a math coprocessor connected to said microcontroller core, said math coprocessor being for handling complex mathematics of encryption and decryption;

memory circuitry which can be programmed by a service provider to enable said microcontroller based secure transaction integrated circuit to perform predetermined functions on behalf of the service provider and for the benefit of an end user, said memory circuitry being connected to said microcontroller core; and

B1 cont.

an input/output circuit, connected to said microcontroller core, for exchanging information with a device external to said microcontroller based secure transaction integrated circuit, and for obtaining electrical energy to power at least a portion of said microcontroller based secure transaction integrated circuit.

~~33~~ 2. The microcontroller based secure transaction integrated circuit of claim ~~32~~ 1, further comprising a real time clock, connected to said microcontroller core, for providing a time measurement for time stamping a predetermined function.

Sub D2

~~34~~ 3. The microcontroller based secure transaction integrated circuit of claim ~~33~~ 2, wherein said predetermined function is an encrypted data transaction.

3 ~~4~~ ~~35~~. The microcontroller based secure transaction integrated circuit of claim ~~32~~ 1, further comprising an energy circuit connected to said memory circuitry.

4 ~~5~~ ~~36~~. The microcontroller based secure transaction integrated circuit of claim ~~35~~ 3 ~~4~~, wherein said memory circuitry is non-volatile RAM.

5 ~~6~~ ~~37~~. The microcontroller based secure transaction integrated circuit of claim ~~32~~ 2, wherein said microcontroller based secure transaction integrated circuit is programmed in a script programming language.

B12 cont

6 ~~7~~ ~~38~~. The microcontroller based secure transaction integrated circuit of claim ~~32~~ 1, wherein said microcontroller based secure transaction integrated circuit is incorporated into an articulatable item.

7 ~~8~~ ~~39~~. The microcontroller based secure transaction integrated circuit of claim 6 ~~7~~ ~~38~~, wherein said articulatable item is selected forma group comprising a ring, a bracelet, a credit card, a smart card, a necklace, an identification badge, a key fob, and a token shaped object.

8 ~~9~~ ~~40~~. The microcontroller based secure transaction integrated circuit of claim 1 ~~32~~, further comprising the ability to create encryption key pairs.

Sub D3

10 ~~41~~. A secure transaction integrated circuit comprising:

a microcontroller core;

a memory circuit, in communication with said microcontroller core, for storing a transaction program;

a modular exponentiation accelerator circuit, in communication with said microcontroller core, for performing encryption and decryption calculations; and

an input/output circuit, in communication with said microcontroller core, for receiving and transmitting data information with another electronic device.

B4 Cont'd

10 ~~11~~ ~~42~~. The secure transaction integrated circuit of claim 9 ~~40~~ ~~41~~, wherein said memory circuit is a nonvolatile RAM.

11 ~~12~~ ~~43~~. The secure transaction integrated circuit of claim 9 ~~10~~ ~~41~~, wherein said memory circuit can comprise a plurality of transaction groups wherein each said transaction group can comprise a transaction program created by a service provider.

12 ~~13~~ ~~44~~. The secure transaction integrated circuit of claim 9 ~~10~~ ~~41~~, further comprising an energy circuit connected at least to said memory circuit.

14 ~~45~~. The secure transaction integrated circuit of claim 10 ~~41~~, further comprising a real time clock circuit for measuring time and providing time stamp information when predetermined functions are performed by said microcontroller core.

13 ~~15~~ ~~46~~. The secure transaction integrated circuit of claim 9 ~~10~~ ~~41~~, wherein said input /output circuit is a bidirectional one-wire bus comprising a communication/power connection and a ground connection.

B1 CONT

47. The secure transaction integrated circuit of claim 41, wherein said transaction program can enable said secure transaction integrated circuit to perform digital cash transactions.

48 ~~42~~. The secure transaction integrated circuit of claim 41, wherein said secure transaction integrated circuit is further integrated into an articulatable item.

RULE 126 JEA

16 ~~49~~ ~~18~~ ~~48~~. The secure transaction integrated circuit of claim 15 ~~17~~ ~~51~~ ~~47~~, wherein said articulatable item is selected from a group comprising

RULE 126 JEA

B1 Cont'd

3 a ring, a bracelet, a wallet, a credit card, a smart card, a necklace, an identification card, a key fob, and a token shaped object.--

REMARKS

Reconsideration and allowance are respectfully requested in view of the foregoing amendments and the following remarks.

Claims 32-48 are pending in this application.

Claims 23-31 have been canceled without prejudice.

Regarding the Non-statutory Double Patenting Rejection

The present application has been rejected under the non-statutory double patenting rejection based on a judicially created doctrine grounded in public policy. Applicant will timely file a terminal disclaimer in compliance with 37 C.F.R. § 1.321(c) if it is deemed necessary after the Examiner has examined the now pending claims.

Regarding the 35 U.S.C. § 101 Double Patenting Rejection

Claim 23 was rejected under 35 U.S.C. § 101 for claiming the same invention as that of claim 1 of prior U.S. Patent No. 5,748,740. Applicant has canceled claims 23-31, thereby rendering this rejection moot. Applicant respectfully requests that the 35 U.S.C. § 101 double patenting rejection be withdrawn.

Regarding New Claims

Applicant has added new claims 32-48 which further claim novel aspects of the present invention. Applicant respectfully believes that these claims are ready for allowance.

In view of the above, it is believed that this application is in condition for allowance, and such a Notice is respectfully requested.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

Steven R. Greenfield
Reg. No. 38,166

Date: Nov 6 1998

Jenkens & Gilchrist,
A Professional Corporation
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
214/855-4789
214/855-4300 (fax)

B

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
09/041,190	03/10/98	CURRY	S	20661-45701

LM02/1216

STEVEN R GREENFIELD
JENKENS & GILCHRIST
3200 FOUNTAIN PLACE
1445 ROSS AVENUE
DALLAS TX 75202-2799

EXAMINER	
GREGORY, B	
ART UNIT	**PAPER NUMBER**
2766	6

DATE MAILED: 12/16/98

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

Commissioner of Patents and Trademarks

PTO-90C (Rev. 2/95)
*U.S. GPO 1996-437-638/80022

1- File Copy

Office Action Summary	Application No. 09/041,190	Applicant(s) **Stephen M. Curry et al.**		
	Examiner **Bernarr Earl Gregory**		Group Art Unit **2766**	

☒ Responsive to communication(s) filed on *9 Nov 1998*.

