applications has been remotely provisioned by the server configured to provide trusted service management (TSM), and the mobile device further includes:

   a card manager proxy for facilitating communication between the TSM server and the TMSM module in the secure element,

   a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

Samsung Ex. 1016, Page 228 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications.

8. (*Original*) The mobile device as recited in claim 6, wherein the TMSM module is configured to:

provide a set of *Application Programming Interfaces* so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

provide a set of *Application Programming Interfaces* to one of the applications to read certain data therefrom;

enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module and later on swapping another one of the applications to the emulator;

enable the TSM server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Original*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone, a portable computer and a smart card.

11. (*Original*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

Samsung Ex. 1016, Page 229 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

12. (*Previously amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing a plurality of applications in a storage device of the mobile device, each of the applications pertaining to one of the cards, wherein the mobile device is used in lieu of the cards;

providing an emulator in the mobile device to receive a first application;

facilitating data exchange between a reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application;

causing the second application to replace the first application being loaded and executed in the emulator, wherein functions of the mobile device related to one of the cards offered by the first application are changed to functions offered by the application to functions offered by the second application related to another one of the cards when the second application is activated and executed in the emulator.

13. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication between the mobile device and a designated server providing trusted service management (TSM);

receiving device information of the secure element in responding to a request from the server after the server determines that the secure element is

Samsung Ex. 1016, Page 230 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Previously amended*) The mobile device as recited in claim 15, further comprising

facilitating communication between the TSM server and the TMSM module in the secure element;

querying via a user interface (UI) one or more of the applications in detail; and

conducting operations that modify one or more sectors in one or more of the applications.

17. (*Original*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

Samsung Ex. 1016, Page 231 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

18. (*Original*) The method as recited in claim 12, wherein the mobile device is a smartphone, a portable computer and a smart card.

19. (*Original*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

Samsung Ex. 1016, Page 232 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

IX. EVIDENCE APPENDIX

None.

Samsung Ex. 1016, Page 233 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

X. RELATED PROCEEDING APPENDIX

None.

Samsung Ex. 1016, Page 234 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Summary

It is respectfully concluded that the Examiner is erroneous in rejecting pending Claims 1-19 based on her overlook or misunderstanding of certain structure limitations in the claimed invention.

the rejections of the pending claims 1, 2, 4-9 and 11-13 under 35 U.S.C. 101, 35 U.S.C. 112(b) and under 35 USC 103(a) should be hereby reversed.

Respectfully Submitted,

/ joe zheng /

Joe Zheng
Reg. No.: 39,450
Tel: (408)777-8873

Samsung Ex. 1016, Page 235 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Electronic Acknowledgement Receipt

EFS ID:	29254586
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	19-MAY-2017
Filing Date:	01-MAR-2013
Time Stamp:	03:52:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	AppealBriefForm.pdf	155467 935b769b5a705826decbb9c44ddf6406c0c0d111	no	25

Warnings:

Information:	
Total Files Size (in bytes):	155467

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 05/24/2017

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/24/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Applicant-Initiated Interview Summary	Application No.	Applicant(s)		
	13/782,948	XIE ET AL.		
	Examiner	Art Unit	AIA (First Inventor to File) Status	Page
	ISIDORA IMMANUEL	3685	No	1 of 1

All participants (applicant, applicant's representative, PTO personnel):

1. ISIDORA IMMANUEL (Examiner); Telephonic 2. JOE ZHENG (Attorney); Telephonic

Date of Interview: 19 April 2017

Claim(s) discussed: 1

Amendment Proposed: Discussed the proposed amendments

Brief Description of main topic of discussion: Discussed porssible changes to the claims limitations

Issues Discussed:

Proposed Amendments:
Discussed the amendments and future prosecution

Attachment(s): Proposed Amendments

/I. I./ Examiner, Art Unit 3685	/JAMES DANIEL NIGH/ Primary Examiner, Art Unit 3685

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable time limit of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicant's responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04

Please further see:

MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Samsung Ex. 1016, Page 239 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

(Please do not enter, this is for informal discussion)

Proposed amendments for discussion at 2:00pm EST (11:00am PST) on April 19th (Wednesday).

Samsung Ex. 1016, Page 240 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

Please amend Claims 1-2, 11 and 12-13 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a storage device for storing a plurality of applications, each corresponding to one of the cards;

an emulator, coupled to the storage, for receiving one of the applications~~, wherein each of the applications corresponds to one of the cards~~;

a communication interface to facilitate data exchange between a reader and the one of the applications being executed in the emulator, wherein the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications; and

a processor, in communication with the emulator and the storage device, causing the another one of the applications to be loaded into the emulator to replace the one of the applications, wherein functions of the mobile device related to one of the cards offered by ~~the~~ an application are changed to functions offered by ~~the~~ another ~~one of the~~ application~~s~~ related to another one of the cards when the another ~~one of the~~ application~~s~~ is activated and executed in the emulator.~~.~~

2. (*Currently amended*) The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:

initiating data communication between the mobile device and a designated server providing trusted service management (TSM);

receiving device information of the secure element in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

Samsung Ex. 1016, Page 241 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

sending a set of instructions to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the ~~portable~~ mobile device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when one of the applications is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a Mifare contactless card.

6. (*Previously amended*) The mobile device as recited in claim 3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Previously amended*) The mobile device as recited in claim 6, wherein each of the applications has been remotely provisioned by the server configured to provide trusted service management (TSM), and the mobile device further includes:

a card manager proxy for facilitating communication between the TSM server and the TMSM module in the secure element;

Samsung Ex. 1016, Page 242 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications.

8. (*Original*) The mobile device as recited in claim 6, wherein the TMSM module is configured to:

provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module and later on swapping another one of the applications to the emulator;

enable the TSM server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Original*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone, a portable computer and a smart card.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application ~~to be~~being provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the installed application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the installed application; and

notifying the application provider of a status of the installed application with the portable device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing a plurality of applications in a storage device of the mobile device, each of the applications pertaining to one of the cards, wherein the mobile device is used in lieu of the cards;

providing an emulator in the mobile device to receive a first application;

facilitating data exchange between a reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application; and

causing the second application to replace the first application being loaded and executed in the emulator, wherein functions of the mobile device related to one of the cards offered by the first application are changed to ~~functions offered by the application to~~ functions offered by the second application related to another one of the cards when the second application is activated and executed in the emulator.

Samsung Ex. 1016, Page 244 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

13. (*Currently amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication between the mobile device and a designated server providing trusted service management (TSM);

receiving device information of the secure element in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information ~~from~~ of the secure element ~~therein~~; and

sending a set of instructions to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Previously amended*) The mobile device as recited in claim 15, further comprising

facilitating communication between the TSM server and the TMSM module in the secure element;

Samsung Ex. 1016, Page 245 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

querying via a user interface (UI) one or more of the applications in detail; and conducting operations that modify one or more sectors in one or more of the applications.

17. (*Original*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Original*) The method as recited in claim 12, wherein the mobile device is a smartphone, a portable computer and a smart card.

19. (*Original*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the TSM server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

Samsung Ex. 1016, Page 246 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 10/10/2017

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
10/10/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Samsung Ex. 1016, Page 247 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Office Action Summary	Application No. 13/782,948	Applicant(s) XIE ET AL.	
	Examiner ISIDORA IMMANUEL	Art Unit 3685	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/19/2017*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-19* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-19* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 05/19/2017.

2. Claims 1, 2, 4-7, 9, 12, 13, 15 and 16 amended.

3. Claims 1-19 are pending.

4. Claims 1-19 have been examined.

Notice of Pre-AIA or AIA Status

5. The present application is being examined under the pre-AIA first to invent provisions.

Response to Arguments

6. Applicant's arguments filed 05/19/2017 have been fully considered but they are not persuasive. Applicant's arguments with respect to the claims have been considered but are moot because the arguments do not apply to the combination of the references being used in the current rejection.

7. 101

8. The newly amended claim 12 recites the steps of "installing a plurality of applications…providing an emulator in the mobile device to receive a first application…, causing the second application to replace the first application..." The claim is directed towards an idea of itself as it is directed to the acts of a user, specifically, the acts of loading software (applications, emulator) onto a device. Therefore, based on case law precedent, the claims are claiming subject matter similar to concepts already identified

by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)).

9. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Similar to using a processor or software for the acts of loading software (applications, emulator) onto a device, are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

10. 112

11. Applicant argues "the claim limitations must use the phrase 'means for' or 'step for'". It appears Applicant might not be referencing the most recent version of the MPEP 2181. Additionally, courts have argued that "Our consideration of this case has led us to conclude that such a heightened burden is unjustified and that we should abandon characterizing as "strong" the presumption that a limitation lacking the word "means" is not subject to § 112, para. 6. That characterization is unwarranted, is uncertain in meaning and application, and has the inappropriate practical effect of placing a thumb on what should otherwise be a balanced analytical scale. It has shifted the balance struck by Congress in passing § 112, para. 6 and has resulted in a proliferation of functional claiming untethered to § 112, para. 6 and free of the strictures set forth in the statute. Henceforth, we will apply the presumption as we have done prior to *Lighting World,* without requiring any heightened evidentiary showing and expressly overrule the characterization of that presumption as "strong." We also overrule the strict requirement

of “a showing that the limitation essentially is devoid of anything that can be construed as structure.” *Williamson v. Citrix Online, LLC,* 115 USPQ2d 1105 (Fed. Cir. 2015).

12. When the claim limitation does not use the term “means,” examiners should determine whether the presumption that 35 U.S.C.112(f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term “means”). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112,paragraph 6: “mechanism for,” “module for,” “device for,” “unit for,” “component for,” “element for,” “member for,” “apparatus for,” “machine for,” or “system for.” This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f)or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d 1344, 1354,80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206, 1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are “used as a substitute for ‘means’ that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)” MPEP 2181.

Examiner’s Comments

13. Regarding claim 1, with respect to claim language "device for storing…", "emulator is replaceable…", "applications to be loaded into the emulator to replace…", claims 2 and 13, "a command causing…device to retrieve…", "sending a set of instruction to cause…device to receive…", "wherein the set of keys… facilitates…", claim 4, "provided respectively to perform…", claims 7 and 16, "server configured to provide…", claim 8, "server to remotely provision…", "server to manage…", claims 9 and 17, "that is determined to be updates…", claim 11, "a request to provision…", "the application to be provisioned…", claim 12, "device to receive…", "application to replace…", "emulator is replaceable…", claim 13, "instruction to cause…", claim 15, "Module configured to provide… to store", claim 16, "Card manager proxy configured to facilitate", "user interface application provided to query", "UI application for conducting" and claim 19, "request to provision…", "application to be provisioned…", "(SSD) to be associated…" recites intended use and therefore does not have patentable weight. See MPEP 2114.

14. Regarding claim 1, the language "storage device for storing…", "processor,…, causing…", recites functional language, and therefore does not have patentable weight. See MPEP 2111, 2114, 2181.

15. Regarding claims 2 and 13, "information is a sequence…", "request is a command…", claims 11 and 19, "the data includes…", claim 13, "information is a sequence…", and claim 15, "secure element further includes…" are nonfunctional descriptive material and therefore do not have patentable weight. See *In re Gulack*, 217

USPQ 401 (Fed. Cir. 1983), *In re Ngai,* 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01. MPEP 2111.05 III.

16. Regarding claim 14, “wherein the emulator…the secure element is enclosed…”, and claim 15, “the secure element further includes…” is a structural limitation in a method claim and has no patentable weight. *Ex parte Pfeiffer*, 135 USPQ 31 (Bd. App. 1961).

17. Regarding claim 12, the language ”wherein the mobile device is used…”, “wherein functions of the mobile device…”, “application being executed...”, “application are changed to functions offered… to functions offered”, “the second application is activated…”, claim 13, “the server determines….”, “keys are generated…”, “secure element facilitates...", claim 14, “emulator is implemented…”, “secure element is enclosed...", claim 15, "cards is loaded...", claim 16, “proxy configured to facilitate…”, “application provided to query…”, “information stored…", claim 17, “element is preloaded…” and claim 19, the language "application has been remotely…”, “application installed…”, “element is distributed…” does not disclose a positively recited step and therefore does not patentable weight. See MPEP 2111.04.

18. Regarding claim 12, “application is replaceable…" is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I) (c).

19. Regarding claim 12, the language “application are changed to functions offered… when the second application is activated…” is a result and therefore has not patentable weight (*Minton v. Nat’l Ass’n of Securities Dealers, Inc.,* 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a “‘whereby clause in a method claim is not

given weight when it simply expresses the intended result of a process step positively recited.'" See MPEP 2111.04.

Claim Rejections - 35 USC § 101

20. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

21. Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

22. Claim 1 recites "the mobile device comprising: a storage device…", in this case, the mobile device is transitory and the storage device is directed to a signal. The specification (¶ 239), says "the computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves," explaining that the storage device can be a carrier wave. A signal is a carrier wave or other propagation media, according to MPEP 2106 II IV, however, there are four categories of invention: process, machine, article of manufacture or composition of matter, therefore, as a "signal" is not a category of invention nor a subset of one of the categories, it does not represent patent eligible subject matter. As the storage device (i.e. signal) is an essential part of the mobile device, the mobile device would not continue to be a mobile device without the storage device (i.e. signal) present. See *In re*

Nuijten, 84 U.S.P.Q.2d 1495 (Fed. Cir. 2007), *Gottschalk v. Benson, 409 U.S. at 72, 175 USPQ at 676-77*. Dependent claims 2-11 are also rejected.

Subject Matter Eligibility Standard

23. When considering subject matter eligibility under 35 U.S.C. 101, it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and abstract idea), and if so, it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. (*Alice Corporation Pty. Ltd. v. CLS Bank International, et al. US Supreme Court, No. 13-298, June 19, 2014*).

Analysis

24. In the instant case, claim 12 is directed to a method.

25. The newly amended claims recite the steps of “installing a plurality of applications…providing an emulator in the mobile device to receive a first application…, causing the second application to replace the first application...” The claim is directed

towards an idea of itself as it is directed to the acts of a user, specifically, the acts of loading software (applications, emulator) onto a device. Therefore, based on case law precedent, the claims are claiming subject matter similar to concepts already identified by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)).

26. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Similar to using a processor or software for the acts of loading software (applications, emulator) onto a device, are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

27. Viewed as a whole, instructions/method claims simply recite the concept of receiving, sending and automating data processing, as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of an idea of itself as it is directed to the acts of a user, specifically, the acts of loading software (applications, emulator) onto a device using some unspecified, generic computer. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2360.

28. The use of a processor implementing the abstract idea does not render the claim patent eligible because it does not provide meaningful limitations beyond generally

linking the use of an abstract idea to a particular technology environment and requires no more than a generic computer to perform generic computer functions.

Conclusion

29. The claim as a whole, does not amount to significantly more than the abstract idea itself. This is because the claim does not affect an improvement to another technology or technical filed; the claim does not amount to an improvement to the functioning of a computer system itself; and the claim does not move beyond a general link of the use of an abstract idea to a particular technological environment.

30. Accordingly, the Examiner concludes that there are no meaningful limitations in the claim that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

31. Dependent claims do not resolve the deficiency of independent claims and accordingly stand rejected under 35 USC 101 based on the same rationale.

32. Dependent claims 13-19 are also rejected.

Claim Rejections - 35 USC § 112

33. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly

> connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

34. Claims 1-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

35. Claim 1 recites "causing the another one of the applications to be loaded into the emulator...", similarly, claim 12 recites "causing the second application to replace…." The specification (¶ 62-69) explains that "when instructed by an user, can be caused to swap (ie. Activate on an emulator) an application in and out the Mifare emulator…." The specification provides support for a user command being the catalyst for the application replacement. The specification does not provide for an algorithm that gives "a processor", or non-human entity the ability or operation to cause an application "to be loaded into the emulator to replace the one of the applications..." without user instruction, as directed by the specification. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

36. Claim 13 recites "after the server determines that the secure element is registered therewith…." To satisfy the written description requirement, the specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. *LizardTech, Inc. v. Earth Res.Mapping, Inc.,* 424 F.3d 1336, 1344-45, 76 USPQ2d1724,

1731-32 (Fed. Cir. 2005). *Enzo Biochem, Inc. v. Gen-Probe, Inc.,* 323 F.3d956, 968, 63 USPQ2d 1609, 1616 (Fed. Cir. 2002)(holding that generic claim language appearing in *ipsis verbis* in the original specification did not satisfy the written description requirement because it failed to support the scope of the genus claimed). The specification at (¶ 60, 61) explains " the new NFC device is determined if it is a genuine NFC device. One example is to check a serial number associated with the NFC device. The serial number may be verified with a database associated with a TSM server. In the example of a NFC mobile device, the device serial number of the mobile device may be used for verification. It is now assumed that the NFC device is a genuine device (recognizable by a mobile operator). The process**110** goes to **114** to have the NFC device communicated with a dedicated server… the NFC device is registered with the server. Once the NFC device becomes part of the system, various services or data may be communicated to the device via the network. As part of the personalization process, the server requests device information of the SE at **118**. In one embodiment, the server is configured to send a data request (e.g., a WAP PUSH) to the device." The specification does not provide support for the limitation "after the server determines that the secure element is registered therewith…". There is no support for the server to determine the secure element is registered, the specification simply states " the NFC device is registered with the server." The server never verifies the secure element is registered. There is a regurgitation of the exact same language in the claims and specification (¶ 15, 16) but the body of the specification does not provide any support of the scope of the genus claimed.

37. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

38. Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

39. The claim(s) are narrative in form and replete with indefinite language. The structure which goes to make up the device must be clearly and positively specified. The structure must be organized and correlated in such a manner as to present a complete operative device. The claim(s) must be in one sentence form only.

40. Claim 1 recites “a storage device for storing…”, similarly, claim 12 recites “installing a plurality of applications in a storage device….” It is unclear whether the device refers to a secure element that stores the applications, as described by the specification (¶ 133-138), a secure element in the mobile device that could be software and without structure (¶ 58, 101), or whether the device refers to the secured memory space of the mobile device (Figure 1C, element 137; ¶ 101) or whether the storage device refers to the computer readable medium that could also be software and without structure (¶ 239), which says “the computer readable medium is any data storage device that can store data which can thereafter be read by a computer system.

Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves," explaining that the storage device can be a carrier wave. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

41. Claim 1 recites "the one of the applications being executed in the emulator, wherein the one of the applications in the emulator…", similarly, claim 12 recites " facilitating data exchange between a reader and the first application being executed in the emulator, wherein the first application in the emulator…." It is unclear how applications exist in the emulator to be executed when no applications are located nor have been received in or by the emulator. As explained by Applicant's limitation, the applications are located in the "storage device", not the emulator, and while "an emulator in the mobile device" can receive an application, one has not yet been received. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

42. As per claims 1, 2, 6, 7, 8 the claims recite the following means plus functions limitations:

a. interface to facilitate…(claim 1)

b. storage device for storing (claim 1)

c. an emulator… for receiving (claim 1)

d. communication interface to facilitate data exchange (claim 1)

e. instruction to cause… (claim 2)

f. Module configured to provide… to store (claim 6)

g. Card manager proxy for facilitating (claim 7)

h. user interface application provided to query (claim 7)

i. UI application for conducting (claim 7)

j. Interfaces…to read (claim 8)

k. TMSM module is configured to (claim 8)

l. Applications… is caused to swap (claim 8)

m. Mechanism to make …for storing (claim 8)

43. This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112(f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112,paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for," "apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f)or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d

1344, 1354,80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206, 1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56, 57, 59-61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56, 57, 61, 75, 76 describe the module interchangeable with software modules, applications and applets but there is no indication of what structure is used. ¶ 59 describes the "card manager proxy" as a "software module". ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards" but there is no indication of what structure is used. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-11 are rejected.

44. Regarding claim 1 recites ""wherein functions of the mobile device related to… are changed… offered… when… is activated…", claim 2 recites "… a secure element

that has been personalized by operations of…", claim 4 recites "wherein each of the applications… of cards provided…", claim 8, the claim recites "provide…., when instructed by a user" and claim 11, "wherein each of the application has been remotely provisioned by the TSM server with operations of:…" However, claim 1, from which claims 2, 4, 8 and 11 depends, is directed to a mobile device. The claim is a hybrid claim as the cited language is not directed to the mobile device but to external use of claimed structural elements. Therefore, it would be unclear whether infringement of claims 1, 2, 4, 8 and 11 occurs based on possession of the mobile device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990). Dependent claims 2-11 are rejected.

45. Claim 1 recites "and the one of the applications being executed…", claim 2, "a designated…", claims 2, 11, 13 and 19 recite the limitation "the portable device", similarly, claims 7, 8 and 16 recite the limitation "the TSM server" and "the TMSM module", claim 9 "wherein the secure element is preloaded…", claim 12, "cards offered" and claim 19 "has been remotely provisioned…". There is insufficient antecedent basis for this limitation in the claim. Dependent claims 2-11 and 13-19 are rejected as each depends on rejected claims 1 and 12, respectively.

46. Claim 1 is directed to a mobile device and therefore cannot claim itself, claim 1 recites "a mobile device for emulating a plurality of cards, the mobile device comprising: … wherein functions of the mobile device…", but the claim adopts circular reasoning in

the explanation of not what the device comprises but what it does, " wherein functions of the mobile device....", similarly, claim 2 recites "command causing the mobile device…", "claim 4, “the mobile device is used to emulate…”, just to name a few examples. Dependent claims 2-11 are rejected.

47. Claims 2 and 13 recite “after the server determines that the secure element…,” claim 8 recites “enable the TSM server to remotely provision…” and “enable the TSM server to manage…”, and claims 11 and 19 recite "applications has been remotely provisioned by the TSM server with operations of: receiving… establishing... preparing... notifying..." The scope of the claims are unclear as to whether the server or the TSM server are part of the claimed mobile device or the claimed method for a mobile device.

48. Claim 2 recites “a set of keys from a designated place", the claim is unclear as to where this designated place is or why there should ambiguity as to where the keys come from, thereby rendering the claim indefinite. Similarly, claim 8 recites “to read certain data therefrom”, the claim language creates ambiguity, making the claim unclear and rendering the claim indefinite.

49. Claim 12 recites “causing the second application to replace… when the second application is activated....” since “causing” cannot occur without the activation of the second application activating. The claims are missing an essential step. Dependent claims 13-19 are rejected as each depends on rejected claim 12.

50. Claim 16 recites “querying via a user interface (UI) one or more of the applications in detail…” The term "in detail" in claim 16 is a relative term which renders the claim indefinite. The term "in detail" is not defined by the claim, the specification

does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

51. Claim 19 recites “has been remote provisioned by the TSM server”, and “distributed by an application provider”. The claim has an unclear scope. The claim is directed to “a method for a mobile device…” but it is unclear whether the claim limitations recited are directed to the mobile device or combination of a mobile device/TSM server/Application provider.

Claim Rejections - 35 USC § 102

52. The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

53. Claim(s) 12-19 are rejected under pre-AIA 35 U.S.C. 102(a) as being anticipated by Gernert et al. (7,206,849) (“Gernert”).

54. Regarding claim 12, Gernert teaches installing a plurality of applications in a storage device of the mobile device, each of the applications pertaining to one of the cards, wherein the mobile device is used in lieu the cards (column 5, line 60-67); providing an emulator in the mobile device to receive a first application; facilitating data exchange between a reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application (column 5, line 60-67, column 6, line 37-46, column 8, line 36-62).

The remaining limitations "causing the second application to replace…" are intended use, as the function is associated with what the computer is implemented to perform and therefore does not have patentable weight. See MPEP 2103(I) (c). Claims 12-19 are, therefore, rejected as being anticipated by Gernert.

Claim Rejections - 35 USC § 103

55. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

56. Claims 1, 4, and 12 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), and in view of Vayssiere (2006/0065741) ("Vayssiere").

57. Regarding claims 1 and 12, Davis teaches a storage device for storing a plurality of applications, each corresponding to one of the cards (column 25, line 6-13; claim 1, 22); an emulator, coupled to the storage, for receiving one of the applications, wherein each of the applications corresponds to one of the cards (Abstract; column 25, line 6-13, column 29, line 23-31; claim 1); a communication interface to facilitate data exchange between a reader and the one of the applications being executed in the emulator, in the emulator (Abstract; column 7, line 52-67, column 10, line 57-60, column 25, line 6-13, column 29, line 23-31; claim 1, 22); and a processor in communication with the emulator

and the storage device, into the emulator (column 10, line 33-60, column 25, line 6-13, column 29, line 23-31; claim 1, 22), into the emulator, and executed in the emulator (Abstract; column 25, line 6-13, column 29, line 23-31; claim 1).

Davis does not teach wherein the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications, causing the another one of the applications to be loaded to replace the one of the applications wherein functions of the mobile device related to one of the cards offered by the application are changed to functions offered by the another one of the applications related to another one of the cards when the another one of the applications is activated. Vayssiere teaches wherein the one of the applications is replaceable in entirety or in part by another one of the applications (¶ 22, 35, 38), causing the another one of the applications to be loaded to replace the one of the applications, wherein functions of the mobile device related to one of the cards offered by the application are changed to functions offered by the another one of the applications related to another one of the cards when the another one of the applications is activated (¶ 22, 30, 31, 37, 38, 43). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis and Vayssiere in order to provide a smartcard to perform multiple functions (Vayssiere; ¶ 3).

58. Regarding claim 4, Davis teaches wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction (column 25, line 6-13), the mobile device is used to emulate each

of the cards when one of the applications is loaded into and executed in the emulator (column 7, line 39-67).

59. Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vayssiere (2006/0065741) ("Vayssiere") in view of Wentker et al. (6,481,632) ("Wentker") and further in view of De Groot (2006/0141987) ("Groot").

60. Regarding claims 2 and 13, Neither Davis nor Vayssiere teaches initiating data communication between the mobile device; receiving device information of the secure element from the mobile device in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider and a designated server providing trusted service management. Wentker teaches and a designated server providing trusted service management (TSM) (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31). Groot teaches initiating data communication between the mobile device (¶ 36, 40, 44); receiving device information of the secure element from the mobile device in responding to a request from the server after the server determines

that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (¶ 30, 34, 36, 37, 39, 40, 43, 47, 48, 53); and sending a set of instruction to cause the mobile device to receive in the secure element at least a set of keys from a designated place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the portable device and a service provider (Figure 1, element M1-3; ¶ 30, 31, 34, 40-45, 47-49, 53). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere, Wentker, and Groot in order to provide secure transmissions with a terminal and a server using an identifier (Groot; ¶ 1-7).

61. Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) (“Davis”), in view of Vayssiere (2006/0065741) (“Vayssiere”) and further in view of Huomo et al. (8,005,426) (“Huomo”).

62. Regarding claims 3 and 14, Davis teaches the emulator (Abstract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere teaches implemented in the secure element (¶ 22, 23, 30). Neither Davis nor Vayssiere teaches the secure element is enclosed in the mobile device or in a detachable card to the mobile device. Huomo teaches the secure element is enclosed in the mobile device or in a detachable card to the mobile device (column 8, line 3-23). Therefore, it would have been obvious to one

of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere and Huomo in order to provide transactions with mobile devices equipped with a smartcard (Huomo; column 1, line 7-23, 54-67).

63. Regarding claim 5, Huomo teaches wherein at least one of the cards is a Mifare contactless card (column 2, line 27-61, column 8, line 3-37).

64. Regarding claims 10 and 18, Huomo teaches wherein the mobile device is a smartphone, a portable computer and a smart card (column 16, line 26-36, 43-67, column 17, line 1-5).

65. Claims 6, 7, 9, 11, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vayssiere (2006/0065741) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker").

66. Regarding claims 6 and 15, Neither Davis nor Vayssiere teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications. Wentker teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications (column 9, line 1-33, column 13, line 11-39, column 14, line 24-43, column 21, line 17-31). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere and Wentker in

order to provide efficient management of card applications (Wentker; column 1, line 12-67).

67. Regarding claims 7 and 16, Davis teaches a user interface (UI) (column 10, line 10-32). Wentker teaches wherein each of the applications has been remotely provisioned by the server configured to provide trusted service management(TSM) (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and the mobile device further includes a card manager proxy for facilitating communication between the TSM server and the TMSM module in the secure element, interface application provided to query one or more of the applications on information stored therein but not to modify the information (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications (column 10, line 8-56). Wentker does not teach a user interface (UI). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

68. Regarding claim 8, Davis teaches to the emulator (Abstract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere and later on swapping another one of the applications (¶ 35). Wentker teaches provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator (column 6, line 36-55, column 7, line 1-7, column 8, line 17-32); provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom (column 6, line 36-55, column 8, line 17-32);

enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module (column 7, line 15-37, column 16, line 3-23, column 17, line 21-35, column 22, line 17-31) enable the TSM server to manage each of the applications by locking or unlocking one of the applications (column 7, line 1-7, column 9, line 34-44, column 10, line 24-44); provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module (column 22, line 51-67, column 23, line 1-24).

69. Regarding claims 9 and 17, Wentker teaches wherein the secure element is preloaded with default Issuer Security Domain (ISD) information determined to be updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element (column 7, line 38-56, column 13, line 11-39, column 19, line 1-8).

70. Regarding claims 11 and 19, Wentker teaches receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider (column 7, line 15-37, column 8, line 1-10, column 14, line 24-43, column 15, line 1-19, column 16, line 25-35, 49-67, column 17, line 21-35); establishing a secured channel with the secure element using a set of keys (column 7, line 15-37, column 10, line 15-23, column 13, line 11-39, column 15, line 52-67, preparing data for the application being provisioned, wherein the

data includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67); and notifying the application provider of a status of the application with the portable device (column 12, line 58-67, column 13, line 1-10, column 17, line 4-20, column 18, line 62-67, column 19, line 44-46).

Conclusion

71. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA IMMANUELEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Thursday 8am-5pm EDT.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. I./
Examiner, Art Unit 3685

/CALVIN L HEWITT II/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination XIE ET AL.	
	Examiner ISIDORA IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6,481,632 B2	11-2002	Wentker; David C.	G06F8/60	235/376
*	B	US-2006/0065741 A1	03-2006	Vayssiere; Julien JP.	G06K19/07703	235/492
*	C	US-2006/0141987 A1	06-2006	De Groot; Max	H04L63/0414	455/411
*	D	US-7,206,849 B1	04-2007	Gernert; Alex M.	G06F1/3203	370/249
*	E	US-7,908,216 B1	03-2011	Davis; Virgil M.	G06Q20/02	705/41
*	F	US-8,005,426 B2	08-2011	Huomo; Heikki	G06Q20/20	235/441
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13782948	XIE ET AL.
	Examiner	**Art Unit**
	ISIDORA IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016	09/17/2017						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						

Samsung Ex. 1016, Page 277 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13782948	XIE ET AL.
	Examiner	Art Unit
	ISIDORA IMMANUEL	3685

CPC- SEARCHED		
Symbol	Date	Examiner
G06Q	2/1/2016	II

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705			

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
See attached notes	2/1/2016	II

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/I.I./ Examiner.Art Unit 3685	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

January 9, 2018

Mail Stop: No-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to First OA after Appeal

Dear Sir:

In response to Office Action dated 10/10/2017, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

AMENDMENTS TO THE SPECIFICATION begin on page 2 of this Response

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begins on page 3 of this Response.

REMARKS/ARGUMENTS begin on page 10 of this Response.

Samsung Ex. 1016, Page 279 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE SPECIFICATION

1. Please amend Paragraph [0054] as follows:

[0054] According to one embodiment of the present invention, FIG. 1A shows a simplified system 100 in which two exemplary computing devices 102 and 104 are being configured to support multiple contactless cards or used in lieu of multiple contactless cards. Instead of bringing a number of cards, each for one purpose, one embodiment of the current invention allows a user to bring only one mobile device for all uses for the cards. Unless otherwise explicitly indicated, the term of "computing device", "mobile device", "smart phone", "portable device" or "handset" will be interchangeably used herein, but those skilled in the art will understand the description herein shall be equally applicable to other devices such as a smart phone, a tablet, a laptop computer, and other portable device with the capability of near field communication.

2. Please amend Paragraph [0089] as follows:

[0089] In the real-time approach, the server is configured to communicate with the manufacturer (i.e., its server thereof) when an SE by the manufacturer is being personalized by the TSM server. The default key set is, thus, retrieved on demand from the server of the manufacturer. In one embodiment, the TSM server includes a plug-in module for each of the manufacturers to communicate therewith.

Samsung Ex. 1016, Page 280 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

Please amend Claims 1-2, 4-13 and 17-19 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided by a module downloaded from a designated server;

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;

an emulator, coupled to the storage, for receiving ~~one of the~~ a first application~~s~~ corresponding to a first card, the first application being one of the applications~~, wherein each of the applications corresponds to one of the cards~~;

a communication interface to facilitate data exchange wirelessly between a reader and the first ~~one of the~~ application~~s~~ being executed in the emulator, wherein the reader is external to the mobile device, and the first ~~one of the~~ application~~s~~ in the emulator is replaceable in entirety or in part by ~~another one of the~~ a second application~~s~~ corresponding to a second card; and

a processor, in communication with the emulator and the storage device, performing an operation of causing ~~the another one of~~ the second application~~s to be~~ loaded into the emulator to replace ~~the one of~~ the first application~~s~~ when the second card is selected via the display screen and the second application is unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server, and wherein

Samsung Ex. 1016, Page 281 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

functions of the mobile device related to ~~one of~~ the first cards offered by the first application are changed to functions offered by ~~the another one of~~ the second applications related to ~~another one of~~ the second cards when ~~the another one of~~ the second applications is activated and executed in the emulator.

2. (*Currently amended*) The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:

initiating data communication ~~between~~ by the mobile device ~~and a~~ with the designated server providing trusted service management (TSM);

~~receiving~~ sending device information of the secure element in responding to a request from the designated server after the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

~~sending a set of instruction to cause the mobile device to receive~~ receiving in the secure element at least a set of keys from ~~a~~ the designated ~~server~~place, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the ~~portable~~ mobile device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Currently amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when ~~one of the~~ a corresponding applications is loaded into and executed in the emulator.

Samsung Ex. 1016, Page 282 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

5. (*Currently amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a ~~Mifare~~ contactless card.

6. (*Currently amended*) The mobile device as recited in claim 3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Currently amended*) The mobile device as recited in claim 6, wherein ~~each of the applications has been remotely provisioned by the server configured to provide trusted service management (TSM), and~~ the mobile device further includes:

   a card manager proxy for facilitating communication between the ~~TSM~~ designated server and the TMSM module in the secure element,

   a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

   a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications.

8. (*Currently amended*) The mobile device as recited in claim 6, wherein the TMSM module is configured to:

   provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

   provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

   enable the TSM server to remotely provision each of the applications by installing application keys and application data to the TMSM module and later on swapping another one of the applications to the emulator;

Samsung Ex. 1016, Page 283 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

enable the ~~TSM~~ designated server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Currently amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information ~~determined to be~~ updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Currently amended*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone~~,~~ or a portable computer ~~and a smart card~~.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the ~~TSM~~ designated server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application ~~to be~~being provisioned ~~with the secure element~~ is distributed by an application provider;

establishing a secured channel ~~with the secure element~~between the mobile device and the designated server using a set of keys;

~~preparing~~ receiving data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the ~~portable~~ mobile device.

Samsung Ex. 1016, Page 284 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing ~~a plurality of applications~~ in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device ~~is used~~ communicates wirelessly with an external reader provided to read one ~~in lieu~~ of the cards;

showing a list of the cards on a display of the mobile device for a user to choose one therefrom, wherein the display is provided by a module downloaded from the designated server and executed in the mobile device;

~~providing~~ receiving an emulator in the mobile device ~~to receive~~ a first application corresponding to a first card;

facilitating data exchange between ~~a~~ the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card;

causing the second application to replace the first application ~~being~~ loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server, and wherein functions of the mobile device related to ~~one of~~ the first card~~s~~ offered by the first application are changed to functions offered by the second application ~~to functions offered by the second application~~ related to ~~another one of~~ the second cards when the second application is activated and executed in the emulator.

Samsung Ex. 1016, Page 285 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

13. (*Currently amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication ~~between~~ by the mobile device ~~and~~ with ~~a~~ the designated server providing trusted service management (TSM);

~~receiving~~ sending device information of the secure element in responding to a request from the designated server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

~~sending a set of instruction to cause the mobile device to receive~~ receiving in the secure element at least a set of keys from ~~a~~ the designated ~~place~~server, wherein the keys are generated in accordance with the device information of the secure element, ~~wherein~~ the set of keys in the secure element facilitates a subsequent transaction between the ~~portable~~ mobile device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Previously amended*) The mobile device as recited in claim 15, further comprising

facilitating communication between the TSM server and the TMSM module in the secure element;

Samsung Ex. 1016, Page 286 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

querying via a user interface (UI) one or more of the applications in detail; and conducting operations that modify one or more sectors in one or more of the applications.

17. (*Currently amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updatable ~~that is determined to be updated~~ entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Currently amended*) The method as recited in claim 12, wherein the mobile device is a smartphone~~,~~ or a portable computer ~~and a smart card~~.

19. (*Currently amended*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the ~~TSM~~ designated server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the portable device.

Samsung Ex. 1016, Page 287 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

REMARKS

Claims 1 - 19 were examined again. In the Office Action dated 10/10/2017, Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, Claims 1-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement, Claim(s) 12-19 are rejected under pre-AIA 35 U.S.C. 102(a) as being anticipated by Gernert et al. (7,206,849) ("Gernert"), Claims 1, 4, and 12 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), and in view of Vayssiere (2006/00657 41) ("Vayssiere"), Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vayssiere in view of Wentker et al. (6,481,632) ("Wentker") and further in view of De Groot (2006/0141987) ("Groot"), Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vayssiere and further in view of Huomo et al. (8,005,426) ("Huomo"), Claims 6, 7, 9, 11, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vayssiere and further in view of Wentker, Claims 12-19 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Wentker, and Claims 1, 3-7, 9-12, and 14-19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker, and further in view of Huomo, Claim 2 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Huomo and further in view of Groot, and Claim 8 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Huomo and further in view of Vayssiere.

The Applicant appreciates the Examiner for providing detailed comments in the Office Action. In the foregoing amendments, Claims 1-2, 4-13 and 17-19 have been amended to further distinguish from the cited references. No new matters have been introduced. Reconsideration of pending claims is respectfully requested.

Re: Examiner's Comments

On page 5, Section 13, the Examiner alleges that the phrases "device for storing ... ", "emulator is replaceable ... ", "applications to be loaded into the emulator

Samsung Ex. 1016, Page 288 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

to replace ... ", etc. recite intended use and therefore are not given patentable weight. The Examiner even cites MPEP 2114. The Applicant respectfully disagrees and submits that the Examiner has misinterprets MPEP 2114.

MPEP 2114 explicitly states "Features of an apparatus may be recited either structurally or functionally. *In re Schreiber,* 128 F.3d 1473, 1478, 44 USPQ2d 1429, 1432 (Fed. Cir. 1997)". Claim 1 recites "*a storage device for storing a plurality of applications*". There is nothing wrong with the functional language used to define what a storage does. The Applicant believes that the Examiner renders the conclusion of "not given patentable weight" by only looking at a sentence structure without reading the sentence completely in Claim 1.

MPEP 2173.05(g) states clearly a claim term is functional when it recites a feature "by what it does rather than by what it is" (e.g., as evidenced by its specific structure or specific ingredients). In re Swinehart, 439 F.2d 210, 212, 169 USPQ 226, 229 (CCPA 1971). There is nothing inherently wrong with defining some part of an invention in functional terms. Functional language does not, in and of itself, render a claim improper. As another example, Claim 1 recites "*an emulator, coupled to the storage, for receiving a first application*", it means explicitly what function the emulator is performing, there is nothing implied that the function being performed by the emulator is only an intended use. It is believed that the Examiner fails to read the claims in whole but focuses only on the certain structure of the claim language.

On page 5, Section 14, the Examiner alleges Regarding claim 1, the language "storage device for storing ... ", "processor, ... , causing ... ", recites functional language, and therefore does not have patentable weight. MPEP 2114 explicitly states "Features of an apparatus may be recited either structurally or functionally. *In re Schreiber,* 128 F.3d 1473, 1478, 44 USPQ2d 1429, 1432 (Fed. Cir. 1997)." Claim 1 recites "*a storage device for storing a plurality of applications*". There is nothing wrong with the functional language according to MPEP 2114 and MPEP 2173.05(g).

On page 5, Section 15, the Examiner alleges claims 2 and 13 reciting "information is a sequence ... ", "request is a command ... ", claims 11 and 19, "the data

Samsung Ex. 1016, Page 289 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

includes ... ", claim 13, "information is a sequence ... ", and claim 15, "secure element further includes ... " are nonfunctional descriptive material and therefore do not have patentable weight. The Examiner even cites MPEP 2106.01 and MPEP 2111.05 III. The Applicant respectfully advises the Examiner that there is not such section titled as MPEP 2106.01 while MPEP 2111.05 III is related to Machine-Readable Media. It is believed that the Examiner rendered the conclusion of "not given patentable weight" based on improper sections in MPEP.

Claim Rejections - 35 USC§ 101

On Page 7, Section 21, of this Office Action, Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter under 35 U.S.C. 101. The Examiner alleges Claim 1 recites "the mobile device comprising: a storage device ... ", in this case, the mobile device is transitory and the storage device is directed to a signal.

The Applicant respectfully disagrees with the Examiner on the ground of rejection on Claims 1-19 under 35 USC 101 and submits the Examiner is conceptually and technically wrong when considering that the mobile device is transitory and the storage device is directed to a signal.

Both a mobile device and a storage device are tangible and physical things while a signal in general is intangible. A mobile device or a storage device can process or store a signal. Given the fact that the Examiner admits "*A signal is a carrier wave or other propagation media*", which is non-physical, the Examiner still misclassifies the physical elements as non-physical and then applies MPEP 2106 II IV to reject Claims 1-11. The Applicant respectfully challenges the Examiner to show how a mobile device or a storage device becomes a "signal" in the real world. The rejections of Claims 1-11 under 101 shall be withdrawn.

On Page 8, Section 25, of this Office Action, the Examiner alleges that the claim is directed towards an idea of itself as it is directed to the acts of a user, specifically, the acts of loading software (applications, emulator) onto a device. The Applicant respectfully disagrees and challenges the Examiner to show how

Samsung Ex. 1016, Page 290 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

"*installing in a storage device of the mobile device a plurality of applications downloaded from a designated server*" and "*facilitating data exchange between the external reader and the first application being executed in the emulator*" could be performed mentally or by human activities. It is believed that the Examiner renders the conclusion of the claim being abstract without considering all the elements in a whole. The rejections of Claims 12-19 under USC 101 shall be withdrawn.

On Page 9, Section 26, of this Office Action, the Examiner alleges the functions performed by the machine at each step of the process are purely conventional. Given the amendments in the foregoing entered, the Applicant respectfully challenges the Examiner to show a reference that teaches or suggests every element recited in Claim 1 or 12.

On Page 9, Section 27, of this Office Action, the Examiner alleges instructions/method claims simply recite the concept of receiving, sending and automating data processing, as performed by a generic computer. First of all, the Applicant wishes to call the attention of the Examiner, neither Claim 1 nor Claim 12 recites the concept of receiving, sending and automating data processing. The claim is directed to emulating different physical cards by a mobile device that can wirelessly communicate with an external reader that otherwise reads one of these cards. It is believed that the Examiner has rendered the statement without fully understanding what is being recited in Claim 1 or Claim 12.

With regard to the present application, the Applicant respectfully submits that the rejection of the claims under 35 USC 101 is defective in view of the USPTO's MEMORANDUM dated May 19, 2016, for the reason that the Office Action: 1) fails to compare the claim to claims already found to be directed to an abstract idea in a previous court decision when determining whether a claim is directed to an abstract idea, 2) fails to apply a filter to the claims, when interpreted in view of the specification, based on whether their character as a whole is directed to a patent ineligible concept, 3) interprets or describes a claim at a high level of abstraction untethered from the language of the claim when determining the focus of the

Samsung Ex. 1016, Page 291 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

claimed invention, and 4) fail to realize the fact that an invention's ability to run on a general purpose computer does not automatically doom the claim.

Accordingly, the Applicant respectfully requests the Examiner to withdraw the rejection of Claims 1-19 under 35 USC 101 in view of the amendments thereto.

Claim Rejections - 35 USC § 112

On Page 11 Section 34, of this Office Action, Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

In the foregoing amendments, Claims 1-2, 4-7, 9, 12-13 and 15-16 have been amended. It is believed that most of the claim rejections under 35 U.S.C. 112 shall have been overcome.

On Page 11, Section 35, of this Office Action, the Examiner alleges The specification does not provide for an algorithm that gives "a processor", or non-human entity the ability or operation to cause an application "to be loaded into the emulator to replace the one of the applications ... " without user instruction. Claim 1 explicitly recites "*a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen and the second application is unlocked by the designated server*". Claim 1 does not imply that there is an algorithm used to control the operation. The Applicant respectfully challenges the Examiner to show where in Claim 1 or 12 that an algorithm or non-human entity controls the operation.

On Page 11, Section 36, of this Office Action, the Examiner alleges There is no support for the server to determine the secure element is registered, the specification simply states "the NFC device is registered with the server." The Applicant respectfully believes that the Examiner has misunderstood the invention. A secure element can be verified by a server even if the secure element has not been

Samsung Ex. 1016, Page 292 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

registered. It is the mobile device that carries the secure element, where the mobile device has to be registered with the server first regardless whether the secure element has been registered or not. There is nothing wrong in that operation. It appears that the unique operation is indeed misunderstood by the Examiner, which leads the Examiner to the erroneous rejections of the claims. Accordingly, withdrawal of the rejection under 35 USC § 112 is respectfully requested.

On Page 13, Section 40, of this Office Action, the Examiner questions Claim 1 recites "a storage device for storing ... ", similarly, claim 12 recites "installing a plurality of applications in a storage device .... " It is unclear whether the device refers to a secure element that stores the applications, as described by the specification. The Applicant submits both Claims 1 and 12 explicitly recite it is the storage device that stores the application as shown FIG. 1A, which is described in paragraph [0011].

Other issues raised by the Examiner in Sections 41-51 have been either answered in addressing similar issues above or rectified in the amendments in the foregoing. The Applicant submits all rejections under 35 USC § 112 shall be withdrawn.

Claim Rejections - 35 USC § 102

On Page 19, Section 53, of this Office Action, Claims 12-19 are rejected under pre-AIA 35 U.S.C. 102(a) as being anticipated by Gernert. The Applicant respectfully traverses the rejections of Claims 12-19 under 35 USC 102, assuming the foregoing amendments are entered. A cited prior art reference anticipates a claimed invention under 35 USC 102 only if every element of the claimed invention is identically shown in the single reference, arranged as they are in the claim. MPEP 2131; in re Bond, 910 F.2d 831, 832, 15 USPQ2d 1566, 1567 (Fed. Cir. 1990). Each and every limitation of the claimed invention is significant and must be found in the single cited prior reference. In re Donohue, 766 F2.d 531, 534, 266 USPQ 619, 621 (Feb. Cir. 1985). As set forth more fully below, Gernert neither discloses nor suggests each and every element of the claimed invention.

As amended, Claim 12 now recites:

Samsung Ex. 1016, Page 293 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

installing in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards;

showing a list of the cards on a display of the mobile device for a user to choose one therefrom, wherein the display is provided by a module downloaded from the designated server and executed in the mobile device;

receiving an emulator in the mobile device a first application corresponding to a first card;

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card;

causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second cards when the second application is activated and executed in the emulator.

(*emphasis added*)

One of the purposes in the instant application is to emulate multiple cards in a mobile device to interact with an external reader that otherwise reads one of the cards directly. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality of applications controlled and managed by a designated (TSM) server, each of the applications pertaining to one of cards. When a card is needed, a user can select one from a display showing a list of cards available in the mobile device. A corresponding application is loaded into an emulator that turns the mobile device to function as the card. One of the important features is that the data for one of the cards can be accessed by the designated control (e.g., to lock or unlock an application).

Samsung Ex. 1016, Page 294 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

In contrast, Gernert teaches a mobile device sending a message to a host when the mobile device is unreachable. As explicitly described in Col. 5, lines 60-67, Gernert states "this embodiment allows the host computer application to switch from application to application, and to implement new applications, without having the mobile computer terminal set up in advance to handle a specific formatting scheme". Besides being silent on "*the data can only be modified by the designated server over a secured channel* ", Gernert neither teaches nor suggests "*showing a list of the cards on a display of the mobile device for a user to choose one therefrom*".

The Examiner further states the remaining limitations "causing the second application to replace ... " are intended use, as the function is associated with what the computer is implemented to perform and therefore does not have patentable weight. The Applicant respectfully disagrees. "*causing the second application to replace the first application loaded and executed in the emulator*" is one of the inventative steps or limitation, which should be given the patentable weight. Nevertheless, the Applicant submits Claim 12 as amended shall be allowable over Gernert as Gernert neither discloses nor suggests each and every element of the claimed invention. Reconsideration of Claims 12-19 is kindly requested.

Claim Rejections - 35 USC § 103

On Page 20, Section 56, of this Office Action, Claims 1, 4, and 12 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vayssiere. The Applicant traverses the rejections, assuming the foregoing amendments are entered.

As amended, Claim 1 now recites:

a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided by a module downloaded from a designated server;
a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs

Samsung Ex. 1016, Page 295 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;

an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications;

a communication interface to facilitate data exchange wirelessly between a reader and the first application being executed in the emulator, wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card; and

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen and the second application is unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server, and wherein

functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator.

(*emphasis added*)

As shown in FIG. 1A, there are at least four entities involved to achieve what Claim 1 recites, a trusted service manager (a designated server) 114, a mobile device 102 or 104 and a (external) reader 110. One of the purposes in the instant application is to emulate multiple cards in the mobile device. Instead of using a physical card to be read by the reader, a user can now use the mobile device to communicate with the reader. When dealing with multiple cards, as described in [0057] - [0060], all cards being supported are shown in a display and the user can choose one of them from the display, where the display is supplied from a module downloaded from a server (trusted service manager 114). When a card is selected, a corresponding application is loaded into an emulator that turns the mobile device to function as the card. When another card is selected, another corresponding application is loaded into the emulator, essentially replacing the already loaded

Samsung Ex. 1016, Page 296 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

application in the emulator, turning the mobile device to act as the another card. The subtle limitations recited in Claim 1 as amended distinguish from cited references.

Davis teaches a virtual smart card for payment of goods and/or services purchased on-line over the Internet. When purchasing something online, Davis allows a server to include a smart card emulator that emulates a smart card by using a card data base and a hardware security module, thus a user can settle a transaction with the emulated card. However, the user must store the card information on the server. In other words, Davis does not allow other device(s) to access the card information stored by the user on the server, which teaches away from "*the data can only be modified by the designated server over a secured channel* ". In another perspective, David teaches away from "*said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server*" as recited in Claim 1 as amended. The Applicant wishes to call the attention of the Examiner that Davis allows the emulated card to be read by a pseudo card reader module 264, both of the emulated card and the card reader module are within the same device while Claim 1 recites "*a communication interface to facilitate data exchange wirelessly between a reader and the first application being executed in the emulator, wherein the reader is external to the mobile device*". Accordingly, Claim 1 as amended shall be allowable over Davis.

On Page 21, the Examiner admits Davis does not teach "wherein the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications" and then cites Vayssiere to suggest the teaching in combination.

Vayssiere teaches a smartcard having a dynamic display portion that changes when an application is switched. As described in [0038], Vayssiere explicitly describes that when the user completes the use [of] the smartcard as a calling card, Application 2 (410) terminates, and OS 406 activates Display Chooser application 422 again. First of all, Vayssiere is silent about "*the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications*". Even if the Examiner insists Vayssiere may imply the replacement action, the modification of

Samsung Ex. 1016, Page 297 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

David with Vayssiere would still not cure the deficiency of "*the data can only be modified by the designated server over a secured channel* " as the card itself in Vayssiere does not allow another device to remotely control an application therein. In fact, Vayssiere has no such need. Accordingly, the Applicant submits Claim 1 as amended shall be allowable over Davis and Vayssiere, viewed alone or in combination. Reconsideration of Claims 1-11 is kindly requested.

The patentability of the independent claims has been argued specifically as set forth above and thus the Applicant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, Applicant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

In view of the above amendments and remark, the Applicant believes that Claims 1-19 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", January 9, 2018. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng
Reg.: No. 39,450

Samsung Ex. 1016, Page 298 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Electronic Acknowledgement Receipt

EFS ID:	31452532
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	09-JAN-2018
Filing Date:	01-MAR-2013
Time Stamp:	17:57:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ResponseTo1stOAAfterAppeal.pdf	204438 b3c4ff8ec4688a508c26b8a58e5080446e6362f3	no	20

Warnings:

Information:	
Total Files Size (in bytes):	204438

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 06/12/2018

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CALIFORNIA 95015
UNITED STATES OF AMERICA

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
06/12/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Office Action Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 01/09/2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-19 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-19 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 01/09/2018.

2. Claims 1, 2, 4-13, and 17-19 amended.

3. Claims 1-19 are pending.

4. Claims 1-19 have been examined.

Notice of Pre-AIA or AIA Status

5. The present application is being examined under the pre-AIA first to invent provisions.

Claim Objections

6. Claim 12 is objected to because of the following informalities: the claim recites "receiving an emulator in the mobile device a first application…." Appropriate correction is required.

Response to Arguments

7. Applicant's arguments filed 01/09/2018 have been fully considered but they are not persuasive.

8. 112

9. Claim 1 recites "a display screen showing a list of the cards…" According to the specification (Figure 9; ¶ 238), "FIG. 9, it shows a snapshot of a screen display of an account for a personalized SE. As shown in the menu **902**, the account maintains detailed information **904** about the SE that has been personalized. In addition, the

account includes a list of provisioned applications as well as security keys." Neither the drawings nor the specification provide a display screen that shows a list of cards or written description for displaying a list of cards on the mobile device.

10. 103

11. Applicant's arguments with respect to the claims have been considered but are moot because the arguments do not apply to the combination of references being used in the current rejection.

Claim Rejections - 35 USC § 112

12. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

13. Claims 1-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

14. Claim 1 recites "a display screen showing a list of the cards…" According to the specification (Figure 9; ¶ 238), "FIG. 9, it shows a snapshot of a screen display of an account for a personalized SE. As shown in the menu **902**, the account maintains detailed information **904** about the SE that has been personalized. In addition, the account includes a list of provisioned applications as well as security keys." Neither the drawings nor the specification provide a display screen that shows a list of cards or written description for displaying a list of cards on the mobile device. Dependent claims 2-11 are rejected as each depend on rejected claim 1.

15. Claim 1 recites "causing the second application loaded into the emulator... wherein said causing the second application...", similarly, claim 12 recites "causing the second application to replace…." The specification (¶ 62-69) explains that "when instructed by a user, can be caused to swap (i.e. Activate on an emulator) an application in and out the Mifare emulator…." The specification provides support for a user command being the catalyst for the application replacement. The specification does not provide for an algorithm that gives "a processor", or non-human entity the ability or operation to cause an application "to be loaded into the emulator to replace the one of the applications..." without user instruction, as directed by the specification. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

16. Claim 13 recites "after the server determines that the secure element is registered therewith…." To satisfy the written description requirement, the specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention.

LizardTech, Inc. v. Earth Res.Mapping, Inc., 424 F.3d 1336, 1344-45, 76 USPQ2d1724, 1731-32 (Fed. Cir. 2005). *Enzo Biochem, Inc. v. Gen-Probe, Inc.,* 323 F.3d956, 968, 63 USPQ2d 1609, 1616 (Fed. Cir. 2002)(holding that generic claim language appearing in *ipsis verbis* in the original specification did not satisfy the written description requirement because it failed to support the scope of the genus claimed). The specification at (¶ 60, 61) explains " the new NFC device is determined if it is a genuine NFC device. One example is to check a serial number associated with the NFC device. The serial number may be verified with a database associated with a TSM server. In the example of a NFC mobile device, the device serial number of the mobile device may be used for verification. It is now assumed that the NFC device is a genuine device (recognizable by a mobile operator). The process**110** goes to **114** to have the NFC device communicated with a dedicated server… the NFC device is registered with the server. Once the NFC device becomes part of the system, various services or data may be communicated to the device via the network. As part of the personalization process, the server requests device information of the SE at **118**. In one embodiment, the server is configured to send a data request (e.g., a WAP PUSH) to the device." The specification does not provide support for the limitation "after the server determines that the secure element is registered therewith…". There is no support for the server to determine the secure element is registered, the specification simply states " the NFC device is registered with the server." The server never verifies the secure element is registered. There is a regurgitation of the exact same language in the claims and specification (¶ 15, 16) but the body of the specification does not provide any support of the scope of the genus claimed.

17. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

18. Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

19. The claim(s) are narrative in form and replete with indefinite language. The structure which goes to make up the device must be clearly and positively specified. The structure must be organized and correlated in such a manner as to present a complete operative device. The claim(s) must be in one sentence form only.

20. Claim 1 recites “a storage device for storing…”, similarly, claim 12 recites “installing in a storage device… a plurality of applications….” It is unclear whether the device refers to a secure element that stores the applications, as described by the specification (¶ 133-138), a secure element in the mobile device that could be software and without structure (¶ 58, 101), or whether the device refers to the secured memory space of the mobile device (Figure 1C, element 137; ¶ 101) or whether the storage device refers to the computer readable medium that could also be software and without structure (¶ 239), which says “the computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access

memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves," explaining that the storage device can be a carrier wave. Dependent claims 2-11 and 13-19 are rejected as each depend on rejected claims 1 and 12.

21. Claim 12 recites " facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator…." It is unclear how applications exist in the emulator to be executed when no applications are located nor have been received in or by the emulator. As explained by Applicant's limitation, the applications are located in the "storage device", not the emulator, and while "an emulator in the mobile device" can receive an application, one has not yet been received. Dependent 13-19 are rejected as each depend on rejected claim 12.

22. As per claims 1, 6, 7, 8 the claims recite the following means plus functions limitations:

a. storage device for storing (claim 1)

b. an emulator… for receiving (claim 1)

c. communication interface to facilitate data exchange (claim 1)

d. Module configured to provide… to store (claim 6)

e. Card manager proxy for facilitating (claim 7)

f. user interface application provided to query (claim 7)

g. UI application for conducting (claim 7)

h. Interfaces…to read (claim 8)

i. TMSM module is configured to (claim 8)

j. Mechanism to make …for storing (claim 8)

23. This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112(f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112,paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for," "apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f)or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d 1344, 1354,80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206, 1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56, 57, 59-61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56, 57, 61, 75, 76 describe the module interchangeable with software modules, applications and applets but there is no indication of what structure is used. ¶ 59 describes the "card manager proxy" as a "software module". ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards" but there is no indication of what structure is used. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-11 are rejected.

24. Claim 1 is directed to a product. Specifically, the claim is directed to "A mobile device...." However, the body of the claim and following dependent claims also recite method steps including "cards provided by a module downloaded from a designated server... wherein the reader is external to the mobile device...the second application is unlocked by the designated server... the second application is locked by the designated server ", claim 2 recites "... responding to a request from the designated server after the designated server determines that the secure element is registered ...", and claim 11, "wherein each of the application has been remotely provisioned by the designated server with operations of:..." However, claim 1, from which claims 2, and 11 depends, is directed to a mobile device. The claim is a hybrid claim as the cited language is not directed to the mobile device but to functions of claimed structural elements, for

example the designated server is not a part of the claimed mobile device, but functions of the designated server are claimed within the scope of the mobile device. Therefore, it would be unclear whether infringement of claims 1, 2, and 11 occurs based on possession of the mobile device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990). Dependent claims 2-11 are rejected.

25. Claim 1 recites “and the first applications being executed…”, there are no previous first applications that were executed, claim 19 recites the limitation "the portable device", similarly, claims 7, and 16 recite the limitation "the TMSM module", claim 8 recites “TSM server”, claim 12, “the first cards offered”, there is no recitation for offering cards, claim 16 recites the TMSM module", and “TSM server” There is insufficient antecedent basis for this limitation in the claim. Dependent claims 2-11 and 13-19 are rejected as each depends on rejected claims 1 and 12, respectively.

26. Claim 1 is directed to “a mobile device” However, the body of the claim recites “user of the mobile device.. cards in the mobile device…external to the mobile device… functions of the mobile device…”,, therefore, the scope of the claim is unclear as a mobile device cannot comprise itself. Similarly, claim 2 recites "command causing the mobile device…between the mobile device“, "claim 4, “the mobile device is used to emulate…”, claim 11, “between the mobile device…”. See *In re Zletz*, 13 USPQ2d 1320 (Fed. Cir. 1989)(“An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed…”). Dependent claims 2-11 are rejected.

27. Claims 2 and 13 recite "after the designated server determines that the secure element…," claim 8 recites "enable the TSM server to remotely provision…" and "enable the TSM server to manage…", and claims 11 and 19 recite "applications has been remotely provisioned by the designated server with operations of: receiving… establishing... preparing... notifying..." The scope of the claims are unclear as to whether the server or the TSM server or designated server are part of the claimed mobile device or the claimed method for a mobile device.

28. Claim 16 recites "querying via a user interface (UI) one or more of the applications in detail…" The term "in detail" in claim 16 is a relative term which renders the claim indefinite. The term "in detail" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

29. Claim 19 recites "has been remote provisioned by the designated server", and "distributed by an application provider". The claim has an unclear scope. The claim is directed to "a method for a mobile device…" but it is unclear whether the claim limitations recited are directed to the mobile device or combination of a mobile device/designated server/Application provider.

Claim Rejections - 35 USC § 103

30. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would

> have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vayssiere (2006/0065741) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker").

32. Regarding claims 1 and 12, Davis teaches a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided by a module downloaded from a designated server (Figure 5; column 9, line 2-13, column 13, line 62-67, column 14, line 1-7); a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated _server over a secured channel (column 6, line 60-67, column 7, line 31-38, column 8, line 53-59, column 28, line 20-36, column 33, line 48-64); an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications (Abstract; column 6, line 60-63, column 12, line 24-37, column 25, line 6-13, column 29, line 23-31), a communication interface to facilitate data exchange wirelessly between a reader and the first applications being executed in the emulator, wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety or in part by a second application: corresponding to a second card (Abstract; column 7, line 52-67, column 10, line 57-60, column 25, line 6-13, column 29, line 23-31; claim 1, 22); and

a processor, in communication with the emulator and the storage device (column 10, line 33-60, column 25, line 6-13, column 29, line 23-31; claim 1, 22); into the emulator(Abstract; column 6, line 60-63, column 12, line 24-37, column 25, line 6-13, column 29, line 23-31).

Davis does not teach performing an operation of causing the second applications loaded to replace the first applications when the second card is selected via the display screen and the second application is unlocked by the designated server, wherein said causing the second application loaded to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server, and wherein functions of the mobile device related the first card offered by the first application are changed to functions offered by the second application related to the second cards when the second applications is activated and executed. Vayssiere teaches performing an operation of causing the second applications loaded to replace the first applications (¶ 22, 35, 38), wherein said causing the second application loaded to replace the first application fails when the second card is selected via the display screen and wherein functions of the mobile device related the first card offered by the first application are changed to functions offered by the second application related to the second cards when the second applications is activated and executed(¶ 22, 26, 30, 31, 35, 37, 38, 41, 43). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis and Vayssiere in order to provide a smartcard to perform multiple functions (Vayssiere; ¶ 3).

Wentker teaches when the second card is selected via the display screen and the second application is unlocked by the designated server but the second application is locked by the designated server (Figure 5; column 9, line 34-44, column 10, line 31-44, column 16, line 11-24, column 17, line 4-20), Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

33. Regarding claim 4, Davis teaches wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction (column 25, line 6-13), the mobile device is used to emulate each of the cards when a corresponding applications is loaded into and executed in the emulator (column 7, line 39-67).

34. Regarding claims 6 and 15, Neither Davis nor Vayssiere teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications. Wentker teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications (column 9, line 1-33, column 13, line 11-39, column 14, line 24-43, column 21, line 17-31). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere and Wentker in

order to provide efficient management of card applications (Wentker; column 1, line 12-67).

35. Regarding claims 7 and 16, Davis teaches a user interface (UI) (column 10, line 10-32). Wentker teaches wherein the mobile device further includes a card manager proxy for facilitating communication between the designated server and the TMSM module in the secure element, interface application provided to query one or more of the applications on information stored therein but not to modify the information (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications (column 10, line 8-56). Wentker does not teach a user interface (UI). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

36. Regarding claim 8, Davis teaches to the emulator (Abstract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere and later on swapping another one of the applications (¶ 35). Wentker teaches provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator (column 6, line 36-55, column 7, line 1-7, column 8, line 17-32); provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom (column 6, line 36-55, column 8, line 17-32); enable the designated server to remotely provision each of the applications by installing application keys and application data to the TMSM module (column 7, line 15-37, column 16, line 3-23, column 17, line 21-35, column 22, line 17-31) enable the TSM

server to manage each of the applications by locking or unlocking one of the applications (column 7, line 1-7, column 9, line 34-44, column 10, line 24-44); provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module (column 22, line 51-67, column 23, line 1-24).

37. Regarding claims 9 and 17, Wentker teaches wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element (column 7, line 38-56, column 13, line 11-39, column 19, line 1-8).

38. Regarding claims 11 and 19, Wentker teaches receiving a request to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider (column 7, line 15-37, column 8, line 1-10, column 14, line 24-43, column 15, line 1-19, column 16, line 25-35, 49-67, column 17, line 21-35); establishing a secured channel between the mobile device and the designated server using a set of keys (column 7, line 15-37, column 10, line 15-23, column 13, line 11-39, column 15, line 52-67, receiving data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67); and notifying the application provider of a status of the application with

the mobile device (column 12, line 58-67, column 13, line 1-10, column 17, line 4-20, column 18, line 62-67, column 19, line 44-46).

39. Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vayssiere (2006/0065741) ("Vayssiere"), in view of Wentker et al. (6,481,632) ("Wentker") and further in view of De Groot (2006/0141987) ("Groot").

40. Regarding claims 2 and 13, Neither Davis nor Vayssiere teaches initiating data communication by the mobile device with the designated server; sending device information of the secure element from the mobile device in responding to a request from the designated server after the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider and a designated server providing trusted service management. Wentker teaches and with designated server providing trusted service management (TSM) (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31). Groot teaches initiating data communication by the mobile device (¶ 36, 40, 44); sending device information of the secure element from the mobile device in responding to a request from the designated server after the designated server determines that the secure element is registered therewith, wherein the device

information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (¶ 30, 34, 36, 37, 39, 40, 43, 47, 48, 53); receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider (Figure 1, element M1-3; ¶ 30, 31, 34, 40-45, 47-49, 53). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere, Wentker, and Groot in order to provide secure transmissions with a terminal and a server using an identifier (Groot; ¶ 1-7).

41. Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vayssiere (2006/0065741) ("Vayssiere"), in view of Wentker et al. (6,481,632) ("Wentker") and further in view of Huomo et al. (8,005,426) ("Huomo").

42. Regarding claims 3 and 14, Davis teaches the emulator (Abs-tract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere teaches implemented in the secure element (¶ 22, 23, 30). Neither Davis nor Vayssiere teaches the secure element is enclosed in the mobile device or in a detachable card to the mobile device. Huomo teaches the secure element is enclosed in the mobile device or in a detachable card to the mobile device (column 8, line 3-23). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vayssiere and

Huomo in order to provide transactions with mobile devices equipped with a smartcard (Huomo; column 1, line 7-23, 54-67).

43. Regarding claim 5, Huomo teaches wherein at least one of the cards is a contactless card (column 2, line 27-61, column 8, line 3-37).

44. Regarding claims 10 and 18, Huomo teaches wherein the mobile device is a smartphone, or a portable computer (column 16, line 26-36, 43-67, column 17, line 1-5).

Conclusion

45. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

46. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUELEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. I./
Examiner, Art Unit 3685/

/NEHA PATEL/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination Xie et al.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	6,481,632 B2	11-2002	Wentker; David C.	G06F8/60	235/376
*	B	2006/0065741 A1	03-2006	Vayssiere; Julien JP.	G06K19/07703	235/492
*	C	2006/0141987 A1	06-2006	De Groot; Max	H04L63/0414	455/411
*	D	7,206,849 B1	04-2007	Gernert; Alex M.	G06F1/3203	370/249
*	E	7,908,216 B1	03-2011	Davis; Virgil M.	G06Q20/02	705/41
*	F	8,005,426 B2	08-2011	Huomo; Heikki	G06Q20/20	235/441
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant					☐ CPA		☐ T.D.		☐ R.1.47	
CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016	09/17/2017	05/22/2018					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	✓					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	✓	✓	✓					
	17	✓	✓	✓	✓					
	18	✓	✓	✓	✓					
	19	✓	✓	✓	✓					

Samsung Ex. 1016, Page 323 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

CPC - Searched*		
Symbol	Date	Examiner
G06Q	2/1/2016	II

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
705			

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See attached notes	2/1/2016	II
101 withdrawal - Weinhart	06/06/2018	III

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/I.I./ Examiner.Art Unit 3685

Samsung Ex. 1016, Page 324 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PTO/AIA/31 (03-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD

Docket Number (Optional): RFID-084

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, on Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on 02/27/2017.

Signature: / joe zheng /

Typed or printed name: Joe Zheng

In re Application of: Xiangzhen Xie et al

Application Number	Filed
13/782,948	03/01/2013

For: Method and apparatus for emulating multiple cards in mobile devices

Art Unit	Examiner
3685	Isidora I. Iuonakhamhe

Applicant hereby **appeals** to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

[✓] Applicant asserts small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by 50%, and the resulting fee is: $ 400.00

[ ] Applicant certifies micro entity status. See 37 CFR 1.29. Therefore, the fee shown above is reduced by 75%, and the resulting fee is: $ _____
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

[ ] A check in the amount of the fee is enclosed.

[ ] Payment by credit card. Form PTO-2038 is attached.

[✓] The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 502436.

[✓] Payment made via EFS-Web.

[ ] A petition for an extension of time under 37 CFR 1.136(a) (PTO/AIA/22 or equivalent) is enclosed.
For extensions of time in reexamination proceedings, see 37 CFR 1.550.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

[ ] applicant

[✓] attorney or agent of record
Registration number 39,450

[ ] attorney or agent acting under 37 CFR 1.34
Registration number _____

Signature: / joe zheng /

Typed or printed name: Joe Zheng

Telephone Number: (408)777-8873 or (408)891-9381

Date: 09/12/2018

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

[✓] * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.20(b)(1) and 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: AP.PRE.REQ

PTO/AIA/33 (03-13)
Approved for use through 07/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): RFID-084

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]
on 9/12/2018

Signature / joe zheng /

Typed or printed name Joe Zheng

Application Number	Filed
13/782,948	03/01/2013

First Named Inventor: Xiangzhen Xie

Art Unit	Examiner
3685	Isidora I. Immanuel

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 39,450.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/ joe zheng /
Signature

Joe Zheng
Typed or printed name

(408)777-8873
Telephone number

9/12/2018
Date

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of One forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

Mail Stop: APPEAL

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Pre-Appeal Brief Request for Review

Dear Sir:

Claims 1-19 are currently pending. In the final Office Action dated 06/12/2018,

A. Claims 1-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement.

B. Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention;

C. Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vayssiere (2006/00657 41) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker").

The Appellant respectfully disagrees with the Examiner on these rejections.

1. **Arguments with respect to Issue A**:

On Page 4, in Section 14, the Examiner alleges "Neither the drawings nor the specification provide a display screen that shows a list of cards or written description for displaying a list of cards on the mobile device". At the very first, Para [0001] states "*the present*

Samsung Ex. 1016, Page 328 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

invention is related to a mobile device configured to support multiple cards (e.g., Mifare) or applications of similar type". Para [0057] describes a mechanism (UI) to show multiple cards (applications), see "The readonly wallet UI 116 provides an interface to ...". Further, Para [0060] describes "providing a set of APIs so that a wallet application (e.g., simulating a Mifare card), when instructed by an user, can be caused to swap (i.e., activate on an emulator) an application in and out ...". Since a user initiates the swapping (changing from one card to another), the user has to see what is being swapped. Accordingly, it is believed that the rejection under 35 USC § 112 is erroneous.

On Page 4, in Section 15, the Examiner alleges "The specification does not provide for an algorithm that gives "a processor", or non-human entity the ability or operation to cause an application "to be loaded into the emulator to replace the one of the applications ...". The Appellant respectfully argues that the Examiner has either misread or mischaracterized Claim 1 as Claim 1 recites "causing the second application loaded into the emulator ... ", because "anything" including human intervention can "cause" the recited act to happen. The Appellant respectfully challenges the Examiner to show where in Claim 1 or 12 that an algorithm or non-human entity is required to control the operation. The Appellant submits the rejection under 35 USC § 112 is erroneous.

On Page 4, in Section 15, the Examiner alleges further "The specification does not provide support for the limitation "after the server determines that the secure element is registered therewith ... ". The Appellant believes that the Examiner has misunderstood the invention or is confused with the technical aspects of the operation. It is well known in the art that a secure element has to be verified first by a server before the server can do any anything with the secure element. In Claim 13, it recites "*sending device information of the secure element in responding to a request from the designated server after the server determines that the secure element is registered therewith* ". There is nothing wrong in the operation by itself in the art. Accordingly, withdrawal of the rejection under 35 USC § 112 is respectfully requested.

2. **Arguments with respect to Issue B**:

On Page 6, Section 20, the Examiner asks whether the device refers to a secure element that stores the applications in reference to Claim 1. The claim itself explicitly recites "*a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards*". Paragraph [0070] clearly describes a persistent storage device and the need for it. The Appellant is wondering why the Examiner raises this question by interpreting the

Samsung Ex. 1016, Page 329 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

storage device as a secure element in the mobile device, a secured memory space or something else. The Appellant has to conclude that the Examiner has not reviewed the Specification in detail or simply misunderstood what is being described. The rejection under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, shall be withdrawn.

On Page 7, Section 21, the Examiner asks how applications exist in the emulator to be executed when no applications are located nor have been received in or by the emulator. The Appellant respectfully points out that the Examiner has mischaracterized or simply misunderstands the claim. Claim 12 explicitly recites " *receiving [in] an emulator in the mobile device a first application corresponding to a first card*" and "*facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator ....* ", which states clearly the first application is loaded in the emulator. Accordingly, the rejection under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, shall be reversed.

On Page 7, Section 22, the Examiner states claims 1, 6, 7, 8 recite the following means plus functions and alleges that the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. The Appellant respectfully disagrees. Each of the cited names on Page 7 is a recognized term for a structure. They are introduced not for their internal structure but for what they do. Each of the claims 1, 6, 7, 8 recites a feature "by what it does rather than by what it is" (e.g., as evidenced by its specific structure or specific ingredients), See 2173.05(g). The specification and drawings provide sufficient description of "acts for performing the claimed function". Accordingly, the rejection under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, shall be reversed.

On Page 9, Section 24, the Examiner states Claim 1 is a hybrid claim as the cited language is not directed to the mobile device but to functions of claimed structural elements. The Appellant respectfully disagrees. There is nothing inherently wrong with defining some part of an invention in functional terms. Functional language does not, in and of itself, render a claim improper. Claim 1 is an apparatus claim reciting common elements uniquely combined to perform uniquely designed functions. A functional limitation is just like any other limitation of a claim, for what it fairly conveys to a person of ordinary skill in the pertinent art in the context in which it is used, defining a particular capability or purpose that is served by the recited element. Therefore, the apparatus claim is properly presented.

3. **Arguments with respect to Issue C**:

Samsung Ex. 1016, Page 330 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

On Page 12, In Section 21, the Examiner rejects Claims 1, 4, 6-9, 11, 12, 15-17 and 19 under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vayssiere and further in view of Wentker. The Appellant respectfully disagrees with the Examiner.

One of the purposes in the instant application is to emulate multiple cards in a mobile device to interact with an external reader. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality of applications controlled and managed by a designated (TSM) server, each of the applications pertaining to one of cards (e.g., Bank of America Visa, Chase Visa, and American Express). When a card is needed for payment, a user can select one of the cards available in the mobile device. A corresponding application is loaded into an emulator that turns the mobile device as the selected card. One of the additional features is that the data for the selected card can be accessed by the designated control (e.g., to lock or unlock the application or card, if there is a need).

In contrast, Davis teaches a payment system having a mobile device 204 **AND** a card reader 210 which accepts a smart card having a stored-value application. Even if the mobile device 204 and the card read card reader 210 were viewed as a single unit, the card reader 210 would only accept one card at a time, which immediately teaches away from "*storing a plurality of applications, each of the applications corresponding to one of the cards* " recited in Claim 1. Next, Davis does teach an emulator but the emulator is located in a OPAL server 260, which again teaches away from Claim 1 that recites the mobile device comprising: ... an emulator. In fact, there is no need for an emulator in Davis as Davis accommodates only one card in the card reader 210. Accordingly, Claim 1 shall be allowable over Davis.

On Page 13, the Examiner admits Davis does not teach a number of elements recited in Claim 1 and thus cites Vayssiere to show the teaching in combination. Vayssiere in fact teaches a smartcard having a dynamic display portion that changes when an application is switched. As described in [0038], Vayssiere explicitly describes that when the user completes the use [of] the smartcard as a calling card, Application 2 (410) terminates, and OS 406 activates Display Chooser application 422 again. First of all, Vayssiere is silent about "*the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications*". Even if the Examiner insists Vayssiere may imply the replacement action, the modification of David with Vayssiere would still not cure the deficiency of "*the data can only be modified by the designated server over a secured channel* " as the card itself in Vayssiere does not allow another device to remotely control an application therein. In fact, Vayssiere has no such need. Accordingly, the Appellant submits Claim 1 as amended shall be allowable over Davis and Vayssiere, viewed alone or in combination.

Samsung Ex. 1016, Page 331 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

On Page 14, the Examiner cites Wentker to show the teaching of an application unlocked by a server. The Appellant contests the combination of Davis, Vayssiere and Wentker as it is believed that there is no motivation to combine these three references in the manner proposed by the Examiner. Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. The functions of the smart card CANNOT be replaced by another application so that the smart card would function as a different card. To emulate a number of different cards, an emulator is needed. Wentker is completely silent about an emulator. In other words, Wentker neither teaches nor suggests a mobile device to emulate a plurality of cards. In a perspective, Wentker teaches away from Claim 1 by managing only one card via the provided APIs. Accordingly, the Appellant submits Claim 1 as amended shall be allowable over avis, Vayssiere and Wentker.

The patentability of the independent claims has been argued specifically as set forth above and thus Appellant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, the Appellant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

The undersigned can be reached at (408)777-8873 if there is a need to respond to any inquiry from the Panel.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", on Sept. 12, 2018

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Reg. No.: 39,450

Samsung Ex. 1016, Page 332 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Electronic Patent Application Fee Transmittal

Application Number:	13782948
Filing Date:	01-Mar-2013
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Filer:	Joe Zheng
Attorney Docket Number:	RFID-084

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
NOTICE OF APPEAL	2401	1	400	400
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**400**

Electronic Acknowledgement Receipt	
EFS ID:	33706077
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	12-SEP-2018
Filing Date:	01-MAR-2013
Time Stamp:	23:10:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$400
RAM confirmation Number	091318INTEFSW23125400
Deposit Account	502436
Authorized User	Joe Zheng
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	NoticeOfAppeal.pdf	233840 d645e73a595f1f7aac4e2f8239aa4bf41590dd10	no	2
Warnings:					
Information:					
2	Pre-Brief Conference request	PreAppealBriefRequest.pdf	226812 b51c5a8eb8cfce1f94180b472fde44a1ff5e8930	no	6
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30394 b9e6be75670769b3f3b060bde8f3f08275e2dc63	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	491046		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 11/14/2018

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
11/14/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Notice of Panel Decision from Pre-Appeal Brief Review

Application No.	Applicant(s)		
13/782,948	Xie et al.		
Examiner	**Art Unit**	**AIA Status**	
ISIDORA I IMMANUEL	3685	No	

This is in response to the Pre-Appeal Brief Request for Review filed 12 September 2018 .

1. ☐ **Improper Request** - The Request is improper and a conference will not be held for the following reason(s):

☐ The Notice of Appeal has not been filed concurrent with the Pre-Appeal Brief Request.
☐ The request does not include reasons why a review is appropriate.
☐ A proposed amendment is included with the Pre-Appeal Brief request.
☐ Other: _____ .

The time period for filing a response continues to run from the receipt date of the Notice of Appeal or from the mail date of the last Office communication, if no Notice of Appeal has been received.

2. ☐ **Proceed to Board of Patent Appeals and Interferences** - A Pre-Appeal Brief conference has been held. The application remains under appeal because there is at least one actual issue for appeal. Applicant is required to submit an appeal brief in accordance with 37 CFR 41.37. The time period for filing an appeal brief will be reset to be one month from mailing this decision, or the balance of the two-month time period running from the receipt of the notice of appeal, whichever is greater. Further, the time period for filing of the appeal brief is extendible under 37 CFR 1.136 based upon the mail date of this decision or the receipt date of the notice of appeal, as applicable.

☐ The panel has determined the status of the claim(s) is as follows:
Claim(s) allowed: _____ .
Claim(s) objected to: _____ .
Claim(s) rejected: _____ .
Claim(s) withdrawn from consideration: _____ .

3. ☐ **Allowable application** - A conference has been held. The rejection is withdrawn and a Notice of Allowance will be mailed. Prosecution on the merits remains closed. No further action is required by applicant at this time.

4. ☑ **Reopen Prosecution** - A conference has been held. The rejection is withdrawn and a new Office action will be mailed. No further action is required by applicant at this time.

All participants:

(1) ISIDORA I IMMANUEL .	(3) Traci Casler .
(2) Neha Patel .	(4) _____ .

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685	/TRACI CASLER/ RQAS, OPQA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 04/18/2019

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
04/18/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Samsung Ex. 1016, Page 339 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Office Action Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 01/09/2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-19 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-19 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 01/09/2018.

2. Claims 1, 2, 4-13, and 17-19 amended.

3. Claims 1-19 are pending.

4. Claims 1-19 have been examined.

Notice of Pre-AIA or AIA Status

5. The present application is being examined under the pre-AIA first to invent provisions.

Claim Objections

6. Claim 12 is objected to because of the following informalities: the claim recites "receiving an emulator in the mobile device a first application…." Appropriate correction is required.

Response to Arguments

7. Applicant's arguments filed 01/09/2018 have been fully considered.

8. 112

9. The prior 112(a) rejections have been withdrawn.

10. 103

11. Applicant argues Davis teaches an emulator but it is located in the Opal server. Although Davis does not explicitly place an emulator within the client terminal, Davis does claim the client terminal is capable of emulation, stating "alternatively, **the**

emulation of the card commands can be done by the payment server using the terminal as a card reader, or **may even be performed by client terminal 204.**" (column 8, line 49-52). Davis's client terminal is capable of emulation of the cards, hence the combination with Vitikainen to explicitly teach an emulator.

12. Applicant also argues Vayssiere is silent about "the first application is replaceable in entirety or in part by a second application". Examiner disagrees. Vayssiere states- The smartcard, in one embodiment, may be loaded with multiple applications … When used for a particular application (e.g., as a payphone calling card), the smartcard is first powered through the interface with a smartcard reader, …With the proper display data retrieved, the dynamic display portion is changed or updated with the image associated with the application(Abstract; ¶ 26, 30, 42, 43).

13. Applicant then argues neither Davis nor Vayssiere teach "the data can only be modified by the designated _server over a secured channel". Examiner disagrees. Davis states - the consumer is able to download value from bank server 860 onto his virtual card. OPAL server 260 communicates with load server 862 to receive authorization for the load and for higher security. The virtual card may then be used to make purchases over the Internet as described above. Once the bank has downloaded value to the virtual card, a corresponding amount of funds is transferred from the bank to card issuer 108. Additionally, the same consumer account at the bank can be used to fund multiple OPAL accounts. **Preferably card 5 includes any number of keys known to the card issuer** that are used during the course of a payment or load transaction to generate signatures for validation of the stored value card, validation of the security card or module, and validation of the system itself. HSM **268** would include

not only cryptographic keys normally held within OPAL server, but also the issuer keys normally held within HSM **864**. (Alternatively, HSM **268**may hold only a master key, while all other keys are passed from an encrypted database.) (column 6, line 60-67, column 7, line 31-38, column 8, line 53-59, column 28, line 20-50, column 29, line 50-65, column 33, line 48-64).

14. Applicant argues against the combination of the prior art including Wentker, citing "to emulate a number of different card, an emulator is needed." Davis teaches emulation is maybe done by the client terminal and Vitikainen explicitly teaches an emulator. Wentker teaches "delegated management of smart card applications… The card issuer empowers application providers to initiate changes to the issuer's smart cards"(Abstract). Furthermore, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Interpretation

15. The following is a quotation of 35 U.S.C. 112(f):

> (f) Element in Claim for a Combination. – An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

16. This application includes one or more claim limitations that do not use the word "means," but are nonetheless being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because the claim limitation(s) uses a generic placeholder that is coupled with functional language without reciting sufficient structure to perform the recited function and the generic placeholder is not preceded by a structural modifier. Such claim limitation(s) is/are:

a. storage device for storing (claim 1)

b. an emulator… for receiving (claim 1)

c. communication interface to facilitate data exchange (claim 1)

d. Module configured to provide… to store (claim 6)

e. Card manager proxy for facilitating (claim 7)

f. user interface application provided to query (claim 7)

g. UI application for conducting (claim 7)

h. Interfaces…to read (claim 8)

i. TMSM module is configured to (claim 8)

j. Mechanism to make …for storing (claim 8)

Because this/these claim limitation(s) is/are being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, it/they is/are being interpreted to cover the corresponding structure described in the specification as performing the claimed function, and equivalents thereof.

If applicant does not intend to have this/these limitation(s) interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, applicant may: (1) amend the

claim limitation(s) to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph (e.g., by reciting sufficient structure to perform the claimed function); or (2) present a sufficient showing that the claim limitation(s) recite(s) sufficient structure to perform the claimed function so as to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph.

Claim Rejections - 35 USC § 112

17. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

18. Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

19. As per claims 1, 6, 7, 8 the claims recite the following means plus functions limitations:

k. storage device for storing (claim 1)

l. an emulator… for receiving (claim 1)

m. communication interface to facilitate data exchange (claim 1)

n. Module configured to provide… to store (claim 6)

o. Card manager proxy for facilitating (claim 7)

p. user interface application provided to query (claim 7)

q. UI application for conducting (claim 7)

r. Interfaces…to read (claim 8)

s. TMSM module is configured to (claim 8)

t. Mechanism to make …for storing (claim 8)

20. This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112(f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112,paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for," "apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f)or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d 1344, 1354,80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206,

1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56, 57, 59-61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56, 57, 61, 75, 76 describe the module interchangeable with software modules, applications and applets but there is no indication of what structure is used. ¶ 59 describes the "card manager proxy" as a "software module". ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards" but there is no indication of what structure is used. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-11 are rejected.

21. Claim 1 recites "and the first applications being executed…", there are no previous first applications that were executed, claim 19 recites the limitation "the portable device", similarly, claims 7, and 16 recite the limitation "the TMSM module", claim 8 recites "TSM server", claim 12, "the first cards offered", there is no recitation for offering cards, claim 16 recites the TMSM module", and "TSM server" There is

insufficient antecedent basis for this limitation in the claim. Dependent claims 2-11 and 13-19 are rejected as each depends on rejected claims 1 and 12, respectively.

22. Claim 1 recites "application is unlocked by the designated server", claim 2 recites "after the designated server determines that the secure element…," and claim 11 recites "applications has been remotely provisioned by the designated server with operations of: receiving… establishing... preparing... notifying..." A designated server is not recited as an element of the mobile device of independent claim 1, but claims 1, 2 and 11 claim the functions of a designated server. The scope of the claims are unclear as to whether the designated server is part of the claimed mobile device. Dependent claims 2-11 are rejected.

23. Claim 16 recites "querying via a user interface (UI) one or more of the applications in detail…" The term "in detail" in claim 16 is a relative term which renders the claim indefinite. The term "in detail" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

24. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

25. Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vitikainen et al. (2006/0052080) ("Vitikainen"), in view of Vayssiere (2006/0065741) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker").

26. Regarding claims 1 and 12, Davis teaches a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided by a module downloaded from a designated server (Figure 5; column 6, line 47-49, column 7, line 45-51, column 9, line 2-13, column 13, line 62-67, column 14, line 1-7, column 28, line 39-46, column 29, line 32-36);

- Davis states - client terminal 204 may also be embodied in any portable device such as a laptop computer, a cellular telephone…Local cardholder functions including a consumer card interface, display and accept/ cancel options are performed at client terminal 204. A security card also stores signature algorithms for all Smart cards in use. A security card may also contain a transaction identifier for the current transaction, a financial Sum of all transactions remaining to be settled, a session key, and master keys for all Smart cards in use. At this point a load amount screen is presented to the user. The funding account number, expiration date, the virtual card number, maximum load amount and current balance of the virtual card are displayed and the user is directed to enter the value to be loaded onto the card. (column 6, line 47-49, column 7, line 45-51column 9, line 2-13, column 29, line 32-36)

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated _server over a secured channel (column 6, line 60-67, column 7, line 31-38, column 8, line 53-59, column 28, line 20-50, column 29, line 50-65, column 33, line 48-64);

- Davis states - the consumer is able to download value from bank server 860 onto his virtual card. OPAL server 260 communicates with load server 862 to receive authorization for the load and for higher security. The virtual card may then be used to make purchases over the Internet as described above. Once the bank has downloaded value to the virtual card, a corresponding amount of funds is transferred from the bank to card issuer 108. Additionally, the same consumer account at the bank can be used to fund multiple OPAL accounts. Preferably card 5 includes any number of keys known to the card issuer that are used during the course of a payment or load transaction to generate signatures for validation of the stored value card, validation of the security card or module, and validation of the system itself. (column 7, line 31-38, column 28, line 41-50)

a communication interface to facilitate data exchange wirelessly between a reader and wherein the reader is external to the mobile device, (Abstract; Figure 2; column 7, line 52-67, column 8, line 49-52, column 10, line 10-14, 57-60, column 25, line 6-13, column 29, line 23-31; claim 1, 22); and

- Davis states - Concurrently, or at a later date when smart cards and readers are more common, system **250** is then easily upgradeable to make use of the physical card and reader attached to client terminal **204**. Client terminal 204 includes client code module 224 and card reader module 226. Reader module 226 may be implemented using any Suitable software and libraries for communicating with card reader 210 and its actual implementation will depend upon the type of card reader used. Client module 224 controls communication between the client terminal, the card reader, Client code module 224 is now functionally part of OPAL server 260 instead of being part of client terminal 204. Further, the functionality of card reader module 226 of FIG. 2 is now included within client code module 224 to allow communication with pseudo card reader module 264. (column 7, line 52-67, column 10, line 10-14,)

a processor, in communication and the storage device (column 7, line 45-51, column 10, line 33-60, column 25, line 6-13, column 29, line 23-31; column 34, line 21-23, claim 1, 22);

- Davis states - client terminal 204 may also be embodied in any portable device such as a laptop computer, a cellular telephone (including GSM tele phones), or any variety of a personal digital assistant (PDA). Processor(s) **922** (also referred to as central processing units, or CPUs) are coupled to storage devices including memory **924**. (column 7, line 45-51, column 34, line 21-23)

Davis does not teach an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the

applications; into the emulator; the first applications being executed in the emulator, performing an operation of causing the second applications loaded to replace the first applications when the second card is selected via the display screen and the second application is unlocked by the designated server, wherein said causing the second application loaded to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server, and the first application in the emulator is replaceable in entirety or in part by a second application: corresponding to a second card and wherein functions of the mobile device related the first card offered by the first application are changed to functions offered by the second application related to the second cards when the second applications is activated and executed.

Vitikainen teaches an emulator, coupled to the storage, for receiving a first application corresponding to user information, the first application being one of the applications; into the emulator, in the emulator the first applications being executed in the emulator, (¶ 85, 86, 88; claim 16)

- Vitikainen states - the emulator **50** comprises a CPU **51**, which is connected to each of a voice UI **52**, a graphical user interface (GUI) **53**, a voice UI profile storage device **54**, an application storage device **55** and an emulator software storage device **56**. Of course, the storage devices **55**, **54**and **56** could form part of the same physical device, the application is loaded into the

application storage device **55** at step **62**. the modified application tested using the emulator apparatus **50** (¶ 85, 86, 88)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis and Vitikainen in order to determine whether an application is compatible with a mobile device in order to refrain from using inappropriate features (Vitikainen; ¶ 1-3).

Vayssiere teaches performing an operation of causing the second applications loaded to replace the first applications (¶ 22, 35, 37, 38, 41, 43),

- Vayssiere states-When the reader of the public phone detects the smartcard, OS **406** first activates Display Chooser application **422**. OS **406** sends to Display Chooser application **422** a command that indicates "Application 2 (**410**) is to be activated next." In one method, Application **2** (**610**) sends complete pictures to Display Chooser application **618**, which then updates the dynamic display portion similar to that of an image obtained from Display Data **620**. In an alternative method, Application **2** (**610**) may send text which is displayed line by line to generate a complete image. (¶ 37, 41)

wherein said causing the second application loaded to replace the first application fails when the second card is selected via the display screen and wherein functions of the mobile device related the first card offered by the first application are changed to

functions offered by the second application related to the second cards when the second applications is activated and executed(¶ 22, 26, 30, 31, 33, 35-39, 41, 43),

- Vayssiere states- In particular, OS **306** is responsible for the isolation of the different applications, i.e., making sure that the applications stored on the smartcard do not engage in cross-talk or read, write, modify, or delete data from each other. With multi-application features for smartcard **200**, one physical appearance is associated with each application stored on the smartcard **200**, and that particular physical appearance could automatically change depending on the context in which smartcard **200** is used. (¶ 26, 33)

and the first application is replaceable in entirety or in part by a second application: corresponding to a second card (Abstract; ¶ 26, 30, 42, 43).

- Vayssiere states- The smartcard, in one embodiment, may be loaded with multiple applications … When used for a particular application (e.g., as a payphone calling card), the smartcard is first powered through the interface with a smartcard reader, …With the proper display data retrieved, the dynamic display portion is changed or updated with the image associated with the application,(¶ 42, 43)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis Vitikainen and Vayssiere in order to provide a smartcard to perform multiple functions (Vayssiere; ¶ 3).

Wentker teaches when the second card is selected via the display screen and the second application is unlocked by the designated server but the second application is locked by the designated server (Figure 5; column 9, line 34-44, column 10, line 31-44, column 16, line 11-24, column 17, line 4-20).

- Wentker states - Card Manager (CM) Locked state 210 is used to tell card manager 104 to temporarily disable all applications on the card except for the card manager. This State provides the issuer with the ability to detect security threats either internal or external to the card and to be able to temporarily disable the functionality of the card. While in this state, there is an option to determine that the threat is either no longer present or is of limited Severity Such that the issuer can reset the card to the normal operating State of Secured. (column 9, line 34-44)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

27. Regarding claim 4, Davis teaches wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction (column 25, line 6-13), the mobile device is used to emulate each of the cards when a corresponding applications is loaded into and executed in the emulator (column 7, line 39-67).

28. Regarding claims 6 and 15, Neither Davis, Vitikainen nor Vayssiere teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along

with a plurality of key indexes, each of the service objects corresponding to one of the applications. Wentker teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications (column 9, line 1-33, column 13, line 11-39, column 14, line 24-43, column 21, line 17-31). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

29. Regarding claims 7 and 16, Davis teaches a user interface (UI) (column 10, line 10-32). Wentker teaches wherein the mobile device further includes a card manager proxy for facilitating communication between the designated server and the TMSM module in the secure element, interface application provided to query one or more of the applications on information stored therein but not to modify the information (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications (column 10, line 8-56). Wentker does not teach a user interface (UI). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

30. Regarding claim 8, Davis teaches to the emulator (Abstract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere and later on swapping another one of the applications (¶ 35). Wentker teaches provide a set of Application Programming

Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator (column 6, line 36-55, column 7, line 1-7, column 8, line 17-32); provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom (column 6, line 36-55, column 8, line 17-32); enable the designated server to remotely provision each of the applications by installing application keys and application data to the TMSM module (column 7, line 15-37, column 16, line 3-23, column 17, line 21-35, column 22, line 17-31) enable the TSM server to manage each of the applications by locking or unlocking one of the applications (column 7, line 1-7, column 9, line 34-44, column 10, line 24-44); provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module (column 22, line 51-67, column 23, line 1-24).

31. Regarding claims 9 and 17, Wentker teaches wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element (column 7, line 38-56, column 13, line 11-39, column 19, line 1-8).

32. Regarding claims 11 and 19, Wentker teaches receiving a request to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider (column 7, line 15-37, column 8, line 1-10, column 14, line 24-43, column 15, line 1-19, column 16, line 25-35, 49-67, column 17,

line 21-35); establishing a secured channel between the mobile device and the designated server using a set of keys (column 7, line 15-37, column 10, line 15-23, column 13, line 11-39, column 15, line 52-67, receiving data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67); and notifying the application provider of a status of the application with the mobile device (column 12, line 58-67, column 13, line 1-10, column 17, line 4-20, column 18, line 62-67, column 19, line 44-46).

33. Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vitikainen et al. (2006/0052080) ("Vitikainen"), in view of Vayssiere (2006/0065741) ("Vayssiere"), in view of Wentker et al. (6,481,632) ("Wentker") and further in view of De Groot (2006/0141987) ("Groot").

34. Regarding claims 2 and 13, Neither Davis, Vitikainen nor Vayssiere teaches initiating data communication by the mobile device with the designated server; sending device information of the secure element from the mobile device in responding to a request from the designated server after the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent

transaction between the mobile device and a service provider and a designated server providing trusted service management. Wentker teaches and with designated server providing trusted service management (TSM) (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31). Groot teaches initiating data communication by the mobile device (¶ 36, 40, 44); sending device information of the secure element from the mobile device in responding to a request from the designated server after the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (¶ 30, 34, 36, 37, 39, 40, 43, 47, 48, 53); receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider (Figure 1, element M1-3; ¶ 30, 31, 34, 40-45, 47-49, 53). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere, Wentker, and Groot in order to provide secure transmissions with a terminal and a server using an identifier (Groot; ¶ 1-7).

35. Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vitikainen et al. (2006/0052080) ("Vitikainen"), in view of Vayssiere (2006/0065741) ("Vayssiere"), in view of Wentker et al. (6,481,632) ("Wentker") and further in view of Huomo et al. (8,005,426) ("Huomo").

36. Regarding claims 3 and 14, Davis teaches the emulator (Abs-tract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere teaches implemented in the secure element (¶ 22, 23, 30). Neither Davis, Vitikainen nor Vayssiere teaches the secure element is enclosed in the mobile device or in a detachable card to the mobile device. Huomo teaches the secure element is enclosed in the mobile device or in a detachable card to the mobile device (column 8, line 3-23). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Huomo in order to provide transactions with mobile devices equipped with a smartcard (Huomo; column 1, line 7-23, 54-67).

37. Regarding claim 5, Huomo teaches wherein at least one of the cards is a contactless card (column 2, line 27-61, column 8, line 3-37).

38. Regarding claims 10 and 18, Huomo teaches wherein the mobile device is a smartphone, or a portable computer (column 16, line 26-36, 43-67, column 17, line 1-5).

Conclusion

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUELEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ISIDORA I IMMANUEL/
Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination Xie et al.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	6,481,632 B2	11-2002	Wentker; David C.	G06F8/60	235/376
*	B	2006/0065741 A1	03-2006	Vayssiere; Julien JP.	G06K19/07703	235/492
*	C	2006/0141987 A1	06-2006	De Groot; Max	H04L63/0414	455/411
*	D	US-20060052080-A1	03-2006	Vitikainen; Timo	G10L15/30	455/403
*	E	7,908,216 B1	03-2011	Davis; Virgil M.	G06Q20/02	705/41
*	F	8,005,426 B2	08-2011	Huomo; Heikki	G06Q20/20	235/441
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016	09/17/2017	05/22/2018	04/15/2019				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	✓				
	5	✓	✓	✓	✓	✓				
	6	✓	✓	✓	✓	✓				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	✓				
	15	✓	✓	✓	✓	✓				
	16	✓	✓	✓	✓	✓				
	17	✓	✓	✓	✓	✓				
	18	✓	✓	✓	✓	✓				
	19	✓	✓	✓	✓	✓				

Samsung Ex. 1016, Page 363 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

CPC - Searched*		
Symbol	Date	Examiner
G06Q	2/1/2016	II

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
705			

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See attached notes	2/1/2016	II
101 withdrawal - Weinhart	06/06/2018	III
See attached notes (EAST)	04/15/2019	III

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/I.I./ Examiner.Art Unit 3685

Samsung Ex. 1016, Page 364 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(2006/0052080).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/15 08:09
L2	3	("20060052080").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/04/15 08:09
S1	635	(emulat$4 near4 application) with card	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/14 19:12
S2	635	(emulat$4 near4 application) with card	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 02:18
S3	65	(emulat$4 with application near3 (run or running or execut$4)) and S2 and (mobile adj device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 02:18
S4	150	(emulat$4 with application near3 (run or running or execut$4)) and S2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 02:20
S5	8	(online adj purchase adj load adj4 (device or comput$4 or mobile or phone or machine or server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 04:13
S6	8	(online adj2 purchase adj2 load adj4 (device or comput$4 or mobile or phone or machine or server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 04:14
S7	146	(((online adj2 purchase adj2 load) or opal)adj4 (device or comput$4 or mobile or phone or machine or server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 04:15
S8	8	((online adj2 purchase adj2 load) adj4 (device or comput$4 or mobile or phone or machine or server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 04:15
S9	146	((opal)adj4 (device or comput$4 or mobile or phone or machine or server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 04:16
S10	8	S9 and (online adj2 purchase adj2 load)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/04/15 04:16

Samsung Ex. 1016, Page 365 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

4/15/2019 8:10:20 AM
C:\Users\iimmanuel\Documents\EAST\Workspaces\13782948.wsp

Electronic Patent Application Fee Transmittal

Application Number:	13782948
Filing Date:	01-Mar-2013
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Filer:	Joe Zheng
Attorney Docket Number:	RFID-084

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	2252	1	300	300
Miscellaneous:				
		Total in USD ($)		**300**

Electronic Acknowledgement Receipt	
EFS ID:	37205525
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	18-SEP-2019
Filing Date:	01-MAR-2013
Time Stamp:	17:25:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$300
RAM confirmation Number	E20199HH25350382
Deposit Account	502436
Authorized User	Joe Zheng
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ResponseTo1stOAAfter2ndAppeal.pdf	170506 611b85e5f4f7c84593fdfa7bbb4982f632c54114	no	15
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30324 8df0bec435d643fdae62ece70a91d31e339b27c9	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	200830		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

Sept. 15, 2019

Mail Stop: No-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to First OA after 2nd Appeal

Dear Sir:

In response to Office Action dated 04/18/2019, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begins on page 2 of this Response.

REMARKS/ARGUMENTS begin on page 9 of this Response.

Samsung Ex. 1016, Page 371 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

Please amend Claims 1-2, 7-8, 11-12, 16 and 19 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided ~~by a module downloaded from~~ via a designated server;

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;

an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications;

a communication interface to facilitate data exchange wirelessly between a reader and the first application being executed in the emulator, wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card; and

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen ~~and~~ when the second application is unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server, and wherein

functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related

Samsung Ex. 1016, Page 372 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

to the second card when the second application is activated and executed in the emulator.

2. (*Currently amended*) The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the designated server ~~after~~ when the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

Samsung Ex. 1016, Page 373 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

6. (*Previously amended*) The mobile device as recited in claim 3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Currently amended*) The mobile device as recited in claim 6, wherein the mobile device further includes:

   a card manager proxy for facilitating communication between the designated server and the ~~TMSM~~ module in the secure element,

   a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

   a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications.

8. (*Currently amended*) The mobile device as recited in claim 6, wherein the ~~TMSM~~ module is configured to:

   provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

   provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

   enable the ~~TSM~~ designated server to remotely provision each of the applications by installing application keys and application data to the ~~TMSM~~ module and later on swapping another one of the applications to the emulator;

   enable the designated server to manage each of the applications by locking or unlocking one of the applications;

Samsung Ex. 1016, Page 374 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Previously amended*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone or a portable computer.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the designated server with operations of:

~~receiving~~ sending a request from the mobile device to the designated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider;

establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server;

receiving data for the application being provisioned from the designated server, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

Samsung Ex. 1016, Page 375 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

installing in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards;

showing a list of the cards on a display of the mobile device for a user to choose one therefrom, wherein the display is provided by a module downloaded from the designated server and executed in the mobile device;

receiving in an emulator of the mobile device a first application corresponding to a first card;

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card;

causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second cards when the second application is activated and executed in the emulator.

13. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

Samsung Ex. 1016, Page 376 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

sending device information of the secure element in responding to a request from the designated server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Currently amended*) The mobile device as recited in claim 15, further comprising facilitating communication between the ~~TSM~~ designated server and the ~~TMSM~~ module configured to provide (TMSM) in the secure element;

querying via a user interface (UI) one or more of the applications ~~in detail~~; and

conducting operations that modify one or more sectors in one or more of the applications.

17. (*Previously amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information

Samsung Ex. 1016, Page 377 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

updatable entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Currently amended*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the designated server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the ~~portable~~ mobile device.

Samsung Ex. 1016, Page 378 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

REMARKS

Claims 1 - 19 were examined again. In the Office Action dated 04/18/2019, Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention, Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis") in view of Vitikainen et al. (2006/0052080) ("Vitikainen") in view of Vayssiere (2006/0065741) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker"), Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere in view of Wentker and further in view of De Groot (2006/0141987) ("Groot"), and Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere inview of Wentker and further in view of Huomo et al. (8,005,426) ("Huomo").

In the foregoing amendments, Claims 1-2, 7-8, 11-12, 16 and 19 have been amended to correct some informalities. No new matters are introduced. Claims 1-19 are still pending.

Claim Objections

On page 2, Section 6, of the Office Action, the Examiner objects to Claim 12. In the foregoing amendments, Claim 12 has been amended. It is believed that the claim objections shall be withdrawn.

Re: Examiner's Comments

On page 2, Section 11, the Examiner argues, although Davis does not explicitly place an emulator within the client terminal, Davis does claim the client terminal is capable of emulation, stating "alternatively, the emulation of the card commands can be done by the payment server using the terminal as a card reader, or may even be performed by client terminal 204." (column 8, line 49-52). The

Samsung Ex. 1016, Page 379 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Applicant respectfully points out that the Examiner has mischaracterized Davis. As described in column 8, line 49-52, David explicitly teaches the **emulation of the card commands**. Conceptually, the Examiner is mistaken "emulation of the card commands" with an emulator in a mobile device, one being receiving the card commands and the other being a particular processor. These are two very different concepts.

On page 3, Section 12, the Examiner argues that Vayssiere states "The smartcard, in one embodiment, may be loaded with multiple applications ... When used for a particular application (e.g., as a payphone calling card), the smartcard is first powered through the interface with a smartcard reader, ... With the proper display data retrieved, the dynamic display portion is changed or updated with the image associated with the application (Abstract; ~ 26, 30, 42, 43). It appears that the Examiner misunderstands Claim 1 of the instant application or mischaracterizes Vayssiere. Claim 1 recites "*causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen and the second application is unlocked by the designated server*". There is a subtle difference between an emulator and a microprocessor. FIG. 1C of the instant application explicitly shows the use of a processor or microprocessor 135. One of the important features in the instant application is the use of an emulator that functions solely as a first type of card when a first application is running therein and functions solely as a second type of card when a second application is running therein. The first application and the second application DO NOT co-exist in the emulator. In other words, the first application is replaced by the second application when the second type of card is selected. Vayssiere is silent about "the first application is replaceable in entirety or in part by the second application" because Vayssiere teaches a multi-application smartcard, each of the loaded applications can be executed by a microprocessor, there is no need to replace one application with another in the microprocessor.

Claim Rejections - 35 USC § 112

Samsung Ex. 1016, Page 380 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

On page 8, Section 21, of the Office Action, the Examiner lists some examples of claims that are lack of antecedent basis. For example, Claim 1 recites "and the first applications being executed ... ", there are no previous first applications that were executed. The Applicant wishes to refer the Examiner to Claim 1 that does not seem to use “the first applications”, accordingly there are no previous first applications that were executed. Should the Examiner question “the first application”, “*an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications*;” is used first.

Claim Rejections - 35 USC § 112

On Page 11 Section 34, of this Office Action, Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

In the foregoing amendments, Claims 1-2, 7-8, 11-12, 16 and 19 have been amended. It is believed that most of the claim rejections under 35 U.S.C. 112 shall have been overcome.

Claim Rejections - 35 USC § 103

On Page 10, Section 25, of this Office Action, Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere and further in view of Wentker. The Applicant respectfully traverses the rejections of Claims 1, 4, 6-9, 11, 12, 15-17 and 19 under pre-AIA 35 U.S.C. 103(a).

In the Pre-Appeal Brief Request for Review dated Sept. 12, 2018, the Applicant presents the arguments why the combination Davis, Vayssiere and Wentker does not render Claim 1 obvious. The Applicant appreciates the Examiner for returning the instant application to prosecution. In the This Office Action, the Examiner adds another reference Vitikainen to show the teaching and rejects Claims 1, 4, 6-9, 11, 12, 15-17 and 19 under pre-AIA 35 U.S.C. 103(a).

Samsung Ex. 1016, Page 381 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

As previously reasoned, one of the purposes in the instant application is to emulate multiple cards using an emulator in a mobile device to interact with an external reader. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality of applications controlled and managed by a designated (TSM) server, each of the applications pertaining to one of cards (e.g., Bank of America Visa, Chase Visa, and American Express). When a card is needed for payment, a user can select one of the cards available in the mobile device. A corresponding application is loaded into the emulator that turns the mobile device as the corresponding selected card. The loaded application is replaced in part or entirety with another application when another card is selected. One of the additional features is that the data for a selected card is accessed and controlled by a designated server (e.g., to lock or unlock an application or card, if there is a need).

In contrast, Davis teaches a payment system having a mobile device 204 **AND** a card reader 210 which accepts a smart card having a stored-value application. Even if the mobile device 204 and the card reader 210 were viewed as a single unit, the card reader 210 would only accept one card at a time, which immediately teaches away from "*storing a plurality of applications, each of the applications corresponding to one of the cards*" recited in Claim 1. Next, Davis does teach an emulator but the emulator is located in an OPAL server 260, which again teaches away from Claim 1 reciting “the mobile device comprising: ... an emulator”. In fact, there is no need for an emulator in the mobile device 204 in Davis as Davis accommodates only one card in the card reader 210. Accordingly, Claim 1 shall be allowable over Davis.

On Pages 12-13 of this Office Action, the Examiner admits Davis does not teach a number of elements recited in Claim 1 and thus cites Vitikainen (a new reference) to show the teaching in combination. The Applicant respectfully contests the combination of Davis and Vitikainen as it is believed that there is no motivation to combine these two references in the manner proposed by the Examiner. In order to establish a *prima facie* case of obviousness under 35 USC 103, *Graham v. John Deer Co. of Kansas City*, 383 US 1 (1966) requires determining, respectively, the scope and content of the prior art, the difference between the prior art and the claims

Samsung Ex. 1016, Page 382 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

at issue, and the level of ordinary skilled in the art. Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning, to support the legal conclusion of obviousness. *KSR v. Teleflex*, No. 04-1350 (US Apr. 30, 2007) (citing In re Kahn, 441 F. 3d 977, 988 (Canada Fed. 2006)). The suggestion to make the claim combination must be found in the prior art, not in the Applicant's disclosure. In re Vaek, 20 USPQ2d 1438 (Fed. Cir. 1991). Moreover, in accordance with MPEP 2142.02, each prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L.Gore & Associates Inc. v. Garlock, Inc.* 220 USPQ 303 (Fed. Cir. 1993). A third essential requirement for establishing a *prima facie* case, set forth in MPEP 2143.01 is that the proposed modification cannot render the prior art unsatisfactory for its intended purpose.

Vitikainen teaches a mobile device having voice user interface used to test the compatibility of an application with the mobile device. Vitikainen has nothing to do with or is remotely related to mobile payments. As shown in FIG. 2, Vitikainen explicitly teaches that an application is downloaded to a terminal device 11 for testing in the terminal device, which clearly teaches away from "[a mobile device comprising] *a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards*". As Vitikainen is in the subject of testing an application in a mobile device, it is impractical for Vitikainen to pre-store all the applications in the mobile device. In contrast, the subject in the instant application is to run locally one of the stored applications so the mobile device functions as one of the cards (e.g., Visa card, American Express or Discovery). Accordingly, the Applicant submits Claim 1 as amended shall be allowable over Davis and Vitikainen, viewed along or in combination.

On Page 14 of this Office Action, the Examiner adds Vayssiere to show the teaching in combination with Davis and Vitikainen. The Applicant respectfully contests the combination of Davis, Vitikainen and Vayssiere as it is believed that there is no motivation to combine these three references in the manner proposed by the Examiner. Vayssiere teaches a smartcard having a dynamic display portion that

Samsung Ex. 1016, Page 383 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

changes when an application is switched. As described in [0038], Vayssiere explicitly describes that when the user completes the use [of] the smartcard as a calling card, Application 2 (410) terminates, and OS 406 activates Display Chooser application 422 again. As reasoned above, Vayssiere is silent about "*the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications*". In fact, Vayssiere has no such need. Accordingly, the Applicant submits Claim 1 as previously amended shall be allowable over Davis, Vitikainen and Vayssiere, viewed alone or in combination.

On Page 16, the Examiner cites Wentker to show the teaching of an application unlocked by a server. The Appellant again contests the combination of Davis, Vitikainen, Vayssiere and Wentker as it is believed that there is no motivation to combine these four references in the manner proposed by the Examiner. Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. The functions of the smart card CANNOT be replaced by another application so that the smart card would function as a different card. To emulate a number of different cards, an emulator is needed. Wentker is completely silent about an emulator. In other words, Wentker neither teaches nor suggests a mobile device to emulate a plurality of cards. In a perspective, Wentker teaches away from Claim 1 by managing only one card via the provided APIs. Accordingly, the Appellant submits Claim 1 as previously amended shall be allowable over Davis, Vitikainen, Vayssiere and Wentker. Reconsideration of Claims 1-11 is kindly requested.

Claim 12 was amended similarly to Claim 1. Without repeating the same, the Applicant wishes to rely upon the above arguments supporting Claim 1 to support Claim 12 and submits the combination of Davis, Vitikainen, Vayssiere and Wentker is improper. The combination of Davis, Vitikainen, Vayssiere and Wentker fails to suggest "*installing in a storage device of the mobile device a plurality of applications downloaded from a designated server*" (vs. one at a time in Vitikainen) and "*said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server*". Accordingly, the Appellant submits

Samsung Ex. 1016, Page 384 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Claim 12 as previously amended shall be allowable over Davis, Vitikainen, Vayssiere and Wentker. Reconsideration of Claims 12-19 is kindly requested.

The patentability of the independent claims has been argued specifically as set forth above and thus the Applicant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, Applicant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

In view of the above amendments and remark, the Applicant believes that Claims 1-19 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", Sept. 18, 2019. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng
Reg.: No. 39,450

Samsung Ex. 1016, Page 385 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/782,948	Filing Date 03/01/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $31 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $ 125 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	09/18/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 19	Minus	** 20	= 0		x $ 50 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $ 230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $ 0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $ 0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/ROCHELLE C. GETER/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 12/26/2019

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
12/26/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Office Action Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 09/18/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-19 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-19 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 09/18/2019.

2. Claims 1, 2, 7, 8, 11, 12, 16, and 19 amended.

3. Claims 1-19 are pending.

4. Claims 1-19 have been examined.

Notice of Pre-AIA or AIA Status

5. The present application is being examined under the pre-AIA first to invent provisions.

Claim Objections

6. Claim 12 is objected to because of the following informalities: the claim recites "receiving in an emulator **of** the mobile device a first application…", first the limitation is grammatically incorrect and secondly, the previous claim recited "receiving an emulator **in the** mobile device a first application…", the amendment is improper as Applicant did not designate/underline to highlight other amendments made to the claim. Appropriate correction is required.

Response to Arguments

7. Applicant's arguments filed 09/18/2019 have been fully considered.

8. 112

9. The prior 112(b) 'means for' rejection was not addressed.

10. 103

11. Applicant argues Davis does not teach "the mobile device comprising….an emulator…." First, this is not in contention. Davis is not being used to teach an emulator and the storage device in claim 1 is claimed "**for storing** a plurality of applications". Davis neither claims that only a single card can be used with the mobile device nor the card reader only accepts one card at a time.

12. In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007).

13. The combination of Davis and Vitikainen teach the emulator. Vitikainen states **"**the emulator **50** comprises a CPU **51**, which is connected to each of a voice UI **52**, a graphical user interface (GUI) **53**, a voice UI profile storage device **54**, an application storage device **55** and an emulator software storage device **56**. Of course, the storage devices **55**, **54**and **56** could form part of the same physical device, the application is loaded into the application storage device **55** at step **62**. The modified application tested using the emulator apparatus **50"** (¶ 85, 86, 88).

14. Applicant argues against the combination of Davis and Vitikainen, arguing "Vitikainen has nothing to do with or is remotely related to mobile payments". First,

Applicant's claims do not perform a single mobile payment, the limitations are focused on emulating card applications. Davis discloses smart card emulation and whilst Davis does not explicitly teach an emulator in a mobile device, Vitikainen teaches an application emulator, hence the motivation to combine.

15. Applicant next argues against the combination of Davis, Vitikainen and Vayssiere, arguing "Vayssiere is silent about 'the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications." First, Vayssiere (¶35) states "only one application (e.g., Application 2 (310)) may be active at a time. Application 2 (310) is active as illustrated by its connection to external interface 302 through OS 3.06 and firewall 304. As such, when a new application (e.g., Application 1 (308)) is initiated by OS 306, Application 2 (310) first shuts down." To clarify, this means, one application runs at a time and when one runs the other shuts down. Again, the application that was once running is replaced by another. Vayssiere is not silent on that limitation, furthermore, Applicant's argument on Vayssiere's silence is not a sound argument in relation to a motivation to combine. It is still unclear why Applicant is against the motivation to combine Davis, Vitikainen and Vayssiere.

16. Next, Applicant argues against the combination of Davis, Vitikainen, Vayssiere and Wentker, arguing Wentker does not teach switching cards with an emulator. Again, Davis teaches an emulator, emulating multiple cards, but the emulator is not located in a mobile device, Vitikainen teaches an emulator in a mobile device, Vayssiere teaches an application replacing another application, and Wentker (Abstract; column 8, line 12-16) teaches multi-application smart cards and the installing and

provisioning of these applications. Therefore, it would've been obvious to one of ordinary skill in the art to combine Davis, Vitikainen, Vayssiere and Wentker.

17. Applicant argues in Claim 12 that the combination of Davis, Vitikainen, Vayssiere and Wentker does not teach "installing in a storage device of the mobile device a plurality of applications … (vs. one at a time in Vitikainen)". First, Applicant has highlighted a limitation without support in the disclosure, as there is no recitation of bulk installation of applications. But Wentker does teach installing and loading multiple applications into memory (column 8, line 1-16, column 9, line 2-9, column 20, line 15-64) *See load files*.

18. Furthermore, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Interpretation

19. The following is a quotation of 35 U.S.C. 112(f):

> (f) Element in Claim for a Combination. – An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

20. This application includes one or more claim limitations that do not use the word "means," but are nonetheless being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because the claim limitation(s) uses a generic placeholder that is coupled with functional language without reciting sufficient structure to perform the recited function and the generic placeholder is not preceded by a structural modifier. Such claim limitation(s) is/are:

a. storage device for storing (claim 1)

b. an emulator… for receiving (claim 1)

c. communication interface to facilitate data exchange (claim 1)

d. Module configured to provide… to store (claim 6)

e. Card manager proxy for facilitating (claim 7)

f. user interface application provided to query (claim 7)

g. UI application for conducting (claim 7)

h. Interfaces…to read (claim 8)

i. Mechanism to make …for storing (claim 8)

Because this/these claim limitation(s) is/are being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, it/they is/are being interpreted to cover the corresponding structure described in the specification as performing the claimed function, and equivalents thereof.

If applicant does not intend to have this/these limitation(s) interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, applicant may: (1) amend the claim limitation(s) to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA

35 U.S.C. 112, sixth paragraph (e.g., by reciting sufficient structure to perform the claimed function); or (2) present a sufficient showing that the claim limitation(s) recite(s) sufficient structure to perform the claimed function so as to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

21. Claim 11 is rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

22. Claim 11 recites "establishing a secured channel between the mobile device and the designated server using a set of keys from the designated server.". According to the specification (¶ 110-112, 121), "depending on the arrangement between an SE and a

service provider, an application can either be downloaded/ installed/personalized using the ISD keyset of the SE or a specific SSD keyset of the service provider. If a SSD keyset has not been installed on the SE, it can be installed during an application installation… the server is configured to include an interface to retrieve a derived SE key set from the mobile device. According to one embodiment, the derived key set is generated with the device information (e.g., ISD) of the SE." The disclosure does not provide support for the mobile device receiving keys from the designated server and using those keys to establish a secure channel.

23. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

24. Claims 1-11 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

25. As per claims 1, 6, 7, 8 the claims recite the following means plus functions limitations:

j. storage device for storing (claim 1)

k. an emulator… for receiving (claim 1)

l. communication interface to facilitate data exchange (claim 1)

m. Module configured to provide… to store (claim 6)

n. Card manager proxy for facilitating (claim 7)

o. user interface application provided to query (claim 7)

p. UI application for conducting (claim 7)

q. Interfaces…to read (claim 8)

r. Mechanism to make …for storing (claim 8)

26. This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112 (f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for," "apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d 1344, 1354, 80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206,

1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56, 57, 59-61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56, 57, 61, 75, 76 describe the module interchangeable with software modules, applications and applets but there is no indication of what structure is used. ¶ 59 describes the "card manager proxy" as a "software module". ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards" but there is no indication of what structure is used. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-11 are rejected.

27. Claim 8 recites "the TMSM module". There is insufficient antecedent basis for this limitation in the claim.

28. Claim 1 recites "application is unlocked by the designated server", claim 2 recites "when the designated server determines that the secure element…," and claim 11 recites "applications has been remotely provisioned by the designated server with

operations of: notifying..." See disclosure ¶ 112, 143. A designated server is not recited as an element of the mobile device of independent claim 1, but claims 1, 2 and 11 claim the functions of a designated server. The scope of the claims are unclear as to whether the designated server is part of the claimed mobile device. Dependent claims 2-11 are rejected.

Claim Rejections - 35 USC § 103

29. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

30. Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vitikainen et al. (2006/0052080) ("Vitikainen"), in view of Vayssiere (2006/0065741) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker").

31. Regarding claims 1 and 12, Davis discloses a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided via a designated server (Figure 5; column 6, line 47-49, column 7, line 45-51, column 9, line 2-13, column 13, line 62-67, column 14, line 1-7, column 28, line 39-46, column 29, line 32-36);

- **Davis states -** client terminal 204 may also be embodied in any portable device such as a laptop computer, a cellular telephone…Local cardholder functions

including a consumer card interface, display and accept/ cancel options are performed at client terminal 204. A security card also stores signature algorithms for all Smart cards in use. A security card may also contain a transaction identifier for the current transaction, a financial Sum of all transactions remaining to be settled, a session key, and master keys for all Smart cards in use. At this point a load amount screen is presented to the user. The funding account number, expiration date, the virtual card number, maximum load amount and current balance of the virtual card are displayed and the user is directed to enter the value to be loaded onto the card. (column 6, line 47-49, column 7, line 45-51, column 9, line 2-13, column 29, line 32-36)

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated _server over a secured channel (column 6, line 60-67, column 7, line 31-38, column 8, line 53-59, column 28, line 20-50, column 29, line 50-65, column 33, line 48-64);

- **Davis states -** the consumer is able to download value from bank server 860 onto his virtual card. OPAL server 260 communicates with load server 862 to receive authorization for the load and for higher security. The virtual card may then be used to make purchases over the Internet as described above. Once the bank has downloaded value to the virtual card, a corresponding amount of funds

is transferred from the bank to card issuer 108. Additionally, the same consumer account at the bank can be used to fund multiple OPAL accounts. Preferably card 5 includes any number of keys known to the card issuer that are used during the course of a payment or load transaction to generate signatures for validation of the stored value card, validation of the security card or module, and validation of the system itself. (column 7, line 31-38, column 28, line 41-50)

a communication interface to facilitate data exchange wirelessly between a reader and wherein the reader is external to the mobile device, (Abstract; Figure 2; column 7, line 52-67, column 8, line 49-52, column 10, line 10-14, 57-60, column 25, line 6-13, column 29, line 23-31; claim 1, 22); and

- **Davis states -** Concurrently, or at a later date when smart cards and readers are more common, system **250** is then easily upgradeable to make use of the physical card and reader attached to client terminal **204**. Client terminal 204 includes client code module 224 and card reader module 226. Reader module 226 may be implemented using any Suitable software and libraries for communicating with card reader 210 and its actual implementation will depend upon the type of card reader used. Client module 224 controls communication between the client terminal, the card reader, Client code module 224 is now functionally part of OPAL server 260 instead of being part of client terminal 204. Further, the functionality of card reader module 226 of FIG. 2 is now included within client code module 224 to allow communication with pseudo card reader module 264. (column 7, line 52-67, column 10, line 10-14,)

a processor, in communication and the storage device (column 7, line 45-51, column 10, line 33-60, column 25, line 6-13, column 29, line 23-31; column 34, line 21-23, claim 1, 22);

- **Davis states -** client terminal 204 may also be embodied in any portable device such as a laptop computer, a cellular telephone (including GSM tele phones), or any variety of a personal digital assistant (PDA). Processor(s) **922** (also referred to as central processing units, or CPUs) are coupled to storage devices including memory **924**. (column 7, line 45-51, column 34, line 21-23)

Davis does not disclose an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications; into the emulator; the first applications being executed in the emulator, performing an operation of causing the second applications loaded to replace the first applications when the second card is selected via the display screen when the second application is unlocked by the designated server, wherein said causing the second application loaded to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server, and the first application in the emulator is replaceable in entirety or in part by a second application: corresponding to a second card and wherein functions of the mobile device related the first card offered by the first application are changed to functions offered by the second application related to the second cards when the second applications is activated and executed.

Vitikainen teaches an emulator, coupled to the storage, for receiving a first application corresponding to user information, the first application being one of the applications; into the emulator, in the emulator the first applications being executed in the emulator, (¶ 85, 86, 88; claim 16)

- **Vitikainen states -** the emulator **50** comprises a CPU **51**, which is connected to each of a voice UI **52**, a graphical user interface (GUI) **53**, a voice UI profile storage device **54**, an application storage device **55** and an emulator software storage device **56**. Of course, the storage devices **55**, **54**and **56** could form part of the same physical device, the application is loaded into the application storage device **55** at step **62**. the modified application tested using the emulator apparatus **50** (¶ 85, 86, 88)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis and Vitikainen in order to determine whether an application is compatible with a mobile device in order to refrain from using inappropriate features (Vitikainen; ¶ 1-3).

Vayssiere teaches performing an operation of causing the second applications loaded to replace the first applications (Figure 11, 12; ¶ 22, 35, 37, 38, 41, 43),

- **Vayssiere states-** only one application (e.g., Application 2 (310)) may be active at a time. Application 2 (310) is active as illustrated by its connection to external interface 302 through OS 3.06 and firewall 304. As

> such, when a new application (e.g., Application 1 (308)) is initiated by OS 306, Application 2 (310) first shuts down… When the reader of the public phone detects the smartcard, OS **406** first activates Display Chooser application **422**. OS **406** sends to Display Chooser application **422** a command that indicates "Application 2 (**410**) is to be activated next." In one method, Application **2** (**610**) sends complete pictures to Display Chooser application **618**, which then updates the dynamic display portion similar to that of an image obtained from Display Data **620**. In an alternative method, Application **2** (**610**) may send text which is displayed line by line to generate a complete image. (¶ 35, 37, 41)

wherein said causing the second application loaded to replace the first application fails when the second card is selected via the display screen and wherein functions of the mobile device related the first card offered by the first application are changed to functions offered by the second application related to the second cards when the second applications is activated and executed (¶ 22, 26, 30, 31, 33, 35-39, 41, 43),

- **Vayssiere states-** only one application (e.g., Application 2 (310)) may be active at a time. Application 2 (310) is active as illustrated by its connection to external interface 302 through OS 3.06 and firewall 304. As such, when a new application (e.g., Application 1 (308)) is initiated by OS 306, Application 2 (310) first shuts down. …In particular, OS **306** is responsible for the isolation of the different applications, i.e., making sure that the applications stored on the smartcard do not engage in cross-talk

> or read, write, modify, or delete data from each other. With multi-application features for smartcard **200**, one physical appearance is associated with each application stored on the smartcard **200**, and that particular physical appearance could automatically change depending on the context in which smartcard **200** is used. (¶ 26, 33, 35)

and the first application is replaceable in entirety or in part by a second application: corresponding to a second card (Abstract; Figure 11; ¶ 26, 30, 42, 43).

- **Vayssiere states-** The smartcard, in one embodiment, may be loaded with multiple applications so that the Smartcard may be used as, for example, a calling card, bank card, health card, etc. … When used for a particular application (e.g., as a payphone calling card), the smartcard is first powered through the interface with a smartcard reader, …With the proper display data retrieved, the dynamic display portion is changed or updated with the image associated with the application,(¶ 42, 43)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis Vitikainen and Vayssiere in order to provide a smartcard to perform multiple functions (Vayssiere; ¶ 3).

Wentker teaches when the second card is selected via the display screen when the second application is unlocked by the designated server but the second application is locked by the designated server (Figure 5; column 9, line 34-44, column 10, line 31-44, column 16, line 11-24, column 17, line 4-20).

- **Wentker states -** Card Manager (CM) Locked state 210 is used to tell card manager 104 to temporarily disable all applications on the card except for the card manager. This State provides the issuer with the ability to detect security threats either internal or external to the card and to be able to temporarily disable the functionality of the card. While in this state, there is an option to determine that the threat is either no longer present or is of limited Severity Such that the issuer can reset the card to the normal operating State of Secured. (column 9, line 34-44)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

32. Regarding claim 4, Davis teaches wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction (column 25, line 6-13), the mobile device is used to emulate each of the cards when a corresponding applications is loaded into and executed in the emulator (column 7, line 39-67).

33. Regarding claims 6 and 15, Neither Davis, Vitikainen nor Vayssiere teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications. Wentker teaches wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service

objects corresponding to one of the applications (column 9, line 1-33, column 13, line 11-39, column 14, line 24-43, column 21, line 17-31). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

34. Regarding claim 7, Davis discloses a user interface (UI) (column 10, line 10-32). Wentker teaches wherein the mobile device further includes a card manager proxy for facilitating communication between the designated server and the module in the secure element, interface application provided to query one or more of the applications on information stored therein but not to modify the information (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications (column 10, line 8-56). Wentker does not teach a user interface (UI). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

35. Regarding claim 8, Davis discloses to the emulator (Abstract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere and later on swapping another one of the applications (¶ 35). Wentker teaches provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator (column 6, line 36-55, column 7, line 1-7, column 8, line 17-32); provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom (column 6, line 36-55, column 8, line 17-32);

enable the designated server to remotely provision each of the applications by installing application keys and application data to the module (column 7, line 15-37, column 16, line 3-23, column 17, line 21-35, column 22, line 17-31) enable the designated server to manage each of the applications by locking or unlocking one of the applications (column 7, line 1-7, column 9, line 34-44, column 10, line 24-44); provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module (column 22, line 51-67, column 23, line 1-24).

36. Regarding claims 9 and 17, Wentker teaches wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element (column 7, line 38-56, column 13, line 11-39, column 19, line 1-8).

37. Regarding claim 11, Wentker teaches sending a request from the mobile device to the designated sever to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider (column 7, line 15-37, column 8, line 1-10, column 14, line 24-43, column 15, line 1-19, column 16, line 25-35, 49-67, column 17, line 21-35); establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server(column 7, line 15-37, column 10, line 15-23, column 13, line 11-39, column 15, line 52-67, receiving data for the application being provisioned from the designated server, wherein the data includes supplemental security domains (SSD) to

be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67); and notifying the application provider of a status of the application with the mobile device (column 12, line 58-67, column 13, line 1-10, column 17, line 4-20, column 18, line 62-67, column 19, line 44-46).

38. Regarding claim 16, Davis discloses a user interface (UI) (column 10, line 10-32). Wentker teaches facilitating communication between the designated server and the TMSM module configured to provide (TMSM) in the secure element (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31); querying via a user interface (UI) one or more of the applications (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31) and conducting operations that modify one or more sectors in one or more of the applications (column 10, line 8-56). Wentker does not teach a user interface (UI). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

39. Regarding claim 19, Wentker teaches receiving a request to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider (column 7, line 15-37, column 8, line 1-10, column 14, line 24-43, column 15, line 1-19, column 16, line 25-35, 49-67, column 17, line 21-35); establishing a secured channel with the secure element using a set of keys (column 7, line 15-37, column 10, line 15-23, column 13, line 11-39, column 15, line 52-67, preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67); and notifying the application

provider of a status of the application with the mobile device (column 12, line 58-67, column 13, line 1-10, column 17, line 4-20, column 18, line 62-67, column 19, line 44-46).

40. Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vitikainen et al. (2006/0052080) ("Vitikainen"), in view of Vayssiere (2006/0065741) ("Vayssiere"), in view of Wentker et al. (6,481,632) ("Wentker") and further in view of De Groot (2006/0141987) ("Groot").

41. Regarding claims 2 and 13, Neither Davis, Vitikainen nor Vayssiere teaches initiating data communication by the mobile device with the designated server; sending device information of the secure element from the mobile device in responding to a request from the designated server when the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider and a designated server providing trusted service management. Wentker teaches and with designated server providing trusted service management (TSM) (column 6, line 13-67, column 8, line 17-32, column 21, line 1-31). Groot teaches initiating data communication by the mobile device (¶ 36, 40, 44); sending device information of the secure element from the mobile

device in responding to a request from the designated server when the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (¶ 30, 34, 36, 37, 39, 40, 43, 47, 48, 53); receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider (Figure 1, element M1-3; ¶ 30, 31, 34, 40-45, 47-49, 53). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere, Wentker, and Groot in order to provide secure transmissions with a terminal and a server using an identifier (Groot; ¶ 1-7).

42. Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis"), in view of Vitikainen et al. (2006/0052080) ("Vitikainen"), in view of Vayssiere (2006/0065741) ("Vayssiere"), in view of Wentker et al. (6,481,632) ("Wentker") and further in view of Huomo et al. (8,005,426) ("Huomo").

43. Regarding claims 3 and 14, Davis discloses the emulator (Abs-tract; column 25, line 6-13, column 29, line 23-31; claim 1). Vayssiere teaches implemented in the secure element (¶ 22, 23, 30). Neither Davis, Vitikainen nor Vayssiere teaches the secure element is enclosed in the mobile device or in a detachable card to the mobile device. Huomo teaches the secure element is enclosed in the mobile device or in a detachable

card to the mobile device (column 8, line 3-23). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Davis, Vitikainen, Vayssiere and Huomo in order to provide transactions with mobile devices equipped with a smartcard (Huomo; column 1, line 7-23, 54-67).

44. Regarding claim 5, Huomo teaches wherein at least one of the cards is a contactless card (column 2, line 27-61, column 8, line 3-37).

45. Regarding claims 10 and 18, Huomo teaches wherein the mobile device is a smartphone, or a portable computer (column 16, line 26-36, 43-67, column 17, line 1-5).

Conclusion

46. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUEL whose telephone number is

(469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I.I.I./
Examiner, Art Unit 3685

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination Xie et al.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	6,481,632 B2	11-2002	Wentker; David C.	G06F8/60	235/376
*	B	2006/0065741 A1	03-2006	Vayssiere; Julien JP.	G06K19/07703	235/492
*	C	2006/0141987 A1	06-2006	De Groot; Max	H04L63/0414	455/411
*	D	US-20060052080-A1	03-2006	Vitikainen; Timo	G10L15/30	455/403
*	E	7,908,216 B1	03-2011	Davis; Virgil M.	G06Q20/02	705/41
*	F	8,005,426 B2	08-2011	Huomo; Heikki	G06Q20/20	235/441
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

CPC - Searched*		
Symbol	Date	Examiner
G06Q	2/1/2016	II

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
705			

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See attached notes	2/1/2016	II
101 withdrawal - Weinhart	06/06/2018	III
See attached notes (EAST)	04/15/2019	III

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/I.I./ Examiner.Art Unit 3685

Samsung Ex. 1016, Page 414 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016	09/17/2017	05/22/2018	04/15/2019	12/18/2019			
	1	✓	✓	✓	✓	✓	✓			
	2	✓	✓	✓	✓	✓	✓			
	3	✓	✓	✓	✓	✓	✓			
	4	✓	✓	✓	✓	✓	✓			
	5	✓	✓	✓	✓	✓	✓			
	6	✓	✓	✓	✓	✓	✓			
	7	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	✓			
	9	✓	✓	✓	✓	✓	✓			
	10	✓	✓	✓	✓	✓	✓			
	11	✓	✓	✓	✓	✓	✓			
	12	✓	✓	✓	✓	✓	✓			
	13	✓	✓	✓	✓	✓	✓			
	14	✓	✓	✓	✓	✓	✓			
	15	✓	✓	✓	✓	✓	✓			
	16	✓	✓	✓	✓	✓	✓			
	17	✓	✓	✓	✓	✓	✓			
	18	✓	✓	✓	✓	✓	✓			
	19	✓	✓	✓	✓	✓	✓			

Samsung Ex. 1016, Page 415 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 01/22/2020

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
01/22/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Applicant-Initiated Interview Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.		
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No	**Page** **1 of** 2

All participants (applicant, applicants representative, PTO personnel):

1. ISIDORA I IMMANUEL (Examiner); Telephonic
2. NEHA PATEL (SPE); Telephonic
3. JOE ZHENG (Attorney); Telephonic
4. LIANGSENG KOH (Inventor); Telephonic

Date of Interview: 16 January 2020

Claims Discussed: Discussed claim 1. No agreements reached.

Prior Art Discussed: Discussed Davis and Vayssiere. No agreements reached.

Brief Description of the main topic(s) of discussion: Discussed claim background and 103 rejection. No agreements reached.

Issues Discussed:

Item(s) under 35 U.S.C. 103:
Discussed the Davis reference. No agreements reached.

Attachment(s): Agenda, Proposed Arguments,

/I.I.I./ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

U.S. Patent and Trademark Office
PTOL-413/413b (Rev. 01/01/2015) **Interview Summary** Paper No. 20200116

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

1. The Applicant has authorized the communication with the Examiner via the Internet
2. This is for informal discussion with the Examiner, content of which is not intended for entry as record.

Interview Agenda

Time: 02:00PM EST (11:00 AM PST)

Date: Thursday, January 15, 2020

Participants: SPE: Neha Patel

Examiner: Isidora I. Immanuel

Inventor: Liangseng Koh

Representative: Joe Zheng (Reg. No.: 39,450, Cell: 408-891-9381)

Connection: Dialing in: **(415)363-6338**, and conference ID:**987987**

Agenda:

1. Clarification on Claim Objections to Claim 12;
2. Joe briefly describes what this invention is about with respect to Claim 1;
3. Joe presents the distinctions between Claim 1 and four cited references Davis et al. (7,908,216) ("Davis"), Vitikainen et al. (2006/0052080) ("Vitikainen"), Vayssiere (2006/0065741)("Vayssiere") and Wentker et al. (6,481,632) ("Wentker").
4. Examiner presents her view on the distinctions;
5. Examiner suggests possible amendments to overcome the references;
6. Conclusion (Interview Summary)

Samsung Ex. 1016, Page 419 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Explanation of Claim 1

One of the purposes in the instant application is to emulate multiple cards in a mobile device to interact with an external reader. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality of applications controlled and managed by a designated (TSM) server, each of the applications pertaining to one of cards (e.g., Visa and transportation card). So the mobile device can be used as a Visa Card to pay for purchased items or a ticket for riding a bus, which requires the user to do something on the mobile device to act such. When a credit card is needed for payment, the user can select one of the applications available in the mobile device to act as Visa. A corresponding application is loaded into an emulator that turns the mobile device as the selected card. When a ticket is needed for transaction, the user can again select another application available in the mobile device to act as a ticket, in which case a corresponding application is loaded into the emulator that turns the mobile device as the ticket. The data or modules for each of the applications can be accessed by the designated server (e.g., to lock or unlock the application or card, if needed), all of the installed applications must be provisioned remotely with the designated server that subsequently installs corresponding data and keys for each of the installed applications.

Combination of the four references is improper

In the Pre-Appeal Brief Request for Review dated Sept. 12, 2018, the Applicant presents the arguments why the combination Davis, Vayssiere and Wentker does not render Claim 1 obvious. The Examiner returns the instant application back to prosecution but uses the same combination + 4th reference Vitikainen to show the teaching and rejects Claims 1, 4, 6-9, 11, 12, 15-17 and 19 under pre-AIA 35 U.S.C. 103(a).

Review of the four references in view of Claim 1

Davis:

teaches a virtual smart card for payment of goods and/or services purchased online over the Internet. As shown in FIG. 2, there are a merchant server 208, a

Samsung Ex. 1016, Page 420 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

mobile device 204 **AND** a card reader 210 which accepts a smart card having a stored-value application. Even if the mobile device 204 and the card reader 210 were viewed as a single unit, the card reader 210 would only accept a physical card at a time, which immediately teaches away from "*storing a plurality of applications, each of the applications corresponding to one of the cards*" recited in Claim 1. Next, Davis does teach an emulator but the emulator is located in an OPAL server 260 (FIG. 4), which is not in the mobile device 204, again teaching away from Claim 1 that recites the mobile device comprising: ... an emulator. In fact, there is no need for an emulator in Davis as Davis uses the card reader 210 to accommodate a physical card, where the card reader 210 transports the card payment info to the payment server 206. Davis is remotely related to Claim 1 of the instant application.

Vitikainen

is related to a voice user interface for testing the compatibility of an application with the mobile device. Vitikainen does teach an emulator but it is used to emulate the voice user interface features of the device. It is believed that this reference only cited because it uses the word “emulator”. On Page 15 of the OA, the Examiner states that Davis and Vitikainen are combined in order to determine whether an application is compatible with a mobile device in order to refrain from using inappropriate features, which has nothing to do with Claim 1. The Examiner fails to demonstrate how to modify Davis with Vitikainen. The combination of Davis and Vitikainen is improper.

Vayssiere

teaches a smartcard having a dynamic display portion that changes when an application is switched. As described in [0038], Vayssiere explicitly describes that when the user completes the use [of] the smartcard as a calling card, Application 2 (410) terminates, and OS 406 activates Display Chooser application 422 again. First of all, Vayssiere is silent about "*the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications*". Even if the Examiner insists Vayssiere may imply the replacement action, the modification of

Samsung Ex. 1016, Page 421 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Davis and Vitikainen with Vayssiere would still not cure the deficiency of "*the data can only be modified by the designated server over a secured channel*" as the card itself in Vayssiere does not allow another device to remotely control an application therein. In fact, Vayssiere has no such need. Accordingly, the Appellant submits the combination of Davis, Vitikainen and Vayssiere is improper and Claim 1 shall be allowable over Davis, Vitikainen and Vayssiere.

Wentker:

Wentker is cited to show the teaching of an application unlocked by a server. Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. The functions of the smart card CANNOT be replaced by another application so that the smart card would function as a different card. To emulate a number of different cards, an emulator is needed. Wentker is completely silent about an emulator. In other words, Wentker neither teaches nor suggests a mobile device to emulate a plurality of cards. In a perspective, Wentker teaches away from Claim 1 by managing only one card via the provided APIs.

Samsung Ex. 1016, Page 422 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided via a designated server;

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;

an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications;

a communication interface to facilitate data exchange wirelessly between a reader and the first application being executed in the emulator, wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card; and

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen when the second application is unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application is locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator.

Samsung Ex. 1016, Page 423 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

2. (*Currently amended*) The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the designated server when the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

Samsung Ex. 1016, Page 424 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

6. (*Previously amended*) The mobile device as recited in claim 3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Currently amended*) The mobile device as recited in claim 6, wherein the mobile device further includes:

a card manager proxy for facilitating communication between the designated server and the module in the secure element,

a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications.

8. (*Currently amended*) The mobile device as recited in claim 6, wherein the module is configured to:

provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

enable the designated server to remotely provision each of the applications by installing application keys and application data to the module and later on swapping another one of the applications to the emulator;

enable the designated server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

Samsung Ex. 1016, Page 425 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Previously amended*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone or a portable computer.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the designated server with operations of:

sending a request from the mobile device to the designated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider;

establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server;

receiving data for the application being provisioned from the designated server, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein

Samsung Ex. 1016, Page 426 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards;

showing a list of the cards on a display of the mobile device for a user to choose one therefrom, wherein the display is provided by a module downloaded from the designated server and executed in the mobile device;

receiving in an emulator of the mobile device a first application corresponding to a first card;

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card;

causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator.

Claim Objections to Claim 12

The Examiner states "*receiving in an emulator of the mobile device a first application*" is grammatically incorrect. The Applicant is unsure why it is grammatically incorrect

13. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

Samsung Ex. 1016, Page 427 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

sending device information of the secure element in responding to a request from the designated server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Currently amended*) The mobile device as recited in claim 15, further comprising

facilitating communication between the designated server and the module configured to provide (TMSM) in the secure element;

querying via a user interface (UI) one or more of the applications; and

conducting operations that modify one or more sectors in one or more of the applications.

17. (*Previously amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information

Samsung Ex. 1016, Page 428 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

updatable entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Currently amended*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the designated server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

Samsung Ex. 1016, Page 429 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (05-13)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
RFID-084	13/782,948	03/01/2013
First Named Inventor:	**Title:**	
Xiangzhen Xie	Method and apparatus for emulating multiple cards in mobile devices	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
    - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
    - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
        - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
        - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
            - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
            - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date
/ joe zheng /	1/20/2020
Name (Print/Typed) Joe Zheng	**Practitioner Registration No.** 39,450

***Note**: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

☐ * Total of _____ forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	38360117
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	22-JAN-2020
Filing Date:	01-MAR-2013
Time Stamp:	02:16:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	ResponseToFinalOAAfter2ndAppeal.pdf	170068 182faeceec4a52927e4cb9efc4d0403a8bd06211	no	15

Warnings:

Information:					
2	After Final Consideration Program Request	AfterFinalConsideration.pdf	211048 73df82b0331755db071e4bd7b2737d06a69153ea	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	381116	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

January 22, 2020

Mail Stop: After Final
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to Final OA after 2nd Appeal
Under After Final Consideration Pilot Program 2.0

Dear Sir:

In response to the Final Office Action dated 12/26/2019, the Applicant encloses herewith Certification and Request for Consideration under After Final Consideration Pilot Program 2.0 and respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begins on page 2 of this Response.

REMARKS/ARGUMENTS begin on page 9 of this Response.

Samsung Ex. 1016, Page 434 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

Please amend Claims 1 and 12 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided via a designated server;

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;

an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications;

a communication interface to facilitate data exchange wirelessly between a reader and the first application being executed in the emulator, wherein the reader is external to the mobile device and reads the corresponding data and keys of the first card from the mobile device, and the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when replaced by the second application; and

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen when the second application is unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the

Samsung Ex. 1016, Page 435 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

display screen but the second application is locked by the designated server, and wherein

functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator.

2. (*Previously amended*) The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the designated server when the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to

Samsung Ex. 1016, Page 436 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

emulate each of the cards when a corresponding application is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

6. (*Previously amended*) The mobile device as recited in claim 3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Previously amended*) The mobile device as recited in claim 6, wherein the mobile device further includes:

   a card manager proxy for facilitating communication between the designated server and the module in the secure element,

   a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

   a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications.

8. (*Previously amended*) The mobile device as recited in claim 6, wherein the module is configured to:

   provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

   provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

Samsung Ex. 1016, Page 437 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

enable the designated server to remotely provision each of the applications by installing application keys and application data to the module and later on swapping another one of the applications to the emulator;

enable the designated server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Previously amended*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone or a portable computer.

11. (*Previously amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the designated server with operations of:

sending a request from the mobile device to the designated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider;

establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server;

receiving data for the application being provisioned from the designated server, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

Samsung Ex. 1016, Page 438 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

notifying the application provider of a status of the application with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards from the mobile device;

showing a list of the cards on a display of the mobile device for a user to choose one therefrom, wherein the display is provided by a module downloaded from the designated server and executed in the mobile device;

receiving in an emulator ~~in~~ of the mobile device a first application corresponding to a first card;

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when replaced by the second application in the emulator;

causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the

Samsung Ex. 1016, Page 439 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

second application related to the second card when the second application is activated and executed in the emulator.

13. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the designated server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Previously amended*) The mobile device as recited in claim 15, further comprising

Samsung Ex. 1016, Page 440 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

facilitating communication between the designated server and the module configured to provide (TMSM) in the secure element;

querying via a user interface (UI) one or more of the applications; and

conducting operations that modify one or more sectors in one or more of the applications.

17. (*Previously amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updatable entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Previously amended*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the designated server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

Samsung Ex. 1016, Page 441 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

REMARKS

Claims 1 - 19 were examined again. In the Office Action dated 04/18/2019, Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention, Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis") in view of Vitikainen et al. (2006/0052080) ("Vitikainen") in view of Vayssiere (2006/0065741) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker"), Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere in view of Wentker and further in view of De Groot (2006/0141987) ("Groot"), and Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere inview of Wentker and further in view of Huomo et al. (8,005,426) ("Huomo").

In the foregoing amendments, Claims 1 and 12 have been amended to further distinguish from the cited references. No new matters are introduced. Claims 1-19 are still pending.

Interview Summary

The Applicant appreciates the Examiner for granting a conference call among the Examiner herself, her Supervisor Neha Patel, co-inventor Liang Seng Koh and the undersigned. The call took place on January 16, 2020. The Applicant had the opportunity to argue that the combination of Davis, Vitikainen, Vayssiere and Wentker is improper and listen to the interpretation by the Examiner on Claim 1 in view of the cited references. Possible amendments to Claim 1 were discussed. No agreement was reached. The Examiner would reconsider proposed amendments when a formal response is filed.

Claim Objections

Samsung Ex. 1016, Page 442 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

On page 2, Section 6, of the Office Action, the Examiner objects to Claim 12. In the foregoing amendments, Claim 12 has been amended. It is believed that the claim objections shall be withdrawn.

Claim Rejections - 35 USC § 112

On page 7, Section 21, of the Office Action, Claim 11 is rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The Examiner alleges the disclosure does not provide support for the mobile device receiving keys from the designated server and using those keys to establish a secure channel.

The Applicant respectfully disagrees and wished to refer the Examiner to the quoted section in the OA. "*an application can either be downloaded/ installed/personalized using the ISO keyset of the SE or a specific SSO keyset of the service provider*" and also shown as 234 in FIG. 2B clearly describes that a secured channel is established per the keys from the service provider to download the applications. The claim rejection of Claim 11 under 35 U.S.C. 112 shall be withdrawn.

Claim Rejections - 35 USC § 112

On Page 8, Section 24, of this Office Action, Claims 1-11 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

The Applicant respectfully disagrees and traverses the rejection as follows.

Before the Examiner can assert that "storage device", "emulator", or "communication interface" and etc. is a single means, the Examiner must determine whether the claim limitation invokes the sixth paragraph of 35 U.S.C. § 112. MPEP § 2181(I) states that a claim feature will be presumed to invoke the sixth paragraph of 35 U.S.C. § 112 if the feature meets the following 3-prong analysis:

(A) the claim limitations must use the phrase "means for" or "step for";
(B) the "means for" or "step for" must be modified by functional language; and

Samsung Ex. 1016, Page 443 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

(C) the phrase "means for" or "step for" must not be modified by sufficient structure, material, or acts for achieving the specified function.

In this case, Claim 1 does not include the recitation “means for” or “step for” and, therefore, cannot be considered to invoke the sixth paragraph of 35 U.S.C. § 112. In addition, the claim features are not written as a function to be performed, but instead recited as sufficient structure to preclude application of the sixth paragraph of 35 U.S.C. § 112. Because these terms cannot be interpreted to invoke the sixth paragraph of 35 U.S.C. § 112, the Applicant respectfully submits that Claim 1 does not recite a single means, as alleged by the Examiner. Rejections of Claims 1-11 under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, shall be withdrawn.

Claim Rejections - 35 USC § 103

On Page 11, Section 30, of this Office Action, Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere and further in view of Wentker. The Applicant respectfully traverses the rejections of Claims 1, 4, 6-9, 11, 12, 15-17 and 19 under pre-AIA 35 U.S.C. 103(a).

One of the purposes in the instant application is to emulate multiple cards using an emulator in a mobile device to interact with an external reader. It should be noted that this external reader operated by a merchant reads **from** the mobile device one of the cards represented by an application being executed in an emulator of the mobile device. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality of applications controlled and managed by a designated (TSM) server, each of the applications pertaining to one of cards (e.g., Bank of America Visa, Chase Visa, and American Express). When a card is needed for payment, a user can select one of the cards available in the mobile device. A corresponding application is then loaded into the emulator that turns the mobile device as the corresponding selected card. Such a card is to be read off by the external reader. The loaded application in the emulator is replaced in part or entirety with another application when another card is selected. In other words, the loaded

Samsung Ex. 1016, Page 444 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

application is now out of the emulator. The emulator is now loaded with the another application. One of the important features is that the data for a selected card is accessed and controlled by a designated server (e.g., to lock or unlock an application or card, if there is a need).

In contrast, Davis teaches a payment system having a mobile device 204 **AND** a card reader 210 which accepts a smart card having a stored-value application. The Applicant wished to call the Examiner's attention to the structure and conceptual differences between the external reader recited in Claim 1 and the card reader 210 in Davis. As shown in FIG. 2, Davis explicitly shows that the card reader 210 is provided to read payment information from a smartcard 5 and **send the info to the mobile device 204** while the external reader recited in Claim 1 is a merchant's device (e.g., Reader 296 in FIG. 2F) **reading data (card) from the mobile device**.

In a perspective, there is no such reader 210 in Claim 1 as the mobile device is recited to function as a card to be read by others (i.e., an external reader). Davis teaches away from "*the reader is external to the mobile device and reads the corresponding data and keys of the first card from the mobile device*". Even if the mobile device 204 and the card reader 210 were viewed as a single unit, the card reader 210 "is any suitable interface device that functions to transfer information and commands between client terminal 204 and card 5" in Davis, which technically teaches away from "*storing a plurality of applications, each of the applications corresponding to one of the cards*" recited in Claim 1. Next, Davis does teach an emulator but the emulator is explicitly located in an OPAL server 260 as shown in FIG. 3, which again teaches away from Claim 1 reciting "the mobile device comprising: ... an emulator". In fact, there is no need for an emulator in the mobile device 204 in Davis as Davis uses it as a terminal to transfer card information from a reader to a payment server. Accordingly, Claim 1 shall be allowable over Davis.

On Pages 14-15 of this Office Action, the Examiner admits Davis does not teach a number of elements recited in Claim 1, including "*an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first*

application being one of the applications; into the emulator" but cites Vitikainen to show the teaching in combination. The Applicant respectfully contests the combination of Davis and Vitikainen as it is believed that there is no motivation to combine these two references in the manner proposed by the Examiner. Vitikainen does teach an emulator but it is used to emulate the voice user interface features of the device.

The Examiner admits that Davis does not teach an emulator in the mobile device but tries to modify Davis with Vitikainen's emulator. The Applicant respectfully challenges the Examiner to demonstrate how Davis' architecture could be modified to include the emulator from Vitikainen without causing Davis to malfunction. It is believed that Vitikainen is only cited because it uses an "emulator". The Applicant submits there are no technical bases to combine Davis with Vitikainen, and the combination of Davis and Vitikainen is improper.

On Page 15 of the Office Action, Vayssiere is cited to show the teaching of performing an operation of causing the second applications loaded to replace the first applications. The Applicant respectfully contests the combination of Davis, Vitikainen and Vayssiere as it is believed that there is no motivation to combine these three references in the manner proposed by the Examiner. Vayssiere explicitly describes an OS to run multiple applications. It is believed that the Examiner mischaracterizes the emulator recited in Claim 1 with an OS. None of the applications in an OS would be moved out from the OS while an application can be moved out from an emulator. An emulator is a special piece of hardware or software provided in the mobile device to enable the mobile device (called the *host*) to behave like another computing device (called the *guest*), see Wikipedia (https://en.wikipedia.org/wiki/Emulator). Conceptually, a mobile device works fine without an emulator but delivers something unique when equipped with such an emulator as described in the instant application.