☐ This action is **FINAL.**

☒ 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.

A shortened statutory period for response to this action is set to expire *two (2)* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *32-47, 47, and 48* is/are pending in the application.

Of the above, claim(s) ________ is/are withdrawn from consideration.

☒ Claim(s) *32-47, 47, and 48* is/are allowed.

☐ Claim(s) ________ is/are rejected.

☐ Claim(s) ________ is/are objected to.

☐ Claims ________ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on ________ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on ________ is ☐approved ☐disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

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

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) ________.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ________.

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). ________

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

1. This application is in condition for allowance except for the following formal matters:

It appears that either there has been an error in claim numbering or that a claim has been omitted in the most-recent amendment. The present claim numbering goes 32, 33, 34, ..., 46, 47, 47, 48. That is to say, there are two claims numbered as claim 47. Appropriate correction is hereby required.

Prosecution on the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

A shortened statutory period for reply to this action is set to expire **TWO MONTHS** from the mailing date of this letter.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bernarr Gregory whose telephone number is (703) 306-4153.

Bernarr E. Gregory
Primary Examiner
Art Unit 2766

beg
December 15, 1998

#7 Amd C
Y.V.
1-20-99

Patent Application
Docket No. 20661-00457C1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:

Stephen Curry et al.	§	
	§	Examiner: Gregory, B.
Serial No.: 09/041,190	§	
	§	Group Art Unit: 2766
Filed: March 10, 1998	§	

For: Method, Apparatus, System and Firmware for Secure Transactions

BOX NON-FEE AMENDMENT
Assistant Commissioner For Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited postage paid with the United States Postal Service postage paid as first class mail in an envelope addressed to: Assistant Commissioner For Patents, Washington, D.C. 20231

on 1/8/99

Carol Mesostaller
Signature

Dear Sir:

AMENDMENT

Responsive to the Official Action mailed on December 16, 1998, reconsideration and allowance of the present application are respectfully requested and believed to be appropriate in view of the following amendments and remarks:

In the Claims:

Please cancel both claims 47, and 47 without prejudice.

Please add the following new claims:

Rule 126 BER

-- 14 ~~50~~ ~~49~~. The secure transaction integrated circuit of claim ~~41~~ ~~70~~ 9, wherein said transaction program can enable said secure transaction integrated circuit to perform digital cash transactions.

C1

RULE 126 8E7 G1 Cont'd

15. ~~17~~ ~~51~~ ~~52~~. The secure transaction integrated circuit of claim 9 ~~10~~ ~~41~~, wherein said secure transaction integrated circuit is further integrated into an articulatable item.--

REMARKS

Reconsideration and allowance are respectfully requested in view of the foregoing amendments and the following remarks.

Claims 32-46 and 48-50 are pending in this application.

Applicant appreciates the Examiner's indication that all the claims in this application are allowable except for a minor formal matter of claim numbering. Applicant further appreciates the Examiner pointing out that two pending claims have both been numbered '47'.

To remedy the problem applicant has canceled both of the claims numbered '47' and inserted two identical claims that are numbered 49 and 50. It is believed that appropriate correction has been made and the formal matter has been remedied. Applicant respectfully submits that this application is ready for allowance.

In view of the above amendments and remarks, reconsideration and allowance of this application is believed to be warranted, and a Notice to such effect is earnestly solicited.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

R. Greenfield

Steven R. Greenfield
Reg. No. 38,166

Date: JAN 8, 1999

Jenkens & Gilchrist,
A Professional Corporation
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
214/855-4789
214/855-4300 (fax)

GP 2766

Patent Application
Docket No. 20661-00457C1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:

STEPHEN M. CURRY ET AL.		§	
		§	Examiner: GREGORY, B.
Serial No.:	09/041,190	§	
		§	Group Art Unit: 2766
Filed:	March 10, 1998	§	

For: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

Assistant Commissioner
for Patents
Washington, D.C. 20231

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231
on 1/8/99
Signature

Dear Sir:

AMENDMENT TRANSMITTAL LETTER

This is an amendment in the above-identified application and includes the transmitted herewith attachments of the same date and subject which are incorporated hereunto by reference. The signature below is to be treated as the signature to the attachments in absence of a signature thereto.

Transmitted herewith in the above-identified application are:

1) Amendment in response to the Office Action dated 12/16/98

2) Acknowledgment Postcard.

______ Small entity status of this application under 37 CFR 1.9 and 1.27 has been established by a verified statement previously submitted.

______ A verified statement claiming small entity status under 37 CFR 1.9 and 1.27 is enclosed.

__X___ No additional fee is required.

FEE REQUIREMENTS FOR CLAIMS AS AMENDED

		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST # PREVIOUSLY PAID FOR		PRESENT EXTRA	SMALL ENTITY RATE			LARGE ENTITY RATE		
1.	TOTAL CLAIMS	18	-	22 (at least 20)	=	0 (at least 0)	x11	=	OR	x22	=	$ 0
2.	INDEP. CLAIMS	2	-	3 (at least 3)	=	0 (at least 0)	x41	=	OR	x82	=	$ 0
3.	FIRST PR SENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a reissue appln)						+130	=	OR	+260	=	$ 0

4. TOTAL FEE FOR ADDED CLAIMS $ 0

5. ______ IDS ATTACHED REQUIRES OFFICIAL FEE - ADD $230 (RULE 1.97(c)) OR $130 (RULE 1.97(d) PETITION) $______

6. ______ IF TERMINAL DISCLAIMER attached add Rule 20(d) Official Fee $55 (Small Entity) $110 (Large Entity) $______

7. ______ **Petition is hereby made** under 37 CFR 1.136(a) to extend the original due date to cover the date this response is filed for which the requisite fee is attached:

	Small Entity	Large Entity
One Month	______ $ 55	____$ 110
Two Months	______ $200	____$ 400
Three Months	______ $475	____$ 950
Four Months	______ $755	____$1,510

ADDITIONAL FEE FOR EXTENDED RESPONSE $______

Applicant has not been notified that the requested extension will not be permitted. The present application is not involved in an interference declared pursuant to 37 CFR 1.611.

8. **TOTAL FEES** $______

9. ______ A check in the amount of $ .00 is attached. Please charge any deficiency or credit any overpayment to Jenkens & Gilchrist Deposit Account No. 10-0447.

10. ______ Please charge Jenkens & Gilchrist Deposit Account No. 10-0447 in the amount of $______ This sheet is attached in duplicate.

CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and may be required under 37 CFR 1.16-1.18 (missing or insufficiencies only) now or hereafter relative to this application and for the resulting Official Document under 37 CFR 1.20, OR credit any overpayment to **Jenkens & Gilchrist Deposit Account No. 10-0447** for which purpose a duplicate copy of this sheet is attached.*

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal form is filed.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

By: Steven R. Greenfield
Steven R. Greenfield
Reg. No. 38,166

Date: Jan 8, 1999

Jenkens & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue

*In the event that Dallas Semiconductor Corporation Deposit Account No. 04-0031 cannot be charged hereby to cover the TOTAL FEE, please charge the TOTAL FEE to our Deposit Account No. 10-0447

Notice of Allowability	Application No. **09/041,190**	Applicant(s) **Stephen M. Curry et al.**
	Examiner **Bernarr Earl Gregory**	Group Art Unit **2766**

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 and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to *Amendment C of 11 January 1999*.

☒ The allowed claim(s) is/are *32-46 and 49-51*.

□ The drawings filed on __________ are acceptable.

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) __________.

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: __________.

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE THREE MONTHS FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

□ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☒ Applicant MUST submit NEW FORMAL DRAWINGS

☒ because the originally filed drawings were declared by applicant to be informal.

□ including changes required by the Notice of Draftsperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. ____.

□ including changes required by the proposed drawing correction filed on __________, which has been approved by the examiner.

□ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal lettter addressed to the Official Draftsperson.

□ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

□ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ________

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

□ Interview Summary, PTO-413

□ Examiner's Amendment/Comment

□ Examiner's Comment Regarding Requirement for Deposit of Biological Material

□ Examiner's Statement of Reasons for Allowance

TEL.1(703)306-4153

BERNARR EARL GREGORY
PRIMARY EXAMINER
ART UNIT 2766

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

LM41/0125

STEVEN R GREENFIELD
JENKENS & GILCHRIST
3200 FOUNTAIN PLACE
1445 ROSS AVENUE
DALLAS TX 75202-2799

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
09/041,190	03/10/98	018	GREGORY, B	2766	01/25/99
First Named Applicant	CURRY,		35 USC 154(b) term ext. =	0 Days.	

TITLE OF INVENTION METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEEDUE	DATE DUE
2 20661-45701	380-025.000	024	UTILITY	NO	$1210.00	04/26/99

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.

THE ISSUE FEE 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.

HOW TO RESPOND TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the Patent and Trademark Office of the change in status, or

B. If the status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay FEE DUE shown above, or

B. File verified statement of Small Entity Status before, or with, payment of 1/2 the FEE DUE shown above.

II. Part B-Issue Fee Transmittal should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B Issue Fee Transmittal should be completed and returned. If you are charging the ISSUE FEE to your deposit account, section "4b" of Part B-Issue Fee Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give application number and batch number.
Please direct all communications prior to issuance to Box ISSUE FEE unless advised to the contrary.

***IMPORTANT REMINDER:** Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.*

PATENT AND TRADEMARK OFFICE COPY

PART B—ISSUE FEE TRANSMITTAL

Co[illegible] this form, together with applicable fees, to:

Box ISSUE FEE
Assistant Commissioner for Patents
Washington, D.C. 20231

LL

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE. Blocks 1 ugh 4 should be completed where appropriate. All further correspondence including the Issue Fee ceipt, the Patent, advance orders and notification of maintenance fees will be mailed to the current respondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) ecifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

Note: The certificate of mailing below can only be used for domestic mailings of the Issue Fee 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.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

Certificate of Mailing

I hereby certify that this Issue Fee Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Box Issue Fee address above on the date indicated below.

Susan Mitchell (Depositor's name)

Susan Mitchell (Signature)

April 16, 1999 (Date)

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED

First Named Applicant

TITLE OF INVENTION

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363). Use of PTO form(s) and Customer Numbers are recommended, but not required.

□ 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) attached.

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 JENKENS and GILCHRIST

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. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE DALLAS SEMICONDUCTOR CORPORATION

(B) RESIDENCE: (CITY & STATE OR COUNTRY) DALLAS, TX

Please check the appropriate assignee category indicated below (will not be printed on the patent)

□ individual ☒ corporation or other private group entity □ government

4a. The following fees are enclosed (make check payable to Commissioner of Patents and Trademarks):

☒ Issue Fee

☒ Advance Order - # of Copies 10

4b. The following fees or deficiency in these fees should be charged to:

DEPOSIT ACCOUNT NUMBER 10-0447
(ENCLOSE AN EXTRA COPY OF THIS FORM)

☒ Issue Fee

☒ Advance Order - # of Copies 10

The COMMISSIONER OF PATENTS AND TRADEMARKS IS requested to apply the Issue Fee to the application identified above.

(Authorized Signature) (Date) Apr. 15, 1999

NOTE: The Issue Fee will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the Patent and Trademark Office.

```
04/20/1999 ZABDALL1 00000050 09041190

01 FC:142                    1210.00 OP
02 FC:561                      30.00 OP
```

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending on the needs of the individual case. Any comments on the amount of time required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ODRESS. SEND FEES AND THIS FORM TO: Box Issue Fee, Assistant Commissioner for ents, Washington D.C. 20231

er the Paperwork Reduction Act of 1995, no persons are required to respond to a collection ormation unless it displays a valid OMB control number.

TRANSMIT THIS FORM WITH FEE

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

#19

Steven R. Greenfield
Jenkens & Gilchrist
3200 Fountain Place
1445 Ross Avenue
Dallas, TX 75202-2799

In re Application of
Stephen M. Curry
SERIAL NO.: 09/041,190
FILED: March 10, 1998
FOR: Apparatus, System and Frimware
for Secure Transactions

: Withdrawal From Issue

The above-identified application is withdrawn from issue after payment of the issue fee due to unpatentability of one or more claims. See 37 CFR 1.313(b)(3).

The above-identified application is hereby withdrawn from issue.

The issue fee is refundable upon written request. If, however, the application is again found allowable, the issue fee can be applied toward payment of the issue fee in the amount identified on the new Notice of Allowance and Issue Fee Due upon written request. This request and any balance due must be received on or before the due date noted in the new Notice of Allowance in order to prevent abandonment of the application.

Telephone inquiries should be directed to Thomas H. Tarcza at (703) 306-4171.

The above-identified application is being forwarded to the examiner for prompt appropriate action, including notifying applicant of the new status of this application.