The rejections of Claim 1 under Davis, Vitikainen and Vayssiere on obviousness grounds are believed made by mere conclusory statements without articulated reasoning to support the legal conclusion of obviousness. *KSR v.*

Samsung Ex. 1016, Page 446 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Teleflex, No. 04-1350 (US Apr. 30, 2007) (citing In re Kahn, 441 F. 3d 977, 988 (Canada Fed. 2006)). As reasoned above, Vayssiere is futher silent about "*the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications*". In fact, Vayssiere has no such need in an OS. Accordingly, the Applicant submits Claim 1 as previously amended shall be allowable over Davis, Vitikainen and Vayssiere, viewed alone or in combination.

On Page 17, the Examiner cites Wentker to show the teaching of an application unlocked by a server. The Appellant again contests the combination of Davis, Vitikainen, Vayssiere and Wentker as it is believed that there is no motivation to combine these four references in the manner proposed by the Examiner. Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. The functions of the smart card CANNOT be replaced by another application so that the smart card would function as a different card. To emulate a number of different cards, an emulator is needed. Wentker is completely silent about an emulator. In other words, Wentker neither teaches nor suggests a mobile device to emulate a plurality of cards. Accordingly, the Appellant submits Claim 1 as previously amended shall be allowable over Davis, Vitikainen, Vayssiere and Wentker. Reconsideration of Claims 1-11 is kindly requested.

Claim 12 was amended similarly to Claim 1. Without repeating the same, the Applicant wishes to rely upon the above arguments supporting Claim 1 to support Claim 12 and submits the combination of Davis, Vitikainen, Vayssiere and Wentker is improper. The combination of Davis, Vitikainen, Vayssiere and Wentker fails to suggest "*installing in a storage device of the mobile device a plurality of applications downloaded from a designated server*" (vs. one at a time in Vitikainen) and "*said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server*". Accordingly, the Appellant submits Claim 12 as previously amended shall be allowable over Davis, Vitikainen, Vayssiere and Wentker. Reconsideration of Claims 12-19 is kindly requested.

Samsung Ex. 1016, Page 447 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

The patentability of the independent claims has been argued specifically as set forth above and thus the Applicant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, Applicant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

In view of the above amendments and remark, the Applicant believes that Claims 1-19 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", 1/22/2020. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng
Reg.: No. 39,450

Samsung Ex. 1016, Page 448 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/782,948	Filing Date 03/01/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $31 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $ 125 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	01/22/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 19	Minus	** 20	= 0		x $ 50 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $ 230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $ 0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $ 0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/TARA A WASHINGTON/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/30 (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

Subsection (b) of 35 U.S.C. § 132, effective on May 29, 2000, provides for continued examination of an utility or plant application filed on or after June 8, 1995.
See The American Inventors Protection Act of 1999 (AIPA).

Application Number	13/782,948
Filing Date	03/01/2013
First Named Inventor	Xiangzhen Xie
Group Art Unit	3685
Examiner Name	Isidora I. Immanuel
Attorney Docket Number	RFID-084

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.

NOTE: *37 C.F.R. § 1.114 is effective on May 29, 2000. If the above-identified application was filed prior to May 29, 2000, applicant may wish to consider filing a continued prosecution application (CPA) under 37 C.F.R. § 1.53 (d) (PTO/SB/29) instead of a RCE to be eligible for the patent term adjustment provisions of the AIPA.* See *Changes to Application Examination and Provisional Application Practice*, Final Rule, 65 *Fed. Reg.* 50092 (Aug. 16, 2000); Interim Rule, 65 *Fed. Reg.* 14865 (Mar. 20, 2000), 1233 *Off. Gaz. Pat. Office* 47 (Apr. 11, 2000), which established RCE practice.

1. Submission required under 37 C.F.R. § 1.114
   - a. ☐ Previously submitted
     - i. ☐ Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on _____ (Any unentered amendment(s) referred to above will be entered).
     - ii. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
     - iii. ☐ Other _____
   - b. ☒ Enclosed
     - i. ☒ Amendment/Reply
     - ii. ☐ Affidavit(s)/Declaration(s)
     - iii. ☐ Information Disclosure Statement (IDS)
     - iv. ☐ Other _____
2. Miscellaneous
   - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. § 1.17(i) **required**)
   - b. ☐ Other _____
3. Fees — The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed.
   - a. ☐ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No._____
     - i. ☒ RCE fee required under 37 C.F.R. § 1.17(e) **Small Entity**
     - ii. ☐ Extension of time fee (37 C.F.R. §§ 1.136 and 1.17)
     - iii. ☐ Other _____
   - b. ☐ Check in the amount of $_____ enclosed
   - c. ☒ Payment by credit card (Form PTO-2038 enclosed) paid via PAIR

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print /Type)	Joe Zheng	Registration No. (Attorney/Agent)	39,450
Signature	/ joe zheng /	Date	02/19/2020

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner For Patents, Box RCE, Washington, DC 20231, or facsimile transmitted to the U.S. Patent and Trademark Office on:

Name (Print/Type)	Joe Zheng		
Signature	/ joe zheng /	Date	02/19/2020

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND Fees and Completed Forms to the following address: Assistant Commissioner for Patents, Box RCE, Washington, DC 20231.

Electronic Patent Application Fee Transmittal

Application Number:	13782948
Filing Date:	01-Mar-2013
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Filer:	Joe Zheng
Attorney Docket Number:	RFID-084

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 1ST REQUEST	2801	1	650	650
		Total in USD ($)		**650**

Electronic Acknowledgement Receipt	
EFS ID:	38635340
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	19-FEB-2020
Filing Date:	01-MAR-2013
Time Stamp:	19:24:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$650
RAM confirmation Number	E20202IJ44426087
Deposit Account	502436
Authorized User	Joe Zheng
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	RCEReqTrns.pdf	124537 eb6a950ccfbb861ca04695c01c7d42c246dc25f9	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	ResponseToFinalOAAfter2ndAppeal.pdf	172022 1643c0472a3a4a242903aead13df7b7dd13da103	no	15
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30439 899cdcbe714453ad849a3de9af1aa98eee53b25c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	326998		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

February 19, 2020

Mail Stop: AF/RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to Final OA
&
Preliminary amendments in a RCE filed concurrently

Dear Sir:

In response to the Final Office Action dated 12/26/2019, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begins on page 2 of this Response.

REMARKS/ARGUMENTS begin on page 9 of this Response.

Samsung Ex. 1016, Page 455 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

Please cancel Claim 8 and amend Claims 1-3, 6-7, 11-13 and 15-16 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, wherein a display of the list of the cards is provided via a designated server;

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;

an emulator, coupled to the storage device and implemented in a secure element, for receiving a first application corresponding to a first card, the first application being one of the plurality of applications;

a communication interface to facilitate data exchange wirelessly between a reader and the first application being received and executed in the emulator, wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety ~~or in part~~ by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator and replaced by the second application; and

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen when the second application ~~is~~ has been unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected

Samsung Ex. 1016, Page 456 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

via the display screen but the second application ~~is~~ has been locked by the designated server, and wherein

functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the first application is out of the emulator and the second application is activated and executed in the emulator.

2. (*Currently amended*) The mobile device as recited in claim 1, further comprising ~~a~~ the secure element that has been personalized by operations of:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the designated server when the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the set of keys are generated in accordance with the device information of the secure element, ~~wherein~~ the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

3. (*Currently*) The mobile device as recited in claim 2, wherein ~~the emulator is implemented in the secure element,~~ the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to

Samsung Ex. 1016, Page 457 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

emulate each of the cards when a corresponding application is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

6. (*Currently amended*) The mobile device as recited in claim 3, wherein the secure element further includes ~~a module configured to provide Trusted Mifare Service Management (TMSM) and to store~~ a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Currently amended*) The mobile device as recited in claim 6, wherein the mobile device further ~~includes~~provides:

~~a card manager proxy for facilitating communication between the designated server and the module in the secure element;~~

a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

a transaction UI application for conducting operations ~~that~~ to modify one or more sectors in one or more of the applications.

8. (*Cancelled*)

9. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Previously amended*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone or a portable computer.

Samsung Ex. 1016, Page 458 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the designated server with operations of:

sending a request from the mobile device to the designated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider;

establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server;

receiving data for the application being provisioned from the designated server, wherein the data for the application includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards on the mobile device;

showing a list of the cards on a display of the mobile device for a user to choose one therefrom~~, wherein the display is provided by a module downloaded from the designated server and executed in the mobile device~~;

receiving in an emulator ~~in~~ of the mobile device a first application corresponding to a first card;

Samsung Ex. 1016, Page 459 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety ~~or in part~~ by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when the second card is selected by the and the first and replaced by the second application in the emulator;

causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application ~~is~~ has been locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator.

13. (*Currently amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication by the mobile device with ~~the~~ designated server; ~~providing trusted service management (TSM);~~

sending device information of the secure element in responding to a request from the designated server after the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

Samsung Ex. 1016, Page 460 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Currently amended*) The method as recited in claim 14, wherein the secure element further includes ~~a module configured to provide Trusted Mifare Service Management (TMSM) and to store~~ a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Currently amended*) The mobile device as recited in claim 15, further ~~comprising~~providing:

~~facilitating communication between the designated server and the module configured to provide (TMSM) in the secure element;~~

querying via a user interface (UI) one or more of the applications; and

conducting operations that modify one or more sectors in one or more of the applications.

17. (*Previously amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updatable entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Previously amended*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the designated server with operations of:

Samsung Ex. 1016, Page 461 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

Samsung Ex. 1016, Page 462 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

REMARKS

Claims 1 - 19 were examined again. In the Office Action dated 04/18/2019, Claims 1-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention, Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis et al. (7,908,216) ("Davis") in view of Vitikainen et al. (2006/0052080) ("Vitikainen") in view of Vayssiere (2006/0065741) ("Vayssiere") and further in view of Wentker et al. (6,481,632) ("Wentker"), Claims 2 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere in view of Wentker and further in view of De Groot (2006/0141987) ("Groot"), and Claims 3, 5, 10, 14 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere inview of Wentker and further in view of Huomo et al. (8,005,426) ("Huomo").

In the foregoing amendments, Claim 8 has been cancelled and Claims 1-3, 6-7, 11-13 and 15-16 have been amended to further distinguish from the cited references. No new matters are introduced. Claims 1-19 are still pending.

Interview Summary

The Applicant appreciates the Examiner for granting a conference call among the Examiner herself, her Supervisor Neha Patel, co-inventor Liang Seng Koh and the undersigned. The call took place on January 16, 2020. The Applicant had the opportunity to argue that the combination of Davis, Vitikainen, Vayssiere and Wentker is improper and listen to the interpretation by the Examiner on Claim 1 in view of the cited references. Possible amendments to Claim 1 were discussed. No agreement was reached. The Examiner would reconsider proposed amendments when a formal response is filed.

Claim Objections

Samsung Ex. 1016, Page 463 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

On page 2, Section 6, of the Office Action, the Examiner objects to Claim 12. In the foregoing amendments, Claim 12 has been amended. It is believed that the claim objections shall be withdrawn.

Claim Rejections - 35 USC § 112

On page 7, Section 21, of the Office Action, Claim 11 is rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The Examiner alleges the disclosure does not provide support for the mobile device receiving keys from the designated server and using those keys to establish a secure channel.

The Applicant respectfully disagrees and wished to refer the Examiner to the quoted section in the OA. "*an application can either be downloaded/ installed/personalized using the ISO keyset of the SE or a specific SSO keyset of the service provider*" and also shown as 234 in FIG. 2B clearly describes that a secured channel is established per the keys from the service provider to download the applications. The claim rejection of Claim 11 under 35 U.S.C. 112 shall be withdrawn.

Claim Rejections - 35 USC § 112

On Page 8, Section 24, of this Office Action, Claims 1-11 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

The Applicant respectfully disagrees and traverses the rejection as follows.

Before the Examiner can assert that "storage device", "emulator", or "communication interface" and etc. is a single means, the Examiner must determine whether the claim limitation invokes the sixth paragraph of 35 U.S.C. § 112. MPEP § 2181(I) states that a claim feature will be presumed to invoke the sixth paragraph of 35 U.S.C. § 112 if the feature meets the following 3-prong analysis:

(A) the claim limitations must use the phrase "means for" or "step for";
(B) the "means for" or "step for" must be modified by functional language; and

Samsung Ex. 1016, Page 464 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

(C) the phrase "means for" or "step for" must not be modified by sufficient structure, material, or acts for achieving the specified function.

In this case, Claim 1 does not include the recitation “means for” or “step for” and, therefore, cannot be considered to invoke the sixth paragraph of 35 U.S.C. § 112. In addition, the claim features are not written as a function to be performed, but instead recited as sufficient structure to preclude application of the sixth paragraph of 35 U.S.C. § 112. Because these terms cannot be interpreted to invoke the sixth paragraph of 35 U.S.C. § 112, the Applicant respectfully submits that Claim 1 does not recite a single means, as alleged by the Examiner. Rejections of Claims 1-11 under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, shall be withdrawn.

Claim Rejections - 35 USC § 103

On Page 11, Section 30, of this Office Action, Claims 1, 4, 6-9, 11, 12, 15-17 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Davis in view of Vitikainen in view of Vayssiere and further in view of Wentker. The Applicant respectfully traverses the rejections of Claims 1, 4, 6-9, 11, 12, 15-17 and 19 under pre-AIA 35 U.S.C. 103(a).

One of the purposes in the instant application is to emulate multiple cards using an emulator in a mobile device to interact with an external reader. It should be noted that this external reader operated by a merchant reads **from** the mobile device one of the cards represented by an application being executed in an emulator of the mobile device. As shown in FIG. 1A and described in paragraphs [0060], a mobile device can be stored with a plurality of applications controlled and managed by a designated (TSM) server, each of the applications pertaining to one of cards (e.g., Bank of America Visa, Chase Visa, and American Express). When a card is needed for payment, a user can select one of the cards available in the mobile device. A corresponding application is then loaded into the emulator that turns the mobile device as the corresponding selected card. Such a card is to be read off by the external reader. The loaded application in the emulator is replaced in part or entirety with another application when another card is selected. In other words, the loaded

Samsung Ex. 1016, Page 465 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

application is now out of the emulator. The emulator is now loaded with the another application. One of the important features is that the data for a selected card is accessed and controlled by a designated server (e.g., to lock or unlock an application or card, if there is a need).

In contrast, Davis teaches a payment system having a mobile device 204 **AND** a card reader 210 which accepts a smart card having a stored-value application. The Applicant wished to call the Examiner's attention to the structure and conceptual differences between the external reader recited in Claim 1 and the card reader 210 in Davis. As shown in FIG. 2, Davis explicitly shows that the card reader 210 is provided to read payment information from a smartcard 5 and **send the info to the mobile device 204** while the external reader recited in Claim 1 is a merchant's device (e.g., Reader 296 in FIG. 2F) **reading data (card) from the mobile device**.

In a perspective, there is no such reader 210 in Claim 1 as the mobile device is recited to function as a card to be read by others (i.e., an external reader). Davis teaches away from "*the reader is external to the mobile device and reads the corresponding data and keys of the first card from the mobile device*". Even if the mobile device 204 and the card reader 210 were viewed as a single unit, the card reader 210 "is any suitable interface device that functions to transfer information and commands between client terminal 204 and card 5" in Davis, which technically teaches away from "*storing a plurality of applications, each of the applications corresponding to one of the cards*" recited in Claim 1. Next, Davis does teach an emulator but the emulator is explicitly located in an OPAL server 260 as shown in FIG. 3, which again teaches away from Claim 1 reciting "the mobile device comprising: ... an emulator". In fact, there is no need for an emulator in the mobile device 204 in Davis as Davis uses it as a terminal to transfer card information from a reader to a payment server. Accordingly, Claim 1 shall be allowable over Davis.

On Pages 14-15 of this Office Action, the Examiner admits Davis does not teach a number of elements recited in Claim 1, including "*an emulator, coupled to the storage device and implemented in a secure element, receiving a first application*

Samsung Ex. 1016, Page 466 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

corresponding to a first card, the first application being one of the applications; into the emulator" but cites Vitikainen to show the teaching in combination. The Applicant respectfully contests the combination of Davis and Vitikainen as it is believed that there is no motivation to combine these two references in the manner proposed by the Examiner. Vitikainen does teach an emulator but it is used to emulate the voice user interface features of the device.

The Examiner admits that Davis does not teach an emulator in the mobile device but tries to modify Davis with Vitikainen's emulator. The Applicant respectfully challenges the Examiner to demonstrate how Davis' architecture could be modified to include the emulator from Vitikainen without causing Davis to malfunction. It is believed that Vitikainen is only cited because it uses an "emulator". The Applicant submits there are no technical bases to combine Davis with Vitikainen, and the combination of Davis and Vitikainen is improper.

On Page 15 of the Office Action, Vayssiere is cited to show the teaching of performing an operation of causing the second applications loaded to replace the first applications. The Applicant respectfully contests the combination of Davis, Vitikainen and Vayssiere as it is believed that there is no motivation to combine these three references in the manner proposed by the Examiner. Vayssiere explicitly describes an OS to run multiple applications. It is believed that the Examiner mischaracterizes the emulator recited in Claim 1 with an OS. None of the applications in an OS would be moved out from the OS while an application can be moved out from an emulator. An emulator is a special piece of hardware or software provided in the mobile device to enable the mobile device (called the *host*) to behave like another computing device (called the *guest*), see Wikipedia (https://en.wikipedia.org/wiki/Emulator). Conceptually, a mobile device works fine without an emulator but delivers something unique when equipped with such an emulator as described in the instant application.

The rejections of Claim 1 under Davis, Vitikainen and Vayssiere on obviousness grounds are believed made by mere conclusory statements without articulated reasoning to support the legal conclusion of obviousness. *KSR v.*

Samsung Ex. 1016, Page 467 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Teleflex, No. 04-1350 (US Apr. 30, 2007) (citing In re Kahn, 441 F. 3d 977, 988 (Canada Fed. 2006)). As reasoned above, Vayssiere is futher silent about "*the one of the applications in the emulator is replaceable in entirety or in part by another one of the applications*". In fact, Vayssiere has no such need in an OS. Accordingly, the Applicant submits Claim 1 as previously amended shall be allowable over Davis, Vitikainen and Vayssiere, viewed alone or in combination.

On Page 17, the Examiner cites Wentker to show the teaching of an application unlocked by a server. The Appellant again contests the combination of Davis, Vitikainen, Vayssiere and Wentker as it is believed that there is no motivation to combine these four references in the manner proposed by the Examiner. Wentker teaches a smart card architecture by APIs to allow the management of an application in the smart card. The functions of the smart card CANNOT be replaced by another application so that the smart card would function as a different card. To emulate a number of different cards, an emulator is needed. Wentker is completely silent about an emulator. In other words, Wentker neither teaches nor suggests a mobile device to emulate a plurality of cards. Accordingly, the Appellant submits Claim 1 as previously amended shall be allowable over Davis, Vitikainen, Vayssiere and Wentker. Reconsideration of Claims 1-7, 9-11 is kindly requested.

Claim 12 was amended similarly to Claim 1. Without repeating the same, the Applicant wishes to rely upon the above arguments supporting Claim 1 to support Claim 12 and submits the combination of Davis, Vitikainen, Vayssiere and Wentker is improper. The combination of Davis, Vitikainen, Vayssiere and Wentker fails to suggest "*installing in a storage device of the mobile device a plurality of applications downloaded from a designated server*" (vs. one at a time in Vitikainen) and "*said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server*". Accordingly, the Appellant submits Claim 12 as previously amended shall be allowable over Davis, Vitikainen, Vayssiere and Wentker. Reconsideration of Claims 12-19 is kindly requested.

Samsung Ex. 1016, Page 468 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

The patentability of the independent claims has been argued specifically as set forth above and thus the Applicant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, Applicant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

In view of the above amendments and remark, the Applicant believes that Claims 1-7, and 9-19 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)891-9381.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to " Mail Stop: AF/RCE Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450", 02/19/2020.

e-filed.
Name: Joe Zheng
Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng
Reg.: No. 39,450

Samsung Ex. 1016, Page 469 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/782,948	Filing Date 03/01/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $31 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $ 125 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	02/19/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0		x $ 50 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $ 230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $ 0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $ 0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/MARGARET R BYARS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 02/26/2020

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
02/26/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 13/782,948	**Applicant(s)** Xie et al.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (FITF) Status** No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 22 January 2020 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☑ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires ____ months from the mailing date of the final rejection.
   b) ☑ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection.The current period for reply expires ____ months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.
   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANTS FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37CFR 41.37(a).

AMENDMENTS

3. ☑ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☑ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____ (See 37CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicants reply has overcome the following rejection(s): _____
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☑ For purposes of appeal, the proposed amendment(s):(a) ☑ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____
9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☑ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☑ Other: PTO 2323, Interview and Annotated claims.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:
    Claim(s) allowed:_____.
    Claim(s) objected to:_____.
    Claim(s) rejected:1-19.
    Claim(s) withdrawn from consideration:_____.

/I.I.I./ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

Samsung Ex. 1016, Page 472 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Continuation of REQUEST FOR RECONSIDERATION/OTHER 12. The request for reconsideration has been considered but does NOT place the application in condition for allowance because: The after final amendment would not overcome all of the rejections in the most recent final Office action. An interview was had with Applicant's representation Joe Zheng and Inventor Liangseng Koh detailing possible allowance language that adds, corrects and deletes some of the language of the after final submission by Applicant. There was an agreement about the proposed allowable claims, but the current after final submission(01/22/2020) would not overcome the current rejection nor is it allowable.

Examiner-Initiated Interview Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.		
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No	**Page** **1 of** 2

All participants (applicant, applicants representative, PTO personnel):

1. ISIDORA I IMMANUEL (Examiner); Telephonic
2. JOE ZHENG (Attorney); Telephonic
3. LIANGSENG KOH (Inventor); Telephonic

Date of Interview: 12 February 2020

Claims Discussed: Claims that needed language modifications towards an allowance were discussed.

Amendment proposed: Examiner proposed claim amendments that clarify, overcome rejections and place the application in condition for an allowance.

Brief Description of the main topic(s) of discussion: Examiner, Zheng and Koh discussed proposed allowable claims and reached a consensus on the claim language.

Issues Discussed:

Proposed Amendments:
Claim amendments were proposed to Applicant that will place the application in condition for an allowance.

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview .

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

AFCP 2.0 Decision

Application No.	Applicant(s)	
13/782,948	Xie et al.	
Examiner	**Art Unit**	**AIA (FITF) Status**
ISIDORA I IMMANUEL	3685	No

This is in response to the After Final Consideration Pilot request filed 22 January 2020.

1. **Improper Request** – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

   ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.

   ☐ A non-broadening amendment to at least one independent claim was not submitted.

   ☐ The request is not the first proper AFCP 2.0 request submitted in response to the most recent final rejection.

   ☐ Other: _____

2. **Proper Request**

   A. After final amendment submitted with the request will not be treated under AFCP 2.0.
   The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

   ☐ The after final amendment will be treated under pre-pilot procedure.

   B. Updated search and/or completed additional consideration.
   The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

   ☐ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.

   ☑ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action . See attached interview summary for further details.

   ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.

   ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.

   ☐ 5. Other: _____

   Examiner Note: Please attach an interview summary when necessary as described above.

Samsung Ex. 1016, Page 476 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

DO NOT ENTER: /I.I.I./

AMENDMENTS TO THE CLAIMS

Please amend Claims 1 and 12 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, a display of the list of the cards provided via a designated server;

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;

an emulator, coupled to the storage, for receiving a first application corresponding to a first card, the first application being one of the applications;

a communication interface to facilitate data exchange wirelessly between a reader and the first application being executed in the emulator, wherein the reader is external to the mobile device and reads the corresponding data and keys of the first card from the mobile device, and the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when replaced by the second application; and

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen when the second application is unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the

Samsung Ex. 1016, Page 477 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

display screen but the second application is locked by the designated server, and wherein

functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator.

2. (*Previously amended*) The mobile device as recited in claim 1, further comprising a secure element that has been personalized by operations of:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the designated server when the designated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, wherein the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

3. (*Original*) The mobile device as recited in claim 2, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to

Samsung Ex. 1016, Page 478 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

emulate each of the cards when a corresponding application is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

6. (*Previously amended*) The mobile device as recited in claim 3, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Previously amended*) The mobile device as recited in claim 6, wherein the mobile device further includes:

   a card manager proxy for facilitating communication between the designated server and the module in the secure element,

   a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

   a transaction UI application for conducting operations that modify one or more sectors in one or more of the applications.

8. (*Previously amended*) The mobile device as recited in claim 6, wherein the module is configured to:

   provide a set of Application Programming Interfaces so that one of the applications, when instructed by an user, is caused to swap an application in and out the emulator;

   provide a set of Application Programming Interfaces to one of the applications to read certain data therefrom;

Samsung Ex. 1016, Page 479 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

enable the designated server to remotely provision each of the applications by installing application keys and application data to the module and later on swapping another one of the applications to the emulator;

enable the designated server to manage each of the applications by locking or unlocking one of the applications;

provide a trusted environment such that an application provider modifies a designated application and meta data thereof owned by the application provider; and

provide a mechanism to make baseband storage as an extension for storing some or all of the applications swapped out from the emulator to the TMSM module.

9. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Previously amended*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone or a portable computer.

11. (*Previously amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the designated server with operations of:

sending a request from the mobile device to the designated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider;

establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server;

receiving data for the application being provisioned from the designated server, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

Samsung Ex. 1016, Page 480 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

notifying the application provider of a status of the application with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards from the mobile device;

showing a list of the cards on a display of the mobile device for a user to choose one therefrom, wherein the display is provided by a module downloaded from the designated server and executed in the mobile device;

receiving in an emulator ~~in~~ of the mobile device a first application corresponding to a first card;

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety or in part by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when replaced by the second application in the emulator;

causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application is locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the

Samsung Ex. 1016, Page 481 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

second application related to the second card when the second application is activated and executed in the emulator.

13. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication by the mobile device with the designated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the designated server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a module configured to provide Trusted Mifare Service Management (TMSM) and to store a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Previously amended*) The mobile device as recited in claim 15, further comprising

Samsung Ex. 1016, Page 482 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

facilitating communication between the designated server and the module configured to provide (TMSM) in the secure element;

querying via a user interface (UI) one or more of the applications; and

conducting operations that modify one or more sectors in one or more of the applications.

17. (*Previously amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updatable entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Previously amended*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the designated server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

Samsung Ex. 1016, Page 483 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PLUS Search Results for S/N 13782948, Searched Wed May 27 17:11:37 EDT 2020

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

6101543 99
20130178159 99
20170323301 99
20170372321 99
20200034849 99
5249218 70
5353334 70
5367563 70
5530703 70
5640444 70
5937421 70
5963650 70
5995839 70
6078314 70
6108003 70
6137791 70
6373820 70
6802058 70
6853851 70
6912389 70
7006964 70
7039434 70
7151931 70
7155381 70
7162408 70
7165191 70
7231330 70
7296190 70
7317912 70
7319874 70
7319948 70
7324588 70
7334162 70
7392060 70
7450936 70
7486927 70
7502626 70
7512402 70
7516451 70
7545386 70
7548804 70
7577887 70
7606261 70
7613453 70
7620015 70
7698121 70
7734288 70
7738426 70
7783261 70
7809578 70

Doc Code: ECOMM.AUTH/ECOMM.WTDW
Doc Description: Internet Communications Authorized/Internet Communications Authorization Withdrawn

PTO/SB/439 (11-15)

AUTHORIZATION FOR INTERNET COMMUNICATIONS IN A PATENT APPLICATION OR REQUEST TO WITHDRAW AUTHORIZATION FOR INTERNET COMMUNICATIONS

Application No.	13/782,948
Filing Date	03/01/2013
First Named Inventor	Xiangzhen Xie
Art Unit	3685
Examiner Name	Isidora I. Immanuel
Practitioner Docket No.	RFID-084

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. To authorize permission for Internet Communications.

☑ Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via video conferencing, instant messaging, or electronic mail. I understand that a copy of these communications will be made of record in the application file. (MPEP 502.03)

II. To withdraw authorization for Internet Communications.

☐ The authorization given on _____, to the USPTO to communicate with the undersigned and any practitioner in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via Internet communications such as video conferencing, instant messaging, or electronic mail is hereby withdrawn. I understand that the withdrawal is effective when approved rather than when received.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 39,450.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/ joe zheng / — Signature

07/29/2020 — Date

Joe Zheng — Typed or printed name

(408)891-9381 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Juristic entities must be represented by a patent practitioner (see 37 CFR 1.31, which is applicable to any paper filed on or after September 16, 2012, that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

Electronic Acknowledgement Receipt

EFS ID:	40131949
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	29-JUL-2020
Filing Date:	01-MAR-2013
Time Stamp:	03:02:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Internet Communications Authorized	InternetAuthorizationAsFiled.pdf	75632 68cb8041b3e2a57235a20c7ecaef149ddb1426a0	no	1

Warnings:

Information:	
Total Files Size (in bytes):	75632

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 08/21/2020

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
08/21/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Applicant-Initiated Interview Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.		
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No	**Page** **1 of** 2

All participants (applicant, applicants representative, PTO personnel):

1. ISIDORA I IMMANUEL (Examiner); Telephonic
2. JOE ZHENG(AGENT); Telephonic
3. LIANG KOH (Inventor); Telephonic

Date of Interview: 11 August 2020

Claims Discussed: Discussed the proposed allowance language. Changed TSM server to dedicated server based on drawings and disclosure support, along with adding the "wherein" clause to explain the TSM is the dedicated server. Discussed the use of TMSM versus the broader "service manager". No agreements reached.

Amendment proposed: Examiner proposed claim amendments and emailed the discussed claims to Applicant. No agreements reached.

Brief Description of the main topic(s) of discussion: Amended the TSM server based on specification support. Discussed the language of the TMSM and the disclosure support for a broader term "service manager ". Discussed the emulator "device" and the use of hardware.

Issues Discussed:

Proposed Amendments:
Potential allowable subject matter was discussed. No agreements reached.

Attachment(s): Proposed Amendments,

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

U.S. Patent and Trademark Office
PTOL-413/413b (Rev. 01/01/2015) **Interview Summary** Paper No. 20200528

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

1. (Currently amended) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of applications for a user of the mobile device to select one therefrom, each application corresponding to a card in the plurality of cards; (62-69, 180, 238)

a secure element (SE) comprising: (58)

an emulator device; (62-69)

a memory storing a Trusted Mifare Service Manager (TMSM), the TMSM, when executed by the secure element causes the secure element to perform: (58)

receiving and installing key sets of a Supplementary Secured Domain (SSD); (65, 72, 80)

establishing, based on the key sets, a secure communication channel with a dedicated server; (80, 141-143)

receiving, a plurality of applications from the dedicated sever, each of the applications including corresponding application data sets and files and a locked or unlocked status, wherein an application with a locked status must be unlocked to be replaced; (63, 65, 80)

installing the plurality of applications; (62)

receiving, from the plurality of applications, a user selection of a first application; (180)

determining the first application has a locked or unlocked status and is activated, wherein an application status is locked or unlocked by the dedicated server; (83-95)

in response to determining the first application has an unlocked status and is activated, sending the first application, corresponding to a first card, to the emulator device, wherein sending the first application comprises sending the first application along with a corresponding first application data sets and files; (62-69)

receiving, from the plurality of applications, a user selection of a second application; (180)

determining the second application has a locked or unlocked status and is activated; (83-95)

in response to determining the second application has an unlocked status and is activated, replacing out of the emulator device, a portion of or in entirety, the first application, wherein replacing out a portion of the first application comprises retaining, in the emulator device, portions of the corresponding first application data sets and files to be utilized by the second application; (63)

sending the second application, corresponding to a second card, to the emulator device, wherein sending the second application comprises sending the second application along with a corresponding second application data sets and files; (62-69)

updating an incrementing counter for each successful application replacement; (82)

wherein the mobile device performs functions of the second card, when the first card related to the first application are changed to functions of the second card related to the second application and the first application is out of the emulator device and the second application is received in the emulator device.

2. (Currently amended) The mobile device as recited in claim 1, further comprising ~~a~~ the ~~secure element that has been personalized by operations of: initiating data communication by the mobile device with the designated server providing trusted service management (TSM);~~

receiving, by the mobile phone, a universal resource identifier (URI) from the dedicated server, when the mobile phone is registered with the dedicated server (106), wherein the dedicated server is a Trusted Service Manager (TSM) server;

sending device information of the secure element in responding to a request from the ~~designated server~~ dedicated server, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from ~~designated server~~ the dedicated server, wherein the set of keys are generated in accordance with the device information of the secure element, ~~wherein~~ the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 08/24/2020

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
08/24/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Office Action Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 02/19/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-7 and 9-19 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-7 and 9-19 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 02/19/2020.

2. Claims 1-3, 6, 7, 11-13, 15 and 16 amended.

3. Claim 8 is cancelled.

4. Claims 1-7, and 9-19 are pending.

5. Claims 1-7, and 9-19 have been examined.

Notice of Pre-AIA or AIA Status

6. The present application is being examined under the pre-AIA first to invent provisions.

Priority

7. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date of 09/24/2006. The emulator is mentioned in App. No. 13/350,832 with a priority date of 01/16/2012, but the use of the emulator in replacing applications is claimed in the provisional 61/606,451, the 9 page specification, giving the application the priority date of 03/04/2012.

Response to Arguments

8. Applicant's arguments filed 02/19/2020 have been fully considered.

9. 112

10. The prior 112(b) 'means for' rejection was not properly addressed. Applicant has not shown specification support for the "sufficient structure" applicant refers to. The

claims recite software applications performing steps. Claims do not need to recite "means for" or "step for" to invoke a 112(f) interpretation. Additionally, courts have argued that "Our consideration of this case has led us to conclude that such a heightened burden is unjustified and that we should abandon characterizing as "strong" the presumption that a limitation lacking the word "means" is not subject to § 112, para. 6. That characterization is unwarranted, is uncertain in meaning and application, and has the inappropriate practical effect of placing a thumb on what should otherwise be a balanced analytical scale. It has shifted the balance struck by Congress in passing § 112, para. 6 and has resulted in a proliferation of functional claiming untethered to § 112, para. 6 and free of the strictures set forth in the statute. Henceforth, we will apply the presumption as we have done prior to *Lighting World,* without requiring any heightened evidentiary showing and expressly overrule the characterization of that presumption as "strong." We also overrule the strict requirement of "a showing that the limitation essentially is devoid of anything that can be construed as structure." *Williamson v. Citrix Online, LLC,* 115 USPQ2d 1105 (Fed. Cir. 2015).

11. 103

12. Applicant's arguments with respect to the claims have been considered but are moot because the arguments do not apply to the references being used in the current rejection.

Claim Interpretation

13. The following is a quotation of 35 U.S.C. 112(f):

> (f) Element in Claim for a Combination. – An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the

corresponding structure, material, or acts described in the specification and equivalents thereof.

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

14. This application includes one or more claim limitations that do not use the word "means," but are nonetheless being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because the claim limitation(s) uses a generic placeholder that is coupled with functional language without reciting sufficient structure to perform the recited function and the generic placeholder is not preceded by a structural modifier. Such claim limitation(s) is/are:

a. an emulator… for receiving (claim 1)

b. communication interface to facilitate data exchange (claim 1)

c. user interface application provided to query (claim 7)

d. UI application for conducting (claim 7)

Because this/these claim limitation(s) is/are being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, it/they is/are being interpreted to cover the corresponding structure described in the specification as performing the claimed function, and equivalents thereof. ¶ 59 explains "a card manager proxy **112** that facilitates the communication between a Trusted Service Manager (i.e., TSM server) **114** and the TMSM **106**, a set of readonly wallet user interface (UI) applications **116** and transaction wallet applications **118**. .. The readonly wallet

UI **116** provides an interface to query one or more Mifare applications on information ", the claimed interfaces are software applications but are currently claimed in a mobile device and claimed to be performing functions. ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards" but there is no indication of what structure is used. . ¶ 62 explains "Once the emulator **122** (implemented in hardware or software) is installed, it responds exactly like a native Mifare chip to an interface". According to the disclosure, the emulator can be either software or hardware, applicant is claiming a machine and the claim is unclear as to whether the emulator written in claim 1 is hardware or software. A software emulator cannot be claimed in the mobile device to be performing functions. As a result, corresponding structure to support the means for the functions has not been clearly provided.

If applicant does not intend to have this/these limitation(s) interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, applicant may: (1) amend the claim limitation(s) to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph (e.g., by reciting sufficient structure to perform the claimed function); or (2) present a sufficient showing that the claim limitation(s) recite(s) sufficient structure to perform the claimed function so as to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph.

Claim Rejections - 35 USC § 112

15. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

16. Claims 1-7, and 9-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

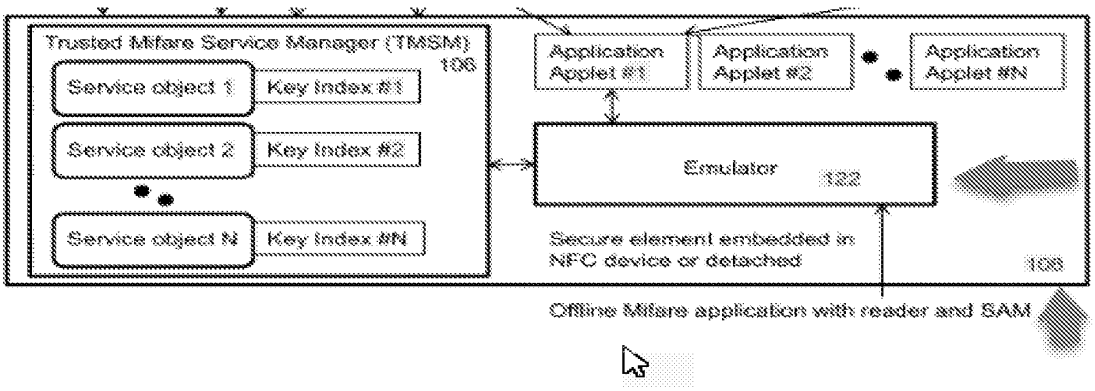
17. Claim 1 recites "the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel", similarly, claim 12 recites "wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device." According to the specification (¶ 65, 67), "enabling the TSM 114 to remotely personalize? provision multiple Milfare applications, which includes installing application keys and application data to the TMSM 106 and later on swapping an activated one to the emulator 122. … providing a trusted environment such that an application provider can only modify its application and meta data thereof that is owned by the application provider." The TSM is not the same entity as the application provider.

The TSM provides application data and keys not the application owner. The term "designated server" is used to encompass the functions of the different entity. There is no written description support for the designated server performing the functions of the claimed TSM server and an application provider. Dependent claims 2-7, 9-11 and 13-19 are rejected.

18. Claim 1 recites "a display screen showing a list of the cards for a user of the mobile device to choose one therefrom… when another one of the cards is selected by the user, wherein the first application is out of the emulator and replaced by the second application… when the second card is selected via the display screen", similarly claim 12 recites "showing a list of the cards on a display of the mobile device for a user to choose one therefrom… ". According to the specification (Figure 9; ¶ 180, 191), "It is assumed that the user has chosen one of the applications from the displayed directory." The displayed information are applications, not cards, the applications can correspond to cards, but the disclosure explains that the user chooses an application not a card. The disclosure does not provide support for a display of cards that the user chooses from. Dependent claims 2-7, 9-11 and 13-19 are rejected.

19. Claim 1 recites "a storage device for storing a plurality of applications wherein each of the applications is provisioned remotely with the designated server… an emulator, coupled to the storage device and implemented in a secure element". According to the specification (Figure 1; ¶ 58-63, 117, 120, 143), "To download/install the application to the SE, the server is configured to establish a secure channel with the SE using this derived SSD at **242..**. it is assumed that an installed application, e-purse or a Mifare card, has been provisioned with the SE… an on-card Trusted Mifare

Service Manager **106** (implemented as a module or an applet) is provided in a secure element (SE) **108**… the TMSM 106 is a component or applet configured to be responsible for installing and personalizing the applications, and Swapping one or another application into or out an emulator 122," the emulator (122) is part of the secure element and the secure element(108) is the storage device that stores the plurality of applications(applet #1-N). The secure element, is not a generic "storage device" that stores the plurality of applications. The applications are not provisioned in a "storage device", they are provisioned in a secure element. Neither the figures nor the specification describe a device other than the secure element that is used to store both the plurality of applications and the emulator. The specification does not provide support for these three entities being different. Dependent claims 2-7, and 9-11 are rejected.



20. Claims 9 and 17 recite "wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element". According to the disclosure (Figure 1; ¶ 61, 62), " the SE **132** of FIG. 1C may be perceived as a preload operating system in a smart card, providing a platform for PIN management and security channels (security domains) for card personalization.

The SE **132** combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple applications running in the smart cards." The same language is regurgitated in original claims 9 and 17. According to MPEP 2163, " issues of adequate written description may arise even for original claims, for example, when an aspect of the claimed invention has not been described with sufficient particularity such that one skilled in the art would recognize that the applicant had possession of the claimed invention at the time of filing." In this case, the specification does not describe or mention the SE being preloaded with and ISD (entirely or partially updated) or that these are based on a retrieved default ISD information from an entity that created the secure element. The claims assertions require more adequate description than is provided in the original claims or the disclosure. The specification does not provide support for these assertions and the original claims do not provide sufficient written description.

21. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

22. Claims 1-7, and 9-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and

distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

23. As per claims 1, 7 the claims recite the following means plus functions limitations:

e. an emulator… for receiving (claim 1)

f. communication interface to facilitate data exchange (claim 1)

g. user interface application provided to query (claim 7)

h. UI application for conducting (claim 7)

24. This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112 (f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for," "apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d

1344, 1354, 80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206, 1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56, 57, 59-61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56, 57, 61, 75, 76 describe the module interchangeable with software modules, applications and applets but there is no indication of what structure is used, ¶ 59 explains "a card manager proxy **112** that facilitates the communication between a Trusted Service Manager (i.e., TSM server) **114** and the TMSM **106**, a set of readonly wallet user interface (UI) applications **116** and transaction wallet applications **118**. .. The readonly wallet UI **116** provides an interface to query one or more Mifare applications on information ", the claimed interfaces are software applications but are currently claimed in a mobile device and claimed to be performing functions. ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards" but there is no indication of what structure is used. . ¶ 62 explains "Once the

emulator **122** (implemented in hardware or software) is installed, it responds exactly like a native Mifare chip to an interface". According to the disclosure, the emulator can be either software or hardware, applicant is claiming a machine and the claim is unclear as to whether the emulator written in claim 1 is hardware or software. A software emulator cannot be claimed in the mobile device to be performing functions. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-7, and 9-11 are rejected.

25. Claim 1 recites "wherein a display of the list of the cards s provided via a designated server". The designated server is not a part of the claimed mobile device, the limitation is therefore unclear and indefinite as to the display on the mobile device being provided through a designated server. Dependent claims 2-7, and 9-11 are rejected.

26. Claim 1 recites "the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel… application is unlocked by the designated server", claims 2 and 13 recites "in responding to a request from the designated server when the designated server determines that the secure element is registered therewith…," claim 11 recites "wherein the application being provisioned is distributed by an application provider…applications has been remotely provisioned by the designated server with operations of: notifying...", claim 12 recites ", wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device… an external reader provided to read one of the cards on the mobile device," See disclosure

¶ 112, 143. A designated server, external reader and application providers are not recited as an elements of the mobile device of independent claims 1, and 12 but claims 1, 2 and 11 claim the functions or intended functions of a designated server, reader and/or an application provider, which are both remote to the claimed mobile device. The scope of the claims are unclear and indefinite as Applicant has claimed functions outside the scope of the mobile device's functions. Dependent claims 2-11 are rejected. Dependent claims 2-7, 9-11 and 13-19 are rejected.

27. Claim 2 and 13 recite "sending device information of the secure element in responding to a request from the designated server when the designated server determines that the secure element is registered therewith." The claims are unclear and indefinite. The claim is directed to the mobile device, not the functions of the designated server. But the recites functions are dependent on the designated server. Given that the designated server is remote to the mobile device, it would be impossible for the mobile device to know for example, that the designated server has determined the secure element is registered with it without receiving such communication. Therefore the claims is unclear as the functions of the mobile device are written to also claim knowledge of the functions of the designated server.

28. Claim 4 recites the limitation "the cards provided respectively". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

29. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

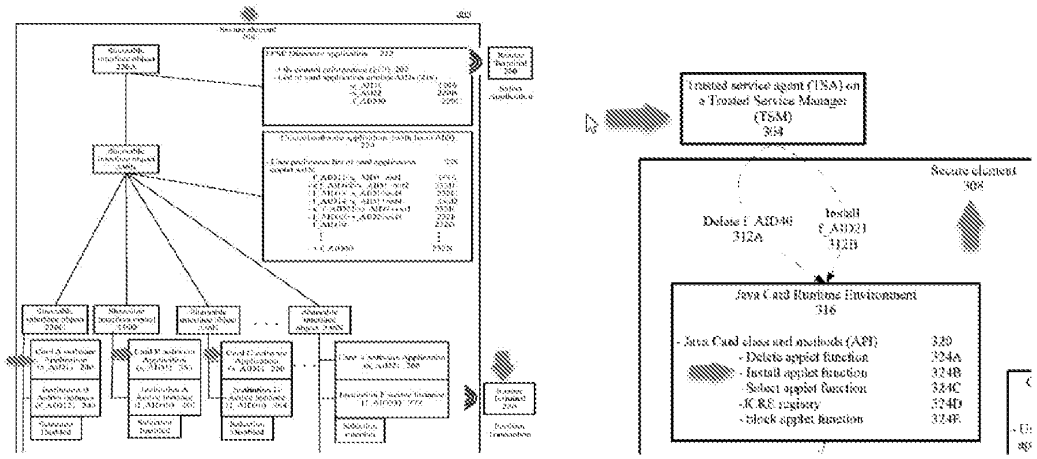
30. Claims 1-7, 9, 10, and 13-18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over von Behren et al. (8,646,059) ("Behren"), in view of Corda et al. (9,128,829) ("Corda"), and further in view of Hosogoe et al. (2003/0151125) ("Hosogoe").

31. Regarding claim 1, Behren discloses a display screen showing a list of the cards for a user of the mobile device to choose one therefrom, wherein a display of the list of the cards s provided via a designated server (Figure 1; column 5, line 41-67, column 7, line 38-42, column 9, line 3-27, column 10, line 13-49, column 13, line 18-26, column 18, line 27-35, column 20, line 48-61)

- **Behren** - the user may choose from different card types (for example, PayPass, Paywave, debit cards, or other types) from different credit card companies (for example, MasterCard, Visa, Discover, or other companies), as well as different bank instances (for example, Bank A, B, C, and D) for each card type on the user-interface… the wallet application can be used by the contactless payment device user to select certain card Software applications as preferred applications via a user-inter face, thereby creating an order based on the type of card Software application. … When a full sized AID is selected, the directory software application then routes payment transaction commands according to user selected settings, directly to the selected instance… Here, all the data in the PPSE may not be distributed to merchants' reader by default, but is available to

the user for selection via the user-interface. The user may choose to use the access functionality for specific payments on short distance contactless communication with a specific merchant terminal. T (column 5, line 41-67, column 7, line 38-42, column 9, line 14-18, column 18, line 27-32)

a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel (Figure 2, 3; column 4, line 49-67, column 5, line 11-67, column 7, line 22-67, column 8, line 1-14, column 13, line 45-62, column 19, line 27-38, column 22, line 25-53, column 26, line 1-43) ;



- **Behren** - An external trusted service manager (TSM) 108 controlled by a near field communications (NFC) service provider 104 hosts and transmits card software applications for installation within the secure element 152 of a contactless Smart card in mobile device 140. The NFC service provider 104

provides a secure key encrypted Software card application for decryption and installation in the Secure element 152. .. The term “card software application' and “card applet” are used interchangeably in this disclosure to refer to a software applications running within the secure element of a Smart card… to instantiate a Trusted Service Manager (TSM) Security Domain for download of payment and other card Software applications, to lock/unlock card Software applications, and to terminate secure element Software applications.,… The payment applications may be loaded on the mobile device as a card Software application package, where each package, for example, a MasterCard package, typically contains Software code for all Supported payment applications within MasterCards' offerings, e.g., Mstripe, Mchip, and any other Suitable payment application. (column 4, line 63-66, column 5, line 11-33, column 7, line 62-67, column 8, line 1, 2)

emulation mode implemented in a secure element, (column 8, line 38-53, column 21, line 1-21);

- **Behren-** an application host OS 144 on the mobile device 140 provides the user of the mobile device with the capability to manage multiple card Software applications and its instances 160-164 using a wallet Software application 148,.. The management of the card software applications may be performed via a control software application 156, which communicates with the wallet Software application 148 using APDUs, transmitted and received, through a secure and encrypted communication channel. The control Software application may freely

communicate with the multiple card software applications and its instances 160-164 because each of the card and control software applications are resident within the same secure element 152. (column 8, line 38-53)

a communication interface to facilitate data exchange wirelessly between a reader and the first application ; and (Figurer 2, 3; column 7, line 49-57, column 20, line 48-61, column 21, line 34-65)

- **Behren -** The proximity payment service environment (PPSE) is a directory software application that is selected by the terminal reader when the contactless payment device is presented to the reader…The control software application can prevent the reader terminal from applying certain forceful methods to select a payment card Software application from a list of available options. (column 7, line 49-52, column 20, line 56-59)

wherein said causing the second application loaded fails when the second card is selected via the display screen but the second application has been locked by the designated server, and (column 5, line 11-17, column 9, line 28-65, column 15, line 36-63, column 16, line 55- 67, column 17, line 1-60, column 19, line 8-17, column 24, line 1-67)

- **Behren -** Alter natively, the TSM may issue pre-defined instructions for such exemplary external functions, as blocking/unblocking a card Software application… to instantiate a Trusted Service Manager (TSM) Security Domain for download of payment and other card Software applications, to lock/unlock

> card Software applications, and to terminate secure element Software applications… The control software application includes a list 232 of the activate/inactive/non-activatable card Software application AIDs in certain format…When a card Software application 240,252,260, and 268 is enabled, the SIO is active and is accessed by the client mode control Software application 224…. In certain exemplary embodiments, for the UNBLOCKED/BLOCKED functions from the JCRE 316, based on requests from the TSA 304 may be rendered on a selected AID of the card software application 360 for blocking. The instruction for blocking or unblocking may be defined by the control software application 328 using APIs from the JCRE that causes a selected card software application360 to trigger an event to the control software application 328… In certain exemplary embodiments, the internal method calls applicable may include Such custom functions as, a enableSelection (byte aid): Boolean, for enabling selection of a payment card Software application and returning values as true if enabled or false for a general error (for example, the applet is locked). Another exemplary method call includes the disableSelection (byte aid): Void, which disables selection of a payment type card Software application… (column 5, line 11-17, column 9, line 41-65, column 15, line 36-43, column 16, line 66, 67, column 17, line 1-7, column 24, line 41-44)

Behren does not disclose an emulator, coupled to the storage device and receiving a first application corresponding to a first card, the first application being one of the plurality of applications; the first application received and executed in the emulator,

wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator and replaced by the second application; a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen when the second application has been unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application; wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the first application is out of the emulator and the second application is activated and executed in the emulator.

Corda teaches an emulator, coupled to the storage device and receiving a first application corresponding to a first card, the first application being one of the plurality of applications (column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

- **Corda -** The mobile communication device further comprises a MIFARE memory MM which can either be configured as a MIFARE Classic card or a MIFARE Emulation card… The mobile communication device 1 further comprises a swap memory SM. …For instance, the Swap memory SM is located in a secure memory of a Smartcard 4, e.g. a SmartMX card, being schematically represented in FIG. 4 by dotted lines. In the present example the Smartcard 4 also comprises

> a memory portion that emulates the MIFARE memory MM. However, it should be emphasized that the MIFARE memory MM can also be a MIFARE Classic card, e.g. 1 kB or 4 kB card… by enabling the user to manage MIFARE applications Swapping the user will be able to choose which coupons he needs to be located in the MIFARE memory MM at the moment…. The MIFARE applications manager MAM first stores this MIFARE application "Ticket 7' in the swap memory SM and then searches for a free sector in the MIFARE memory MM. A free sector (sector 0x2) is found and swapping can be done between the free MIFARE memory sector 0x2 and the "Ticket 7", meaning the MIFARE application "Ticket 7' is written into sector 0x2 of the MIFARE memory MM by the MIFARE applications manager MAM. (column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

the first application received and executed in the emulator, wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator and replaced by the second application (column 5, line 58-67, column 8, line 40-49);

- **Corda -** or by means of a NFC reader/writer when the mobile communication device 1 has NFC capabilities and is located within the range of such a NFC reader/writer… the MIFARE applications manager MAM carries out swapping between these two tickets "Ticket1 and "Ticket7". The final state (FIG. 8C) shows the result of the Swapping operation. In the Swap memory SM "Ticket1 is still

> stored, but has no longer a sector indication (meaning that it is no longer located in the MIFARE memory MM). On the other hand, a sector indication (sector 0x2) has been added to the “Ticket 7' in the swap memory SM and this MIFARE application “Ticket 7' is now also stored in sector 0x2 of the MIFARE memory MM. (column 5, line 58-67, column 8, line 40-49)

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen when the second application has been unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application (Figure 1; column 5, line 9-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

- **Corda -** The mobile communication device 1 has a user interface comprising a keyboard 3 and a display 2. It further comprises a processor and memory…The trigger signals TS that are detectable by the MIFARE applications manager MAM may also be signals generated by the user interface of the mobile communication device 1, particularly by the keyboard 3. Thereby the MIFARE applications manager MAM offers an interface to the user of the mobile communication device 1 to enable him/her to trigger a MIFARE applications swapping by himself/herself. …A swapping instruction sent by a Service Provider etc. to the mobile communication device either as an SMS via the over-the-air service of a Mobile Network Operator or via RFID reader/writers which are connected to the

Service Provider via a communication network. For the implementation of this feature the MIFARE applications manager MAM comprises an interface to the SMS stack in order to give the mobile communication device 1 being configured as a NFC phone the ability to trigger MIFARE application Swapping operation on reception of a "Swapping-SMS which contains all the information about the Swapping operation to be done. (Figure 1; column 5, line 13-15, 58-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the first application is out of the emulator and the second application is activated and executed in the emulator (column 5, line 56, 57, column 6, line 35-67; claim 1, 18)

- **Corda -** MIFARE applications are for instance tickets, coupons, access controls, e-purse functions, etc… in order to instruct the MIFARE applications manager MAM to perform a Swap and put the right concert ticket into the MIFARE memory MM. … an applications manager configured to Swap applications between the first memory and the Swap memory Such that a first application that is stored at a first location on the first memory prior to Swapping replaces a second application that is store data second location on the Swap memory, and Such that the second application replaces the first application at the first location on the first memory, wherein the first application is different from the second application. (column 5, line 56, 57, column 6, line 35-67; claim 1)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*" and Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" in order to provide enough memory for multiple applications and store them in a secure way (Corda; column 3, line 43-67).

Neither Behren nor Corda use the term "emulator". Hosogoe uses the term "emulator" (Abstract; ¶44-51).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*", Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" and Hosogoe(¶1), which teaches "*a multi-application type IC card having a plurality of functions including credit card and electronic money functions*" in order to ensure higher

security and great data volume to enact more monetary functions than a conventional magnetic card (Hosogoe; ¶ 2-4).

32. Regarding claims 2 and 13, Behren discloses further comprising a the secure element that has been personalized by operations of: initiating data communication by the mobile device with the designated server providing trusted service management (TSM) (column 5, line 11-33, column 7, line 59-67, column 8, line 1-14, column 23, line 33-67, column 24, line 1-56, column 26, line 1-16); sending device information of the secure element in responding to a request from the designated server when the designated server determines that the secure element is registered therewith (column 23, line 33-67, column 24, line 1-56, column 26, line 1-16), wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (column 7, line 1-21); and receiving in the secure element at least a set of keys from the designated server, wherein the set of keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider (column 19, line 28-67, column 25, line 1-26, column 26, line 1-16).

- **Claim Interpretation-** The claim is directed to the mobile device, not the functions of the designated server, Therefore, it would be impossible for the mobile device to know for example, that the designated server has determined the secure element is registered with it. For the purpose of claim interpretations, the limitation will be understood to mean the secure element, comprised in the phone is sending device information.

33. Regarding claims 3 and 14, Behren discloses wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device (column 4, line 38-67).

34. Regarding claim 4, Corda teaches wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator (Figure 1; column 5, line 9-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18).

35. Regarding claim 5, Behren discloses wherein at least one of the cards is a contactless card (Figure 1; column 4, line (38-66).

36. Regarding claims 6 and 15, Behren discloses wherein the secure further includes a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications (column 6, line 37-67, column 19, line 28-67, column 23, line 1-32, column 25, line 1-26).

- **Claim Interpretation** – According to the specification(¶ 69, 72), "a service provider can access to all Mifare service objects (i.e., Mifare applications)… the TMSM **106** includes a set of service objects and corresponding key indexes. Each logical Mifare card in the TMSM **106** is called a service object… Each application can be associated with a key set index (also called key version number) of the installed SSD (Supplementary Secured Domain) key. " For the purpose of claim interpretation, the service objects will be understood to mean the applications and/or cards they correspond to.

37. Regarding claims 7 and 16, Behren discloses wherein the mobile device further provides: a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information (Figure 1; column 5, line 41-67, column 7, line 38-42, column 9, line 3-27, column 10, line 13-49, column 13, line 18-26, column 18, line 27-35, column 20, line 48-61); and a transaction UI application for conducting operations to modify one or more sectors in one or more of the applications (column 5, line 7-33, column 8, line 1-59, column 21, line 6-21).

38. Regarding claims 9 and 17, Behren discloses wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element (column 5, line 11-33, column 7, line 59-67, column 19, line 28-67, column 25, line 1-26, column 26, line 1-16).

39. Regarding claims 10 and 18, Behren discloses wherein the mobile device is a smartphone or a portable computer (column 4, line 38-67).

40. Claims 11 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over von Behren et al. (8,646,059) ("Behren"), in view of Corda et al. (9,128,829) ("Corda"), in view of Hosogoe et al. (2003/0151125) ("Hosogoe") and further in view of Wentker et al. (6,481,632) ("Wentker").

41. Regarding claim 11, Behren discloses wherein each of the applications has been remotely provisioned by the designated server with operations of: sending a request from the mobile device to the designated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider (column 5, line 11-33, column 7, line 59-67, column 8, line 1-14,

column 23, line 33-67, column 24, line 1-56, column 26, line 1-16); establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server; receiving data for the application being provisioned from the designated server (Figure 3; column 5, line 11-33, column 7, line 59-67, column 8, line 1-14, column 23, line 33-67, column 24, line 1-56, column 26, line 1-16), and notifying the application provider of a status of the application with the mobile device (column 24, line 1-56, column 25, line 8-26).

Neither Behren, Corda nor Hosogoe teaches wherein the data for the application includes supplemental security domains (SSD) to be associated with the application. Wentker teaches wherein the data for the application includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Behren, Corda, Hosogoe and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

42. Claim 12 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over von Behren et al. (8,646,059) ("Behren"), in view of Corda et al. (9,128,829) ("Corda"), and further in view of Hosogoe et al. (2003/0151125) ("Hosogoe").

43. Regarding claim 12, Corda discloses installing in a storage device of the mobile device a plurality of applications downloaded from a designated server, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated server (column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

- **Corda -** The mobile communication device further comprises a MIFARE memory MM which can either be configured as a MIFARE Classic card or a MIFARE Emulation card… The mobile communication device 1 further comprises a swap memory SM. …For instance, the Swap memory SM is located in a secure memory of a Smartcard 4, e.g. a SmartMX card, being schematically represented in FIG. 4 by dotted lines. In the present example the Smartcard 4 also comprises a memory portion that emulates the MIFARE memory MM. However, it should be emphasized that the MIFARE memory MM can also be a MIFARE Classic card, e.g. 1 kB or 4 kB card… by enabling the user to manage MIFARE applications Swapping the user will be able to choose which coupons he needs to be located in the MIFARE memory MM at the moment…. The MIFARE applications manager MAM first stores this MIFARE application "Ticket 7' in the swap memory SM and then searches for a free sector in the MIFARE memory MM. A free sector (sector 0x2) is found and swapping can be done between the free MIFARE memory sector 0x2 and the "Ticket 7", meaning the MIFARE application "Ticket 7' is written into sector 0x2 of the MIFARE memory MM by the MIFARE applications manager MAM. (column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

receiving in an emulator of the mobile device a first application corresponding to a first card(column 5, line 58-67, column 8, line 40-49);

- **Corda -** or by means of a NFC reader/writer when the mobile communication device 1 has NFC capabilities and is located within the range of such a NFC reader/writer… the MIFARE applications manager MAM carries out swapping between these two tickets “Ticket1 and “Ticket7”. The final state (FIG. 8C) shows the result of the Swapping operation. In the Swap memory SM “Ticket1 is still stored, but has no longer a sector indication (meaning that it is no longer located in the MIFARE memory MM). On the other hand, a sector indication (sector 0x2) has been added to the “Ticket 7' in the swap memory SM and this MIFARE application “Ticket 7' is now also stored in sector 0x2 of the MIFARE memory MM. (column 5, line 58-67, column 8, line 40-49)

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in entirety by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when the second card is selected by the and the first and replaced by the second application in the emulator(Figure 1; column 5, line 9-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

- **Corda -** The mobile communication device 1 has a user interface comprising a keyboard 3 and a display 2. It further comprises a processor and memory…The trigger signals TS that are detectable by the MIFARE applications manager MAM may also be signals generated by the user interface of the mobile communication

> device 1, particularly by the keyboard 3. Thereby the MIFARE applications manager MAM offers an interface to the user of the mobile communication device 1 to enable him/her to trigger a MIFARE applications swapping by himself/herself. …A swapping instruction sent by a Service Provider etc. to the mobile communication device either as an SMS via the over-the-air service of a Mobile Network Operator or via RFID reader/writers which are connected to the Service Provider via a communication network. For the implementation of this feature the MIFARE applications manager MAM comprises an interface to the SMS stack in order to give the mobile communication device 1 being configured as a NFC phone the ability to trigger a MIFARE application Swapping operation on reception of a "Swapping-SMS which contains all the information about the Swapping operation to be done. (Figure 1; column 5, line 13-15, 58-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

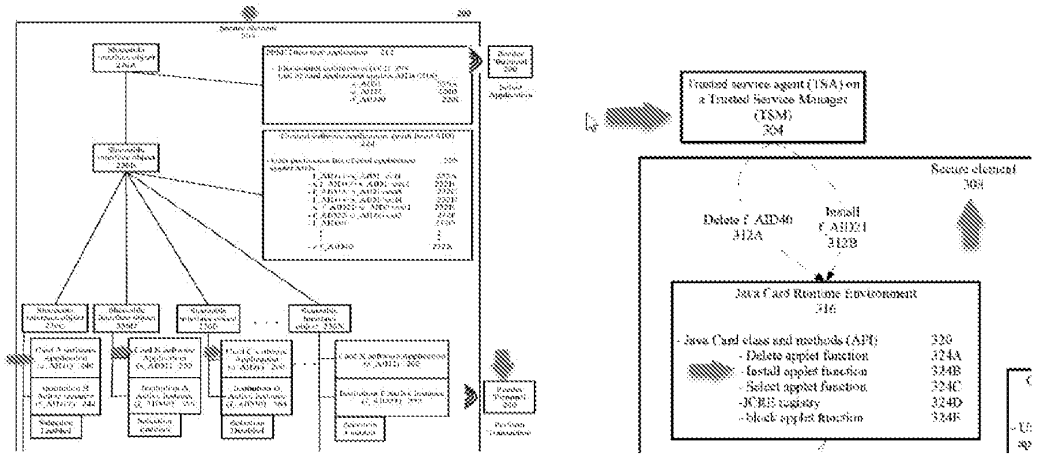
causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator(column 5, line 56, 57, column 6, line 35-67; claim 1, 18)

- **Corda -** MIFARE applications are for instance tickets, coupons, access controls, e-purse functions, etc… in order to instruct the MIFARE applications manager MAM to perform a Swap and put the right concert ticket into the MIFARE memory MM. … an applications manager configured to Swap applications between the first memory and the Swap memory Such that a first application that is stored at a first location on the first memory prior to Swapping replaces a second application that is store data second location on the Swap memory, and Such that the second application replaces the first application at the first location on the first memory, wherein the first application is different from the second application. (column 5, line 56, 57, column 6, line 35-67; claim 1)

Corda does not disclose that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards on the mobile device; showing a list of the cards on a display of the mobile device for a user to choose one therefrom; but the second application has been locked by the designated server.

Behren teaches that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards on the mobile device(Figure 2, 3; column 4,

line 49-67, column 5, line 11-67, column 7, line 22-67, column 8, line 1-14, column 13, line 45-62, column 19, line 27-38, column 22, line 25-53, column 26, line 1-43) ;



- **Behren** - An external trusted service manager (TSM) 108 controlled by a near field communications (NFC) service provider 104 hosts and transmits card software applications for installation within the secure element 152 of a contactless Smart card in mobile device 140. The NFC service provider 104 provides a secure key encrypted Software card application for decryption and installation in the Secure element 152. .. The term “card software application' and “card applet” are used interchangeably in this disclosure to refer to a software applications running within the secure element of a Smart card… to instantiate a Trusted Service Manager (TSM) Security Domain for download of payment and other card Software applications, to lock/unlock card Software applications, and to terminate secure element Software applications.,… The payment applications may be loaded on the mobile device as a card Software application package, where each package, for example, a MasterCard package, typically contains Software code for all Supported payment applications within MasterCards'

offerings, e.g., Mstripe, Mchip, and any other Suitable payment application. (column 4, line 63-66, column 5, line 11-33, column 7, line 62-67, column 8, line 1, 2)

showing a list of the cards on a display of the mobile device for a user to choose one therefrom(Figure 1; column 5, line 41-67, column 7, line 38-42, column 9, line 3-27, column 10, line 13-49, column 13, line 18-26, column 18, line 27-35, column 20, line 48-61)

- **Behren** - the user may choose from different card types (for example, PayPass, Paywave, debit cards, or other types) from different credit card companies (for example, MasterCard, Visa, Discover, or other companies), as well as different bank instances (for example, Bank A, B, C, and D) for each card type on the user-interface… the wallet application can be used by the contactless payment device user to select certain card Software applications as preferred applications via a user-inter face, thereby creating an order based on the type of card Software application. … When a full sized AID is selected, the directory software application then routes payment transaction commands according to user selected settings, directly to the selected instance… Here, all the data in the PPSE may not be distributed to merchants' reader by default, but is available to the user for selection via the user-interface. The user may choose to use the access functionality for specific payments on short distance contactless communication with a specific merchant terminal. T (column 5, line 41-67, column 7, line 38-42, column 9, line 14-18, column 18, line 27-32)

but the second application has been locked by the designated server(column 5, line 11-17, column 9, line 28-65, column 15, line 36-63, column 16, line 55- 67, column 17, line 1-60, column 19, line 8-17, column 24, line 1-67)

- **Behren -** Alter natively, the TSM may issue pre-defined instructions for such exemplary external functions, as blocking/unblocking a card Software application… to instantiate a Trusted Service Manager (TSM) Security Domain for download of payment and other card Software applications, to lock/unlock card Software applications, and to terminate secure element Software applications… The control software application includes a list 232 of the activate/inactive/non-activatable card Software application AIDs in certain format…When a card Software application 240,252,260, and 268 is enabled, the SIO is active and is accessed by the client mode control Software application 224…. In certain exemplary embodiments, for the UNBLOCKED/BLOCKED functions from the JCRE 316, based on requests from the TSA 304 may be rendered on a selected AID of the card software application 360 for blocking. The instruction for blocking or unblocking may be defined by the control software application 328 using APIs from the JCRE that causes a selected card software application360 to trigger an event to the control software application 328… In certain exemplary embodiments, the internal method calls applicable may include Such custom functions as, a enableSelection (byte aid): Boolean, for enabling selection of a payment card Software application and returning values as true if enabled or false for a general error (for example, the applet is locked). Another exemplary method call includes the disableSelection (byte aid): Void, which

disables selection of a payment type card Software application… (column 5, line 11-17, column 9, line 41-65, column 15, line 36-43, column 16, line 66, 67, column 17, line 1-7, column 24, line 41-44)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" and Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*" in order to provide a device owner access to several types of services that range from financial transactions to secure authentication (Behren; column 1, line 43-66).

Neither Corda nor Behren use the term "emulator". Hosogoe uses the term "emulator" (Abstract; ¶44-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" and Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*" and Hosogoe(¶1), which teaches "*a multi-application type IC card having a plurality of functions including credit card and electronic money functions*"

in order to ensure higher security and great data volume to enact more monetary functions than a conventional magnetic card (Hosogoe; ¶ 2-4).

Conclusion

44. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Hisano et al., (US 20060034043) teaches emulating first information and converting to second information.
- Spodak et al. (US 20130134216) teaches a universal card with multiple cards that emulates the different cards.
- Sklovsky et al (US 20090247077) teaches switching between applications on a mobile device.
- Tang et al. (US 20130331029) teaches secure elements with emulating functions for multiple applications.
- Finkenzeller et al. (US 20090199206) teaches switching between applications and utilizing a reading device to communicate with the applications.

45. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ISIDORA I IMMANUEL/
Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination Xie et al.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20030151125-A1	08-2003	Hosogoe, Takashi	G06Q20/3574	257/679
*	B	US-9128829-B2	09-2015	Corda; Alexandre	G06F12/0638	1/1
*	C	US-8646059-B1	02-2014	von Behren; Rob	G06Q20/3574	726/9
*	D	US-6481632-B2	11-2002	Wentker; David C.	G06F8/60	235/376
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Samsung Ex. 1016, Page 533 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

CPC - Searched*		
Symbol	Date	Examiner
G06Q20	08/17/2020	III
G06Q2220	08/17/2020	III

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
705			

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See attached notes	2/1/2016	II
101 withdrawal - Weinhart	06/06/2018	III
See attached notes (EAST)	04/15/2019	III
EAST search report	08/17/2020	III
NPL search	08/17/2020	III

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	

Samsung Ex. 1016, Page 534 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	**Art Unit**
	ISIDORA I IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016	09/17/2017	05/22/2018	04/15/2019	12/18/2019	08/17/2020		
	1	✓	✓	✓	✓	✓	✓	✓		
	2	✓	✓	✓	✓	✓	✓	✓		
	3	✓	✓	✓	✓	✓	✓	✓		
	4	✓	✓	✓	✓	✓	✓	✓		
	5	✓	✓	✓	✓	✓	✓	✓		
	6	✓	✓	✓	✓	✓	✓	✓		
	7	✓	✓	✓	✓	✓	✓	✓		
	8	✓	✓	✓	✓	✓	✓	-		
	9	✓	✓	✓	✓	✓	✓	✓		
	10	✓	✓	✓	✓	✓	✓	✓		
	11	✓	✓	✓	✓	✓	✓	✓		
	12	✓	✓	✓	✓	✓	✓	✓		
	13	✓	✓	✓	✓	✓	✓	✓		
	14	✓	✓	✓	✓	✓	✓	✓		
	15	✓	✓	✓	✓	✓	✓	✓		
	16	✓	✓	✓	✓	✓	✓	✓		
	17	✓	✓	✓	✓	✓	✓	✓		
	18	✓	✓	✓	✓	✓	✓	✓		
	19	✓	✓	✓	✓	✓	✓	✓		

Samsung Ex. 1016, Page 535 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	10	(("9128829") or ("8646059") or ("20030151125") or ("6481632")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 13:45
S2	178	((("(6101543") or ("20130178159") or ("20170323301") or ("20170372321") or ("20200034849") or ("5249218") or ("5353334") or ("5367563") or ("5530703") or ("5640444") or ("5937421") or ("5963650") or ("5995839") or ("6078314") or ("6108003") or ("6137791") or ("6373820") or ("6802058") or ("6853851") or ("6912389") or ("7006964") or ("7039434") or ("7151931") or ("7155381") or ("7162408") or ("7165191") or ("7231330") or ("7296190") or ("7317912") or ("7319874") or ("7319948") or ("7324588") or ("7334162") or ("7392060") or ("7450936") or ("7486927") or ("7502626") or ("7512402") or ("7516451") or ("7545386") or ("7548804") or ("7577887") or ("7606261") or ("7613453") or ("7620015") or ("7698121") or ("7734288") or ("7738426") or ("7783261") or ("7809578") or (").pn.")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 11:43
S3	596	(emulat$4 with application) and (secure adj element)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:32
S4	272	(emulat$4 with application) same (secure adj element)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:32

S5	245	S3 AND ((G06Q20/3278 OR G06Q20/3829 OR G06Q20/3821 OR G06Q2220/00 OR G06Q20/3226 OR G06Q20/3825 OR G06Q2220/14).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:34
S6	108	S4 AND ((G06Q20/3278 OR G06Q20/3829 OR G06Q20/3821 OR G06Q2220/00 OR G06Q20/3226 OR G06Q20/3825 OR G06Q2220/14).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:34
S7	6	(("9128829") or ("8646059") or ("20030151125")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:36

EAST Search History (Interference)

<This search history is empty>

8/17/2020 1:46:43 PM
C:\Users\iimmanuel\Documents\EAST\Workspaces\13782948.wsp

STIC Scientific & Technical Information Center

EIC 3600 Search Report

Requester	Immanuel, Isidora Emp#: 90925 TAB-55086 (469) 295-9094 isidora.immanuel@uspto.gov
Case Serial Number:	13/782948
Access Search Log Number:	619540

Searcher:	Sylvia Keys
Location:	EIC 3600, Knox 4B68
Phone:	571-272-3534
Email:	sylvia.keys@uspto.gov
Date Completed:	6/11/2020

This search report contains the following content:

- **Search Histories**
  Keyword/synonym strings and search strategies used by the EIC Searcher in completing the prior art search are included. The search history for each database or resource utilized appears at the top of each database/resource section, indicated by the database/resource section headings.
- **Search Results**
  Only on-topic results are included in the search report. On-topic results include all references found that are related to the art area being searched. These references may not necessarily be useful for a rejection or other office action, but are included for the Examiner's review. Off-topic, unrelated, or irrelevant search results ("false drops" or "false hits") were removed by the Searcher. Off-topic results include all references that are unrelated to the art area being searched.

If you have any questions about this search, or about how to interpret this search report, please do not hesitate to contact the Searcher using the contact information listed above.

If you need assistance retrieving the full text of any of the references contained in this report, please contact the Searcher listed above, or the EIC 3600 Reference Desk at 571-272-3488 (x23488) or STIC-EIC3600@uspto.gov.

Thank you for using the EIC, and we look forward to your next search!

Samsung Ex. 1016, Page 538 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Potential References of Interest

7

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Cho, Fu-Liang; Cho, Fu-Tong; Fung, Daniel; Pan, Hsin (Inventors). RFCyber Corporation (Assignee). **US 20060161878 A1**. (Published 20 Jul 2006).

... system **10**, alternatively termed RFCyberWork, is a platform for ...

- 8

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Fu-Tong, Cho; Fu-Liang, Cho; PAN HSIN (Inventors). RFCYBER CORP (Assignee). **TW 200632705 A**. (Published 16 Sep 2006).

- 1

NFC - The intuitive contactless technology becomes reality

Dachs, C.. **Elektrotechnik und Informationstechnik** 122.12: 466-471. Springer Wien. (Dec 2005)

EnglishENGEnglish

Near Field Communication (NFC) is opening-up completely new ... mobile communication industry. It enables contactless peer-to-peer communication, reading/writing of contactless ...

Dialog –Patent Files and Inventors

Search Strategy

Databases: Argentina Patents Fulltext, Australia Patents Fulltext, Austria Patents Fulltext, Belgium Patents Fulltext, Brazil Patents Fulltext, Canada Patents Fulltext, China Patents Fulltext, Denmark Patents Fulltext, Derwent Chemistry Resource, Derwent Patents Citation Index®, Derwent World Patents Index®, Eurasia Patents Fulltext, European Patents Fulltext, Finland Patents Fulltext, France Patents Fulltext, Germany Patents Fulltext, Global Patents Bibliographic, Great Britain Patents Fulltext, IFI CLAIMS® US Patents and Legal Status, IMS Patent Focus, India Patents Fulltext™, INPADOC / Family and Legal Status, Ireland Patents Fulltext, Italy Patents Fulltext, Japan Patents Fulltext, JAPIO - Patent Abstracts of Japan, Korea Patents Fulltext, LitAlert®, Luxembourg Patents Fulltext, Mexico Patents Fulltext, Monaco Patents Fulltext, Netherlands Patents Fulltext, Norway Patents Fulltext, Portugal Patents Fulltext, Russia Patents Fulltext, Spain Patents Fulltext, Sweden Patents Fulltext, Switzerland Patents Fulltext, United States Patents Fulltext, WIPO PCT Patents Fulltext

Set#	Searched for	Results
S1	au((xie or koh or pan))	2732377
S2	rfcyber*	633
S3	s1 and s2	132
S4	py(2006) and s3	8

Samsung Ex. 1016, Page 539 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

- ☐ 2

SYSTEM FOR DEVELOPING AND DEPLOYING RADIO FREQUENCY IDENTIFICATION ENABLED SOFTWARE APPLICATIONS

Koh, Liang Seng; Fu-Liang, Cho; Fung, Daniel; PAN HSIN (Inventors). RFCYBER CORP (Assignee). **WO 2006074096 A2.** (Published 13 Jul 2006).

☐ 7

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Cho, Fu-Liang; Cho, Fu-Tong; Fung, Daniel; Pan, Hsin (Inventors). RFCyber Corporation (Assignee). **US 20060161878 A1.** (Published 20 Jul 2006).

... system **10**, alternatively termed RFCyberWork, is a platform for ...

- ☐ 8

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Fu-Tong, Cho; Fu-Liang, Cho; PAN HSIN (Inventors). RFCYBER CORP (Assignee). **TW 200632705 A.** (Published 16 Sep 2006).

Dialog – NPL and Inventor(s)

Search Strategy

Databases: ABI/INFORM® Professional Advanced, Abstracts in New Technology & Engineering, AdisInsight: Drugs, AdisInsight: Trials, Adis Pharmacoeconomics & Outcomes News, AGRICOLA, AGRIS, Allied & Complementary Medicine™, Analytical Abstracts, APA PsycInfo®, Aqualine, Aquatic Science & Fisheries Abstracts (ASFA), Australian Education Index, BIOSIS® Toxicology, BIOSIS Previews®, British Library Inside Conferences, British Nursing Index, Business & Industry, CAB ABSTRACTS, Chemical Business Newsbase, Chemical Engineering & Biotechnology Abstracts, Chemical Safety Newsbase, Civil Engineering Abstracts, Current Contents® Search, DH-DATA: Health Administration, Medical Toxicology & Environmental Health, DIOGENES® FDA Regulatory Updates, Drug Information Fulltext, Earthquake Engineering Abstracts, Ei Compendex®, Embase®, EMCare®, ESPICOM Pharmaceutical & Medical Device News, FDAnews, FLUIDEX (Fluid Engineering Abstracts), Foodline®: MARKET, Foodline®: PRODUCT, Foodline®: SCIENCE, FSTA®, Gale Group Computer Database™, Gale Group Health Periodicals Database, Gale Group New Product Announcements / Plus®, Gale Group Newsletter Database™, Gale Group PharmaBiomed Business Journals, Gale Group PROMT®, Gale Group Trade & Industry Database™, GEOBASE™, GeoRef, HSELINE: Health and Safety, ICONDA - International Construction Database, IMS Company Profiles, IMS New Product Focus, IMS Pharma Trademarks, IMS R&D Focus, IMS R&D Focus Drug News, Inspec®, International Pharmaceutical Abstracts, Jane's Defense & Aerospace News, King's Fund, KOSMET: Cosmetic Science, Lancet Titles, Material Safety Datasheets -OHS™, Mechanical & Transportation Engineering Abstracts, MEDLINE®, Meteorological & Geoastrophysical Abstracts, New England Journal of Medicine, NTIS: National Technical Information Service, Oceanic Abstracts, PAIS International, Paperbase, PAPERCHEM, ProQuest Advanced Tech & Aerospace Professional, ProQuest Biological & Health Science Professional, ProQuest Environmental Science Professional, ProQuest Materials Research Professional, ProQuest Newsstand Professional, ProQuest Technology Research Professional, Prous Science Daily Essentials, Prous Science Drug Data Report, Prous Science Drugs Of The Future™,

Samsung Ex. 1016, Page 540 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Registry of Toxic Effects of Chemical Substances (RTECS®), SciSearch®: a Cited Reference Science Database, Social SciSearch®, ToxFile®, Transport Research International Documentation, TULSA™ (Petroleum Abstracts), UBM Computer Full Text, Weldasearch®, Zoological Record Plus

Set#	Searched for	Results
S1	“smart card$1” or smartcard$1	369847*
S2	contactless and (“smart card$1” or smartcard or card$1)	101277*
S3	card$ and (transaction$1 or interact$3 or payment$1 or “monetary function$1”)	4099506*
S4	mifare* or “micron fare collection system”	3361°
S5	(s1 or s2 or s3 or s4) and (switch$3 or replac$3 or substitute$1 or substitution or “back$3 up”)	696777*
S6	(s1 or s2 or s3 or s4) and (activate$1 or activation or activating)	159179*
S7	(s1 or s2 or s3 or s4) and emulat* or imitat* or copy or copies or mimic or mirror or match	56927115*
S8	(nfc or “near field communication$1”) and interface$1	34616*
S9	smartphone (mobile or web or smart or cell or cellular or wireless or cordless or handheld or “hand held” or media or user) n/5 (phone or telephone or fone or device or apparatus or equipment)	640291*
S10	pda or “personal digital assistant” or wireless or cellphone or webphone or palmpilot or "palm pilot" or ipad or iphone or smartphone or tablet or android or pc or “personal computer$1”	26128177*
S11	au((xie or koh or pan))	2541829*
S12	rfcyber*	34°
S13	(s5 or s6 or s7) and s8	11622*
S14	s13 and (s9 or s10)	9968*
S15	su(contactless*) and s14	12°
S16	py(2006) and s14	36°
S17	su(contactless) and s16	0°
S18	su(emulat*) and s14	16°
S19	su("smartcard*") and s14	3°
S20	su("smart card*") and s14	244°
S21	s20 not s19	243°
S22	su(emulat*) and s21	2°
S23	py(2006) and s21	6°
S24	(s11 or s12) and s21	1°
S25	(s11 and s12) and contactless	0°

NFC - The intuitive contactless technology becomes reality

Dachs, C.. **Elektrotechnik und Informationstechnik** 122.12: 466-471. Springer Wien. (Dec 2005)

EnglishENGEnglish

Near Field Communication (NFC) is opening-up completely new ... mobile communication industry. It enables contactless peer-to-peer communication, reading/writing of contactless ...

er already carries around (e. g. ...

CASHLESS PAYMENTS: Contactless cuts out cash and cards

Electronic Payments International: 8-9. London: Lafferty Ltd. (Feb 2006)

... major trials using MasterCard International's contactless payment technology PayPass. The Royal Bank ... on a Maestro or MasterCard card or be offered as a ...

Electronic Acknowledgement Receipt

EFS ID:	41220781
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	24-NOV-2020
Filing Date:	01-MAR-2013
Time Stamp:	21:49:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	ResponseTo1stOAAfter2ndAppeal.pdf	167607 4c6dd618765dc7b377cef5aaf466f6ce3eb95aa1	no	14

Warnings:

Information:	
Total Files Size (in bytes):	167607

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

November 24, 2020

Mail Stop: No-Fee Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to 1st OA (in RCE proceeding)

Dear Sir:

In response to the Final Office Action dated 08/24/2020, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

AMENDMENTS TO THE CLAIMS are reflected in the listing of claims which begins on page 2 of this Response.

REMARKS/ARGUMENTS begin on page 9 of this Response.

Samsung Ex. 1016, Page 545 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

Please amend Claims 1-2, 11-13 and 19 as follows:

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of applications~~the cards~~ for a user of the mobile device to choose one therefrom, each of the applications corresponding to one of the cards ~~wherein a display of the list of the cards is provided via a designated server~~;

~~a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards~~a secure element including a memory for storing the application and executing a service manager to manage the applications, wherein the service manager includes a table to keep track of the applications and cause the applications provisioned remotely via ~~, wherein each of the applications is provisioned remotely with~~ the ~~designated~~dedicated server that subsequently installs corresponding data and keys for ~~the one~~ each of the cards in the mobile device, the data ~~can~~ is only be modified by the ~~designated~~dedicated server over a secured channel;

an emulator, ~~coupled to the storage device and~~ coupled to the memory ~~implemented in a secure element,~~ receiving a first application corresponding to a first card in accordance with the service manager, the first application being one of the plurality of applications, wherein the table in the service manager updates a counter when the first application is successfully loaded in the emulator;

a communication interface, coupled to the secure element, ~~to~~ facilitating data exchange wirelessly between a reader and the first application received and executed in the emulator, wherein the reader is external to the mobile device, the secure element communicates with the reader via the communication interface, ~~and~~ the first application in the emulator is replaced~~able~~ in entirety or partially by a second application corresponding to a second card when another

Samsung Ex. 1016, Page 546 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

one of the cards is selected by the user, wherein the service manager receives a request to activate the second application and performs a validation to the second application, the first application is out of the emulator and replaced by the second application with the table updated per the second application; and the service manager conducts ~~a processor, in communication with the emulator and the storage device, performing~~ an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen and when the second application has been unlocked by the ~~designated~~dedicated server, wherein said operation of causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application has been locked remotely by the ~~designated~~dedicated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the first application is out of the emulator and the second application is activated and executed in the emulator.

2. (*Currently amended*) The mobile device as recited in claim 1, further comprising the secure element that has been personalized by operations of:

initiating data communication by the mobile device with the ~~designated~~dedicated server providing trusted service management (TSM);

sending device information of the secure element in responding to a request from the ~~designated~~dedicated server when the ~~designated~~dedicated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the ~~designated~~dedicated server, wherein the set of keys are generated in accordance with the device information of the secure element, the set of keys

Samsung Ex. 1016, Page 547 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

3. (*Previously amended*) The mobile device as recited in claim 2, wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

6. (*Previously amended*) The mobile device as recited in claim 3, wherein the secure element further includes a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

7. (*Previously amended*) The mobile device as recited in claim 6, wherein the mobile device further provides:

   a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information; and

   a transaction UI application for conducting operations to modify one or more sectors in one or more of the applications.

8. (*Cancelled*)

Samsung Ex. 1016, Page 548 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

9. (*Currently amended*) The mobile device as recited in claim 2, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information ~~updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element~~.

10. (*Previously amended*) The mobile device as recited in claim 2, wherein the mobile device is a smartphone or a portable computer.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the ~~designated~~dedicated server with operations of:

sending a request from the mobile device to the ~~designated~~dedicated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider;

establishing a secured channel between the mobile device and the ~~designated~~dedicated server using a set of keys received from the ~~designated~~dedicated server;

receiving data for the application being provisioned from the ~~designated~~dedicated server, wherein the data for the application includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

installing in a memory~~storage device~~ of the mobile device a plurality of applications downloaded from a ~~designated~~dedicated server, each of the applications being managed by a service manager executed in a secure element in communication with the memory~~the designated server pertaining to one of the cards~~, wherein the memory is included in the secure element.

Samsung Ex. 1016, Page 549 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

the service manager includes a table to keep track of the applications and cause the applications provisioned remotely via ~~each of the applications is provisioned remotely with~~ the ~~designated~~dedicated server that subsequently installs corresponding data and keys for ~~the one~~each of the cards in the mobile device, the data ~~can~~ is only be modified by the ~~designated~~dedicated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards on the mobile device;

showing ~~a list of~~ the applications ~~the cards~~ on a display of the mobile device for a user to choose one therefrom, each of the applications corresponding to one of the cards;

receiving in an emulator of the mobile device a first application corresponding to a first card, wherein the table in the service manager updates a counter when the first application is successfully loaded in the emulator;

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replace~~dable~~ in entirety by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when the second card is selected by the user, ~~and~~ the first application is~~and~~ replaced by the second application in the emulator;

causing the second application to replace the first application loaded and executed in the emulator, wherein the table is updated per the second application, said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application has been locked by the ~~designated~~dedicated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator.

Samsung Ex. 1016, Page 550 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

13. (*Currently amended*) The method as recited in claim 12, wherein the mobile device is associated with a secure element, and the method further comprises:

initiating data communication by the mobile device with the ~~designated~~dedicated server;

sending device information of the secure element in responding to a request from the ~~designated~~dedicated server after the ~~designated~~dedicated server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein; and

receiving in the secure element at least a set of keys from the ~~designated~~dedicated server, wherein the keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.

14. (*Original*) The method as recited in claim 13, wherein the emulator is implemented in the secure element, the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Previously amended*) The method as recited in claim 14, wherein the secure element further includes a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications.

16. (*Previously amended*) The mobile device as recited in claim 15, further providing:

querying via a user interface (UI) one or more of the applications; and

conducting operations that modify one or more sectors in one or more of the applications.

Samsung Ex. 1016, Page 551 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

17. (*Currently amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information ~~updatable entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element~~.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Currently amended*) The method as recited in claim 12, wherein each of the applications has been remotely provisioned by the ~~designated~~dedicated server with operations of:

receiving a request to provision an application installed in the mobile device, wherein the application to be provisioned with the secure element is distributed by an application provider;

establishing a secured channel with the secure element using a set of keys;

preparing data for the application being provisioned, wherein the data includes supplemental security domains (SSD) to be associated with the application; and

notifying the application provider of a status of the application with the mobile device.

Samsung Ex. 1016, Page 552 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

REMARKS

Claims 1 – 7 and 9 - 19 were examined again. In the Office Action dated 08/24/2020, Claims 1-7, 9, 10, and 13-18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over van Behren et al. (8,646,059) ("Behren"), in view of Corda et al. (9, 128,829) ("Corda"), and further in view of Hosogoe et al. (2003/0151125) ("Hosogoe"), Claims 11 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Behren in view of Corda in view of Hosogoe et al. (2003/0151125) ("Hosogoe") and further in view of Wentker et al. (6,481,632) ("Wentker"), and Claim 12 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Behren in view of Corda and further in view of Hosogoe.

In the foregoing amendments, Claims 1-2, 11-13 and 19 have been amended to further distinguish from the cited references. No new matters are introduced. Claims 1 – 7 and 9 - 19 are still pending.

Interview Summary

The Applicant appreciates the Examiner for granting a conference call among the Examiner herself, co-inventor Liang Seng Koh and the undersigned. The call took place on August 11, 2020. The Applicant and the Examiner had the opportunity to discuss proposed allowable claims by the Examiner on Claim 1. No agreement was reached. The Examiner will reconsider proposed amendments when a formal response is filed.

Claim Interpretation

Claim Rejections - 35 USC § 112

On page 4, Section 14, of the Office Action, the Examiner states that this application includes one or more claim limitations that do not use the word "means," but are nonetheless being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because the claim limitation(s) uses a generic placeholder that is coupled with functional language without reciting sufficient structure to perform the recited function.

Samsung Ex. 1016, Page 553 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Assuming the foregoing amendments are entered, the Applicant respectfully disagrees with the interpretation by the Examiner under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph. Claim 1 as amended recites explicitly the sufficient structure, such as "*a secure element including a memory for storing the application and executing a service manager to manage the applications*" and "*an emulator, coupled to the memory…*". Other terms such as "*a communication interface facilitating data exchange wirelessly between a reader and the first application received and executed in the emulator*" are well known structural. It is believed that the interpretation under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph is moot.

Claim Rejections - 35 USC § 112

On Page 6, Section 16, of this Office Action, Claims 1-7, and 9-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The Applicant respectfully disagrees and traverses the rejections as follows.

In Section 17, the Examiner alleges "There is no written description support for the designated server performing the functions of the claimed TSM server and an application provider." The Applicant wishes to refer the Examiner to FIG. 1D, Block 154 that explicitly uses "a dedicated server". It is believed that there is no difference between "dedicated server" and "designated server" in meaning. Nevertheless, the Applicant has amended the claims to recite "dedicated server".

In Section 18, the Examiner alleges "*The displayed information are applications, not cards*". The Applicant wishes to state that a mobile device or a display device would not be able to display a physical card. When a card is being displayed, it is well known to those skilled in the art that the card is an electronic representation of an application. Nevertheless, the Applicant has amended Claim 1 to clarify the wording.

In Section 19, the Examiner alleges "Neither the figures nor the specification describe a device other than the secure element that is used to store both the plurality of applications and the emulator." The Applicant respectfully points out that

Samsung Ex. 1016, Page 554 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

a secure element shown in FIG. 1A is a type of processor that includes a store (e.g., memory) for storing data and applications. The store (often RAM devices) acts as memory or storage and is certainly not a generic storage device (e.g., a hard disk). Accordingly, the Applicant has amended Claim 1 to refer such a store as memory.

In Section 20, the Examiner alleges "the specification does not describe or mention the SE being preloaded with and ISO (entirely or partially updated) or that these are based on [a] retrieved default ISO information from an entity that created the secure element". The Applicant has amended Claims 9 and 17 to clarify the wording.

On Page 9, Section 22, of this Office Action, Claims 1-7, and 9-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), second paragraph, as failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

The Applicant respectfully disagrees and traverses the rejections. As reasoned above, the foregoing amendments are believed to have made the interpretation under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112 moot. The Drawings show the structural details, together with the Specification. On Page 11, the Examiner admits "In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification [paragraphs] 5, 7, 11, 56, 57, 59-61, 75, 76, 91 and 92." Accordingly, the rejections under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA) shall be withdrawn.

Claim Rejections - 35 USC § 103

On Page 14, Section 30, of this Office Action, Claims 1-7, 9, 10, and 13-18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Behren in view of Corda and further in view of Hosogoe.

As amended, Claim 1 recites:

…

Samsung Ex. 1016, Page 555 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

an emulator, coupled to the memory, receiving a first application corresponding to a first card in accordance with the service manager, the first application being one of the plurality of applications, wherein the table in the service manager updates a counter when the first application is successfully loaded in the emulator;

a communication interface, coupled to the secure element, facilitating data exchange wirelessly between a reader and the first application received and executed in the emulator, wherein the reader is external to the mobile device, the secure element communicates with the reader via the communication interface, …

(*emphasis added*)

As shown in FIG. 1A, the secure element 108 includes an emulator 122, a memory to store the applications (applets) and a service manager 106 managing these applications. The emulator 122 executes one of the applications at a time to emulate one of the cards supported in a mobile device, where a table is provided to track which one of the applications is being executed in the emulator. As admitted by the Examiner on Pages 18-19, Behren does not disclose an emulator and several other limitations recited in Claim 1. Another important distinction between Claim 1 as amended and Behren is that it is the emulator that communicates with a reader (external to the mobile device) while Behren uses an NFC reader to interact directly with individual card software to communicate with an external reader.

On Page 19, the Examiner admits cites Corda to be combined with Behren to show the teaching of an emulator. The Applicant respectfully contests the combination of Behren and Corda as it is believed that there is no motivation to combine these two references in the manner proposed by the Examiner. Corda teaches managing sectors of a memory card with controlling software. As explicitly shown in FIG. 7 - FIGS. 10C and described in corresponding specification, Corda shows how all features of an application are enabled by managing sectors of a memory. The subtle difference between Corda and the instant application is that Corda teaches utilizing all features of an application by swapping relevant data into certain sectors of a

Samsung Ex. 1016, Page 556 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

memory card while the instant application recites emulating a card (running a loaded application entirely by unloading another application from the emulator). The Applicant submits the modification of Behren with Corda would not cure the deficiency in Behren as stated above. The combination of Behren with Corda is improper. Claim 1 as amended shall be allowed over Behren and Corda, viewed alone or in combination.

On Page 23, the Examiner admits "Neither Behren nor Corda use the term "emulator" and then cites Hosogoe to show the use of the term "emulator". Again the Applicant respectfully contests the combination of Behren, Corda and Hosogoe as it is believed that there is no motivation to combine these three references in the manner proposed by the Examiner. Hosogoe teaches a multi-application type IC card that runs emulator programs to process commands from an external terminal. As the name explicitly suggest and shown in FIG. 1(b), this IC card is loaded with multiple programs, an emulator for each of the programs is needed to access ALL of the programs, which contradicts "*the table in the service manager updates a counter when the first application is successfully loaded in the emulator*" and "*the first application is out of the emulator and replaced by the second application with the table updated per the second application*". In a perspective, the emulator is loaded with and executes only one application. Accordingly, the Applicant submits the modification of Behren nor Corda with Hosogoe would not cure the deficiency in Behren combined with Corda as stated above. The combination of Behren, Corda and Hosogoe is improper. Claim 1 as amended shall be allowed over Behren, Corda and Hosogoe, viewed alone or in combination.

Claim 12 was amended similarly to Claim 1. Without repeating the same, the Applicant wishes to rely upon the above arguments supporting Claim 1 to support Claim 12 and submits the combination of Behren, Corda and Hosogoe is improper. Even if they were combined, the combination of Behren, Corda and Hosogoe fails to suggest "*the first application in the emulator is replaced in entirety by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when the second card is selected by the user, the first application is replaced by the second application in the emulator*". Accordingly, the Appellant submits Claim 12 as

Samsung Ex. 1016, Page 557 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

amended shall be allowable over Behren, Corda and Hosogoe. Reconsideration of Claims 12-19 is kindly requested.

The patentability of the independent claims has been argued specifically as set forth above and thus the Applicant will not take this opportunity to argue further the merits of the rejection with regard to each dependent claim. However, Applicant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

In view of the above amendments and remark, the Applicant believes that Claims 1-7, and 9-19 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)891-9381.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to " Mail Stop: AF/RCE Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450", 11/24/2020.

e-filed.
Name: Joe Zheng
Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng
Reg.: No. 39,450

Samsung Ex. 1016, Page 558 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/782,948	Filing Date 03/01/2013	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $62 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $250 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	11/24/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $480 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/VENICE M WILLIAMS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 03/04/2021

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
03/04/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Office Action Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 11/24/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-7 and 9-19 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-7 and 9-19 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 11/24/2020.

2. Claims 1, 2, 9, 11-13, 17 and 19 amended.

3. Claim 8 is cancelled.

4. Claims 1-7, and 9-19 are pending.

5. Claims 1-7, and 9-19 have been examined.

Notice of Pre-AIA or AIA Status

6. The present application is being examined under the pre-AIA first to invent provisions.

Priority

7. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date of 09/24/2006. The emulator is mentioned in App. No. 13/350,832 with a priority date of 01/16/2012, but the use of the emulator in replacing applications is claimed in the provisional 61/606,451, the 9 page specification, giving the application the priority date of 03/04/2012.

Claim Objections

8. Claims 1 and 12 are objected to because of the following informalities: the limitation in claim 1, “cause the applications provisioned remotely via the dedicated server that subsequently installs corresponding data and keys for each of the cards in the mobile device” is in comprehensible, claim 12 recites “wherein the memory is

included in the secure element." The punctuation is improper. Appropriate correction is required.

Response to Arguments

9. Applicant's arguments filed 11/24/2020 have been fully considered.

10. 112

The prior 112(b) 'means for' rejection was not properly addressed. Applicant argues Examiner admits that there are paragraphs that may show support but that is completely incorrect and a misrepresentation of the statement. Reading further shows that this is not the case. The office action clearly states, "In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56-61, 75, 76, 91 and 92. **However,** the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function." The rejection has not been properly addressed as Applicant has yet to provide evidence of the structures of the entities performing structural functions.

11. 103

12. Applicant argues Behren does not disclose that "the emulator that communicates with a reader (external to the mobile device) while Behren uses an NFC reader to interact directly with individual card software to communicate with an external reader." Neither the claims, nor the specification provide support for the emulator communicating with an external reader.

13. Next, Applicant argues against the combination of Behren and Corda. Both Behren and Corda are directed to emulation applications and cards. Behren teaches

emulation and switching applications, for example, "In case the mobile is powered off and running in virtual card emulation mode where the secure element is powered by the field, the control software application may not access the control functions defined within the device." See Behren (column 10, line 1-26). Secondly, Corda also teaches emulation and swapping application "The invention relates to a mobile communication device comprising a MIFARE Classic card or an emulated MIFARE Classic memory and a swap memory." See Corda (column 1, line 7-21). Both art provide systems that perform emulation on applications and cards as claimed in Applicant's limitations, but just the specific term "emulator" is not used. Simply considering the scope of these art, they both teach the functions of an emulator and also it would be obvious to one of ordinary skill in the art at the time of the invention to combine them.

Claim Interpretation

14. The following is a quotation of 35 U.S.C. 112(f):

> (f) Element in Claim for a Combination. – An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

15. This application includes one or more claim limitations that do not use the word "means," but are nonetheless being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because the claim limitation(s) uses a generic placeholder

that is coupled with functional language without reciting sufficient structure to perform the recited function and the generic placeholder is not preceded by a structural modifier. Such claim limitation(s) is/are:

a. an emulator… receiving (claim 1)

b. the service manager… cause the applications provisioned remotely (claim 1)

c. communication interface … facilitating data exchange (claim 1)

d. the table in the service manager updates a counter (claim 1)

e. the service manager receives a request (claim 1)

f. user interface application provided to query (claim 7)

g. UI application for conducting (claim 7)

Because this/these claim limitation(s) is/are being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, it/they is/are being interpreted to cover the corresponding structure described in the specification as performing the claimed function, and equivalents thereof. ¶ 59 explains "a card manager proxy **112** that facilitates the communication between a Trusted Service Manager (i.e., TSM server) **114** and the TMSM **106**, a set of readonly wallet user interface (UI) applications **116** and transaction wallet applications **118**. .. The readonly wallet UI **116** provides an interface to query one or more Mifare applications on information ", the claimed interfaces are software applications but are currently claimed in a mobile device and claimed to be performing functions. ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards"

but there is no indication of what structure is used. . ¶ 62 explains "Once the emulator **122** (implemented in hardware or software) is installed, it responds exactly like a native Mifare chip to an interface". According to the disclosure, the emulator can be either software or hardware, applicant is claiming a machine and the claim is unclear as to whether the emulator written in claim 1 is hardware or software. A software emulator cannot be claimed in the mobile device to be performing functions. As a result, corresponding structure to support the means for the functions has not been clearly provided.

If applicant does not intend to have this/these limitation(s) interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, applicant may: (1) amend the claim limitation(s) to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph (e.g., by reciting sufficient structure to perform the claimed function); or (2) present a sufficient showing that the claim limitation(s) recite(s) sufficient structure to perform the claimed function so as to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph.

Claim Rejections - 35 USC § 112

16. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

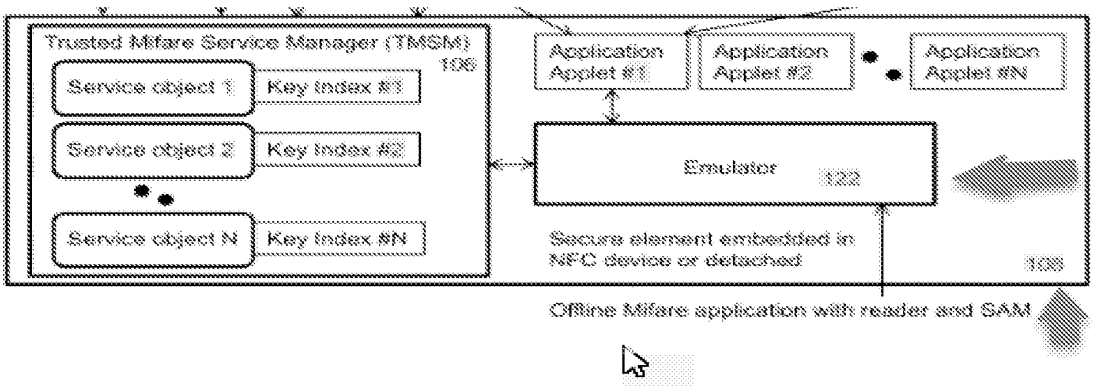
> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly

connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

17. Claims 1-7, and 9-19 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

18. Claim 1 recites "an emulator, coupled to the memory". According to the specification (Figure 1; ¶ 58-63, 117, 120, 143), "To download/install the application to the SE, the server is configured to establish a secure channel with the SE using this derived SSD at **242..**. it is assumed that an installed application, e-purse or a Mifare card, has been provisioned with the SE… an on-card Trusted Mifare Service Manager **106** (implemented as a module or an applet) is provided in a secure element (SE) **108**… the TMSM 106 is a component or applet configured to be responsible for installing and personalizing the applications, and Swapping one or another application into or out an emulator 122," the emulator (122) is part of the secure element and the secure element(108) is the storage device that stores the plurality of applications(applet #1-N). The secure element, is not a generic "storage device" that stores the plurality of applications. The applications are not provisioned in a "storage device", they are provisioned in a secure element. Neither the figures nor the specification describe a device other than the secure element that is used to store both the plurality of applications and the emulator. The specification does not provide support for the

emulator being coupled to the memory of the secure device and as written be a separate structure in the mobile device. Dependent claims 2-7, and 9-11 are rejected.