John F Terapane

John F. Terapane
Director, Technology Center 3600

AH

UNITED STAT DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
09/041,190	03/10/98	CURRY	S	20661-457C1

PM82/0723

STEVEN R GREENFIELD
JENKENS & GILCHRIST
3200 FOUNTAIN PLACE
1445 ROSS AVENUE
DALLAS TX 75202-2799

EXAMINER	
GREGORY, B	
ART UNIT	**PAPER NUMBER**
3662	

DATE MAILED: 07/23/99

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

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 09/041,190	Applicant(s) Stephen M. Curry et al.
	Examiner Bernarr Earl Gregory	Group Art Unit 3662

☒ Responsive to communication(s) filed on *11 Jan 1999* .

□ This action is **FINAL.**

□ 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.

A shortened statutory period for response to this action is set to expire *three (3)* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *32-46 and 49-51* is/are pending in the application.

Of the above, claim(s) ________ is/are withdrawn from consideration.

□ Claim(s) ________ is/are allowed.

☒ Claim(s) *32, 35-39, 41-44, 46, and 49-51* is/are rejected.

☒ Claim(s) *33, 34, 40, and 45* is/are objected to.

□ Claims ________ are subject to restriction or election requirement.

Application Papers

□ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

□ The drawing(s) filed on ________ is/are objected to by the Examiner.

□ The proposed drawing correction, filed on ________ is □approved □disapproved.

□ The specification is objected to by the Examiner.

□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) ________ .

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ________ .

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

□ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ________

□ Interview Summary, PTO-413

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

--- ***SEE OFFICE ACTION ON THE FOLLOWING PAGES*** ---

1. As was indicated in the Letter mailed 25 June 1999 from the Director of Technology Center 3600, prosecution of the instant application is being reopened.

2. The following is a quotation of the appropriate paragraphs of 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.

3. Claims 32, 35, 36-39, 41-44, 46, and 49-51 are rejected under 35 U.S.C. 102(b) as being anticipated by Hirokawa (EPO Publication 0458306 A2).

Claim 41 is taken as an exemplary claim for the purposes of this rejection. Please note the discussion of drawing figures 8 and 9 at column 6, lines 30-47 of Hirokawa (EPO Publication 0458306 A2). The claim 41 "secure transaction integrated circuit" is shown in Figure 9 of Hirokawa (EPO Publication 0458306 A2). Item 31 of Figure 9 of Hirokawa (EPO Publication 0458306 A2) corresponds to the "microcontroller core" of claim 41 of the instant application. Item 33 of Figure 9 corresponds to the claim 41 "memory circuit." Item 32 of Figure 9 corresponds to the claim 41 "modular exponentiation acceleration circuit." And, item 36 of Figure 9 corresponds to the claim 41 "input/output circuit." Item 21 in Figure 6 of Hirokawa (EPO Publication 0458306 A2) corresponds to the claim 41 "another electronic device." Please see column 6, lines 11-24 of Hirokawa (EPO Publication 0458306 A2) concerning Figure 6 of Hirokawa (EPO Publication 0458306 A2). Please also note column 1, line 56 through column 2, line 35 of Hirokawa (EPO Publication 0458306 A2).

4. Claims 32, 35, 36-39, 41-44, 46, and 49-51 are rejected under 35 U.S.C. 102(b) as being anticipated by SGS-Thomson Microelectronics publication ST16xF74 (dated 10/93).

The Figure 1 block diagram in SGS-Thomson Microelectronics publication ST16xF74 (dated 10/93) is very similar to the chip in Hirokawa (EPO Publication 0458306 A2) and similarly shows all of the claimed elements.

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 32, 35, 36-39, 41-44, 46, and 49-51 are rejected under the judicially created doctrine of double patenting over claims 1-13 of U. S. Patent No. 5,748,740 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as explained below.

In accordance with a recent modification of USPTO policy relative to this kind of rejection, in addition to *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968), support for the aforementioned types of question of patentability or rejection is to be provided in a matter similar to the equity-based reasoning employed in *In re Berg*, 140 F.3d 1428, 46 USPQ 2d 1226 (Fed. Cir. 1998).

Initially it should be noted that the present application is a voluntarily filed continuation application of patent application 08/594,983 (U.S. Patent 5,748,740) both having the same inventive entity and the same priority date of 29 September 1995. The disclosures relating to the claims in question in both the application and patents are identical.

A comparison chart is given to compare claim 41 of the instant application to claim 1 of U.S. Patent 5,748,740.

****

Patent Claim 1	**Instant Application Claim 41**
An electronic data carrier used for secure transactions comprising:	A secure transaction integrated circuit comprising:
input/output circuitry for communicating to a data processing circuit;	an input/output circuit, in communication, with said microcontroller core; for receiving and transmitting data information with another electronic device
math coprocessor circuitry electrically connected to said	A modular exponentiation accelerator circuit, in

Patent Claim 1	**Instant Application Claim 41**
input/output circuitry where said math coprocessor performs encryption calculations;	communication with said microcontroller core, for performing encryption and decryption calculations; and
microprocessor circuitry electrically connected to said input/output circuitry; and	a microcontroller core;
memory circuitry electrically connected to said microprocessor circuitry, said electronic data carrier providing secure, encrypted data transfers between said electronic data carrier and said data processing circuit.	A memory circuit, in communication with said microcontroller core, for storing a transaction program,

****

These claims read on the same disclosed embodiment in the Patent and in the instant application. For example, the math coprocessor is defined in the disclosure as being a high speed modular exponentiation accelerator ("the module 10 preferably contains a general-purpose, 8051-compatible micro controller 12 or a reasonably similar product, a continuously running real-time clock 14, a high-speed modular exponentiation accelerator for large integers (math coprocessor) 18 ..."). The electronic data carrier used for secure transactions is the disclosed secure transaction integrated circuit. The microcontroller 12 is labelled as the microprocessor in Figure 1 of the Patent and application.

Both claim 41 of the instant application and claim 1 of the Patent contain "comprising" language as in *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968) and both claim the same disclosed embodiment. This open-ended language covers all the elements of the disclosed embodiment and as such extends the patent protection. The claim comparison above shows the overlapping coverage of both the patent and the instant application.

It is clear that applicant has voluntarily exercised a choice to provide different claims drafted with varying degrees of overlapping scope to the same embodiment in both the instant application and the Patent. The grant of an extension of the right to exclude the public from making and/or using the invention for longer than the statutory life of the Patent can not be justified. Thus, in accordance with the principle of equity as applied in *In re Berg*, 140 F.3d 1428, 46 USPQ 2d 1226 (Fed. Cir. 1998), this rejection is fully supported.

U.S. Patent 5,748,740 was filed on January 31, 1996 (as application 08/594,983) and issued on May 5, 1998. Under the rules of GATT and NAFTA for implementation of the 20-year term effective June 8, 1995, the term of the aforenoted U.S. patent ends January 31, 2016. Similarly, subject to payment of the appropriate fees, the instant application, which makes a specific reference in the specification to the aforenoted application 08/594,983 under 35 USC 120, if issued, is entitled to a term that ends January 31, 2016. Therefore, patent protection rights cannot be timewise extended by issuance of the instant application even without a properly drafted terminal disclaimer in this case. However, in lieu of the cancellation of claims 32, 35, 36-39, 41-44, 46, and 49-51 or abandonment of the instant application, applicants **must** overcome this question of patentability by submission of a paper that at least addresses the "enforceability/common ownership" provision of a terminal disclaimer referred to in 37 CFR 1.321(c)(3).

Portions of MPEP 804 discuss *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968) as used in double patenting rejections.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bernarr Gregory whose telephone number is (703) 603-1787. The Art Unit FAX number is (703) 306-4195.

Bernarr E. Gregory
Primary Examiner
Art Unit 3662

beg

July 19, 1999

Dep & Ref Rm 307

PATENT APPLICATION
Attorney Docket No. 20661-00457 C1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

11/Refn
Refund
(Entd)

In re Application of: STEPHEN M. CURRY

Serial No.: 09/041,190 Filed: 03/10/1998

Examiner: B. Gregory Group No.: 2766

For: METHOD, APPARATUS, SYSTEM AND FIRMWARE
FOR SECURE TRANSACTIONS

To The Assistant Commissioner
For Patents
Washington, D.C. 20231

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner For Patents, Washington, D.C. 20231

on 16 July 1999

Signature P Gudzlik

REQUEST FOR REFUND OF ISSUE FEE

Dear Sir:

Attached is a copy of the correspondence received from the Patent and Trademark Office advising of the Withdrawal from Issuance regarding the above-referenced application. Also attached is a copy of the Issue Fee check. As instructed, applicant respectfully requests that the full amount of the issue fee be refunded.

Respectfully submitted,

W Stacy

Wayne O. Stacy
Reg. No. P-45,125

Jenkens & Gilchrist, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
214/855-4120

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

MAILED

JUN 25 1999

Office of the Director
Group 3600

Steven R. Greenfield
Jenkens & Gilchrist
3200 Fountain Place
1445 Ross Avenue
Dallas, TX 75202-2799

20661-457C1

In re Application of
Stephen M. Curry
SERIAL NO.: 09/041,190
FILED: March 10, 1998
FOR: Apparatus, System and Frimware
for Secure Transactions

: : : Withdrawal From Issue

The above-identified application is withdrawn from issue after payment of the issue fee due to unpatentability of one or more claims. See 37 CFR 1.313(b)(3).

The above-identified application is hereby withdrawn from issue.

The issue fee is refundable upon written request. If, however, the application is again found allowable, the issue fee can be applied toward payment of the issue fee in the amount identified on the new Notice of Allowance and Issue Fee Due upon written request. This request and any balance due must be received on or before the due date noted in the new Notice of Allowance in order to prevent abandonment of the application.

Telephone inquiries should be directed to Thomas H. Tarcza at (703) 306-4171.

The above-identified application is being forwarded to the examiner for prompt appropriate action, including notifying applicant of the new status of this application.

John F. Terapane

John F. Terapane
Director, Technology Center 3600

* DOCKETED
Int: NH DT: 6-30-99
Action Complete Date: 6.25
Comm.

AH

NO.

DATE	INVOICE	DESCRIPTION	AMOUNT
04-15-99	20661.457/GRNFLD	ISSUE FEE	1.240.00
		TOTAL	1.240.00

JENKENS & GILCHRIST
A PROFESSIONAL CORPORATION
1445 ROSS AVE., SUITE 3200
DALLAS, TEXAS 75202-2711

Chase Bank of Texas, N.A.
San Angelo

112631

88-88
1113

CHECK DATE	CHECK AMOUNT
04/15/99	$*****1,240.00

PAY ONE THOUSAND TWO HUNDRED FORTY AND 00/100 Dollars

TO
THE
ORDER
OF

COMMISSIONER OF PATENTS &
TRADEMARKS

TWO SIGNATURES REQUIRED OVER $10,000
VOID AFTER 180 DAYS

⑈112631⑈ ⑆111300880⑆ ⑈0630004432⑈

12
D

PATENT
Docket No.20661-457C1

Cofer
10-28-99

UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	§			
	§	Examiner:	3662	
Stephen M. Curry, et al.	§			
	§			
Serial No.: 09/041,190	§	Group No.:	B. Gregory	
	§			
Filed: March 10, 1998	§			

For: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS.

Assistant Commissioner
for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No: EI269319222US
Date of Deposit: October 25, 1999
I hereby certify that this paper or fee is being deposited with the U S Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Trademarks, Washington, D.C 20231
Type or Print Name: DELLA GONZALES
Della L. Gonzales
Signature

AMENDMENT

Dear Sir:

Responsive to the Official Action mailed on July 23, 1999, the time reconsideration and allowance of the present application are respectfully requested and believed to be appropriate in view of the following remarks and amendments.

In the Claims:

1 ~~32~~. (Amended) A microcontroller based secure transaction integrated circuit comprising:

a microcontroller core;

a math coprocessor connected to said microcontroller core, said math coprocessor being for handling complex mathematics of encryption and decryption;

memory circuitry which can be programmed by a service provider to enable said microcontroller based secure transaction integrated circuit to perform predetermined functions on behalf of the service provider and for the benefit of an end user, said memory circuitry being connected to said microcontroller core; [and]

an input/output circuit, connected to said microcontroller core, for exchanging information with a device external to said microcontroller based secure transaction integrated circuit[, and for obtaining electrical energy to power at least a portion of said microcontroller based secure transaction integrated circuit.]; and

a real time clock, connected to said microcontroller core, for providing a time measurement for time stamping a predetermined function.

2 ~~34~~. (Amended) The microcontroller based secure transaction integrated circuit of claim [33] ~~32~~ 1, wherein said predetermined function is an encrypted data transaction.