19. Claims 9 and 17 recite "wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element". According to the disclosure (Figure 1; ¶ 61, 62), " the SE **132** of FIG. 1C may be perceived as a preload operating system in a smart card, providing a platform for PIN management and security channels (security domains) for card personalization. The SE **132** combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple applications running in the smart cards." The same language is regurgitated in original claims 9 and 17. According to MPEP 2163, " issues of adequate written description may arise even for original claims, for example, when an aspect of the claimed invention has not been described with sufficient particularity such that one skilled in the art would recognize that the applicant had possession of the claimed invention at the time of filing." In this case, the specification does not describe or mention the SE being preloaded with and ISD information.

20. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph: The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

21. Claims 1-7, and 9-19 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

22. Claim 1 recites "wherein the service manager includes a table to keep track of the applications and cause the applications provisioned remotely via the dedicated server that subsequently installs corresponding data and keys for each of the cards in the mobile device, the data is only be modified by the dedicated server over a secured channel." The claim is unclear and indefinite. The claim does not make logical or grammatical sense. It is unclear whether Applicant is claiming the service manager causes Application to be provisioned or what the service manager cause the applications to do. Dependent claims 2-7, and 9-11 are rejected.

23. As per claims 1, 7 the claims recite the following means plus functions limitations:

h. an emulator… receiving (claim 1)

i. the service manager… cause the applications provisioned remotely (claim 1)

j. communication interface … facilitating data exchange (claim 1)

k. the table in the service manager updates a counter (claim 1)

l. the service manager receives a request (claim 1)

m. user interface application provided to query (claim 7)

n. UI application for conducting (claim 7)

24. This limitation invokes 35 USC § 112, ¶ 6 because it meets the 3-prong analysis set forth in MPEP 2181 as it recites a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) and the phrase is modified by functional language and it is not modified by sufficient structure, material, or acts for performing the recited function. When the claim limitation does not use the term "means," examiners should determine whether the presumption that 35 U.S.C.112 (f) or pre-AIA 35 U.S.C. 112, paragraph 6 does not apply is overcome. The presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term "means"). The following is a list of non-structural generic placeholders that may invoke35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, paragraph 6: "mechanism for," "module for," "device for," "unit for," "component for," "element for," "member for," "apparatus for," "machine for," or "system for." This list is not exhaustive, and other generic placeholders may invoke 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, paragraph 6. *Welker BearingCo., v. PHD, Inc.,* 550 F.3d 1090, 1096, 89 USPQ2d1289, 1293-94 (Fed. Cir. 2008); *Massachusetts Inst.of Tech. v. Abacus Software,* 462 F.3d 1344, 1354, 80 USPQ2d 1225, 1228 (Fed. Cir. 2006); *Personalized Media,* 161 F.3d at 704, 48 USPQ2dat 1886–87; *Mas-Hamilton Group v. LaGard, Inc.,*156 F.3d 1206, 1214-1215, 48 USPQ2d 1010, 1017(Fed. Cir. 1998). The terms are "used as a

substitute for 'means' that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning)" MPEP 2181.

In the instant application, the following portions of the specification and drawings may appear to describe the corresponding structure for performing the claimed function: specification ¶ 5, 7, 11, 56-61, 75, 76, 91 and 92.

However, the specification and drawings do not disclose sufficient corresponding structure, material or acts for performing the claimed function. ¶ 91 and 92 describe purse provisioned with the secure element is personalized with keys. The specification does not "send a set of instructions to cause" and does not have a corresponding structure that are the instructions. ¶ 5, 7, 56-58, 61, 75, 76 describe the module interchangeable with software modules, applications and applets but there is no indication of what structure is used, ¶ 58, 59 explains , the "on-card Trusted Mifare **Service Manager** **106** (implemented as a module or an applet) is provided in a secure element (SE) **108**" and "a card manager proxy **112** that facilitates the communication between a Trusted Service Manager (i.e., TSM server) **114** and the TMSM **106**, a set of readonly wallet user interface (UI) applications **116** and transaction wallet applications **118**. .. The readonly wallet UI **116** provides an interface to query one or more Mifare applications on information ", the claimed interfaces are software applications but are currently claimed in a mobile device and claimed to be performing functions. ¶ 61 describes "a mechanism to make baseband storage as an extension for storing the software-based or logical smart cards" but there is no indication of what structure is used. . ¶ 62 explains "Once the emulator **122** (implemented in hardware or software) is installed, it responds exactly like a native Mifare chip to an interface".

According to the disclosure, the emulator can be either software or hardware, applicant is claiming a machine and the claim is unclear as to whether the emulator written in claim 1 is hardware or software. A software emulator cannot be claimed in the mobile device to be performing functions. As a result, corresponding structure to support the means for the functions has not been clearly provided. Dependent claims 2-7, and 9-11 are rejected.

25. Claim 1 recites "receiving a first application corresponding to a first card In accordance with the service manager". The claim is unclear and indefinite as to what Applicant intends "In accordance with the service manager" and how a computing device recognizes this command. Dependent claims 2-7, and 9-11 are rejected.

26. Claim 1 recites "the dedicated server that subsequently installs corresponding data and keys for each of the cards in the mobile device, the data is only be modified by the dedicated server over a secured channel … application is unlocked by the dedicated server", claims 2 and 13 recites "in responding to a request from the dedicated server when the dedicated server determines that the secure element is registered therewith…," claim 11 recites "wherein the application being provisioned is distributed by an application provider…applications has been remotely provisioned by the dedicated server with operations of: notifying...", claim 12 recites ", the dedicated server that subsequently installs corresponding data and keys for each of the cards in the mobile device, the data can only be modified by the dedicated server over a secured channel … an external reader provided to read one of the cards on the mobile device," See disclosure ¶ 112, 143. A dedicated server, external reader and application providers are not recited as an elements of the mobile device of independent claims 1,

and 12 but claims 1, 2 and 11 claim the functions or intended functions of a dedicated server, reader and/or an application provider, which are both remote to the claimed mobile device. The scope of the claims are unclear and indefinite as Applicant has claimed functions of entities outside the scope of the mobile device's functions. Dependent claims 2-7, 9-11 and 13-19 are rejected.

27. Claim 1 recites "wherein the table in the service manager updates a counter when the first application is successfully loaded in the emulator". The claim is unclear and indefinite as the table is not recited as a structural entity but Applicant claims the table performs the function of updating a counter. The claim is unclear and indefinite as to the functionality of the claim limitation and the metes and bounds of what a list(table) is capable of. Dependent claims 2-7, and 9-11 are rejected.

28. Claim 2 and 13 recite "sending device information of the secure element in responding to a request from the dedicated server when the dedicated server determines that the secure element is registered therewith." The claims are unclear and indefinite. The claim is directed to the mobile device, not the functions of the dedicated server. But the recites functions are dependent on the dedicated server. Given that the dedicated server is remote to the mobile device, it would be impossible for the mobile device to know for example, that the dedicated server has determined the secure element is registered with it without receiving such communication. Therefore the claims is unclear as the functions of the mobile device are written to also claim knowledge of the functions of the dedicated server.

29. Claim 4 recites the limitation "the cards provided respectively". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

30. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. Claims 1-7, 9, 10, and 13-18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over von Behren et al. (8,646,059) ("Behren"), in view of Corda et al. (9,128,829) ("Corda"), and further in view of Hosogoe et al. (2003/0151125) ("Hosogoe").

32. Regarding claim 1, Behren discloses a display screen showing a list of application for a user of the mobile device to choose one therefrom, each of the applications corresponding to one of the cards(Figure 1; column 5, line 41-67, column 7, line 38-42, column 9, line 3-27, column 10, line 13-49, column 13, line 18-26, column 18, line 27-35, column 20, line 48-61)

- **Behren** - the user may choose from different card types (for example, PayPass, Paywave, debit cards, or other types) from different credit card companies (for example, MasterCard, Visa, Discover, or other companies), as well as different bank instances (for example, Bank A, B, C, and D) for each card type on the user-interface… the wallet application can be used by the contactless payment device user to select certain card Software applications as preferred applications via a user-inter face, thereby creating an order based on the type of card Software application. … When a full sized AID is selected, the directory software

> application then routes payment transaction commands according to user selected settings, directly to the selected instance… Here, all the data in the PPSE may not be distributed to merchants' reader by default, but is available to the user for selection via the user-interface. The user may choose to use the access functionality for specific payments on short distance contactless communication with a specific merchant terminal. T (column 5, line 41-67, column 7, line 38-42, column 9, line 14-18, column 18, line 27-32)

a secure element including a memory for storing the application and executing a service manager to manage applications, wherein the service manager includes a table to keep track of the applications and cause the applications provisioned remotely via the dedicated server that subsequently installs corresponding data and keys for each of the cards in the mobile device, the data is only be modified by the dedicated server over a secured channel (Figure 2, 3; Table 1; column 4, line 49-67, column 5, line 11-67, column 7, line 22-67, column 8, line 1-58, column 9, line 49-67, column 10, 1-67 column 13, line 45-62, column 19, line 27-38, column 22, line 25-53, column 26, line 1-43)

- **Claim Interpretation-** According to the disclosure(¶ 58, 59), the "on-card Trusted Mifare **Service Manager 106** (implemented as a module or an applet) is provided in a secure element (SE) **108**.… the NFC device **102** or **104** includes a card manager proxy **112** that facilitates the communication between a Trusted Service Manager (i.e., TSM server) **114** and the TMSM **106**." The TSM server is remote to the secure element and the TMSM that is a module or application inside the secure element. Additionally, the limitation starting with "cause…" is

incomprehensible, given the dedicated server is not a part of the claimed limitations, and it's functions are outside the scope of the mobile device claimed, and for purposes of claim interpretation, the limitation will be understood to mean the mobile device has applications installed with corresponding data and keys for each card.

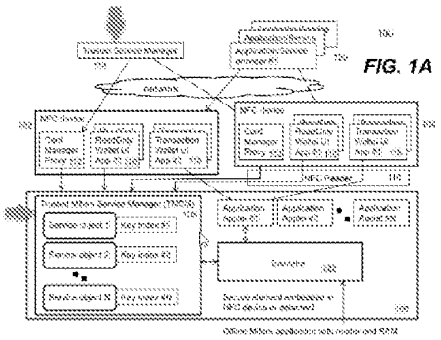
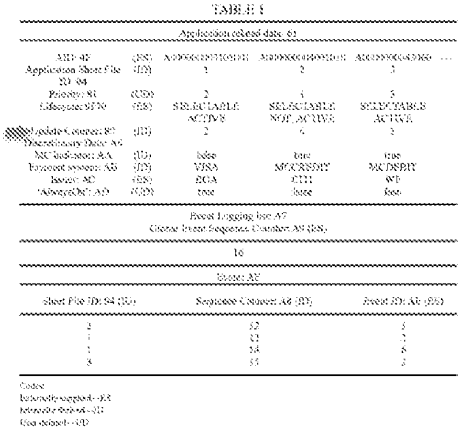
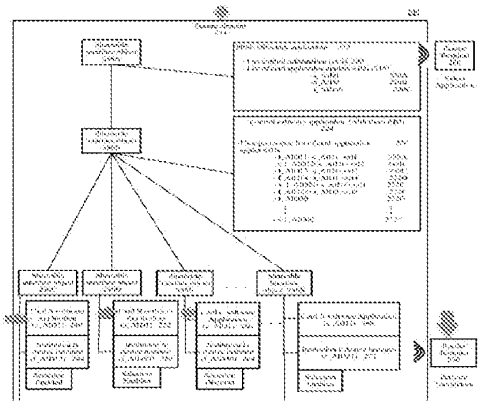


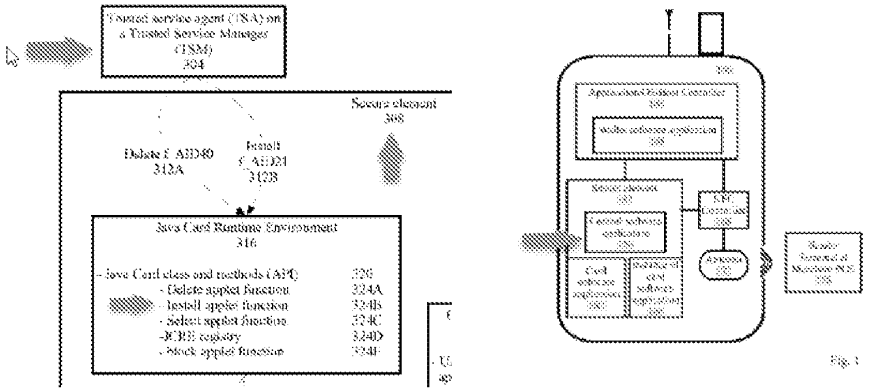
FIG. 1A

- **Behren** - An external trusted service manager (TSM) 108 controlled by a near field communications (NFC) service provider 104 hosts and transmits card software applications for installation within the secure element 152 of a contactless Smart card in mobile device 140. The NFC service provider 104 provides a secure key encrypted Software card application for decryption and installation in the Secure element 152. .. The term "card software application' and "card applet" are used interchangeably in this disclosure to refer to a software applications running within the secure element of a Smart card... to instantiate a Trusted Service Manager (TSM) Security Domain for download of payment and other card Software applications, to lock/unlock card Software applications, and to terminate secure element Software applications.,... The payment applications may be loaded on the mobile device as a card Software application package,

where each package, for example, a MasterCard package, typically contains Software code for all Supported payment applications within MasterCards' offerings, e.g., Mstripe, Mchip, and any other Suitable payment application. .. The control software application may freely communicate with the multiple card software applications and its instances **160**-**164** because each of the card and control software applications are resident within the same secure element **152**. Alternatively, multiple secure elements providing a secure communication channels will provide the same functionality as disclosed herein. The user may engage the control software application **156** (SERVICE MANAGER) using commands to activate, deactivate, prioritize, delete, and install card software applications within the secure element... the active AIDs from the control Software application 224 typically updates the directory software application 212... The control Software application maintains a UPL 228 of a list 232 of card software applications and their status from each card software application server SIOS 236. (column 4, line 63-66, column 5, line 11-33, column 7, line 62-67, column 8, line 1, 2, 49-58, column 9, line 49-67)







receiving a first application corresponding to a first card In accordance with the service manager, the first application being one of the plurality of applications, wherein the table In the service manager updates a counter when the first application is successfully loaded in the mobile device (column 7, line 1-48, column 8, line 38-53, column 9, line 49-67, column 12, line 31-67, column 18, line 1-67, column 21, line 1-21);

- **Behren** - an application host OS 144 on the mobile device 140 provides the user of the mobile device with the capability to manage multiple card Software applications and its instances 160-164 using a wallet Software application 148,.. The management of the card software applications may be performed via a control software application 156, which communicates with the wallet Software application 148 using APDUs, transmitted and received, through a secure and encrypted communication channel. The control Software application may freely communicate with the multiple card software applications and its instances 160-164 because each of the card and control software applications are resident within the same secure element 152... Alternatively, multiple secure elements providing a secure communication channels will provide the same functionality as

> disclosed herein. The user may engage the control software application **156** (SERVICE MANAGER) using commands to activate, deactivate, prioritize, delete, and install card software applications within the secure element… the active AIDs from the control Software application 224 typically updates the directory software application 212… The control Software application maintains a UPL 228 of a list 232 of card software applications and their status from each card software application server SIOS 236… , the server-client SIO definition within the JCRE allows a "wallet" software appli cation to track all instances of the card software applications in the secure element via the control software application in the Smart card. (column 7, line 22-26, column 8, line 38-58, column 9, line 49-67)

a communication interface, coupled to the secure element, facilitating data exchange wirelessly between a reader and the first application (Figurer 2, 3; column 7, line 49-57, column 20, line 48-61, column 21, line 34-65)

- **Behren -** The proximity payment service environment (PPSE) is a directory software application that is selected by the terminal reader when the contactless payment device is presented to the reader…The control software application can prevent the reader terminal from applying certain forceful methods to select a payment card Software application from a list of available options. (column 7, line 49-52, column 20, line 56-59)

wherein the service manager receives a request to activate the second application and performs a validation to the second application, with the table updated per the second application (column 8, line 55-58, column 9, line 3-48, column 10, line 3-12)

- **Behren -** The user may engage the control software application 156 using commands to activate, deactivate, prioritize, delete, and install card Software applications within the secure element.... The list of available card software applications 216 are displayed by the AIDS 220 to the reader. The reader then chooses or is defaulted to one of the multiple available card software applications. Accordingly, if the reader 280 chooses s AID2 220B, then the corresponding full AID is retrieved from the control software application. The selected full AID will be f AID21 232F. The corresponding card Software application 268 is triggered and the application itself, or its instance 272, in this case, is activated to the NFC controller for radio transmission of data to the reader. (column 8, line 55-58, column 10, line 3-12)

wherein said operation of causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application has been locked remotely by the dedicated server, and (column 5, line 11-17, column 9, line 28-65, column 15, line 36-63, column 16, line 55-67, column 17, line 1-60, column 19, line 8-17, column 24, line 1-67)

- **Behren -** Alter natively, the TSM may issue pre-defined instructions for such exemplary external functions, as blocking/unblocking a card Software application... to instantiate a Trusted Service Manager (TSM) Security Domain

> for download of payment and other card Software applications, to lock/unlock card Software applications, and to terminate secure element Software applications… The control software application includes a list 232 of the activate/inactive/non-activatable card Software application AIDs in certain format…When a card Software application 240,252,260, and 268 is enabled, the SIO is active and is accessed by the client mode control Software application 224…. In certain exemplary embodiments, for the UNBLOCKED/BLOCKED functions from the JCRE 316, based on requests from the TSA 304 may be rendered on a selected AID of the card software application 360 for blocking. The instruction for blocking or unblocking may be defined by the control software application 328 using APIs from the JCRE that causes a selected card software application360 to trigger an event to the control software application 328… In certain exemplary embodiments, the internal method calls applicable may include Such custom functions as, a enableSelection (byte aid): Boolean, for enabling selection of a payment card Software application and returning values as true if enabled or false for a general error (for example, the applet is locked). Another exemplary method call includes the disableSelection (byte aid): Void, which disables selection of a payment type card Software application… (column 5, line 11-17, column 9, line 41-65, column 15, line 36-43, column 16, line 66, 67, column 17, line 1-7, column 24, line 41-44)

Behren does not disclose an emulator, coupled to the memory, in the emulator;

received and executed in the emulator, wherein the reader is external to the mobile device, the secure element communicates with the reader via the communication interface, the first application in the emulator is replaced in entirety or partially by a second application corresponding to a second card when another one of the cards is selected by the user, the first application is out of the emulator and replaced by the second application; and the service manager conducts an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen and when the second application has been unlocked by the dedicated server, wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the first application is out of the emulator and the second application is activated and executed in the emulator.

Corda teaches an emulator, coupled to the memory, in the emulator (column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

- **Corda -** The mobile communication device further comprises a MIFARE memory MM which can either be configured as a MIFARE Classic card or a MIFARE Emulation card... The mobile communication device 1 further comprises a swap memory SM. ...For instance, the Swap memory SM is located in a secure memory of a Smartcard 4, e.g. a SmartMX card, being schematically represented in FIG. 4 by dotted lines. In the present example the Smartcard 4 also comprises a memory portion that emulates the MIFARE memory MM. However, it should be

> emphasized that the MIFARE memory MM can also be a MIFARE Classic card, e.g. 1 kB or 4 kB card... by enabling the user to manage MIFARE applications Swapping the user will be able to choose which coupons he needs to be located in the MIFARE memory MM at the moment.... The MIFARE applications manager MAM first stores this MIFARE application "Ticket 7' in the swap memory SM and then searches for a free sector in the MIFARE memory MM. A free sector (sector 0x2) is found and swapping can be done between the free MIFARE memory sector 0x2 and the "Ticket 7", meaning the MIFARE application "Ticket 7' is written into sector 0x2 of the MIFARE memory MM by the MIFARE applications manager MAM. (column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

received and executed in the emulator, wherein the reader is external to the mobile device, the secure element communicates with the reader via the communication interface, the first application in the emulator is replaced in entirety or partially by a second application corresponding to a second card when another one of the cards is selected by the user, (column 5, line 58-67, column 8, line 40-49);

- **Corda -** or by means of a NFC reader/writer when the mobile communication device 1 has NFC capabilities and is located within the range of such a NFC reader/writer... the MIFARE applications manager MAM carries out swapping between these two tickets "Ticket1 and "Ticket7". The final state (FIG. 8C) shows the result of the Swapping operation. In the Swap memory SM "Ticket1 is still stored, but has no longer a sector indication (meaning that it is no longer located

in the MIFARE memory MM). On the other hand, a sector indication (sector 0x2) has been added to the "Ticket 7' in the swap memory SM and this MIFARE application "Ticket 7' is now also stored in sector 0x2 of the MIFARE memory MM. (column 5, line 58-67, column 8, line 40-49)

the first application is out of the emulator and replaced by the second application; and the service manager conducts an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen and when the second application has been unlocked by the dedicated server, (Figure 1; column 5, line 9-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

- **Corda -** The mobile communication device 1 has a user interface comprising a keyboard 3 and a display 2. It further comprises a processor and memory…The trigger signals TS that are detectable by the MIFARE applications manager MAM may also be signals generated by the user interface of the mobile communication device 1, particularly by the keyboard 3. Thereby the MIFARE applications manager MAM offers an interface to the user of the mobile communication device 1 to enable him/her to trigger a MIFARE applications swapping by himself/herself. …A swapping instruction sent by a Service Provider etc. to the mobile communication device either as an SMS via the over-the-air service of a Mobile Network Operator or via RFID reader/writers which are connected to the Service Provider via a communication network. For the implementation of this feature the MIFARE applications manager MAM comprises an interface to the

SMS stack in order to give the mobile communication device 1 being configured as a NFC phone the ability to trigger MIFARE application Swapping operation on reception of a "Swapping-SMS which contains all the information about the Swapping operation to be done. (Figure 1; column 5, line 13-15, 58-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the first application is out of the emulator and the second application is activated and executed in the emulator (column 5, line 56, 57, column 6, line 35-67; claim 1, 18)

- **Corda -** MIFARE applications are for instance tickets, coupons, access controls, e-purse functions, etc… in order to instruct the MIFARE applications manager MAM to perform a Swap and put the right concert ticket into the MIFARE memory MM. … an applications manager configured to Swap applications between the first memory and the Swap memory Such that a first application that is stored at a first location on the first memory prior to Swapping replaces a second application that is store data second location on the Swap memory, and Such that the second application replaces the first application at the first location on the first memory, wherein the first application is different from the second application. (column 5, line 56, 57, column 6, line 35-67; claim 1)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*" and Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" in order to provide enough memory for multiple applications and store them in a secure way (Corda; column 3, line 43-67).

Neither Behren nor Corda use the term "emulator". Hosogoe uses the term "emulator" (Abstract; ¶44-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*", Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" and Hosogoe(¶1), which teaches "*a multi-application type IC card having a plurality of functions including credit card and electronic money functions*" in order to ensure higher security and great data volume to enact more monetary functions than a conventional magnetic card (Hosogoe; ¶ 2-4).

33. Regarding claims 2 and 13, Behren discloses further comprising a the secure element that has been personalized by operations of: initiating data communication by the mobile device with the dedicated server providing trusted service management (TSM) (column 5, line 11-33, column 7, line 59-67, column 8, line 1-14, column 23, line 33-67, column 24, line 1-56, column 26, line 1-16); sending device information of the secure element in responding to a request from the dedicated server when the dedicated server determines that the secure element is registered therewith (column 23, line 33-67, column 24, line 1-56, column 26, line 1-16), wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the mobile device to retrieve the device information from the secure element therein (column 7, line 1-21); and receiving in the secure element at least a set of keys from the dedicated server, wherein the set of keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider (column 19, line 28-67, column 25, line 1-26, column 26, line 1-16).

- **Claim Interpretation-** The claim is directed to the mobile device, not the functions of the designated server, Therefore, it would be impossible for the mobile device to know for example, that the designated server has determined the secure element is registered with it. For the purpose of claim interpretations, the limitation will be understood to mean the secure element, comprised in the phone is sending device information.

34. Regarding claims 3 and 14, Behren discloses wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device (column 4, line 38-67).

35. Regarding claim 4, Corda teaches wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator (Figure 1; column 5, line 9-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18).

36. Regarding claim 5, Behren discloses wherein at least one of the cards is a contactless card (Figure 1; column 4, line (38-66).

37. Regarding claims 6 and 15, Behren discloses wherein the secure further includes a plurality of service objects along with a plurality of key indexes, each of the service objects corresponding to one of the applications (column 6, line 37-67, column 19, line 28-67, column 23, line 1-32, column 25, line 1-26).

- **Claim Interpretation** – According to the specification(¶ 69, 72), "a service provider can access to all Mifare service objects (i.e., Mifare applications)… the TMSM **106** includes a set of service objects and corresponding key indexes. Each logical Mifare card in the TMSM **106** is called a service object… Each application can be associated with a key set index (also called key version number) of the installed SSD (Supplementary Secured Domain) key. " For the purpose of claim interpretation, the service objects will be understood to mean the applications and/or cards they correspond to.

38. Regarding claims 7 and 16, Behren discloses wherein the mobile device further provides: a user interface (UI) application provided to query one or more of the applications on information stored therein but not to modify the information (Figure 1; column 5, line 41-67, column 7, line 38-42, column 9, line 3-27, column 10, line 13-49, column 13, line 18-26, column 18, line 27-35, column 20, line 48-61); and a transaction UI application for conducting operations to modify one or more sectors in one or more of the applications (column 5, line 7-33, column 8, line 1-59, column 21, line 6-21).

39. Regarding claims 9 and 17, Behren discloses wherein the secure element is preloaded with default Issuer Security Domain (ISD) information (column 5, line 11-33, column 7, line 59-67, column 19, line 28-67, column 25, line 1-26, column 26, line 1-16).

40. Regarding claims 10 and 18, Behren discloses wherein the mobile device is a smartphone or a portable computer (column 4, line 38-67).

41. Claims 11 and 19 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over von Behren et al. (8,646,059) ("Behren"), in view of Corda et al. (9,128,829) ("Corda"), in view of Hosogoe et al. (2003/0151125) ("Hosogoe") and further in view of Wentker et al. (6,481,632) ("Wentker").

42. Regarding claim 11, Behren discloses wherein each of the applications has been remotely provisioned by the dedicated server with operations of: sending a request from the mobile device to the dedicated server to provision an application installed in the mobile device, wherein the application being provisioned is distributed by an application provider (column 5, line 11-33, column 7, line 59-67, column 8, line 1-14, column 23, line 33-67, column 24, line 1-56, column 26, line 1-16); establishing a secured channel

between the mobile device and the dedicated server using a set of keys received from the dedicated server; receiving data for the application being provisioned from the dedicated server (Figure 3; column 5, line 11-33, column 7, line 59-67, column 8, line 1-14, column 23, line 33-67, column 24, line 1-56, column 26, line 1-16), and notifying the application provider of a status of the application with the mobile device (column 24, line 1-56, column 25, line 8-26).

Neither Behren, Corda nor Hosogoe teaches wherein the data for the application includes supplemental security domains (SSD) to be associated with the application. Wentker teaches wherein the data for the application includes supplemental security domains (SSD) to be associated with the application (column 11, line 21-62, column 14, line 24-43, column 16, 49-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Behren, Corda, Hosogoe and Wentker in order to provide efficient management of card applications (Wentker; column 1, line 12-67).

43. Claim 12 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over von Behren et al. (8,646,059) ("Behren"), in view of Corda et al. (9,128,829) ("Corda"), and further in view of Hosogoe et al. (2003/0151125) ("Hosogoe").

44. Claim 12 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Corda et al. (9,128,829) ("Corda"), in view of von Behren et al. (8,646,059) ("Behren"), and further in view of Hosogoe et al. (2003/0151125) ("Hosogoe").

45. Regarding claim 12, Corda discloses installing in a memory of the mobile device a plurality of applications downloaded from a dedicated server, each of the applications

being managed by a service manager executed in a secure element in communication with the memory, wherein the memory is included in the secure element.

(column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

- **Corda -** The mobile communication device further comprises a MIFARE memory MM which can either be configured as a MIFARE Classic card or a MIFARE Emulation card… The mobile communication device 1 further comprises a swap memory SM. …For instance, the Swap memory SM is located in a secure memory of a Smartcard 4, e.g. a SmartMX card, being schematically represented in FIG. 4 by dotted lines. In the present example the Smartcard 4 also comprises a memory portion that emulates the MIFARE memory MM. However, it should be emphasized that the MIFARE memory MM can also be a MIFARE Classic card, e.g. 1 kB or 4 kB card… by enabling the user to manage MIFARE applications Swapping the user will be able to choose which coupons he needs to be located in the MIFARE memory MM at the moment…. The MIFARE applications manager MAM first stores this MIFARE application "Ticket 7' in the swap memory SM and then searches for a free sector in the MIFARE memory MM. A free sector (sector 0x2) is found and swapping can be done between the free MIFARE memory sector 0x2 and the "Ticket 7", meaning the MIFARE application "Ticket 7' is written into sector 0x2 of the MIFARE memory MM by the MIFARE applications manager MAM. (column 5, line 24-67, column 7, line 33-37, column 8, line 10-18)

receiving in an emulator of the mobile device a first application corresponding to a first card(column 5, line 58-67, column 8, line 40-49);

- **Corda -** or by means of a NFC reader/writer when the mobile communication device 1 has NFC capabilities and is located within the range of such a NFC reader/writer... the MIFARE applications manager MAM carries out swapping between these two tickets "Ticket1 and "Ticket7". The final state (FIG. 8C) shows the result of the Swapping operation. In the Swap memory SM "Ticket1 is still stored, but has no longer a sector indication (meaning that it is no longer located in the MIFARE memory MM). On the other hand, a sector indication (sector 0x2) has been added to the "Ticket 7' in the swap memory SM and this MIFARE application "Ticket 7' is now also stored in sector 0x2 of the MIFARE memory MM. (column 5, line 58-67, column 8, line 40-49)

facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaced in entirety by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when the second card is selected by the user, the first application is replaced by the second application in the emulator (Figure 1; column 5, line 9-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

- **Corda -** The mobile communication device 1 has a user interface comprising a keyboard 3 and a display 2. It further comprises a processor and memory... The trigger signals TS that are detectable by the MIFARE applications manager MAM

> may also be signals generated by the user interface of the mobile communication device 1, particularly by the keyboard 3. Thereby the MIFARE applications manager MAM offers an interface to the user of the mobile communication device 1 to enable him/her to trigger a MIFARE applications swapping by himself/herself. …A swapping instruction sent by a Service Provider etc. to the mobile communication device either as an SMS via the over-the-air service of a Mobile Network Operator or via RFID reader/writers which are connected to the Service Provider via a communication network. For the implementation of this feature the MIFARE applications manager MAM comprises an interface to the SMS stack in order to give the mobile communication device 1 being configured as a NFC phone the ability to trigger a MIFARE application Swapping operation on reception of a "Swapping-SMS which contains all the information about the Swapping operation to be done. (Figure 1; column 5, line 13-15, 58-67, column 6, line 35-67, column 7, line 1-37, Column 9, line 50-67; claim 1, 18)

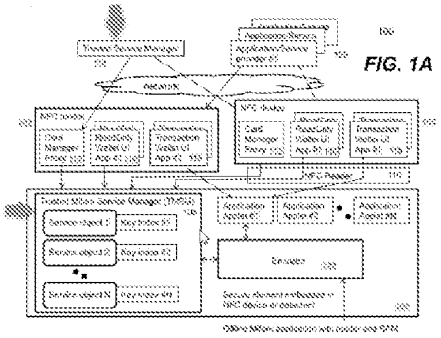
causing the second application to replace the first application loaded and executed in the emulator, said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display and wherein functions of the mobile device related to the first card offered by the first application are changed to functions offered by the second application related to the second card when the second application is activated and executed in the emulator(column 5, line 56, 57, column 6, line 35-67; claim 1, 18)

- **Corda -** MIFARE applications are for instance tickets, coupons, access controls, e-purse functions, etc… in order to instruct the MIFARE applications manager MAM to perform a Swap and put the right concert ticket into the MIFARE memory MM. … an applications manager configured to Swap applications between the first memory and the Swap memory Such that a first application that is stored at a first location on the first memory prior to Swapping replaces a second application that is store data second location on the Swap memory, and Such that the second application replaces the first application at the first location on the first memory, wherein the first application is different from the second application. (column 5, line 56, 57, column 6, line 35-67; claim 1)

Corda does not disclose the service manager includes a table to keep track of the applications and cause the applications provisioned remotely via the dedicated server that subsequently installs corresponding data and keys for each of the cards in the mobile device, the data can only be modified by the dedicated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards on the mobile device; showing the applications on a display of the mobile device for a user to choose one therefrom, each of the application corresponding to oneof the cards; wherein the table in the service manager updates a counter when the first application is successfully loaded in the device; wherein the table Is updated per the second application; but the second application has been locked by the dedicated server.

Behren teaches the service manager includes a table to keep track of the applications and cause the applications provisioned remotely via the dedicated server that subsequently installs corresponding data and keys for each of the cards in the mobile device, the data can only be modified by the dedicated server over a secured channel, the mobile device communicates wirelessly with an external reader provided to read one of the cards on the mobile device(Figure 2, 3; Table 1; column 4, line 49-67, column 5, line 11-67, column 7, line 22-67, column 8, line 1-58, column 9, line 49-67, column 10, 1-67 column 13, line 45-62, column 19, line 27-38, column 22, line 25-53, column 26, line 1-43)

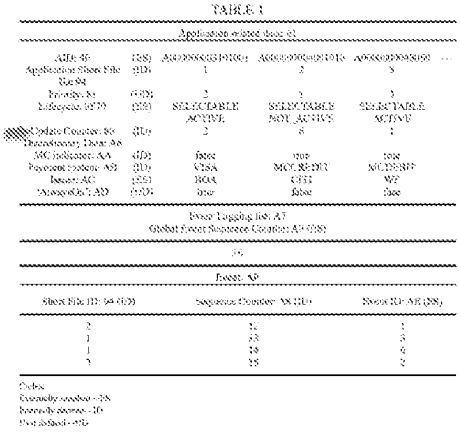
- **Claim Interpretation-** According to the disclosure(¶ 58, 59), the "on-card Trusted Mifare **Service Manager 106** (implemented as a module or an applet) is provided in a secure element (SE) **108**.... the NFC device **102** or **104** includes a card manager proxy **112** that facilitates the communication between a Trusted Service Manager (i.e., TSM server) **114** and the TMSM **106**." The TSM server is remote to the secure element and the TMSM that is a module or application inside the secure element. Additionally, the limitation starting with "cause..." is incomprehensible, given the dedicated server is not a part of the claimed limitations, and it's functions are outside the scope of the mobile device claimed, and for purposes of claim interpretation, the limitation will be understood to mean the mobile device has applications installed with corresponding data and keys for each card.

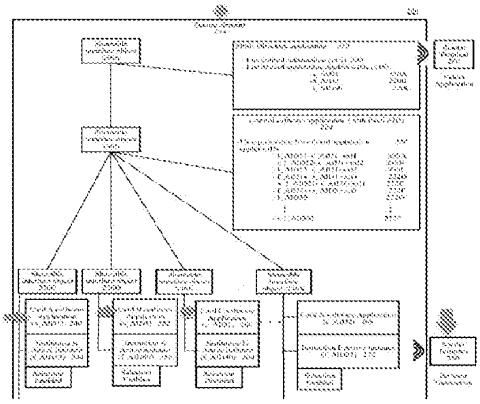


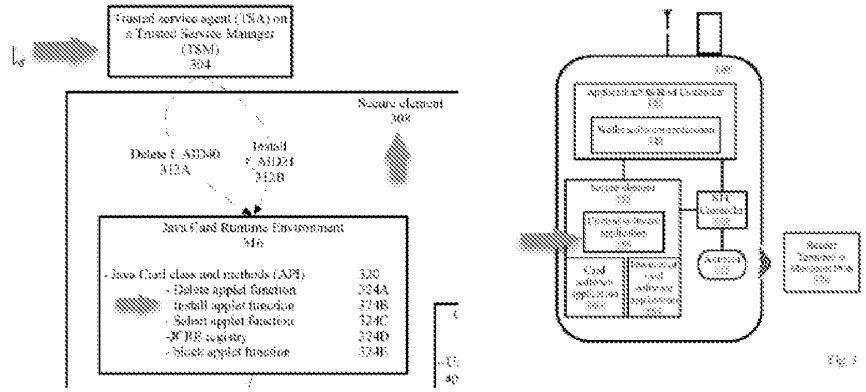
-

- **Behren** - An external trusted service manager (TSM) 108 controlled by a near field communications (NFC) service provider 104 hosts and transmits card software applications for installation within the secure element 152 of a contactless Smart card in mobile device 140. The NFC service provider 104 provides a secure key encrypted Software card application for decryption and installation in the Secure element 152. .. The term “card software application' and “card applet” are used interchangeably in this disclosure to refer to a software applications running within the secure element of a Smart card... to instantiate a Trusted Service Manager (TSM) Security Domain for download of payment and other card Software applications, to lock/unlock card Software applications, and to terminate secure element Software applications.,... The payment applications may be loaded on the mobile device as a card Software application package, where each package, for example, a MasterCard package, typically contains Software code for all Supported payment applications within MasterCards' offerings, e.g., Mstripe, Mchip, and any other Suitable payment application. .. The control software application may freely communicate with the multiple card software applications and its instances **160**-**164** because each of the card and

control software applications are resident within the same secure element **152**. Alternatively, multiple secure elements providing a secure communication channels will provide the same functionality as disclosed herein. The user may engage the control software application **156 (**SERVICE MANAGER**)** using commands to activate, deactivate, prioritize, delete, and install card software applications within the secure element… the active AIDs from the control Software application 224 typically updates the directory software application 212… The control Software application maintains a UPL 228 of a list 232 of card software applications and their status from each card software application server SIOS 236. (column 4, line 63-66, column 5, line 11-33, column 7, line 62-67, column 8, line 1, 2, 49-58, column 9, line 49-67)







showing the applications on a display of the mobile device for a user to choose one therefrom, each of the application corresponding to oneof the cards (Figure 1; column 5, line 41-67, column 7, line 38-42, column 9, line 3-27, column 10, line 13-49, column 13, line 18-26, column 18, line 27-35, column 20, line 48-61)

- **Behren** - the user may choose from different card types (for example, PayPass, Paywave, debit cards, or other types) from different credit card companies (for example, MasterCard, Visa, Discover, or other companies), as well as different bank instances (for example, Bank A, B, C, and D) for each card type on the user-interface… the wallet application can be used by the contactless payment device user to select certain card Software applications as preferred applications via a user-inter face, thereby creating an order based on the type of card Software application. … When a full sized AID is selected, the directory software application then routes payment transaction commands according to user selected settings, directly to the selected instance… Here, all the data in the PPSE may not be distributed to merchants' reader by default, but is available to

the user for selection via the user-interface. The user may choose to use the access functionality for specific payments on short distance contactless communication with a specific merchant terminal. T (column 5, line 41-67, column 7, line 38-42, column 9, line 14-18, column 18, line 27-32)

wherein the table in the service manager updates a counter when the first application is successfully loaded in the device…wherein the table Is updated per the second application, (column 7, line 1-48, column 8, line 38-53, column 9, line 49-67, column 12, line 31-67, column 18, line 1-67, column 21, line 1-21);

- **Behren** - an application host OS 144 on the mobile device 140 provides the user of the mobile device with the capability to manage multiple card Software applications and its instances 160-164 using a wallet Software application 148,.. The management of the card software applications may be performed via a control software application 156, which communicates with the wallet Software application 148 using APDUs, transmitted and received, through a secure and encrypted communication channel. The control Software application may freely communicate with the multiple card software applications and its instances 160-164 because each of the card and control software applications are resident within the same secure element 152… Alternatively, multiple secure elements providing a secure communication channels will provide the same functionality as disclosed herein. The user may engage the control software application **156** (SERVICE MANAGER) using commands to activate, deactivate, prioritize, delete, and install card software applications within the secure element… the

> active AIDs from the control Software application 224 typically updates the directory software application 212… The control Software application maintains a UPL 228 of a list 232 of card software applications and their status from each card software application server SIOS 236… , the server-client SIO definition within the JCRE allows a "wallet" software appli cation to track all instances of the card software applications in the secure element via the control software application in the Smart card. (column 7, line 22-26, column 8, line 38-58, column 9, line 49-67)

but the second application has been locked by the dedicated server, (column 5, line 11-17, column 9, line 28-65, column 15, line 36-63, column 16, line 55- 67, column 17, line 1-60, column 19, line 8-17, column 24, line 1-67)

- **Behren -** Alter natively, the TSM may issue pre-defined instructions for such exemplary external functions, as blocking/unblocking a card Software application… to instantiate a Trusted Service Manager (TSM) Security Domain for download of payment and other card Software applications, to lock/unlock card Software applications, and to terminate secure element Software applications… The control software application includes a list 232 of the activate/inactive/non-activatable card Software application AIDs in certain format…When a card Software application 240,252,260, and 268 is enabled, the SIO is active and is accessed by the client mode control Software application 224…. In certain exemplary embodiments, for the UNBLOCKED/BLOCKED functions from the JCRE 316, based on requests from the TSA 304 may be rendered on a selected AID of the card software application 360 for blocking. The

> instruction for blocking or unblocking may be defined by the control software application 328 using APIs from the JCRE that causes a selected card software application360 to trigger an event to the control software application 328… In certain exemplary embodiments, the internal method calls applicable may include Such custom functions as, a enableSelection (byte aid): Boolean, for enabling selection of a payment card Software application and returning values as true if enabled or false for a general error (for example, the applet is locked). Another exemplary method call includes the disableSelection (byte aid): Void, which disables selection of a payment type card Software application… (column 5, line 11-17, column 9, line 41-65, column 15, line 36-43, column 16, line 66, 67, column 17, line 1-7, column 24, line 41-44)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" and Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*" in order to provide a device owner access to several types of services that range from financial transactions to secure authentication (Behren; column 1, line 43-66).

Neither Corda nor Behren use the term "emulator". Hosogoe uses the term "emulator" (Abstract; ¶44-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Corda(column 1, line 10-13), which teaches "*managing MIFARE applications in a mobile communication device that comprises a MIFARE Classic card or an emulated MIFARE Classic memory and a Swap memory*" and Behren(column 1, line 16-21), which teaches "*systems, methods, and devices for controlling multiple card Software applications using a control Software application, the control and card Software applications resident in a secure element of a con tactless Smart card*" and Hosogoe(¶1), which teaches "*a multi-application type IC card having a plurality of functions including credit card and electronic money functions*" in order to ensure higher security and great data volume to enact more monetary functions than a conventional magnetic card (Hosogoe; ¶ 2-4).

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Hisano et al., (US 20060034043) teaches emulating first information and converting to second information.
- Spodak et al. (US 20130134216) teaches a universal card with multiple cards that emulates the different cards.
- Sklovsky et al (US 20090247077) teaches switching between applications on a mobile device.

- Tang et al. (US 20130331029) teaches secure elements with emulating functions for multiple applications.
- Finkenzeller et al. (US 20090199206) teaches switching between applications and utilizing a reading device to communicate with the applications.

47. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ISIDORA I IMMANUEL/
Examiner, Art Unit 3685

/OLUSEYE IWARERE/
Primary Examiner, Art Unit 3687

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination Xie et al.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20030151125-A1	08-2003	Hosogoe, Takashi	G06Q20/3574	257/679
*	B	US-9128829-B2	09-2015	Corda; Alexandre	G06F12/0638	1/1
*	C	US-8646059-B1	02-2014	von Behren; Rob	G06Q20/3574	726/9
*	D	US-6481632-B2	11-2002	Wentker; David C.	G06F8/60	235/376
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Samsung Ex. 1016, Page 605 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

CPC - Searched*		
Symbol	Date	Examiner
G06Q20	08/17/2020	III
G06Q2220	08/17/2020	III
H04L41	02/27/2021	III
G06F8	02/27/2021	III

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
705			

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
See attached notes	2/1/2016	II
101 withdrawal - Weinhart	06/06/2018	III
See attached notes (EAST)	04/15/2019	III
EAST search report	08/17/2020	III
NPL search	08/17/2020	III
EAST	02/27/2021	III

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	

Samsung Ex. 1016, Page 606 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	

Samsung Ex. 1016, Page 607 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	**Art Unit**
	ISIDORA I IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE							
Final	Original	02/01/2016	09/16/2016	09/17/2017	05/22/2018	04/15/2019	12/18/2019	08/17/2020	02/27/2021
	1	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓
	4	✓	✓	✓	✓	✓	✓	✓	✓
	5	✓	✓	✓	✓	✓	✓	✓	✓
	6	✓	✓	✓	✓	✓	✓	✓	✓
	7	✓	✓	✓	✓	✓	✓	✓	✓
	8	✓	✓	✓	✓	✓	✓	-	-
	9	✓	✓	✓	✓	✓	✓	✓	✓
	10	✓	✓	✓	✓	✓	✓	✓	✓
	11	✓	✓	✓	✓	✓	✓	✓	✓
	12	✓	✓	✓	✓	✓	✓	✓	✓
	13	✓	✓	✓	✓	✓	✓	✓	✓
	14	✓	✓	✓	✓	✓	✓	✓	✓
	15	✓	✓	✓	✓	✓	✓	✓	✓
	16	✓	✓	✓	✓	✓	✓	✓	✓
	17	✓	✓	✓	✓	✓	✓	✓	✓
	18	✓	✓	✓	✓	✓	✓	✓	✓
	19	✓	✓	✓	✓	✓	✓	✓	✓

Samsung Ex. 1016, Page 608 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	207	(service adj manager) and emulator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/02/27 09:34
L2	2,850,311	counter or tracker emulator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/02/27 09:34
L3	16,062	(counter or track$4) and emulator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/02/27 09:34
L4	47	1 AND ((H04L41/0806 OR H04L47/70 OR G06F8/65).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/02/27 09:35

EAST Search History (Interference)

<This search history is empty>

2/27/2021 9:36:02 AM
C:\Users\iimmanuel\Documents\EAST\Workspaces\13782948.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 03/22/2021

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
03/22/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Applicant-Initiated Interview Summary	**Application No.** 13/782,948	**Applicant(s)** Xie et al.		
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
ISIDORA I IMMANUEL	Examiner	Telephonic
JOE ZHENG	PATENT AGENT	

Date of Interview: 16 March 2021

Issues Discussed:

Other

Second attempt proposing allowable subject matter. Discussed specification support (module and claims 9, 17), language clarifications to make ("in response to", "load", function vs replaced, emulator device) and honoring agreed on claims (claim 2 and 13). Applicant will respond with a final draft of the discussed claim language. No agreements finalized.

☑ Attachment

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Applicant(s):	Xiangzhen Xie et al
Title:	Method and apparatus for emulating multiple cards in mobile devices
Serial No.:	13/782,948
Filing Date:	03/01/2013
Confirmation:	5348
Examiner:	Isidora I. Immanuel
Group Art Unit:	3685
Docket No.:	RFID-084

1. The Applicant has authorized the communication with the Examiner via the internet
2. This is for informal discussion with the Examiner, content of which is not intended for entry as record.

Interview Agenda

Time: 04:00PM EST (3:00PM CDT, 1:00 PM PDT)

Date: Tuesday, March 16, 2021

Participants: Examiner: Isidora I. Immanuel

Representative: Joe Zheng (Reg. No.: 39,450, Cell: 408-891-9381)

Connection: Joe will call (469)295-9094

Agenda:

1. Discussion of amendments to proposed allowable claims
2. Examiner suggests further amendments;
3. Conclusion (Interview Summary)

Samsung Ex. 1016, Page 612 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

AMENDMENTS TO THE CLAIMS

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:

a display screen showing a list of a plurality of applications ~~the cards~~ for a user of the mobile device to select ~~choose~~ one therefrom, each application corresponding to a card in the plurality of cards~~wherein a display of the list of the cards is provided via a designated server~~;

~~a storage device for storing a plurality of applications, each of the applications corresponding to one of the cards, wherein each of the applications is provisioned remotely with the designated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the designated server over a secured channel;~~

a secure element (SE) including:

an emulator device; ~~, coupled to the storage device and implemented in a secure element, receiving a first application corresponding to a first card, the first application being one of the plurality of applications;~~

a memory storing at least one ~~a~~ module, when the at least one module is executed by the secure element, the secure element configured to:

receive and install key sets of a Supplementary Secured Domain (SSD);

establish, based on the key sets, a secure communication channel with a dedicated server;

receive and install an application from the dedicated sever, ~~each~~ the application including corresponding application data sets ~~and files~~ and a locked or unlocked status, wherein ~~an~~ the application with a locked status must be unlocked to function~~be replaced~~;

receive, from the plurality of applications, a user selection of a first application corresponding to a first card;

Samsung Ex. 1016, Page 613 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

determine that the first application has a locked or unlocked status and is activated, ~~wherein an application status is locked or unlocked by the dedicated server;~~

in response to said determining that the first application has an unlocked status and is activated, ~~send~~ load the first application to the emulator device~~,~~ along with corresponding first application data sets;

receive, from the plurality of applications, a user selection of a second application corresponding to a second card;

determine that the second application has a locked or unlocked status and is activated;

~~in response to said determining that the second application has an unlocked status and is activated,~~ replace out of the emulator device, a portion of or in entirety, the first application, wherein said replacing out of the emulator device a portion of the first application further comprises retaining~~, in the emulator device,~~ portions of the corresponding first application data sets to be utilized by the second application;

~~send~~ load the second application to the emulator device along with corresponding second application data sets; and

increment a counter for each successful application replacement;

~~a communication interface to facilitate data exchange wirelessly between a reader and the first application received and executed in the emulator, wherein the reader is external to the mobile device, and the first application in the emulator is replaceable in entirety by a second application corresponding~~

Samsung Ex. 1016, Page 614 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator and replaced by the second application; and

a processor, in communication with the emulator and the storage device, performing an operation of causing the second application loaded into the emulator to replace the first application when the second card is selected via the display screen when the second application has been unlocked by the designated server, wherein said causing the second application loaded into the emulator to replace the first application fails when the second card is selected via the display screen but the second application has been locked by the designated server, and wherein

wherein functions of the mobile device performs functions of the second card when the first application is replaced out of the emulator device and the second application is received load in the emulator devicerelated to the first card offered by the first application are changed to functions offered by the second application related to the second card when the first application is out of the emulator and the second application is activated and executed in the emulator.

2. (*Cancelled*)

3. (*Currently amended*) The mobile device as recited in claim 21, wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Previously amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the cards provided respectively to perform a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator.

Samsung Ex. 1016, Page 615 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

6. (*Cancelled*)
7. (*Cancelled*)
8. (*Cancelled*)

9. (*Currently amended*) The mobile device as recited in claim ~~2~~1, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updated entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Currently amended*) The mobile device as recited in claim ~~2~~1, wherein the mobile device is a smartphone or a portable computer.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by the ~~the designated a corresponding~~ dedicated server with operations of:

sending a request from the mobile device to the ~~designated corresponding~~ dedicated server to provision ~~an said each of the~~ applications installed in the mobile device, wherein ~~said each of~~ the applications being provisioned ~~is~~ are distributed by an application provider;

~~establishing a secured channel between the mobile device and the designated server using a set of keys received from the designated server;~~

receiving data for the application being provisioned from the ~~designated~~ dedicated server, wherein the data for ~~said each of~~ the applications includes ~~supplemental security domains (~~the SSD~~)~~ to be associated with ~~said each of~~ the applications; and

notifying the application provider of a status of ~~said each of~~ the applications with the mobile device.