9 ~~41~~. (Amended) A secure transaction integrated circuit comprising:

a microcontroller core;

a memory circuit, in communication with said microcontroller core, for storing a transaction program;

a modular exponentiation accelerator circuit, in communication with said microcontroller core, for performing encryption and decryption calculations; [and]

an input/output circuit, in communication with said microcontroller core, for receiving and transmitting data information with another electronic device[.]; and

a clock circuit for measuring time and providing time stamp information responsive to functions being performed by said microcontroller core.

REMARKS

Reconsideration and allowance are respectfully requested in view of the foregoing amendments and the following remarks.

Claims 32, 34-44, 46 and 48-50 are presented for examination.

Claims 33 and 45 are canceled.

Regarding the Allowable Subject Matter

Claims 33, 34, 40 and 45 are indicated as containing allowable subject matter. Applicants thank the Examiner for the early indication of allowability.

Claims 33 and 45 are canceled, (subject to possible filing in a continuation), and portions of the subject matter of those claims are incorporated into their respective independent claims. Accordingly, Applicants respectfully submit that independent claim 32 and independent claim 41 are now distinguishable over the applied art, whether taken individually or in combination. Applicants, therefore, respectfully request that the Examiner reconsider and withdraw the rejection against claims 32 and 41 and all claims dependent therefrom.

Regarding the Non-Statutory Double Patenting Rejection

Claims 32, 35, 36-39, 41-44, 46 and 49-51 are rejected under the judicially created doctrine of double patenting over claims 1-13 of U.S. Patent 5,748,740. Regarding claim 32, it has been amended to incorporate subject matter recited in claim 33. Because claim 33 is not subject to the applied double patenting rejection. Applicants respectfully submit that claim 32, which now incorporates portions of claim 33, also is not subject to the double patenting rejection. Applicants, therefore, respectfully request that the Examiner reconsider and withdraw the rejection against claim 32 and the claims dependent therefrom.

Similarly, claim 41 now incorporates portions of the subject matter of claim 45, which was not subject to the double patenting rejection. Accordingly, Applicants submit that claim 41, as amended, should not be rejected under the doctrine of double patenting because it incorporates the subject matter of claim 45. Applicants, therefore, respectfully request that the Examiner reconsider and withdraw the double patenting rejection against claim 41 and the claims dependent therefrom.

Conclusion

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance, and an indication of the same is courteously solicited.

Respectfully submitted,

By: Stacy
Wayne O. Stacy
Reg. No. P-45,125

JENKENS & GILCHRIST, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
(214) 855-4160
(214) 855-4300 (Fax)

GP3662

PATENT APPLICATION
DOCKET NO.:20661-457CI

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	§		
	§	Examiner:	B. Gregory
Stephen M. Curry, et al.	§		
	§		
Serial No.: 09/041,190	§		
	§	Group Art Unit:	3662
Filing Date: 3/10/98	§		

For: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

To the Assistant Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No.: EL269319222US
Date of Deposit: October 25, 1999
I hereby certify that this paper or fee is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Trademarks, Washington, D.C. 20231

Type or Print Name: DELLA GONZALES
Della L. Gonzales
Signature

AMENDMENT TRANSMITTAL LETTER

Dear Sir:

This is a response in the above-identified application and includes the transmitted herewith attachments of the same date and subject which are incorporated hereunto by reference. The signature below is to be treated as the signature to the attachments in absence of a signature thereto.

Transmitted herewith in the above-identified application are:

1) Amendment Transmittal Letter (in duplicate);
2) Amendment to Office Action mailed on July 23, 1999; and
3) Acknowledgment Postcard

___ Small entity status of this application under 37 CFR 1.9 and 1.27 has been established by a verified statement previously submitted.

___ A verified statement claiming small entity status under 37 CFR 1.9 and 1.27 is enclosed.

_X_ No additional fee is required.

___ The Fee for entering the attached Amendment is calculated below:

	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST # PREVIOUSLY PAID FOR		PRESENT EXTRA	SMALL ENTITY RATE			LARGE ENTITY RATE		
TOTAL CLAIMS	16	-	22 (at least 20)	=	0 (at least 0)	x9	=	OR	x18	=	$0.00
INDEP. CLAIMS	2	-	3 (at least 3)	=	0 (at least 0)	x39	=	OR	x78	=	$0.00
FIRST PRESENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a reissue appln)						+130	=	OR	+260	=	$___

FEE FOR CLAIM AMENDMENTS $0.00

___ IDS ATTACHED REQUIRES OFFICIAL FEE - ADD $230 (RULE 1.97(c)) PETITION) $___

___ Assignment Recordation Fee ($40) $___

___ IF TERMINAL DISCLAIMER attached add Rule 20(d) Official Fee $55 (Small Entity) $110 (Large Entity) $___

___ Petition is hereby made under 37 CFR 1.136(a) to extend the original due date to cover the date this response is filed for which the requisite fee is attached:

	Small Entity	Large Entity
One Month	___ $ 55	___ $110
Two Months	___ $190	___ $380
Three Months	___ $435	___ $870
Four Months	___ $680	___ $1360

ADDITIONAL FEE FOR EXTENDED RESPONSE $0.00

Applicant has not been notified that the requested extension will not be permitted. The present application is not involved in an interference declared pursuant to 37 CFR 1.611.

TOTAL FEES $0.00

___ A check in the amount of $_____ to cover the TOTAL FEE is attached. Please charge any deficiency or credit any overpayment to Deposit Account No. 10-0447.

____ Please charge my Deposit Account No. 10-0447 in the amount of $____ to cover the TOTAL FEE. This sheet is attached in duplicate.

CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and may be required under 37 CFR 1.16-1.18 (missing or insufficiencies only) now or hereafter relative to this application and for the resulting Official Document under 37 CFR 1.20, OR credit any overpayment to our Deposit Account No. 10-0447, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal form is filed.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

By: ____________
Wayne O. Stacy
Registration No. P45,125

JENKENS & GILCHRIST, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202
Tel: (214) 855-4120
Fax: 214/855-4300

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address : COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	A ORNEY DO KET NO.
09/041,190	03/10/98	CURRY S	20661-457C1

PM82/1101

STEVEN R GREENFIELD
JENKENS & GILCHRIST
3200 FOUNTAIN PLACE
1445 ROSS AVENUE
DALLAS TX 75202-2799

EXAMINER	
GREGORY, B	
ART UNIT	PAPER NUMBER
3662	13

DATE MAILED: 11/01/99

This is a communication from the examiner in charge of your application.

COMMISSIONER OF PATENTS AND TRADEMARKS

1. ☒ The communication filed 25 OCT 199 is informal/non-responsive for the reason(s) checked below and should be corrected. APPLICANT IS GIVEN ONE MONTH FROM THE DATE OF THIS LETTER OR UNTIL THE EXPIRATION OF THE PERIOD FOR RESPONSE SET IN THE LAST OFFICE ACTION (WHICHEVER IS LONGER) WITHIN WHICH TO CORRECT THE INFORMALITY.

   a. □ The amendment to claim(s) ______________________, filed ______________, fails to comply with the provisions of 37 C.F.R. 1.121 and is accordingly held to be non-responsive. A supplemental paper correcting the informal portions and complying with the rule is required.

   b. □ The paper is unsigned. A duplicate paper or ratification, properly signed, is required.

   c. □ The paper is signed by ______________________________, who is not of record. A ratification or a new power of attorney with a ratification, or a duplicate paper signed by a person of record, is required.

   d. □ The communication is presented on paper which will not provide a permanent copy. A permanent copy, or a request that a permanent copy be made by the Office at applicant's expense, is required, see M.P.E.P. 714.07.

   e. ☒ Other APPLICANTS HAVE GIVEN NO CLEAR INSTRUCTIONS TO CANCEL CLAIMS 33 AND 45. CORRECTION IS HEREBY REQUIRED.

2. □ In accordance with applicant's request, THE PERIOD FOR RESPONSE FROM THE OFFICE ACTION DATED ______________ IS EXTENDED TO RUN ______________ MONTH(S).
   No further extension will be granted unless approved by the Commissioner. 37 C.F.R. 1.136 (b)

3. □ Receipt is acknowledged of papers submitted under 35 U.S.C. 119 which papers have been made of record in the file.

4. □ Other

Bernarr E. Gregory
BERNARR E. GREGORY
PRIMARY EXAMINER
A.U. 3662

TEL.: (703) 306-5765

PTOL-327 (rev. 10-79)

NOTICE TO APPLICANT

[illegible] 3662

Patent Application
Docket No. 20661-457C1

#14/E
11/26/99

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Stephen M. Curry, et al.

Serial No.: 09/041,190) Examiner: B. Gregory

Filed: March 10, 1998) Group Art Unit: 3662

For: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

Box NON-FEE AMENDMENT
Assistant Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited postage paid with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231

on November 18, 1999

Della L. Gonzales
Signature

Dear Sir:

AMENDMENT

Responsive to the Office Action dated November 1, 1999, please amend the above-identified application for patent as follows:

IN THE CLAIMS

Please cancel claims 33 and 45 without prejudice.

REMARKS

Reconsideration and allowance of the present application are respectfully requested in view of the foregoing amendments.

Claims 33 and 45 are corrected as required by the Examiner.

CONCLUSION

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance, and an indication of the same is courteously solicited.

Respectfully submitted,

JENKENS & GILCHRIST,
A Professional Corporation

Wayne O. Stacy
Reg. No. 45,125

1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
(214) 855-4120
(214) 855-4300 (fax)

PATENT APPLICATION
DOCKET NO.: 20661-457

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	§	
Stephen M. Curry, et al.	§	
	§	
Serial No.: 09/041,190	§	Group No.: 3662
	§	
Filed: March 10, 1998	§	Examiner: B. Gregory

For: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

Box NON-FEE AMENDMENT
Assistant Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING

I hereby certify that this paper or fee is being deposited with the U.S. Postal Service as first class mail on the date indicated below and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Date November 18, 1999

Della L. Grouzelle
Signature

AMENDMENT TRANSMITTAL LETTER

Dear Sir:

This is a response/amendment/letter in the above-identified application and includes the transmitted herewith attachment(s) of the same date and subject which is/are incorporated hereunto by reference. The signature below is to be treated as the signature to the attachment(s) in absence of a signature thereto.

Transmitted herewith in the above-identified application is/are:

1) Amendment Transmittal Letter (in duplicate);
2) Amendment Responsive to November 11, 1999 Office Action; and
3) Acknowledgment Postcard.

____ Small entity status of this application under 37 CFR 1.9 and 1.27 has been established by a verified statement previously submitted.

____ A verified statement claiming small entity status under 37 CFR 1.9 and 1.27 is enclosed.

_X_ No additional fee is required.

____ The Fee for entering the attached Amendment is calculated below:

	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST # PREVIOUSLY PAID FOR		PRESENT EXTRA	SMALL ENTITY RATE			LARGE ENTITY RATE		
TOTAL CLAIMS	16	-	22 (at least 20)	=	____ (at least 0)	x9	=	OR	x18	=	$0.00
INDEP. CLAIMS	2	-	3 (at least 3)	=	____ (at least 0)	x39	=	OR	x78	=	$0.00
FIRST PRESENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a reissue appln)						+130	=	OR	+260	=	$0.00

FEE FOR CLAIM AMENDMENTS $0.00

____ IDS ATTACHED REQUIRES OFFICIAL FEE - ADD $240 (RULE 1.97(c)) PETITION) $____

____ Assignment Recordation Fee ($40) $____

____ IF TERMINAL DISCLAIMER attached add Rule 20(d) Official Fee $55 (Small Entity) $110 (Large Entity) $____

____ Petition is hereby made under 37 CFR 1.136(a) to extend the original due date to cover the date this response is filed for which the requisite fee is attached:

	Small Entity	Large Entity
One Month	____ $ 55	____ $110
Two Months	____ $190	____ $380
Three Months	____ $435	____ $870
Four Months	____ $680	____ $1360

ADDITIONAL FEE FOR EXTENDED RESPONSE $____

Applicant has not been notified that the requested extension will not be permitted. The present application is not involved in an interference declared pursuant to 37 CFR 1.611.

TOTAL FEES $0.00

____ A check in the amount of $____ to cover the TOTAL FEE is attached. Please charge any deficiency or credit any overpayment to Deposit Account No. 10-0447.

PATENT APPLICATION
DOCKET NO.: 20661-457CI

____ Please charge my Deposit Account No. 10-0447 in the amount of $____ to cover the TOTAL FEE. This sheet is attached in duplicate.