Samsung Ex. 1016, Page 616 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

~~installing in an emulator a storage device of a secure element in the mobile device a plurality of applications, each of the applications downloaded from a designated dedicated server and corresponding to one of the cards, each of the applications being managed by the designated server pertaining to one of the cards, wherein each of the applications is provisioned remotely with the designated a corresponding dedicated server that subsequently installs corresponding data and keys for the one of the cards in the mobile device, the data can only be modified by the corresponding dedicated designated server over a secured channel established with key sets of a Supplementary Secured Domain (SSD), the mobile device communicates wirelessly with an external reader provided to read one of the cards on the mobile device;~~

~~showing~~ displaying a list of ~~the cards~~ a plurality of applications on a display of the mobile device for a user to ~~choose~~ select one therefrom;

~~receiving in an~~ the emulator of the mobile device a first application corresponding to a first card;

~~facilitating data exchange between the external reader and the first application being executed in the emulator, wherein the first application in the emulator is replaceable in a portion or entirety by a second application corresponding to a second card when another one of the cards is selected by the user, wherein the first application is out of the emulator when the second card is selected by the user and the first application is and replaced by the second application in the emulator;~~

~~causing the second application to replace the first application loaded and executed in the emulator, wherein said causing the second application to replace the first application loaded and executed in the emulator fails when the second card is selected via the display but the second application has been locked by the designated server, and wherein functions of the mobile device related to the first card offered by the first application are changed to functions~~

Samsung Ex. 1016, Page 617 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

~~offered by the second application related to the second card when the second application is activated and executed in the emulator.~~

receiving and installing, by a secure element on the mobile device, key sets of a Supplementary Secured Domain (SSD);

establishing, ~~by the secure element and~~ based on the key sets, a secure communication channel with a dedicated server;

receiving and installing, by the secure element, an application from the dedicated sever, each application including corresponding application data sets ~~and files~~ and a locked or unlocked status, wherein ~~an~~ the application with a locked status must be unlocked to function ~~be replaced~~;

receiving, by the mobile device, a user selection of a first application corresponding to a first card;

determining, by the secure element, that the first application has a locked or unlocked status and is activated~~, wherein an application status is locked or unlocked by the dedicated server~~;

in response to said determining that the first application has an unlocked status and is activated, ~~sending, by the secure element,~~ loading the first application to an emulator device in the secure element~~,~~ along with corresponding first application data sets;

receiving, by the mobile device, from the plurality of applications, a user selection of a second application corresponding to a second card;

Samsung Ex. 1016, Page 618 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

determining, by the secure element, that the second application has a locked or unlocked status and is activated;

in response to said determining that the second application has an unlocked status and is activated, replacing out of the emulator device, by the secure element, a portion of or in entirety, the first application, wherein said replacing out of the emulator device a portion of the first application further comprises retaining, in the emulator device, portions of the corresponding first application data sets to be utilized by the second application;

~~sending, by the secure element,~~ loading the second application to the emulator device along with corresponding second application data sets;

incrementing, by the secure element, a counter for each successful application replacement;

wherein the mobile device performs functions of the second card when the first application is replaced out of the emulator device and the second application is received in the emulator device.

13. (*Currently amended*) The method as recited in claim 12, ~~wherein the mobile device is associated with a secure element, and~~ the method further comprises:

initiating data communication by the mobile device with the ~~the designated~~~~another~~ dedicated server, wherein the dedicated server is a Trusted Service Manager(TSM); and

Samsung Ex. 1016, Page 619 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

sending device information of the secure element in responding to a request from the ~~designated~~ ~~another~~ dedicated server ~~after the designated another dedicated server determines that the secure element is mobile device has been registered therewith~~, wherein the device information is a sequence of characters uniquely identifying the secure element, ~~and the request is a command causing the mobile device to retrieve the device information from the secure element therein~~; ~~and~~

~~receiving in the secure element at least a set of keys from the designated server, wherein the keys are generated in accordance with the device information of the secure element, the set of keys in the secure element facilitates a subsequent transaction between the mobile device and a service provider.~~

14. (*Currently amended*) The method as recited in claim 13, wherein ~~the emulator is implemented in the secure element,~~ the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Cancelled*)

16. (*Cancelled*)

17. (*Previously amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information updatable entirely or partially subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Cancelled*)

Samsung Ex. 1016, Page 620 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

26797 7590 04/05/2021

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 04/05/2021

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

TITLE OF INVENTION: Method and apparatus for emulating multiple cards in mobile devices

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	07/06/2021

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

Samsung Ex. 1016, Page 621 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

26797 7590 04/05/2021

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

TITLE OF INVENTION: Method and apparatus for emulating multiple cards in mobile devices

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	07/06/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
IMMANUEL, ISIDORA I	3685	705-050000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (08-18) Approved for use through 01/31/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Samsung Ex. 1016, Page 622 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 04/05/2021

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 04/05/2021

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

Samsung Ex. 1016, Page 623 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/782,948	Applicant(s) Xie et al.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 03/18/2021.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are See Continuation Sheet . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☑ Other NPL search.

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

Continuation of 3. The allowed claim(s) is/are: 1, 3,-5, 9-12, 14, 17,and 18

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

STATUS OF THE APPLICATION

This action is in response to the claims filed 11/24/2020. Claims 2, 6-8, 13, 15, and 16 have been cancelled. Claims 1, 3, 4, 9-12, 14 and 17 are amended as a result of the interview conducted March 16, 2021 and a call March 25, 2021 to discuss final changes. Claims 1, 3-5, 9-12, 14, 17 and 18 are therefore pending and currently under consideration for patentability.

EXAMINER'S AMENDMENT

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:
   a display screen showing a list of a plurality of applications for a user of the mobile device to select one therefrom, each application corresponding to one card in the plurality of cards;
   a secure element (SE) including:
   an emulator device;
   a memory storing a module, when the module is executed by the secure element, the secure element configured to:
   receive and install key sets of a Supplementary Secured Domain (SSD);
   establish, by the secure element based on the key sets, a secure communication channel with a dedicated server;
   receive and install an application from the dedicated server, each application including corresponding application data sets and a locked or unlocked status;

receive, from the plurality of applications, a user selection of a first application corresponding to a first card;

determine that the first application has a locked or unlocked status and is activated,

in response to said determining that the first application has an unlocked status and is activated, load the first application to the emulator device, along with corresponding first application data sets;

receive, from the plurality of applications, a user selection of a second application corresponding to a second card;

determine that the second application has a locked or unlocked status and is activated;

in response to said determining that the second application has an unlocked status and is activated, replace out of the emulator device, a portion of or in entirety, the first application, wherein said replacing out of the emulator device a portion of the first application further comprises retaining the portion of the corresponding first application data sets to be utilized by the second application;

load the second application to the emulator device along with corresponding second application data sets; and

increment a counter for each successful application replacement, wherein the mobile device performs functions of the second card when the first application is replaced out of the emulator device and the second application is loaded in the emulator device.

2. (*Cancelled*)

3. (*Currently amended*) The mobile device as recited in claim 1, wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Currently amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the plurality of cards, performs a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator device.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

6. (*Cancelled*)
7. (*Cancelled*)
8. (*Cancelled*)

9. (*Currently amended*) The mobile device as recited in claim 1, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information and updated subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Currently amended*) The mobile device as recited in claim 1, wherein the mobile device is a smartphone or a portable computer.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by a corresponding dedicated server with operations of:

sending a request from the mobile device to the corresponding dedicated server to provision each of the applications installed in the mobile device, wherein the applications are distributed by an application provider;

receiving data for each of the applications being provisioned from the dedicated server, wherein the data includes the SSD to be associated with the each of the applications; and

notifying the application provider of a status of each of the applications with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

displaying a list of a plurality of applications on a display of the mobile device for a user to select one therefrom, each application corresponding to one card in the plurality of cards;

receiving and installing, by a secure element on the mobile device, key sets of a Supplementary Secured Domain (SSD);

establishing, by the secure element and based on the key sets, a secure communication channel with a dedicated server;

receiving and installing, by the secure element, an application from the dedicated sever, each application including corresponding application data sets and a locked or unlocked status,

receiving, by the mobile device, a user selection of a first application corresponding to a first card;

determining, by the secure element, that the first application has a locked or unlocked status and is activated;

in response to said determining that the first application has an unlocked status and is activated, loading the first application to an emulator device in the secure element, along with corresponding first application data sets;

receiving, by the mobile device, from the plurality of applications, a user selection of a second application corresponding to a second card;

determining, by the secure element, that the second application has a locked or unlocked status and is activated;

in response to said determining that the second application has an unlocked status and is activated, replacing out of the emulator device, by the secure element, a portion of or in entirety, the first application, wherein said replacing out of the emulator device a portion of the first application further comprises retaining, in the

emulator device, the portion of the corresponding first application data sets to be utilized by the second application;

loading the second application to the emulator device along with corresponding second application data sets;

incrementing, by the secure element, a counter for each successful application replacement, wherein the mobile device performs functions of the second card when the first application is replaced out of the emulator device and the second application is loaded in the emulator device.

13. (*Cancelled*):

14. (*Currently amended*) The method as recited in claim 13, wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Cancelled*)

16. (*Cancelled*)

17. (*Currently amended*) The method as recited in claim 13, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is updatable subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Cancelled*)

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:

Claims 1, 3-5, 9-12, 14, 17 and 18 are allowed. The closest prior art of record is Behren et al. (US 8646059), and in view of Corda et al. (US9128829).

Behren describes managing multiple payment card applications on a mobile device, along with the use of multiple secure elements. Corda teaches an emulating device that swaps out tickets. The combination of prior art do not teach the elements of independent claims 1 and 12. The recited emulator device, located in the secure element which includes a tracker for each application replacement, has the ability to retain data from the previous replaced application for use in the current or most recently loaded application. This combination of elements/function/limitations would not have been obvious to one of ordinary skill in the art in light of the available prior art at the time of the invention. Dependent claims 3-5, 9-11, 14, 17 and 18, are also allowable for the same reasons.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ISIDORA I IMMANUEL/
Examiner, Art Unit 3685

/NEHA PATEL/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 13/782,948	Applicant(s)/Patent Under Reexamination Xie et al.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20030151125-A1	08-2003	Hosogoe, Takashi	G06Q20/3574	257/679
*	B	US-9128829-B2	09-2015	Corda; Alexandre	G06F12/0638	1/1
*	C	US-8646059-B1	02-2014	von Behren; Rob	G06Q20/3574	726/9
*	D	US-6481632-B2	11-2002	Wentker; David C.	G06F8/60	235/376
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N	WO-2009083679-A2	07-2009	WO	PICQUENOT DAVID	G06Q20/351
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Chameleon- A versatile emulator for contactless smart cards, Kasper Timo et al. , Information and security cryptology, 2010, Berlin, Heidelberg, 189-206
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	**Art Unit**
	ISIDORA I IMMANUEL	3685

CPC						
Symbol					**Type**	**Version**
H04B	/	5	/	0056	F	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06Q	/	30	/	0601	I	2013-01-01
G06Q	/	20	/	3672	I	2013-01-01
G06Q	/	20	/	3552	I	2013-01-01
G06Q	/	20	/	40	I	2013-01-01
G06Q	/	20	/	322	I	2013-01-01
G06Q	/	20	/	3278	I	2013-01-01
G06Q	/	20	/	3572	I	2013-01-01
G06Q	/	20	/	227	I	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	23 March 2021	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685	26 March 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1A

U.S. Patent and Trademark Office — Part of Paper No.: 20210323

Samsung Ex. 1016, Page 635 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	**Art Unit**
	ISIDORA I IMMANUEL	3685

INTERNATIONAL CLASSIFICATION				
CLAIMED				
	/		/	
H04B5/00	/	5	/	00
G06Q30/06	/	30	/	06
G06Q20/36	/	20	/	36
G06Q20/40	/	20	/	40
G06Q20/32	/	20	/	32
G06Q20/22	/	20	/	22

NON-CLAIMED				
G06Q20/34	/	20	/	34

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
705	50

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	23 March 2021	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685	26 March 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1A

U.S. Patent and Trademark Office — Part of Paper No.: 20210323

Samsung Ex. 1016, Page 636 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	**Art Unit**
	ISIDORA I IMMANUEL	3685

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	6	10		19										
	2	7	11												
2	3	8	12												
3	4		13												
4	5	9	14												
	6		15												
	7		16												
	8	10	17												
5	9	11	18												

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	23 March 2021	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685	26 March 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1A

U.S. Patent and Trademark Office — Part of Paper No.: 20210323

Samsung Ex. 1016, Page 637 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016	09/17/2017	05/22/2018	04/15/2019	12/18/2019	08/17/2020	02/27/2021	03/23/2021
1	1	✓	✓	✓	✓	✓	✓	✓	✓	=
	2	✓	✓	✓	✓	✓	✓	✓	✓	-
2	3	✓	✓	✓	✓	✓	✓	✓	✓	=
3	4	✓	✓	✓	✓	✓	✓	✓	✓	=
4	5	✓	✓	✓	✓	✓	✓	✓	✓	=
	6	✓	✓	✓	✓	✓	✓	✓	✓	-
	7	✓	✓	✓	✓	✓	✓	✓	✓	-
	8	✓	✓	✓	✓	✓	✓	-	-	-
5	9	✓	✓	✓	✓	✓	✓	✓	✓	=
6	10	✓	✓	✓	✓	✓	✓	✓	✓	=
7	11	✓	✓	✓	✓	✓	✓	✓	✓	=
8	12	✓	✓	✓	✓	✓	✓	✓	✓	=
	13	✓	✓	✓	✓	✓	✓	✓	✓	-
9	14	✓	✓	✓	✓	✓	✓	✓	✓	=
	15	✓	✓	✓	✓	✓	✓	✓	✓	-
	16	✓	✓	✓	✓	✓	✓	✓	✓	-
10	17	✓	✓	✓	✓	✓	✓	✓	✓	=
11	18	✓	✓	✓	✓	✓	✓	✓	✓	=
	19	✓	✓	✓	✓	✓	✓	✓	✓	-

Samsung Ex. 1016, Page 638 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q20	08/17/2020	III
G06Q2220	08/17/2020	III
H04L41	02/27/2021	III
G06F8	02/27/2021	III

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705			

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	

Samsung Ex. 1016, Page 639 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

Search Notes		
Search Notes	**Date**	**Examiner**
See attached notes	2/1/2016	II
101 withdrawal - Weinhart	06/06/2018	III
See attached notes (EAST)	04/15/2019	III
EAST search report	08/17/2020	III
NPL search	08/17/2020	III
EAST	02/27/2021	III
STIC Search report from prior allowance discussions	03/23/2021	III
EAST search report	03/23/2021	III
NPL SEARCH	03/23/2021	III

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	See East search report	03/23/2021	III

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	

Samsung Ex. 1016, Page 640 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATIONEN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
9 juillet 2009 (09.07.2009)

PCT

(10) Numéro de publication internationale
W O 2009/083679 A 3

(51) Classification internationale des brevets :
G06K 19/07 (2006.01) ***H04L 9/32*** (2006.01)
G06K 19/077 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2008/052275

(22) Date de dépôt international :
11 décembre 2008 (11.12.2008)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0760201 21 décembre 2007 (21.12.2007) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **ASSADI, Houssem** [FR/FR]; 59 rue Jacques Prévert, F-14000 Caen (FR). **PICQUENOT, David** [FR/FR]; 3 Impasse du Grand Clos, F-14280 Saint Contest (FR).

(74) Mandataire : FRANCE TELECOM R & D/PIV/BREVETS; URBILLAC Chantai, 38-40 rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés ***(sauf** indication **contraire, pour tout titre de protection régionale disponible) :*** **ARIPO (BW, GH,** GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, **FI,** FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, **BJ,** CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17(v))*

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

[Suite sur la page suivante]

(54) Title : METHOD OF READING AN ELECTRONIC TAG BY A TERMINAL

(54) Titre : PROCEDE DE LECTURE D'UNE ETIQUETTE ELECTRONIQUE PAR UN TERMINAL

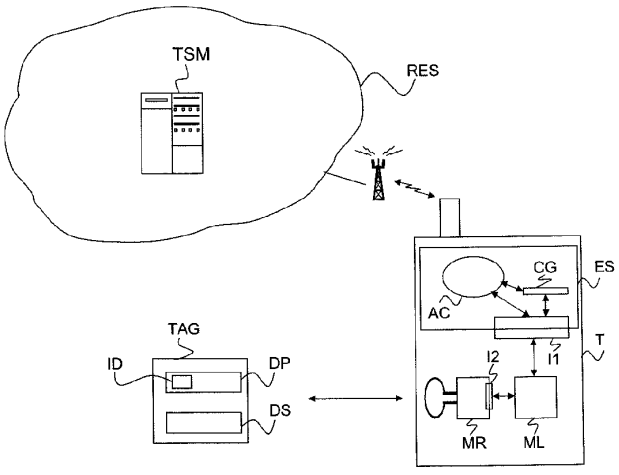


Fig. 1

(57) Abstract : The invention relates to a method of reading an electronic tag (TAG) storing data comprising an identifier (ID), by a terminal (T) furnished with a short-range radio reading module (ML) and with a card émulation application (AC), associated with said identifier (ID) and situated in a secure élément (ES) of said terminal (T), said method being characterized in that it comprises the steps of: - reading by said reading module (ML) of said identifier (ID), - establishment of a communication session between said card émulation application (AC) and said electronic tag (TAG), said reading module (ML) being used as agent server by said card émulation application (AC), said card émulation application (AC) having been previously authenticated, - and reading by said card émulation application (AC) of data (DS) stored in said electronic tag (TAG) and intended for said card émulation application (AC).

(57) **Abrégé** : L'invention concerne un procédé de lecture d'une étiquette électronique (TAG) stockant des données comportant un identifiant **(ID),**

[Suite sur la page suivante]

WO 2009/083679 A3

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.K))*

(88) Date de publication du rapport de recherche internationale :

XX septembre 2009

par un terminal (T) muni d'un module de lecture (ML) radio courte distance et d'une application (AC) d'émulation de carte, associée audit identifiant (ID) et située dans un élément sécurisé (ES) dudit terminal (T), ledit procédé étant caractérisé en ce qu'il comporte les étapes de : - lecture par ledit module de lecture (ML) dudit identifiant (ID), - établissement d'une session de communication entre ladite application (AC) d'émulation de carte et ladite étiquette électronique (TAG), ledit module de lecture (ML) étant utilisé comme serveur mandataire par ladite application d'émulation de carte (AC), ladite application d'émulation de carte (AC) ayant été préalablement authentifiée, - et lecture par ladite application (AC) d'émulation de carte de données (DS) stockées dans ladite étiquette électronique (TAG) et destinées à ladite application (AC) d'émulation de carte.

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2008/052275

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06Q30/00

According to International Patent Classification (IPC) orto both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification System followed by classification symbols)
G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted dunng the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where approp πate, of the relevant passages	Relevant to daim No
Y	EP 1 798 867 A (INNOVISION RES & TECH PLC [GB]) 20 June 2007 (2007-06-20) paragraph [0021] - paragraph [0097] paragraph [0119] - paragraph [0134]; figure 18	1-10
Y	US 2004/002305 A1 (BYMAN-KI VIVUORI BIRGIT [FI] ET AL) 1 January 2004 (2004-01-01) paragraphs [0008], [0009], [0012] paragraph [0036] - paragraph [0039] paragraph [0052] - paragraph [0055] paragraph [0067] - paragraph [0068] paragraph [0078] - paragraph [0082] paragraph [0104] - paragraph [0113]	1-10
A		1-7,9,10

-/--

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Spécial catégories of cited documents

"A" document defimng the gênerai state of the art which is not considered to be of particular relevance

"E" βarlier document but published on or afterthe international filing date

"L[1]" document which may throw doubts on pnoπty claιm(s) or which is cited to establish the publication date of another citation or other spécial reason (as specified)

"O[1]" document refernng to an oral disclosure, use, exhibition or other means

"P" document published pnor to the international filing date but laterthan the pnoπty date claimed

"T" later document published afterthe international filing date or pnoπty date and not in conflict with the application but cited to understand the pnnciple or theory underlying the invention

"X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y[1]" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such docu¬ments, such combination being obvious to a person skilled in the art

'&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 jui l let 2009	27/07/2009

Name and mailing address of the ISA/	Authoπzed officer
Européen Patent Office, P B. 5818 Patentlaan 2 NL- 2280 HV Rijswijk Tel (+31-70) 340-2040, Fax (+31-70) 340-3016	Aupiais, Brigitte

Foim PCT/ISA/210 (second sheet) (Apnl 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2008/052275

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to daim No.
X	WO 2006/015617 A (TELECOM ITALIA SPA [IT]; ALESSIO ELISA [IT]; RICCIATO FABIO [IT]; TURO) 16 February 2006 (2006-02-16) page 4, Iine 21 - page 5, Iine 8 page 6, Iine 4 - page 6, une 35 page 7, une 14 - page 9, une 25 page 10, une 7 - page 10, une 26	1,2,4, 8-10
A	EP 1 837 781 A (NOKIA CORP [FI]) 26 September 2007 (2007-09-26) paragraph [0108] - paragraph [0146]	1-10
A	EP 1 855 229 A (INSIDE CONTACTLESS [FR]) 14 November 2007 (2007-11-14) paragraph [0041] - paragraph [0067]	1-10
A	EP 1 571 591 A (SWISSCOM MOBILE AG [CH]) 7 September 2005 (2005-09-07) paragraph [0014] - paragraph [0036]	1-10

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2008/052275

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1798867 A	20-06-2007	GB 2433386 A	20-06-2007
US 2004002305 A1	01-01-2004	TW 277002 B	21-03-2007
		US 2004203944 A1	14-10-2004
WO 2006015617 A	16-02-2006	BR PI0419000 A	11-12-2007
		CN 101027699 A	29-08-2007
		EP 1776675 A1	25-04-2007
		JP 2008509490 T	27-03-2008
		US 2008175390 A1	24-07-2008
EP 1837781 A	26-09-2007	NONE	
EP 1855229 A	14-11-2007	CA 2587119 A1	10-11-2007
		CA 2587122 A1	10-11-2007
		EP 1855389 A1	14-11-2007
		JP 2008047094 A	28-02-2008
		JP 2008022533 A	31-01-2008
		US 2007263595 A1	15-11-2007
		US 2007263596 A1	15-11-2007
EP 1571591 A	07-09-2005	NONE	

Form PCT/ISA/210 (patentfamily annex) (April 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2008/052275

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06 G06Q30/00

Selon la classification Internationale des brevets (CIB) ou a la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification SUIVI des symboles de classement)
G07F

Documentation consultée autre que la documentation minimale dans la mesure ou ces documents relèvent des domaines sur lesquels a porte la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilises)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cites avec le cas échéant, l indication des passages pertinents	no des revendications visées
Y	EP 1 798 867 A (INNOVISION RES & TECH PLC [GB]) 20 juin 2007 (2007-06-20) alinéa [0021] - alinéa [0097] alinéa [0119] - alinéa [0134]; figure 18	1-10
Y	US 2004/002305 A1 (BYMAN-KIVIVUORI BIRGIT [FI] ET AL) 1 janvier 2004 (2004-01-01) alinéas [0008], [0009], [0012] alinéa [0036] - alinéa [0039] alinéa [0052] - alinéa [0055] alinéa [0067] - alinéa [0068] alinéa [0078] - alinéa [0082] alinéa [0104] - alinéa [0113]	1-10
A		1-7,9,10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiques en annexe

* Catégories spéciales de documents cités

"A" document définissant l'état gênerai dθ la technique non considère comme particulièrement pertinent

"E" document antéπeur, mais publie à la date de dépôt international ou aprés cette date

"L" document pouvant jeter un doute sur une revθndication de pnoπtê ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publie avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publie après la date de dépôt international ou la date de priorité et n appartenena πt pas à l'état de la technique pertinent, mais cite pour comprendre le principe *ou* la theo πe constituant la base de l'iπvantion

"X" document particulièrement pertinent l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considère isolement

"Y" document particulièrement pertinent l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associe à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

'&' document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d expédition du présent rapport de recherche Internationale
10 jui l let 2009	27/07/2009

Nom et adresse postale de l administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P B 5818 Patentlaa π2 **NL** -2280 HV Rijswijk Tel (+31-70) 340-2040, Fax (+31-70) 340-3016	Aupïais, Brigitte

Formulaire PCT/ISA/21 0 (deux eme feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2008/052275

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'Indication des passages pertinents	no. des revendications visées
X	WO 2006/015617 A (TELECOM ITALIA SPA [IT]; ALESSIO ELISA [IT]; RICCIATO FABIO [IT]; TURO) 16 février 2006 (2006-02-16) page 4, ligne 21 - page 5, ligne 8 page 6, ligne 4 - page 6, ligne 35 page 7, ligne 14 - page 9, ligne 25 page 10, ligne 7 - page 10, ligne 26	1,2,4, 8-10
A	EP 1 837 781 A (NOKIA CORP [FI]) 26 septembre 2007 (2007-09-26) alinéa [0108] - alinéa [0146]	1-10
A	EP 1 855 229 A (INSIDE CONTACTLESS [FR]) 14 novembre 2007 (2007-11-14) alinéa [0041] - alinéa [0067]	1-10
A	EP 1 571 591 A (SWISSCOM MOBILE AG [CH]) 7 septembre 2005 (2005-09-07) alinéa [0014] - alinéa [0036]	1-10

Samsung Ex. 1016, Page 647 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2008/052275

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1798867 A	20-06-2007	GB 2433386 A	20-06-2007
US 2004002305 A1	01-01-2004	TW 277002 B	21-03-2007
		US 2004203944 A1	14-10-2004
WO 2006015617 A	16-02-2006	BR PI0419000 A	11-12-2007
		CN 101027699 A	29-08-2007
		EP 1776675 A1	25-04-2007
		JP 2008509490 T	27-03-2008
		US 2008175390 A1	24-07-2008
EP 1837781 A	26-09-2007	AUCUN	
EP 1855229 A	14-11-2007	CA 2587119 A1	10-11-2007
		CA 2587122 A1	10-11-2007
		EP 1855389 A1	14-11-2007
		JP 2008047094 A	28-02-2008
		JP 2008022533 A	31-01-2008
		US 2007263595 A1	15-11-2007
		US 2007263596 A1	15-11-2007
EP 1571591 A	07-09-2005	AUCUN	

Samsung Ex. 1016, Page 648 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S2	178	(("(6101543") or ("20130178159") or ("20170323301") or ("20170372321") or ("20200034849") or ("5249218") or ("5353334") or ("5367563") or ("5530703") or ("5640444") or ("5937421") or ("5963650") or ("5995839") or ("6078314") or ("6108003") or ("6137791") or ("6373820") or ("6802058") or ("6853851") or ("6912389") or ("7006964") or ("7039434") or ("7151931") or ("7155381") or ("7162408") or ("7165191") or ("7231330") or ("7296190") or ("7317912") or ("7319874") or ("7319948") or ("7324588") or ("7334162") or ("7392060") or ("7450936") or ("7486927") or ("7502626") or ("7512402") or ("7516451") or ("7545386") or ("7548804") or ("7577887") or ("7606261") or ("7613453") or ("7620015") or ("7698121") or ("7734288") or ("7738426") or ("7783261") or ("7809578") or (").pn.")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 11:43
S3	596	(emulat$4 with application) and (secure adj element)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:32
S4	272	(emulat$4 with application) same (secure adj element)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:32
S5	245	S3 AND ((G06Q20/3278 OR G06Q20/3829 OR G06Q20/3821 OR G06Q2220/00 OR G06Q20/3226 OR G06Q20/3825 OR G06Q2220/14).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2020/08/17 12:34

			DERWENT; IBM_TDB			
S6	108	S4 AND ((G06Q20/3278 OR G06Q20/3829 OR G06Q20/3821 OR G06Q2220/00 OR G06Q20/3226 OR G06Q20/3825 OR G06Q2220/14).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:34
S7	6	(("9128829") or ("8646059") or ("20030151125")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 12:36
S8	10	(("9128829") or ("8646059") or ("20030151125") or ("6481632")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/08/17 13:45
S9	207	(service adj manager) and emulator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/02/27 09:34
S10	2,850,311	counter or tracker emulator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/02/27 09:34
S11	16,062	(counter or track$4) and emulator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/02/27 09:34
S12	47	S9 AND ((H04L41/0806 OR H04L47/70 OR G06F8/65).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2021/02/27 09:35

			DERWENT; IBM_TDB			
S13	180	((("(6101543") or ("20130178159") or ("20170323301") or ("20170372321") or ("20200034849") or ("5249218") or ("5353334") or ("5367563") or ("5530703") or ("5640444") or ("5937421") or ("5963650") or ("5995839") or ("6078314") or ("6108003") or ("6137791") or ("6373820") or ("6802058") or ("6853851") or ("6912389") or ("7006964") or ("7039434") or ("7151931") or ("7155381") or ("7162408") or ("7165191") or ("7231330") or ("7296190") or ("7317912") or ("7319874") or ("7319948") or ("7324588") or ("7334162") or ("7392060") or ("7450936") or ("7486927") or ("7502626") or ("7512402") or ("7516451") or ("7545386") or ("7548804") or ("7577887") or ("7606261") or ("7613453") or ("7620015") or ("7698121") or ("7734288") or ("7738426") or ("7783261") or ("7809578") or (").pn.")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/03/23 16:47
S14	0	((counter or track$4) with emulator with (application or card)) same (secure adj element)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/03/23 18:34

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	((switch$4 or replac$4 or swap$5) with emulator with (application or card)) same (secure adj element)	US-PGPUB; USPAT	OR	OFF	2021/03/23 19:50
L2	1	1 AND ((G06Q20/322 OR G06Q20/352 OR G06Q20/3552 OR G06Q20/3572 OR G06Q20/3672).CPC.)	US-PGPUB; USPAT	OR	OFF	2021/03/23 19:52
S15	0	((counter or track$4) with emulator with (application or card)) same (secure adj element)	USPAT	OR	OFF	2021/03/23 18:34

S16	0	((counter or track$4) with emulator with (application or card)) same (secure adj element)	US-PGPUB; USPAT	OR	OFF	2021/03/23 18:34

3/23/2021 7:53:28 PM
C:\Users\iimmanuel\Documents\EAST\Workspaces\13782948.wsp

STIC Scientific & Technical Information Center

EIC 3600 Search Report

Requester	Immanuel, Isidora Emp#: 90925 TAB-55086 (469) 295-9094 isidora.immanuel@uspto.gov
Case Serial Number:	13/782948
Access Search Log Number:	619540

Searcher:	Sylvia Keys
Location:	EIC 3600, Knox 4B68
Phone:	571-272-3534
Email:	sylvia.keys@uspto.gov
Date Completed:	6/11/2020

This search report contains the following content:

- **Search Histories**
  Keyword/synonym strings and search strategies used by the EIC Searcher in completing the prior art search are included. The search history for each database or resource utilized appears at the top of each database/resource section, indicated by the database/resource section headings.
- **Search Results**
  Only on-topic results are included in the search report. On-topic results include all references found that are related to the art area being searched. These references may not necessarily be useful for a rejection or other office action, but are included for the Examiner's review. Off-topic, unrelated, or irrelevant search results ("false drops" or "false hits") were removed by the Searcher. Off-topic results include all references that are unrelated to the art area being searched.

If you have any questions about this search, or about how to interpret this search report, please do not hesitate to contact the Searcher using the contact information listed above.

If you need assistance retrieving the full text of any of the references contained in this report, please contact the Searcher listed above, or the EIC 3600 Reference Desk at 571-272-3488 (x23488) or STIC-EIC3600@uspto.gov.

Thank you for using the EIC, and we look forward to your next search!

Samsung Ex. 1016, Page 653 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Potential References of Interest

7

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Cho, Fu-Liang; Cho, Fu-Tong; Fung, Daniel; Pan, Hsin (Inventors). RFCyber Corporation (Assignee). **US 20060161878 A1**. (Published 20 Jul 2006).

... system **10**, alternatively termed RFCyberWork, is a platform for ...

- 8

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Fu-Tong, Cho; Fu-Liang, Cho; PAN HSIN (Inventors). RFCYBER CORP (Assignee). **TW 200632705 A**. (Published 16 Sep 2006).

- 1

NFC - The intuitive contactless technology becomes reality

Dachs, C.. **Elektrotechnik und Informationstechnik** 122.12: 466-471. Springer Wien. (Dec 2005)

EnglishENGEnglish

Near Field Communication (NFC) is opening-up completely new ... mobile communication industry. It enables contactless peer-to-peer communication, reading/writing of contactless ...

Dialog –Patent Files and Inventors

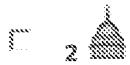
Search Strategy

Databases: Argentina Patents Fulltext, Australia Patents Fulltext, Austria Patents Fulltext, Belgium Patents Fulltext, Brazil Patents Fulltext, Canada Patents Fulltext, China Patents Fulltext, Denmark Patents Fulltext, Derwent Chemistry Resource, Derwent Patents Citation Index®, Derwent World Patents Index®, Eurasia Patents Fulltext, European Patents Fulltext, Finland Patents Fulltext, France Patents Fulltext, Germany Patents Fulltext, Global Patents Bibliographic, Great Britain Patents Fulltext, IFI CLAIMS® US Patents and Legal Status, IMS Patent Focus, India Patents Fulltext™, INPADOC / Family and Legal Status, Ireland Patents Fulltext, Italy Patents Fulltext, Japan Patents Fulltext, JAPIO - Patent Abstracts of Japan, Korea Patents Fulltext, LitAlert®, Luxembourg Patents Fulltext, Mexico Patents Fulltext, Monaco Patents Fulltext, Netherlands Patents Fulltext, Norway Patents Fulltext, Portugal Patents Fulltext, Russia Patents Fulltext, Spain Patents Fulltext, Sweden Patents Fulltext, Switzerland Patents Fulltext, United States Patents Fulltext, WIPO PCT Patents Fulltext

Set#	Searched for	Results
S1	au((xie or koh or pan))	2732377
S2	rfcyber*	633
S3	s1 and s2	132
S4	py(2006) and s3	8

Samsung Ex. 1016, Page 654 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

- ☐ 2



SYSTEM FOR DEVELOPING AND DEPLOYING RADIO FREQUENCY IDENTIFICATION ENABLED SOFTWARE APPLICATIONS

Koh, Liang Seng; Fu-Liang, Cho; Fung, Daniel; PAN HSIN (Inventors). RFCYBER CORP (Assignee). **WO 2006074096 A2.** (Published 13 Jul 2006).

☐ 7

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Cho, Fu-Liang; Cho, Fu-Tong; Fung, Daniel; Pan, Hsin (Inventors). RFCyber Corporation (Assignee). **US 20060161878 A1.** (Published 20 Jul 2006).

... system **10**, alternatively termed RFCyberWork, is a platform for ...

- ☐ 8

System for developing and deploying radio frequency identification enabled software applications

Koh, Liang Seng; Fu-Tong, Cho; Fu-Liang, Cho; PAN HSIN (Inventors). RFCYBER CORP (Assignee). **TW 200632705 A.** (Published 16 Sep 2006).

Dialog – NPL and Inventor(s)

Search Strategy

Databases: ABI/INFORM® Professional Advanced, Abstracts in New Technology & Engineering, AdisInsight: Drugs, AdisInsight: Trials, Adis Pharmacoeconomics & Outcomes News, AGRICOLA, AGRIS, Allied & Complementary Medicine™, Analytical Abstracts, APA PsycInfo®, Aqualine, Aquatic Science & Fisheries Abstracts (ASFA), Australian Education Index, BIOSIS® Toxicology, BIOSIS Previews®, British Library Inside Conferences, British Nursing Index, Business & Industry, CAB ABSTRACTS, Chemical Business Newsbase, Chemical Engineering & Biotechnology Abstracts, Chemical Safety Newsbase, Civil Engineering Abstracts, Current Contents® Search, DH-DATA: Health Administration, Medical Toxicology & Environmental Health, DIOGENES® FDA Regulatory Updates, Drug Information Fulltext, Earthquake Engineering Abstracts, Ei Compendex®, Embase®, EMCare®, ESPICOM Pharmaceutical & Medical Device News, FDAnews, FLUIDEX (Fluid Engineering Abstracts), Foodline®: MARKET, Foodline®: PRODUCT, Foodline®: SCIENCE, FSTA®, Gale Group Computer Database™, Gale Group Health Periodicals Database, Gale Group New Product Announcements / Plus®, Gale Group Newsletter Database™, Gale Group PharmaBiomed Business Journals, Gale Group PROMT®, Gale Group Trade & Industry Database™, GEOBASE™, GeoRef, HSELINE: Health and Safety, ICONDA - International Construction Database, IMS Company Profiles, IMS New Product Focus, IMS Pharma Trademarks, IMS R&D Focus, IMS R&D Focus Drug News, Inspec®, International Pharmaceutical Abstracts, Jane's Defense & Aerospace News, King's Fund, KOSMET: Cosmetic Science, Lancet Titles, Material Safety Datasheets -OHS™, Mechanical & Transportation Engineering Abstracts, MEDLINE®, Meteorological & Geoastrophysical Abstracts, New England Journal of Medicine, NTIS: National Technical Information Service, Oceanic Abstracts, PAIS International, Paperbase, PAPERCHEM, ProQuest Advanced Tech & Aerospace Professional, ProQuest Biological & Health Science Professional, ProQuest Environmental Science Professional, ProQuest Materials Research Professional, ProQuest Newsstand Professional, ProQuest Technology Research Professional, Prous Science Daily Essentials, Prous Science Drug Data Report, Prous Science Drugs Of The Future™,

Samsung Ex. 1016, Page 655 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Registry of Toxic Effects of Chemical Substances (RTECS®), SciSearch®: a Cited Reference Science Database, Social SciSearch®, ToxFile®, Transport Research International Documentation, TULSA™ (Petroleum Abstracts), UBM Computer Full Text, Weldasearch®, Zoological Record Plus

Set#	Searched for	Results
S1	“smart card$1” or smartcard$1	369847*
S2	contactless and (“smart card$1” or smartcard or card$1)	101277*
S3	card$ and (transaction$1 or interact$3 or payment$1 or “monetary function$1”)	4099506*
S4	mifare* or “micron fare collection system”	3361°
S5	(s1 or s2 or s3 or s4) and (switch$3 or replac$3 or substitute$1 or substitution or “back$3 up”)	696777*
S6	(s1 or s2 or s3 or s4) and (activate$1 or activation or activating)	159179*
S7	(s1 or s2 or s3 or s4) and emulat* or imitat* or copy or copies or mimic or mirror or match	56927115*
S8	(nfc or “near field communication$1”) and interface$1	34616*
S9	smartphone (mobile or web or smart or cell or cellular or wireless or cordless or handheld or “hand held” or media or user) n/5 (phone or telephone or fone or device or apparatus or equipment)	640291*
S10	pda or “personal digital assistant” or wireless or cellphone or webphone or palmpilot or "palm pilot" or ipad or iphone or smartphone or tablet or android or pc or “personal computer$1”	26128177*
S11	au((xie or koh or pan))	2541829*
S12	rfcyber*	34°
S13	(s5 or s6 or s7) and s8	11622*
S14	s13 and (s9 or s10)	9968*
S15	su(contactless*) and s14	12°
S16	py(2006) and s14	36°
S17	su(contactless) and s16	0°
S18	su(emulat*) and s14	16°
S19	su("smartcard*") and s14	3°
S20	su("smart card*") and s14	244°
S21	s20 not s19	243°
S22	su(emulat*) and s21	2°
S23	py(2006) and s21	6°
S24	(s11 or s12) and s21	1°
S25	(s11 and s12) and contactless	0°

NFC - The intuitive contactless technology becomes reality

Samsung Ex. 1016, Page 656 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Dachs, C.. **Elektrotechnik und Informationstechnik** 122.12: 466-471. Springer Wien. (Dec 2005)

EnglishENGEnglish

Near Field Communication (NFC) is opening-up completely new ... mobile communication industry. It enables contactless peer-to-peer communication, reading/writing of contactless ...

er already carries around (e. g. ...

CASHLESS PAYMENTS: Contactless cuts out cash and cards

Electronic Payments International: 8-9. London: Lafferty Ltd. (Feb 2006)

... major trials using MasterCard International's contactless payment technology PayPass. The Royal Bank ... on a Maestro or MasterCard card or be offered as a ...

Samsung Ex. 1016, Page 657 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Chameleon: A Versatile Emulator for Contactless Smartcards*

Timo Kasper, Ingo von Maurich, David Oswald, Christof Paar

Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany
{timo.kasper, ingo.vonmaurich, david.oswald, christof.paar}@rub.de

Abstract. We develop a new, custom-built hardware for emulating contactless smartcards compliant to ISO 14443. The device is based on a modern low-cost microcontroller and can support basically all relevant (cryptographic) protocols used by contactless smartcards today, e.g., those based on AES or Triple-DES. As a proof of concept, we present a full emulation of Mifare Classic cards on the basis of our highly optimized implementation of the stream cipher Crypto1. The implementation enables the creation of exact clones of such cards, including the UID. We furthermore reverse-engineered the protocol of DESFire EV1 and realize the first emulation of DESFire and DESFire EV1 cards in the literature. We practically demonstrate the capabilities of our emulator by spoofing several real-world systems, e.g., creating a contactless payment card which allows an attacker to set the stored credit balance as desired and hence make an infinite amount of payments.

Keywords: RFID, contactless smartcards, payment systems, access control, efficient implementation

1 Introduction

Radio Frequency Identification (RFID) devices are deployed in a wide range of transportation and access control systems world-wide. If high privacy or security demands have to be met, typically contactless smartcards according to the ISO 14443 standard [13] are employed, as they offer sufficient computational power for cryptographic purposes. Moreover, a growing number of payment systems incorporates secure RFID cards [16], as they offer additional benefits in terms of flexibility and convenience over their contact-based counterpart. State-of-the-art contactless cards, such as the electronic passport ePass [8], provide a high level of security by means of various cryptographic primitives.

In general, RFID technology implies new threats compared to contact-based systems, for instance, a card residing in a pocket or wallet could be read out or modified without the owner taking note of it. Due to the cost sensitivity of such high-volume applications, card manufacturers are tempted to use outdated but "cheap" cryptographic components, e.g., in Mifare Classic products.

Since the reverse-engineering of the Crypto1 cipher used in Mifare Classic cards and the subsequently published attacks (cf. Sect. 3.1), the cards have to be regarded as insecure, as the secret keys can be extracted in seconds by means of card-only attacks. Once all keys of the card are known to an attacker, cards can be modified or duplicated. As many systems in the real world still rely on these weak cards, severe security threats may arise.

Accordingly, recently installed contactless systems, especially those with high security demands, are based on the DESFire variant of the Mifare family, and system integrators

* The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.

upgrade the old Mifare Classic technology to these newer cards wherever possible. While the 3DES cipher employed in these cards is secure from the mathematical point of view, the implementation on the card is vulnerable to side-channel analysis, so that it is again possible to extract the secret keys of a card[1], as detailed in Sect. 3.2. Hence, emulating these modern cards is also practical and renders various attacks in real-world scenarios possible.

The resulting security weaknesses can become very costly – one example is a widespread contactless payment system based on Mifare Classic cards as analyzed in [16], where the credit value on the cards can be modified by an adversary with minimal efforts. For many of these systems, the read-only Unique Identifier (UID) of each card constitutes the only means to detect fraud in the backend, as there are no cards available on the market where the UID can be altered. In this paper, we exhibit the possibility of emulating and cloning RFID-enabled smartcards compliant to ISO 14443, including their UID.

1.1 Background and Related Work

Several research groups have proposed custom devices to emulate and counterfeit RFID devices. However, virtually all emulators presented so far suffer from certain drawbacks, e.g., insufficient computational resources, high cost, or impractical dimensions, limiting the threat they pose in the context of attacking real-world systems.

A custom RFID emulation hardware called Ghost is presented in [24]. The Ghost is able to emulate Mifare Ultralight cards which do not use any encryption. Emulating contactless cards employing secure cryptography seems to be impossible using this device due to computational limitations. The OpenPICC project [20] is mainly an RFID sniffing device. There was an approach to offer support for ISO 14443A, but the project seems to be discontinued. The Proxmark III [21] enables sniffing, reading and cloning of RFID tags. Since the device is based on a Field Programmable Gate Array (FPGA), it is also capable of emulating Mifare Classic cards, but at a comparably high cost of $399. The "HF Demo tag" [12] is based on an Atmel ATMega128 microcontroller which is not computationally powerful enough to perform encryptions with state-of-the-art ciphers in the time window given by the relevant protocols. An embedded system for analyzing the security of contactless smartcards was introduced in [14]. The attack hardware consists of a so-called Fake Tag and an RFID reader and can be used for, e.g., practical relay attacks. The device is based on a Atmel ATMega32 [1] processor with a constrained performance and is designed such that all important functionality is provided by the RFID reader. Hence, in addition to the lack of computational power, the Fake Tag cannot operate independently from the reader, which can be a major drawback for practical attacks. The authors also implemented an emulation of Mifare Classic, but similar to the HF Demo tag, the encryption runs too slow so that timing constraints of the protocol cannot be met. We used this work as a starting point for the development of our new standalone RFID emulator.

1.2 Contribution of this Paper

We built a freely programmable low-cost device that is capable of emulating various types of contactless smartcards, including those employing secure cryptography. The device operates autonomously without the need of a PC, can be powered from a battery, and possesses an Electronically Erasable Programmable Read-only Memory (EEPROM) for storing received bitstreams or other non-volatile information. An attacker using the presented hardware, which can be built for less than $25, is in full control over all data stored on the emulated card, including its UID and the secret keys.

[1] Note that the effort for extracting secret keys from Mifare DESfire cards by means of side-channel analysis is much higher compared to the Mifare Classic attacks.

In order to demonstrate the capabilities of our emulator in the context of real-world attacks, we implemented optimized versions of the Crypto1 stream cipher, the Data Encryption Standard (DES), Triple-DES (3DES) and the Advanced Encryption Standard (AES), as required for emulating the widespread Mifare Classic, Mifare DESFire and Mifare DESFire EV1 cards. With the developed software, it is possible to simulate the presence of one of these cards with an arbitrarily chosen content and identifier, and hence spoof real-world systems in various manners. For example, the emulator can behave as a card that automatically restores its credit value after a payment, or that possesses a new UID and card number on each payment, which impedes the detection of fraud. Besides the simulation of cards, our hardware allows for sniffing, e.g., reverse-engineering of protocols, relay attacks, and testing the vulnerability of RFID readers towards a behavior of the card that does not conform to the specifications, for instance, with respect to timing, intentionally wrong calculation of parity bits, or buffer overflows.

The remainder of this paper is structured as follows: in Sect. 2, we present our custom RFID hardware that serves as a basis for card emulations and attacks. After giving a brief summary of the relevant characteristics and protocols of Mifare Classic, Mifare DESFire and Mifare DESFire EV1 cards in Sect. 3, we detail on our implementations of the respective emulations in Sect. 4. Finally, practical real-world analyses performed with our hardware are described in Sect. 5.

2 Hardware Setup

In the following, we give a brief introduction to the physical characteristics of the RFID technology employed in contactless smartcards. Then, our freely programmable emulator for contactless smartcards is presented.

2.1 RFID Technology

In a typical setup for contactless smartcards, a reading device generates a strong Electro-Magnetic (EM) field at a frequency of 13.56 MHz for supplying the card with energy for its operation. The reader acts as master, while the card serves as slave, thus only the reader can start a communication and issue commands to the card. The ISO 14443 standard specifies the physical characteristics, the data modulation and other characteristics of contactless smartcards. For data transmission, the reader encodes the bits using a pulsed Miller code and transmits it by switching off the EM field for short periods of time. The data to be sent by the card is encoded using a Manchester-code and is afterwards transmitted via the EM field using load-modulation with a 847.5 kHz sub-carrier.

2.2 Our Emulator

For the security analyses in this paper, we developed a custom, freely programmable device termed "Chameleon", which can emulate contactless smartcards compliant to the ISO 14443 standard in a stand-alone manner. Our emulation device consists of off-the-shelf hardware and can be built for less than $25. It is based on an Atmel ATxmega192A3 microcontroller [2, 3] which provides 192 kB of program memory, 16 kB SRAM and 4 kB EEPROM memory. Using an FTDI FT245RL chip [9], the ATxmega is able to communicate with a PC via the Universal Serial Bus (USB). This communication link can be used for debugging purposes and data manipulation at runtime. Figure 1 shows the first version of our RFID emulation device.

We chose the ATxmega because it features a hardware acceleration of both DES and AES-128. After loading the key and the data to the corresponding registers, the ATxmega is able

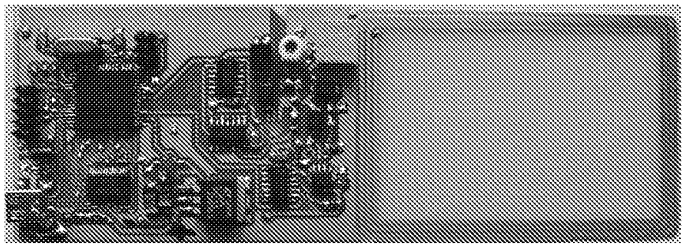


Fig. 1. Our stand-alone RFID emulation device.

to perform a DES en- or decryption in 16 clock cycles, i.e., one DES round per clock cycle, whereas the AES engine runs concurrently to the CPU and requires 375 clock cycles until an en- or decryption of one block is finished. The microcontroller is clocked by an external 13.56 MHz crystal, which is internally doubled using a high frequency Phase Locked Loop (PLL).

The coupling to the reader is established by a rectangular coil on the Printed Circuit Board (PCB). Variable capacitors are placed in parallel to form a parallel resonant circuit that is tuned to the carrier frequency. Analog circuitry assists the microcontroller in extracting the encoded data from the EM field and transmitting bitstreams. The design is similar to [14] and mainly shapes the signals according to the ISO 14443 standard and converts them to the appropriate voltage levels. Our emulation device can either be powered via the USB interface or run on battery. As all functionality is directly provided by the microcontroller, the Chameleon operates autonomously without the support of a PC. The full schematics of the developed hardware are given in the Appendix B.

3 Mifare Cards

This section covers the details of Mifare Classic, DESFire and DESFire EV1 cards. We present important facts required for the emulation of the cards and detail on the different authentication protocols, as implemented in Sect. 4.1 and Sect. 4.2. For reference, the complete protocols including the command codes and the low-level format are provided in Appendix A.

3.1 Mifare Classic

Since its introduction more than a decade ago, allegedly over 1 billion Mifare Classic ICs and 7 million reader components have been sold [18]. The cards provide data encryption and entity authentication based on the proprietary stream cipher Crypto1 for preventing from attacks like eavesdropping, cloning, replay and unauthorized reading or modification of the data stored on the card. Crypto1 is based on a Linear Feedback Shift Register (LFSR) with a length of 48 bit.

Basically, a Mifare Classic card can be regarded as a secured EEPROM memory with an RFID communication interface. In this work, we focus on the by far most widely employed Mifare Classic 1K version with 1024 byte EEPROM. All Mifare Classic variants comply to Parts 1-3 of ISO 14443A [13]. While the standard also allows for higher data rates, the cards communicate at a fixed data rate of 106 kBit/s. In addition, they feature a proprietary high-level protocol that diverges from Part 4 of ISO 14443A.

The memory of a Mifare Classic card is divided into sectors, whereas each sector consists of four blocks, as illustrated in Fig. 2. Each sector can be secured by means of two cryptographic

Samsung Ex. 1016, Page 661 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

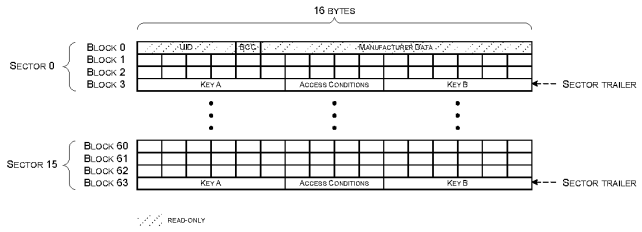


Fig. 2. The memory structure of a Mifare Classic 1K card.

keys A and B that are stored along with a set of access conditions in the last block of each sector. Before a sector can be accessed, a proprietary mutual authentication protocol with the appropriate secret key has to be carried out, cf. Protocol 1. The access conditions determine the commands that are allowed for each block of the sector (read, write, increment, decrement) and define the role of the keys [19]. The other blocks of each sector can be used for data storage. Note that the first block of the first sector differs from this scheme: it always contains a UID, along with some other manufacturer-specific data. The first block is written to the chip at manufacturing time, making it impossible to change the UID.

When a card is placed close to a reader, the anticollision and select procedure as defined in ISO 14443A is carried out. Then, an authentication command is issued by the reader that specifies for which sector the authentication is performed. The card replies with a 32-bit nonce n_C generated by its internal Pseudo-Random Number Generator (PRNG). The reader replies with an encrypted nonce n_R and an answer a_R, which is generated by loading n_C into the PRNG and clocking it 64 times. For the encryption, the keystream generated by the Crypto1 cipher is used in groups ks_1, ks_2, ... of 32 bit each. After the card has sent the encrypted answer a_C, both parties are mutually authenticated. From that point onwards, the reader can read, write or modify blocks in the chosen sector. If another sector has to be accessed, the authentication procedure must be repeated with a slightly modified protocol.

Reader		**Card**
	$\text{AUTH} \,\|\|\, \text{sector} \longrightarrow$	
		$n_C \in_R \{0,1\}^{32}$
	$\longleftarrow n_C$	
$n_R \in_R \{0,1\}^{32}$ $a_R = PRNG(n_C, 64)$		
	$n_R \oplus ks_1 \,\|\|\, a_R \oplus ks_2 \longrightarrow$	
		$a_R \stackrel{?}{=} PRNG(n_C, 64)$
	$\longleftarrow a_C \oplus ks_3$	
$a_C \stackrel{?}{=} PRNG(n_C, 96)$		

Protocol 1. The Mifare Classic authentication protocol.

Security of Mifare Classic Since its invention, the internal structure of Crypto1 was kept secret and no open review process was performed. The cipher and its PRNG were later recovered by [17] using low-cost hardware reverse-engineering techniques. The authors

pointed out several design flaws, i.e., the short key length of 48 bit, mathematical weaknesses in the feedback functions of the LFSR, the weak 16-bit PRNG and the fact that the nonce generated by the PRNG depends on the time elapsed between power-up of the card and the authentication command. Subsequently, strong attacks on Mifare Classic were published: an attack described in [7] utilizes a fixed timing to generate the same nonces for repeated authentications and obtain parts of the keystream. A method to recover a secret sector key is proposed in [10], requiring two recorded genuine authentications to one sector. The most powerful attacks are card-only attacks as presented in [11] and [5]. They exploit amongst others the weakness that a card sends an encrypted NACK (`0x5`) each time the parity bits of the message $n_R \oplus ks_1 \,||\, a_R \oplus ks_2$ are correct but the decrypted a_R is not (cf. Protocol 1). This reveals four bits of keystream with a probability of $\frac{1}{256}$. Finally, a secret key of a Mifare Classic smartcard can be extracted within seconds using a combination of card-only attacks as proposed in [16], hence the cards can be considered fully broken.

3.2 Mifare DESFire and DESFire EV1

Mifare DESFire and Mifare DESFire EV1 cards are compliant to Parts 1-4 of ISO 14443A. Their UID is seven bytes long, and they support high baud rates of up to 848 kBit/s. A communication with the cards can be performed in plain, with an appended Message Authentication Code (MAC), or with full data encryption. Mifare DESFire cards offer 4 kByte of storage and data encryption by hardware DES and 3DES encryption. Mifare DESFire EV1 cards additionally provide AES-128 data encryption and are sold in three variants with 2 kByte, 4 kByte and 8 kByte of non-volatile memory, respectively. Each card holds up to 28 different applications with up to 14 different keys per application. For DESFire, each application may contain up to 16 files, while for DESFire EV1 the maximum number of files is 32. As in Mifare Classic cards, the UID is unchangeably programmed into the card at production time. Depending on the access rights for each application a mutual authentication protocol (see Protocol 2 / Protocol 3), ensuring that the symmetric key of the card K_C and of the reader K_R are identical, has to be completed before reading and manipulation of the data.

Reader		**Card**
	$\xrightarrow{\text{AUTH (02 0A 00)}}$	$n_C \in_R \{0,1\}^{64}$
$n_R \in_R \{0,1\}^{64}$ $b_1 = Dec_{K_R}(n_R)$ $r_0 = Dec_{K_R}(b_0)$ $r_1 = RotLeft_8(r_0)$	$\xleftarrow{b_0}$	$b_0 = Enc_{K_C}(n_C)$
$b_2 = Dec_{K_R}(r_1 \oplus b_1)$	$\xrightarrow{b_1, b_2}$	$r_2 = Enc_{K_C}(b_2)$ $n'_C = RotRight_8(r_2 \oplus b_1)$
	$\xleftarrow{\text{ERROR (02 AE)}}$	if $n'_C \neq n_C$ else if $n'_C = n_C$ $r_3 = Enc_{K_C}(b_1)$ $r_4 = RotRight_8(r_3)$
$r_5 = Dec_{K_R}(b_3)$ $n'_R = RotLeft_8(r_5)$ verify $n'_R \stackrel{?}{=} n_R$	$\xleftarrow{b_3}$	$b_3 = Enc_{K_C}(r_4)$

Protocol 2. The Mifare DESFire authentication protocol [4].

Previous to the authentication, an application represented by its Application Identifier (AID) is selected. The reader starts the authentication protocol [4] with an authenticate command together with the key number that is to be used during the authentication. Note that Mifare DESFire cards only perform (3)DES *en*cryptions $Enc_K(\cdot)$ employing the secret key K, hence, DESFire readers always have to use (3)DES *de*cryption $Dec_K(\cdot)$.

As illustrated in Protocol 2, a DESFire card responds to the authentication command with an encrypted 64-bit random nonce n_C. The reader likewise chooses a 64-bit random nonce n_R, decrypts the received n_C, rotates it eight bits to the left and decrypts n_R as well as the rotated n_C. The card verifies if the rotated value equals n_C after reverting the rotation. If so, the card encrypts the first value to obtain n_R, rotates it eight bits to the right and encrypts the result which is then sent to the reader. The rotated and encrypted nonce is verified by the reader and if this final step is successful, both parties are mutually authenticated.

We furthermore reverse-engineered the DESFire EV1 authentication protocol, as presented in Protocol 3, by eavesdropping on genuine protocol runs. We found that the protocol of Mifare DESFire EV1 cards using AES-128 diverges from Protocol 2 as follows. In Protocol 3, en- and decryption are used in the common sense, i.e., data that is to be sent is encrypted and data that was received has to be decrypted. The CBC mode is modified in a way that all en- or decryptions are chained, even though they operate on different cryptograms. The Initialization Vector (IV) is not reset when en- or decrypting a new message, but instead depends on the previous en- or decryption. The nonces are extended to a length of 128 bit to match the block size of AES-128 and the second rotation is executed in the opposite direction on both sides. Again, AES-128 en- and decryption involving the key K are denoted by $Enc_K(\cdot)$ and $Dec_K(\cdot)$, respectively. Apart from that, the protocol equals the authentication protocol of Mifare DESFire cards and thus mutually authenticates both parties on successful execution.

Reader		**Card**
	$\xrightarrow{\text{AUTH (02 0A 00)}}$	$n_C \in_R \{0,1\}^{128}$
	$\xleftarrow{b_0}$	$b_0 = Enc_{K_C}(n_C)$
$r_0 = Dec_{K_R}(b_0)$		
$r_1 = RotLeft_8(r_0)$		
$n_R \in_R \{0,1\}^{128}$		
$b_1 = Enc_{K_R}(n_R \oplus b_0)$		
$b_2 = Enc_{K_R}(r_1 \oplus b_1)$	$\xrightarrow{b_1, b_2}$	$r_2 = Dec_{K_C}(b_1)$
		$r_3 = Dec_{K_C}(b_2)$
		$n'_C = RotRight_8(r_3 \oplus b_1)$
	$\xleftarrow{\text{ERROR (02 AE)}}$	if $n'_C \neq n_C$
		else if $n'_C = n_C$
		$r_4 = RotLeft_8(r_2 \oplus b_0)$
	$\xleftarrow{b_3}$	$b_3 = Enc_{K_C}(r_4 \oplus b_2)$
$r_5 = Dec_{K_R}(b_3)$		
$n'_R = RotRight_8(r_5 \oplus b_2)$		
verify $n'_R \stackrel{?}{=} n_R$		

Protocol 3. The Mifare DESFire EV1 authentication protocol.

Security of Mifare DESFire / EV1 The non-invasive side-channel attacks on RFID devices presented in [15] allow to extract secret information from contactless cards by measuring the electromagnetic emanations of a card while it carries out a cryptographic operation. The

focus is on devices that make use of DES or 3DES and the first successful key-recovery attack on such devices is accomplished. In a discussion with the authors, we came to know that the attacks have been improved since and are applicable to Mifare DESFire cards. With about 1 000 000 measurements they are able to fully recover the 3DES key stored on a Mifare DESFire card. Note that their side-channel attack is currently *not* applicable to DESFire EV1, which has been certified according to Common Criteria EAL 4+. However, efficient attacks might come up in the future or the secret key could obtained by other means, e.g., by exploiting weaknesses of the backend system.

4 Software Implementations

In this section we detail on our software implementations for emulating several cards with Chameleon.

4.1 Mifare Classic Emulator

The attacks detailed in Sect. 3.1 imply that an adversary can easily read out the secret keys and all content of a Mifare Classic card. To produce a duplicate, the adversary can write all previously read data to a blank Mifare Classic card. This results in an almost perfect clone, differing from the original only in the single block containing the read-only UID of the blank card. If the UID is verified by a contactless system (compare with [16]), this type of card-cloning becomes useless in practice. To allow for perfect clones, we implemented the features of Mifare Classic on Chameleon. Thus, we have complete control of the content of every memory block, including the previously unchangeable manufacturer block.

Optimized Crypto1 A first approach to emulate a Mifare Classic card on an AVR ATmega32 microcontroller [22] revealed difficulties in complying to the timing requirements given in ISO 14443. After a command is issued by the reader, the card has to reply within 4.8 ms, or the reader will reach a timeout and abort the connection. Compiling the open-source Crypto1 C-library [6] for an 8-bit microcontroller results in inefficient code regarding the underlying platform. Hence, in [22] the time limit of 4.8 ms set in the protocol is exceeded with 11.7 ms for an 18-byte encryption, neglecting all other necessary computations, such as encoding the encrypted data. Since an 18-byte encryption is required every time when reading or writing a block with appended CRC checksum, the existing implementation is not suitable.

It became obvious that a significant speedup of Crypto1 is essential for a successful Mifare Classic emulation. Hence, we implemented the cipher from the scratch in AVR assembly. This allows to optimize the code for an 8-bit platform and make use of special commands that may not be considered by the C compiler. Using instructions to access bits of registers directly, the amount of clock cycles required for an encryption was reduced, amongst others by replacing inefficient shifting and masking operations to access single bits with instructions that allow accessing a particular bit in one clock cycle (e.g., SBRC, BST, BLD). We further implemented the non-linear filter functions f_a, f_b and f_c of Crypto1

with lookup tables to avoid time consuming boolean AND, OR and XOR operations. In the first stage, f_a is used two and f_b three times with a 4-bit input of the state LFSR. Their output is used to generate a 5-bit input to f_c, which in turn generates one bit of keystream. For both f_a and f_b, we created a dedicated lookup table that includes the respective shifting of the output. Thereby, the input of f_c can be easily obtained by ORing the five outputs of f_a and f_b. This speed advantage comes at the cost of storing one bit of information in one byte of memory. Finally, the lookup table f_c is a simple 5-bit input, 1-bit output table. The overall size of the lookup tables is 112 byte, formed by two 16-byte tables for f_a, three 16-byte

tables for f_b and one 32-byte table for f_c. With respect to the 192 kByte size of the program memory, the tables are negligibly small.

Furthermore, we applied the idea of precomputation. When the nonce n_C is fixed before the authentication protocol is executed, the card is able to precompute the corresponding answers a_R and a_C which saves time during the authentication process. Precomputation of keystream bits is not possible because of two reasons. Firstly, since the sector to be accessed by the reader cannot be predicted, it is not clear which key has to be loaded into the LFSR. Secondly, the random reader nonce n_R that only becomes known during the authentication process is an input to the cipher.

4.2 Mifare DESFire (EV1) Emulator

Similarly to the Mifare Classic implementation, we additionally implemented the authentication protocols of both Mifare DESFire and Mifare DESFire EV1, as given in Sect. 3.2. For encryption, Mifare DESFire cards use DES/3DES in CBC mode, whereas Mifare DESFire EV1 cards can use either DES/3DES or AES-128 in CBC-mode.

4.3 Practical Results

Before carrying out security analyses in the real-world, we thoroughly tested our emulators in our laboratory. The reliability and accurate timing behaviour of our emulator was successfully verified with different RFID readers, including an ACG passport reader and a Touchatag [23] reader. Further tests with real-world systems are described in Sect.5.

Mifare Classic With the optimized implementation of Crypto1 detailed in Sect. 4.1, we successfully emulated Mifare Classic 1K cards with varying content. Table 4.3 summarizes the execution times for the relevant operations which are now all well within the limits specified in ISO 14443. All features, e.g., authentication, encrypted read and write of blocks, or specifying an arbitrary UID, are fully functional with the used readers.

Command	Execution time	Explanation
setup_crypto1()	98 μs	Initializes the cipher
auth_crypto1()	542 μs	Keystream for the authentication
crypto1_1()	8.3 μs	Generates 1 bit of keystream
crypto1_8()	49 μs	Generates 8 bits of keystream
crypto1_32()	186 μs	Generates 32 bits of keystream

Table 1. Execution times of crucial Crypto1 functions.

Mifare DESFire (EV1) Likewise, we tested our DESFire (EV1) emulations from Sect. 4.2. Table 4.3 shows the execution times for the needed cryptographic functions using the hardware accelerators of the ATxmega. Note that the first call to an en-/decryption function involves some overhead for the initial setup. After that, subsequent blocks can be processed faster. For reference, we included the runtime both for a single block and for ten data blocks in Table 4.3.

According to [4], an original Mifare DESFire card answers 690 μs (9356 clock cycles at 13.56 MHz) after b_1,b_2 was received when Protocol 2 is executed. During this time, two 3DES

encryptions are performed (one encryption of two blocks and one encryption of a single block). Our implementation performs about three times faster than a genuine card, with 219 μs (5932 clock cycles at 27.12 MHz) to produce a valid answer b_3 after b_1,b_2 was received.

Command	Block count	Execution time
TripleDES_CBC_Enc()	1 block	14.1 μs
TripleDES_CBC_Enc()	10 blocks	85.1 μs
AES128_CBC_Enc()	1 block	35.9 μs
AES128_CBC_Enc()	10 blocks	270.2 μs
AES128_CBC_Dec()	1 block	58.4 μs
AES128_CBC_Dec()	10 blocks	304.9 μs

Table 2. Execution times of 3DES and AES-128 en-/decryption functions.

A genuine DESFire EV1 card replies with b_3 approx. 2.2 ms after having received b_1,b_2. In contrast, our implementation only consumes about 438 μs and is thus faster by a factor of five. As we are able to en-/decrypt faster than both DESFire cards, encrypting or MACing data which is the most critical part for Mifare Classic does not pose a problem in the context of emulating DESFire (EV1) cards. For both Mifare DESFire and Mifare DESFire EV1, our implementation performed successfully with the readers in our laboratory. As with the emulation of Mifare Classic cards, we are able to equip our emulator with a UID that is free of choice.

We conclude that the ATxmega microcontroller on our current hardware revision is powerful enough to handle the amount of computation that is needed for the emulation of the simple Mifare Classic cards and also for more sophisticated contactless smartcards using 3DES or AES.

5 Real-World Attacks

We successfully employed the Chameleon to bypass the security mechanisms of several real-world systems, for example, we utilized the Mifare Classic emulation to fake a card that is accepted by a widespread payment system. In the following, we summarize the characteristics of this system and then detail on the attacks carried out with our hardware.

5.1 A Vulnerable Contactless Payment System

For the identification of a customer of the payment system analyzed in [16], in addition to the UID each card contains a card number chosen by the system integrator. The credit balance is stored in plain in a value block on the card, without any extra security measures. The credit can be increased by means of cash or a credit card at charging terminals, while the cash registers are equipped with RFID readers to decrease the credit according to the balance due. The contactless cards furthermore allow to open doors and grant access to restricted areas.

The system can be easily spoofed, because all cards issued have identical secret keys. Hence, once the secret keys of one card have been recovered, the content of any card in the system can be read out or modified. The authors were able to carry out payments by copying the content of original payment cards to blank Mifare Classic cards. The so obtained cards are not exact clones, since the UIDs of the blank cards are different from that of the genuine

ones, as detailed in Sect. 4.1. Consequently, the fraud could be easily detected in the back-end by verifying the correctness of the UID of a card on each payment.

The authors of [16] mention that the existence of a device that can fully clone a card including the UID would allow for devastating attacks, but suppose that these devices, if available, will be very costly so buying and using them for micropayments would not be profitable. With our developed hardware, the presence of an arbitrary valid card, e.g., an exact clone including the UID, can be simulated with minimal effort and cost, as shown in the following.

5.2 Electronically Spoofing a Contactless Payment System

A powerful type of attack that can be conducted with the Chameleon is called state-restoration. Even if the credit value was stored encryptedly on the payment card, e.g., using AES with an individual key per card, the content can be simply reset to the original credit value by dumping the full content of the card before paying and reprogramming the card (respectively our card emulation device) with the previous content after the payment.

As a first step to conduct this attack, we extracted the secret keys using the methods described in Sect. 3.1. Then, we dumped the content of a genuine card, including the UID, and copied it to our emulation device, thereby creating an exact clone. Hiding the device in a wallet, we consequently were able to carry out contactless payments. The credit value was stored in the EEPROM of our emulator and is decreased according to the balance due. As a result, the remaining credit displayed to the cashier appears to be correct and our device was accepted as genuine. The Chameleon allows to recharge the balance to its original value by restoring the initial dump when the attacker presses a push button. Finally, unlimited payments could be carried out with our device. Our practical tests furthermore showed that the Chameleon allows to open doors when cloning a valid card of an employee. However, if the fraud occuring due to the state restoration attack would be detected on the long term, the card number and/or the UID could be blacklisted and blocked for future payments.

For a more powerful attack, we programmed the Chameleon to generate a new random UID and card number for each payment. In our practical tests with the payment system, our emulator now appeared like a new card every time. Again, we were able to carry out payments, but this time, the device cannot be blacklisted and blocked in the backend.

In a similar manner, we were able to spoof a copy-and-print service that relies on contactless smartcards. The printers and copy stations are equipped with RFID readers that decrease the credit stored on the Mifare Classic card according to the amount of copies or printings carried out. By repeatedly using the service and comparing the content of the card between the payments, we found the block in which the amount of remaining credit was stored, again without any encryption. We hence programmed our card emulator to simulate the original card such that the credit appears to be lowered on each payment. However, the previous state of the card, i.e., charged to a high credit value, can again be restored by pressing a button on our hardware. As a consequence, we gain an unlimited amount of copies with our hardware.

Since cards of other customers can be read out from a distance[2], the Chameleon can also be used to clone their cards in a real-world scenario. Reading out the relevant sectors takes less than 100 ms. Several cards of other customers can be stored in the Chameleon and hence payments can be carried out with cloned cards that already exist in the payment system. Note that the original card of the customer remains unmodified and thus still contains the original credit value. Accordingly, a financial damage will only occur for the payment institution, while the customer is not affected. Altogether, taking the above illustrated devastating attacks and its low cost into account, the Chameleon can clearly be profitable for a criminal.

[2] Modified RFID readers allow for reading distances up to 30 cm

6 Conclusion

We present a microcontroller-based, freely programmable emulator for ISO 14443 compliant RFIDs that allows to simulate various contactless smartcards at a very low cost. The device works autonomously, operated from a battery, and its card-sized antenna fits into slots of most readers for contactless smartcards. Due to its small dimensions, the emulator can be used covertly, e.g., hidden in the purse, and is well-suited for real-world attacks. Our hardware can be connected to a PC by means of a USB interface and the non-volatile memory of the microcontroller allows amongst others to monitor the communication with an RFID reader and store the acquired data in order to reverse-engineer unknown protocols.

We exposed the protocol of Mifare DESFire EV1 cards, implemented the (3)DES and AES block ciphers as required, and present the first successful emulation of Mifare DESFire and DESFire EV1 cards in the literature. The current software further includes the emulation of Mifare Classic cards, based on a highly optimized variant of the Crypto1 stream cipher. The firmware of our device is not limited to Mifare cards but can be adapted to support other contactless smartcards and their respective protocols, e.g., the electronic passport and cards from other manufacturers.

We tested the emulations with different RFID readers and show that our implementations of the ciphers and protocols meet the timing requirements of all protocols and that the performance in most cases is even faster than that of original cards. In all our tests, the emulator could not be distinguished from a genuine card. The device proved to be a valuable tool for the security analysis of contactless technology and can be used to practically identify security weaknesses of real-world RFID systems.

Since secret keys of Mifare Classic cards and Mifare DESFire cards can be extracted by means of mathematical cryptanalysis and side-channel analysis, respectively, our emulator poses a severe threat for many commercial applications, if it was used by a criminal. To demonstrate the capabilities of our findings we perform several real-world attacks, amongst others on a contactless payment system. We emulate exact clones (including the UID) of Mifare cards, successfully spoofed an access control system and carried out payments. Furthermore, we implemented a mode of operation in which our emulator appears as a new card with a new UID and new content on every payment, which hinders detection of fraud in the backend.

With contactless payment, ticketing and access control systems being omnipresent today, it is crucial to realize that only strong cryptography, together with sound protocol design and protection against implementation attacks can ensure long-term security. Bug-fixes for broken systems based on false assumptions on certain device characteristics, e.g., UID-based protection schemes for Mifare Classic, are a fatal design choice, as we demonstrate that exact cloning of cards is feasible at a very low cost.

References

1. Atmel. ATmega32 Data Sheet. `http://www.atmel.com/dyn/resources/prod_documents/doc2503.pdf`.
2. Atmel. ATxmega192A3 Data Sheet. `http://www.atmel.com/dyn/resources/prod_documents/doc8068.pdf`.
3. Atmel. AVR XMEGA A Manual. `http://www.atmel.com/dyn/resources/prod_documents/doc8077.pdf`.
4. D. Carluccio. Electromagnetic Side Channel Analysis for Embedded Crypto Devices. Diplomarbeit, Ruhr-University Bochum, March 2005.
5. N. Courtois. The Dark Side of Security by Obscurity and Cloning Mifare Classic Rail and Building Passes, Anywhere, Anytime. In *SECRYPT 2009*, pages 331–338. INSTICC Press.
6. Crapto1. Open Implementation of Crypto1. `http://code.google.com/p/crapto1`, 2008.

7. G. de Koning Gans, J. Hoepman, and F. Garcia. A Practical Attack on the MIFARE Classic. In *Smart Card Research and Advanced Applications 2008*, volume 5189 of *LNCS*, pages 267–282. Springer.
8. Federal Office for Information Security, Germany. Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control. `http://www.bsi.de/fachthem/epass/EACTR03110_v110.pdf`.
9. Future Technology Devices International Ltd.. FT245R Datasheet. `http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT245R.pdf`.
10. F. Garcia, G. de Koning Gans, R. Muijrers, P. Van Rossum, R. Verdult, R. Schreur, and B. Jacobs. Dismantling Mifare Classic. In *ESORICS 2008*, volume 5283 of *LNCS*, pages 97–114. Springer.
11. F. Garcia, P. van Rossum, R. Verdult, and R. Schreur. Wirelessly Pickpocketing a Mifare Classic Card. In *Symposium on Security and Privacy*, pages 3–15. IEEE, 2009.
12. IAIK Graz. HF Demo Tag. `http://www.iaik.tugraz.at/content/research/rfid/tag_emulators`.
13. ISO/IEC 14443-A. Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards - Part 1-4. `www.iso.ch`, 2001.
14. T. Kasper, D. Carluccio, and C. Paar. An Embedded System for Practical Security Analysis of Contactless Smartcards. In *WISTP 2007*, volume 4462 of *LNCS*, pages 150–160. Springer.
15. T. Kasper, D. Oswald, and C. Paar. EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment. In *WISA 2009*, volume 5932 of *LNCS*, pages 79–93. Springer.
16. T. Kasper, M. Silbermann, and C. Paar. All You Can Eat or Breaking a Real-World Contactless Payment System. In *Financial Cryptography 2010*, volume 6052 of *LNCS*, pages 343–350. Springer.
17. K. Nohl and D. Evans. Reverse-engineering a Cryptographic RFID Tag. In *USENIX Security Symposium*, pages 185–193, 2008.
18. NXP. About MIFARE. `http://mifare.net/about/`, 2001.
19. NXP. Mifare Classic 1K MF1 IC S50 Functional Specification. `www.nxp.com`, 2008.
20. OpenPICC. Programmable RFID-tag. `http://www.openpcd.org/openpicc.0.html`.
21. Proxmark III. A Radio Frequency IDentification Tool. `http://www.proxmark.org/`.
22. M. Silbermann. Security Analysis of Contactless Payment Systems in Practice. Diplomarbeit, Ruhr-University Bochum, November 2009.
23. Touchatag. Touchatag RFID Reader. `http://www.touchatag.com/`.
24. R. Verdult. Proof of Concept, Cloning the OV-Chip Card. `http://www.sos.cs.ru.nl/applications/rfid/2008-concept.pdf`.

A Authentication Protocols

This appendix provides the commands and the exact binary format for the authentication protocols used in this paper. Note that for DESFire (EV1), the message format according to ISO 14443A part 4 (including the 16-bit CRC) is taken into account in the following.

A.1 Mifare Classic Authentication Protocol

#	Direction	Protocol Message	Explanation
1	R $\rightarrow$ C	`60, sector (1 byte), CRC1 CRC2 (2 byte)`	Auth $\|\|$ sector $\|\|$ CRC
2	C $\rightarrow$ R	`4 byte`	n_C
3	R $\rightarrow$ C	`4 byte, 4 byte`	$n_R \oplus \mathrm{ks}_1 \,\|\|\, a_R \oplus \mathrm{ks}_2$
4	C $\rightarrow$ R	`4 byte`	$a_C \oplus \mathrm{ks}_3$

Table 3. Authentication protocol between a reader R and a Mifare Classic card C.

A.2 Mifare DESFire Authentication Protocol

#	Direction	Protocol Message	Explanation
1	R $\rightarrow$ C	`02 0A, key (1 byte), CRC1 CRC2`	Auth $\|\|$ key number $\|\|$ CRC
2	C $\rightarrow$ R	`02 AF, 8 byte, CRC1 CRC2`	Card nonce $\|\|$ b_0 $\|\|$ CRC
3	R $\rightarrow$ C	`03 AF, 8 byte, 8 byte, CRC1 CRC2`	Reader response $\|\|$ b_1 $\|\|$ b_2 $\|\|$ CRC
4	C $\rightarrow$ R	`03 00, 8 byte, CRC1 CRC2`	Success $\|\|$ b_3 $\|\|$ CRC

Table 4. Authentication protocol between a reader R and a Mifare DESFire card C.

A.3 Mifare DESFire EV1 Authentication Protocol

#	Direction	Protocol Message	Explanation
1	R $\rightarrow$ C	`02 AA, key (1 byte), CRC1 CRC2`	Auth $\|\|$ key number $\|\|$ CRC
2	C $\rightarrow$ R	`02 AF, 16 byte, CRC1 CRC2`	Card nonce $\|\|$ b_0 $\|\|$ CRC
3	R $\rightarrow$ C	`03 AF, 16 byte, 16 byte, CRC1 CRC2`	Reader response $\|\|$ b_1 $\|\|$ b_2 $\|\|$ CRC
4	C $\rightarrow$ R	`03 00, 16 byte, CRC1 CRC2`	Success $\|\|$ b_3 $\|\|$ CRC

Table 5. Authentication protocol between a reader R and a Mifare DESFire EV1 card C.

B Schematics

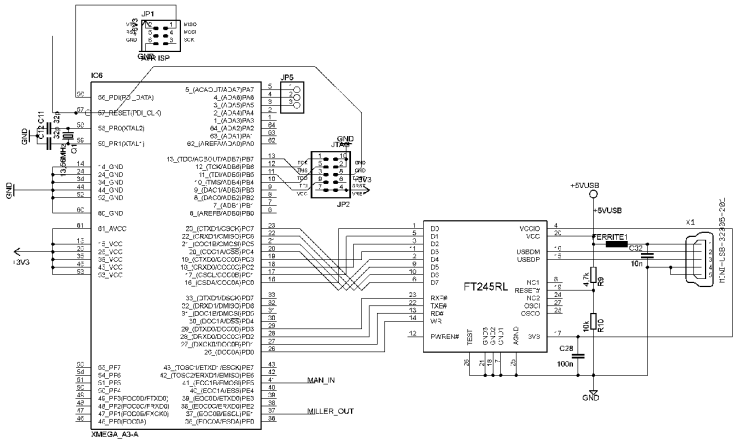


Fig. 3. Schematics of the microcontroller and the USB interface.

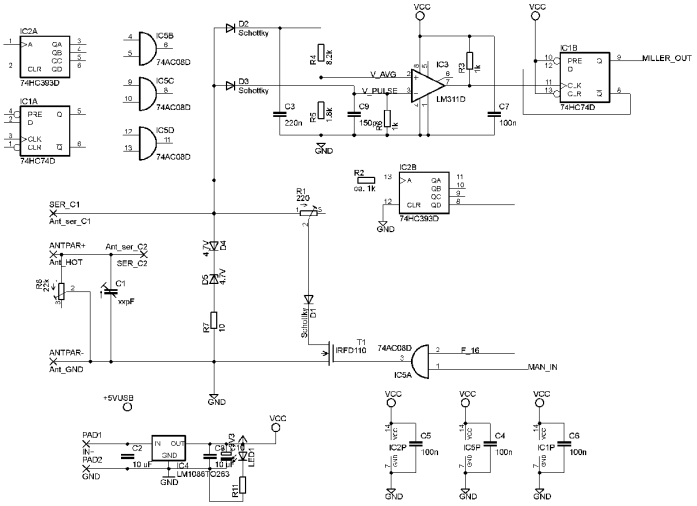


Fig. 4. Schematics of the power supply and the (de)modulation circuitry.

Chameleon: A Versatile Emulator for Contactless Smartcards

- **Creator:** Kasper, Timo ; von Maurich, Ingo ; Oswald, David ; Paar, Christof
- **Is Part Of:** Information Security and Cryptology - ICISC 2010, p.189-206
- **Subject:** RFID ; access control ; contactless smartcards ; efficient implementation ; payment systems
- **Description:** We develop a new, custom-built hardware for emulating contactless smartcards compliant to ISO 14443. The device is based on a modern low-cost microcontroller and can support basically all relevant (cryptographic) protocols used by contactless smartcards today, e.g., those based on AES or Triple-DES. As a proof of concept, we present a full emulation of Mifare Classic cards on the basis of our highly optimized implementation of the stream cipher Crypto1. The implementation enables the creation of exact clones of such cards, including the UID. We furthermore reverse-engineered the protocol of DESFire EV1 and realize the first emulation of DESFire and DESFire EV1 cards in the literature. We practically demonstrate the capabilities of our emulator by spoofing several real-world systems, e.g., creating a contactless payment card which allows an attacker to set the stored credit balance as desired and hence make an infinite amount of payments.
- **Identifier: ISSN:** 0302-9743; **ISBN:** 9783642242083; **ISBN:** 3642242081; **EISSN:** 1611-3349; **EISBN:** 9783642242090; **EISBN:** 364224209X; **DOI:** 10.1007/978-3-642-24209-0_13
- **Publisher:** Berlin, Heidelberg: Springer Berlin Heidelberg
- **Source:** Alma/SFX Local Collection

FPGA-Based Vehicular Channel Emulator for Real-Time Performance Evaluation of IEEE 802.11p Transceivers

- **Creator:** Fernández-Caramés, T M ; González-López, M ; Castedo, L
- **Is Part Of:** EURASIP journal on wireless communications and networking, 2010-12, Vol.2010 (1), p.1-18
- **Subject:** Engineering ; Communications Engineering, Networks ; Information Systems Applications (incl. Internet) ; Signal, Image and Speech Processing
- **Description:** IEEE 802.11p is one of the most promising future wireless standards due to the increasing demand of vehicular communication applications. At the time of writing, the document of the standard is in draft and much research is still required to study and improve the performance of transceivers in common vehicular scenarios. In this paper, we present a framework to evaluate the PHY layer of IEEE 802.11p systems in realistic situations. We detail the design and implementation of an FPGA-based real-time vehicular channel emulator. Contrarily to commercial emulators, ours is cheap, very flexible, and reconfigurable. We show its capabilities by evaluating performance in different high-speed scenarios. We also study the importance of coding and the benefits of using IEEE 802.11p instead of IEEE 802.11a in vehicular environments. Towards this aim, we developed a reference IEEE 802.11p PHY transceiver software model that can be taken as a convenient starting point for transceiver design.
- **Identifier: ISSN:** 1687-1499; **ISSN:** 1687-1472; **EISSN:** 1687-1499; **DOI:** 10.1155/2010/607467
- **Publisher:** Cham: Springer International Publishing
- **Source:** Engineering Source; Computers & Applied Sciences Complete; Applied Science & Technology Source; Academic Search Complete; Directory of Open Access Journals; Alma/SFX Local Collection; ProQuest Central

Emulator Express: A system for optimizing emulator performance for wireless networks

- **Creator:** Housel, B.C ; Shields, I
- **Is Part Of:** IBM systems journal, 2000-06-01, Vol.39 (2), p.384-402
- **Subject:** Emulators ; Usage ; Distributed processing ; Software ; Mobile communications networks ; Protocol

Samsung Ex. 1016, Page 673 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

- **Description:** IBM eNetwork Emulator Express is an IBM program product that optimizes the operation of Telnet 3270 and 5250 emulation over extremely low-bandwidth networks. These optimizations enable mobile workers using laptops, notebooks, or other mobile devices to access legacy host applications effectively over wide-area wireless networks as well as low-bandwidth wireline modem connections. How the Emulator Express system intercepts the data stream and optimizes it transparently to both the client emulator and the Telnet server is described. The optimizations include a new data stream caching technology, a new optimized protocol that reduces the number of Telnet negotiation flows, and traditional compression. The data stream caching technology is particularly significant because it may be applied to other distributed application domains. The results of several performance experiments are reported that illustrate the improvements in data transport volume and response time when using Emulator Express.
- **Identifier: ISSN:** 0018-8670; **DOI:** 10.1147/sj.392.0384; **CODEN:** IBMSA7
- **Publisher:** Armonk: IBM Corp
- **Source:** IEEE Conference Library Plus; IEEE Xplore IBM Journal of Research and Development; ProQuest Central; © ProQuest LLC All rights reserved

Emulation of mobile payment system

- **Creator:** Mohorko, J ; Chowdhury, A ; Planinsic, P
- **Is Part Of:** 2008 15th International Conference on Systems, Signals and Image Processing, 2008-06, p.21-24
- **Subject:** Load test ; Conferences ; Mobile communication ; Mobile handsets ; Servers ; Performance test ; Computer science ; Emulation ; Mobile payment system ; Region 8 ; Application ; Stress test ; Testing
- **Description:** Margento is a mobile payment system, enabling customers to purchase products from vending machines or in retail stores, using their mobile phones. It is designed to complement existing credit and debit card systems, by enabling all mobile phone users to turn their phones into the payment instruments of their choice. This system is based on Ultrapsilas patented mobile payment terminal using the one and only mature feature found with any of todaypsilas phones - voice. It is very important to ensure secure and stable operation of such a system, under various loading conditions. For these reasons, we designed the Margento emulator equipment as the tool, which enables functional testing, performance testing, load testing and stress testing, of the Margento system.
- **Identifier: ISSN:** 2157-8672; **ISBN:** 9788022728560; **ISBN:** 802272856X; **EISBN:** 8022728802; **EISBN:** 9788022728805; **DOI:** 10.1109/IWSSIP.2008.4604357
- **Publisher:** IEEE
- **Source:** IEEE Conference Library Plus; IEEE Electronic Library (IEL) Conference Proceedings; IEEE Electronic Library (IEL)

An Example of Course Project of Real Time Multitask Programming

- **Creator:** Yu, Jianxin ; Zhao, Yinggong ; Li, You ; Kuang, Hongyu
- **Is Part Of:** International Journal of Education and Management Engineering, 2012-08-29, Vol.2 (8), p.65-71
- **Subject:** Vending machines
- **Description:** This paper states a multi-task programming course project experiment item of real time operating system VxWorks. The project is an emulator of railway ticket vending machine. Its research background is Wuhan-Guangzhou high speed railway line ticket vending machine. The contents of the paper includes process flow, function design and analysis, data flow analysis, task division and definition, semaphore control application, test results, etc.
- **Identifier: ISSN:** 2305-3623; **EISSN:** 2305-8463; **DOI:** 10.5815/ijeme.2012.08.11
- **Publisher:** Hong Kong: Modern Education and Computer Science Press

Samsung Ex. 1016, Page 674 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

- **Source:** ProQuest Central; © ProQuest LLC All rights reserved

Bibliographic Data

Application No: 13/782,948

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /ISIDORA IMMANUEL/ (Examiner's Signature) | (Initials)

Title: Method and apparatus for emulating multiple cards in mobile devices

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
03/01/2013	705	3685	RFID-084
RULE			

APPLICANTS

RFCYBER CORPORATION, Fremont, CA, UNITED STATES

INVENTORS

Xiangzhen Xie, Shenzhen, CHINA

Liang Seng Koh, Fremont, CA, UNITED STATES

Hsin Pan, Fremont, CA, UNITED STATES

CONTINUING DATA

This application has PRO of 61606451 03/04/2012

This application is a CIP of 13350832 01/16/2012ABN

13350832 is a CIP of 11534653 09/24/2006 PAT 8118218

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/22/2013

**** SMALL ENTITY ****

STATE OR COUNTRY

CHINA

ADDRESS

LogicPatents, LLC

21701 Stevens Creek Boulevard, #284

CUPERTINO, CA 95015

UNITED STATES

FILING FEE RECEIVED

$533

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	((switch$4 or replac$4 or swap$5) with emulator with (application or card)) same (secure adj element)	US-PGPUB; USPAT	OR	OFF	2021/03/23 19:50
L2	1	1 AND ((G06Q20/322 OR G06Q20/352 OR G06Q20/3552 OR G06Q20/3572 OR G06Q20/3672).CPC.)	US-PGPUB; USPAT	OR	OFF	2021/03/23 19:52
S15	0	((counter or track$4) with emulator with (application or card)) same (secure adj element)	USPAT	OR	OFF	2021/03/23 18:34
S16	0	((counter or track$4) with emulator with (application or card)) same (secure adj element)	US-PGPUB; USPAT	OR	OFF	2021/03/23 18:34

3/23/2021 7:53:39 PM
C:\Users\iimmanuel\Documents\EAST\Workspaces\13782948.wsp

Immanuel, Isidora

From: Joe Zheng <joezheng88@sbcglobal.net>
Sent: Thursday, March 18, 2021 5:11 PM
To: Immanuel, Isidora
Subject: RE: 13/1782,948
Attachments: Clear version.docx

Importance: High

(informal discussion, please do not enter)

Ms. Examiner Immanuel:
Attached is a copy of the clear version, I modified "a lock or unlock status" to "a lock/unlock status" and other minor words.
Let me know if you have any questions.
Thanks
Joe

From: Joe Zheng [mailto:joezheng88@sbcglobal.net]
Sent: Monday, March 15, 2021 12:34 PM
To: 'Immanuel, Isidora'
Subject: RE: 13/1782,948

(informal discussion, please do not enter)

Ms. Examiner Immanuel:
Attached is a copy of the interview agenda for tomorrow.
It has the latest version of your proposed allowable claims sent on Aug. 17, 2020, I made some minor edits. Let us discuss them or further comments.
Thanks
Joe

From: Joe Zheng [mailto:joezheng88@sbcglobal.net]
Sent: Monday, March 8, 2021 11:43 PM
To: 'Immanuel, Isidora'
Subject: 13/1782,948

(informal discussion, please do not enter)

Hi Ms. Examiner Immanuel:
This is the last version I believe I sent to you. Please have a quick look before I follow your instruction Monday.
I will give you a call Tuesday.

Thanks
Joe

==========
Privacy and Confidentiality Notice: The information contained in this electronic mail message is intended for the named recipient(s) only. It may contain privileged and confidential information If you are not an intended recipient, you must not copy, forward, distribute, or take any action in reliance on it. If you have received this

electronic mail message in error, please notify the sender immediately.

LogicPatents, LLC
Tel: (408)777-8873
Fax: (408)677-5779
Email: uspatents@sbcglobal.net
Samples of the patents we prosecuted can be viewed from USPTO

To capitalize on your patents, visit:
www.LogicPatents.com
==========
Please consider the environment before printing this e-mail

Samsung Ex. 1016, Page 679 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

26797 7590 04/05/2021

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

Joe Zheng	(Typed or printed name)
/ joe zheng /	(Signature)
04/06/2021	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

TITLE OF INVENTION: Method and apparatus for emulating multiple cards in mobile devices

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	07/06/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
IMMANUEL, ISIDORA I	3685	705-050000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Joe Zheng
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

RFCyber Corp., Plano, Texas

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No.

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature / joe zheng / Date 04/06/2021

Typed or printed name Joe Zheng Registration No. 39,450

PTOL-85 Part B (08-18) Approved for use through 01/31/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Samsung Ex. 1016, Page 680 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Electronic Patent Application Fee Transmittal

Application Number:	13782948
Filing Date:	01-Mar-2013
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Filer:	Joe Zheng
Attorney Docket Number:	RFID-084

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	600	600

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt	
EFS ID:	42372935
Application Number:	13782948
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Method and apparatus for emulating multiple cards in mobile devices
First Named Inventor/Applicant Name:	Xiangzhen Xie
Customer Number:	26797
Filer:	Joe Zheng
Filer Authorized By:	
Attorney Docket Number:	RFID-084
Receipt Date:	06-APR-2021
Filing Date:	01-MAR-2013
Time Stamp:	03:41:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	E202146442152097
Deposit Account	502436
Authorized User	Joe Zheng
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	FeeTransmittal.pdf	323652 e07134316020271e28faddb989ecfb2dc5a485e8	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30505 c7d32a3d3e5b0b80f24406e3f54057e03bc58df2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	354157		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

Courtesy Reminder for
Application Serial No: 13/782,948

Attorney Docket No: RFID-084
Customer Number: 26797
Date of Electronic Notification: 04/05/2021

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
uspatents@sbcglobal.net

To view your correspondence online or update your email addresses, please visit us anytime at **https://ppair-my.uspto.gov/pair/PrivatePair.**
If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/782,948	03/01/2013	Xiangzhen Xie	RFID-084	5348

26797 7590 04/21/2021

LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
04/21/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@sbcglobal.net

Corrected ***Notice of Allowability***	**Application No.** 13/782,948	**Applicant(s)** Xie et al.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 04/07/2021.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are See Continuation Sheet . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

Continuation of 3. The allowed claim(s) is/are: 1, 3,-5, 9-12, 14, 17,and 18

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

STATUS OF THE APPLICATION

This action is in response to the claims filed 11/24/2020. Claims 2, 6-8, 13, 15, and 16 have been cancelled. Claims 1, 3, 4, 9-12, 14 and 17 are amended as a result of the interview conducted March 16, 2021 and a call March 25, 2021 to discuss final changes. Claims 1, 3-5, 9-12, 14, 17 and 18 are therefore pending and currently under consideration for patentability.

EXAMINER'S AMENDMENT

1. (*Currently amended*) A mobile device for emulating a plurality of cards, the mobile device comprising:
   a display screen showing a list of a plurality of applications for a user of the mobile device to select one therefrom, each application corresponding to one card in the plurality of cards;
   a secure element (SE) including:
   an emulator device;
   a memory storing a module, when the module is executed by the secure element, the secure element configured to:
   receive and install key sets of a Supplementary Secured Domain (SSD);
   establish, by the secure element based on the key sets, a secure communication channel with a dedicated server;
   receive and install an application from the dedicated server, each application including corresponding application data sets and a locked or unlocked status;

receive, from the plurality of applications, a user selection of a first application corresponding to a first card;

determine that the first application has a locked or unlocked status and is activated,

in response to said determining that the first application has an unlocked status and is activated, load the first application to the emulator device, along with corresponding first application data sets;

receive, from the plurality of applications, a user selection of a second application corresponding to a second card;

determine that the second application has a locked or unlocked status and is activated;

in response to said determining that the second application has an unlocked status and is activated, replace out of the emulator device, a portion of or in entirety, the first application, wherein said replacing out of the emulator device a portion of the first application further comprises retaining the portion of the corresponding first application data sets to be utilized by the second application;

load the second application to the emulator device along with corresponding second application data sets; and

increment a counter for each successful application replacement, wherein the mobile device performs functions of the second card when the first application is replaced out of the emulator device and the second application is loaded in the emulator device.

2. (*Cancelled*)

3. (*Currently amended*) The mobile device as recited in claim 1, wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

4. (*Currently amended*) The mobile device as recited in claim 3, wherein each of the applications emulating functions of one of the plurality of cards, performs a function related to a monetary transaction, the mobile device is used to emulate each of the cards when a corresponding application is loaded into and executed in the emulator device.

5. (*Previously amended*) The mobile device as recited in claim 4, wherein at least one of the cards is a contactless card.

6. (*Cancelled*)
7. (*Cancelled*)
8. (*Cancelled*)

9. (*Currently amended*) The mobile device as recited in claim 1, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information and updated subject to retrieved corresponding default ISD information from a party originating the secure element.

10. (*Currently amended*) The mobile device as recited in claim 1, wherein the mobile device is a smartphone or a portable computer.

11. (*Currently amended*) The mobile device as recited in claim 1, wherein each of the applications has been remotely provisioned by a corresponding dedicated server with operations of:

sending a request from the mobile device to the corresponding dedicated server to provision each of the applications installed in the mobile device, wherein the applications are distributed by an application provider;

receiving data for each of the applications being provisioned from the dedicated server, wherein the data includes the SSD to be associated with the each of the applications; and

notifying the application provider of a status of each of the applications with the mobile device.

12. (*Currently amended*) A method for a mobile device to emulate a plurality of cards, the method comprising:

displaying a list of a plurality of applications on a display of the mobile device for a user to select one therefrom, each application corresponding to one card in the plurality of cards;

receiving and installing, by a secure element on the mobile device, key sets of a Supplementary Secured Domain (SSD);

establishing, by the secure element and based on the key sets, a secure communication channel with a dedicated server;

receiving and installing, by the secure element, an application from the dedicated sever, each application including corresponding application data sets and a locked or unlocked status,

receiving, by the mobile device, a user selection of a first application corresponding to a first card;

determining, by the secure element, that the first application has a locked or unlocked status and is activated;

in response to said determining that the first application has an unlocked status and is activated, loading the first application to an emulator device in the secure element, along with corresponding first application data sets;

receiving, by the mobile device, from the plurality of applications, a user selection of a second application corresponding to a second card;

determining, by the secure element, that the second application has a locked or unlocked status and is activated;

in response to said determining that the second application has an unlocked status and is activated, replacing out of the emulator device, by the secure element, a portion of or in entirety, the first application, wherein said replacing out of the emulator device a portion of the first application further comprises retaining, in the

emulator device, the portion of the corresponding first application data sets to be utilized by the second application;

loading the second application to the emulator device along with corresponding second application data sets;

incrementing, by the secure element, a counter for each successful application replacement, wherein the mobile device performs functions of the second card when the first application is replaced out of the emulator device and the second application is loaded in the emulator device.

13. (*Cancelled*):

14. (*Currently amended*) The method as recited in claim 12~~13~~, wherein the secure element is enclosed in the mobile device or in a detachable card to the mobile device.

15. (*Cancelled*)

16. (*Cancelled*)

17. (*Currently amended*) The method as recited in claim 12~~13~~, wherein the secure element is preloaded with default Issuer Security Domain (ISD) information that is updatable subject to retrieved corresponding default ISD information from a party originating the secure element.

18. (*Previously amended*) The method as recited in claim 12, wherein the mobile device is a smartphone or a portable computer.

19. (*Cancelled*)

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:

Claims 1, 3-5, 9-12, 14, 17 and 18 are allowed. The closest prior art of record is Behren et al. (US 8646059), and in view of Corda et al. (US9128829).

Behren describes managing multiple payment card applications on a mobile device, along with the use of multiple secure elements. Corda teaches an emulating device that swaps out tickets. The combination of prior art do not teach the elements of independent claims 1 and 12. The recited emulator device, located in the secure element which includes a tracker for each application replacement, has the ability to retain data from the previous replaced application for use in the current or most recently loaded application. This combination of elements/function/limitations would not have been obvious to one of ordinary skill in the art in light of the available prior art at the time of the invention. Dependent claims 3-5, 9-11, 14, 17 and 18, are also allowable for the same reasons.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ISIDORA I IMMANUEL/
Examiner, Art Unit 3685

/NEHA PATEL/
Supervisory Patent Examiner, Art Unit 3685

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	**Art Unit**
	ISIDORA I IMMANUEL	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/01/2016	09/16/2016	09/17/2017	05/22/2018	04/15/2019	12/18/2019	08/17/2020	02/27/2021	03/23/2021
1	1	✓	✓	✓	✓	✓	✓	✓	✓	=
	2	✓	✓	✓	✓	✓	✓	✓	✓	-
2	3	✓	✓	✓	✓	✓	✓	✓	✓	=
3	4	✓	✓	✓	✓	✓	✓	✓	✓	=
4	5	✓	✓	✓	✓	✓	✓	✓	✓	=
	6	✓	✓	✓	✓	✓	✓	✓	✓	-
	7	✓	✓	✓	✓	✓	✓	✓	✓	-
	8	✓	✓	✓	✓	✓	✓	-	-	-
5	9	✓	✓	✓	✓	✓	✓	✓	✓	=
6	10	✓	✓	✓	✓	✓	✓	✓	✓	=
7	11	✓	✓	✓	✓	✓	✓	✓	✓	=
8	12	✓	✓	✓	✓	✓	✓	✓	✓	=
	13	✓	✓	✓	✓	✓	✓	✓	✓	-
9	14	✓	✓	✓	✓	✓	✓	✓	✓	=
	15	✓	✓	✓	✓	✓	✓	✓	✓	-
	16	✓	✓	✓	✓	✓	✓	✓	✓	-
10	17	✓	✓	✓	✓	✓	✓	✓	✓	=
11	18	✓	✓	✓	✓	✓	✓	✓	✓	=
	19	✓	✓	✓	✓	✓	✓	✓	✓	-

Samsung Ex. 1016, Page 696 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

CPC						
Symbol					Type	Version
H04B	/	5	/	0056	F	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06Q	/	30	/	0601	I	2013-01-01
G06Q	/	20	/	3672	I	2013-01-01
G06Q	/	20	/	3552	I	2013-01-01
G06Q	/	20	/	40	I	2013-01-01
G06Q	/	20	/	322	I	2013-01-01
G06Q	/	20	/	3278	I	2013-01-01
G06Q	/	20	/	3572	I	2013-01-01
G06Q	/	20	/	227	I	2013-01-01

CPC Combination Sets								
Symbol					Type	Set	Ranking	Version
	/		/					

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	16 April 2021	Total Claims Allowed:	
(Assistant Examiner)	(Date)	11	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685	17 April 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1A

U.S. Patent and Trademark Office — Part of Paper No.: 20210415

Samsung Ex. 1016, Page 697 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	**Art Unit**
	ISIDORA I IMMANUEL	3685

INTERNATIONAL CLASSIFICATION				
CLAIMED				
	/		/	
H04B5/00	/	5	/	00
G06Q30/06	/	30	/	06
G06Q20/36	/	20	/	36
G06Q20/40	/	20	/	40
G06Q20/32	/	20	/	32
G06Q20/22	/	20	/	22

NON-CLAIMED				
G06Q20/34	/	20	/	34

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
705	50

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	16 April 2021	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685	17 April 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1A

U.S. Patent and Trademark Office — Part of Paper No.: 20210415

Samsung Ex. 1016, Page 698 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/782,948	Xie et al.
	Examiner	Art Unit
	ISIDORA I IMMANUEL	3685

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	6	10		19										
	2	7	11												
2	3	8	12												
3	4		13												
4	5	9	14												
	6		15												
	7		16												
	8	10	17												
5	9	11	18												

/ISIDORA I IMMANUEL/ Examiner, Art Unit 3685	16 April 2021	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	11	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685	17 April 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1A

U.S. Patent and Trademark Office — Part of Paper No.: 20210415

Samsung Ex. 1016, Page 699 of 699
Samsung Electronics America, Inc. v. RFCyber Corp.
IPR2021-00980