CHARGE STATEMENT: If these papers are not considered timely filed by the Patent and Trademark Office, then a petition is hereby made under 37 C.F.R. §1.136. The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and may be required under 37 CFR 1.16-1.18 (missing or insufficiencies only) now or hereafter relative to this application and for the resulting Official Document under 37 CFR 1.20, OR credit any overpayment to our Deposit Account No. 10-0447, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal form is filed.

Respectfully submitted,

JENKENS & GILCHRIST,
A Professional Corporation

By:
Wayne O. Stacy
Registration No.45,125

1445 Ross Avenue; Suite 3200
Dallas, Texas 75202-2799
Tel: 214/855-4120
Fax: 214/855-4300

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/041,190	03/10/98	CURRY	S 20661-457

FM92/0112

STEVEN R GREENFIELD
JENKENS & GILCHRIST
3200 FOUNTAIN PLACE
1445 ROSS AVENUE
DALLAS TX 75202-2799

EXAMINER	
GREGORY, B	
ART UNIT	PAPER NUMBER
3662	15

DATE MAILED: 01/12/00

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

Commissioner of Patents and Trademarks

Notic~~-~~ Allowability	Application No. 09/041,190	Applicant(s) Stephen M. Curry et al.	
	Examiner Bernarr Earl Gregory		Group Art Unit 3662

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 and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to *Amendment E of 22 November 1999*.

☒ The allowed claim(s) is/are *32, 34-44, 46, and 49-51*.

□ The drawings filed on __________ are acceptable.

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) __________.

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: __________.

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE THREE MONTHS FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

□ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☒ Applicant MUST submit NEW FORMAL DRAWINGS

☒ because the originally filed drawings were declared by applicant to be informal.

□ including changes required by the Notice of Draftsperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. ____.

□ including changes required by the proposed drawing correction filed on __________, which has been approved by the examiner.

□ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal lettter addressed to the Official Draftsperson.

□ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

□ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ______

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

□ Interview Summary, PTO-413

□ Examiner's Amendment/Comment

□ Examiner's Comment Regarding Requirement for Deposit of Biological Material

□ Examiner's Statement of Reasons for Allowance

TEL.:(703) 306-5765

Bernarr Earl Gregory

BERNARR EARL GREGORY
PRIMARY EXAMINER
ART UNIT 3662

UNITED STATE ~~~~PARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

PM92/0412

STEVEN R GREENFIELD
JENKENS & GILCHRIST
3200 FOUNTAIN PLACE
1445 ROSS AVENUE
DALLAS TX 75202-2799

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
09/041,190	03/10/98	016	GREGORY, B	3662	03/12/00

First Named Applicant CURRY,

35 USC 154(b) term ext. = 0 Days.

TITLE OF INVENTION METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
27661-45761	705-065.000	G77	UTILITY	NO	$1210.00	04/12/00

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.

THE ISSUE FEE 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.

HOW TO RESPOND TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the Patent and Trademark Office of the change in status, or

B. If the status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay FEE DUE shown above, or

B. File verified statement of Small Entity Status before, or with, payment of 1/2 the FEE DUE shown above.

II. Part B-Issue Fee Transmittal should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B Issue Fee Transmittal should be completed and returned. If you are charging the ISSUE FEE to your deposit account, section "4b" of Part B-Issue Fee Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give application number and batch number. Please direct all communications prior to issuance to Box ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: ***Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.***

PATENT AND TRADEMARK OFFICE COPY

PART B—ISSUE FEE TRANSMITTAL

Complete and mail this form, together with app... ...ble fees, to:

Box ISSUE FEE
Assistant Commissioner for Patents
Washington, D.C. 20231

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE. Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Issue Fee Receipt, 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: Legibly mark-up with any corrections or use Block 1)

PM92/0112

STEVEN R GREENFIELD
JENKENS & GILCHRIST
3200 FOUNTAIN PLACE
1445 ROSS AVENUE
DALLAS TX 75202-2799

Note: The certificate of mailing below can only be used for domestic mailings of the Issue Fee 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.

Certificate of Mailing

I hereby certify that this Issue Fee Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Box Issue Fee address above on the date indicated below.

Christy Wilson (Depositor's name)
Christy Wilson (Signature)
April 11, 2000 (Date)

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
09/041,190	03/10/98	016	GREGORY, B	3662	01/12/00

First Named Applicant: CURRY

35 USC 154(b) term ext. = 0 Days.

TITLE OF INVENTION: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
20661-457C1	705-065.000	G77	UTILITY	NO	$1210.00	04/12/00

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363). Use of PTO form(s) and Customer Number are recommended, but not required.

□ 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) attached.

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 Jenkens & Gilchrist, a Professional Corporation
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. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE Dallas Semiconductor Corporation

(B) RESIDENCE: (CITY & STATE OR COUNTRY) Dallas, TX

Please check the appropriate assignee category indicated below (will not be printed on the patent)

□ individual ☒ corporation or other private group entity □ government

4a. The following fees are enclosed (make check payable to Commissioner of Patents and Trademarks):

☒ Issue Fee
☒ Advance Order - # of Copies 10

4b. The following fees or deficiency in these fees should be charged to:

EPOSIT ACCOU TNUMBER ______
(ENCLOSE AN EXTRA COPY OF THIS FORM)

□ Issue Fee
□ Advance Order - # of Copies ______

The COMMISSIONER OF PATENTS AND TRADEMARKS IS requested to apply the Issue Fee to the application identified above.

(Authorized Signature) (Date) 4/11/00

NOTE; The Issue Fee will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the Patent and Trademark Office.

04/17/2000 KZEND IE1 00000021 09041190

01 FC:142 1210.00 OP
02 FC:561 30.00 OP

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending on the needs of the individual case. Any comments on the amount of time required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND FEES AND THIS FORM TO: Box Issue Fee, Assistant Commissioner for Patents, Washington D.C. 20231

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.

TRANSMIT THIS FORM WITH FEE

k

B/18

Jenkens & Gilchrist
A PR●FESSIONAL C●RP●RATION

1445 R●ss Avenue
Suite 320●
●allas, Texas 75202

(214) 855-4500
Telecopier (214) 855-430●

www.jenkens.com

Austin, Texas
(512) 499-3800

Houston, Texas
(713) 951-33●●

Los Angeles, California
(310) 820-88●●

San Ant●nio, Texas
(210) 246-5●●●

Washingt●n, ● C
(202) 326-15●0

Affiliate Office

Chicago, Illin●is
(312) 425-390●

Wayne● Stacy
(214) 855-4120
wstacy●jenkens.com

Box ISSUE FEE
Assistant Commissioner for Patents
Washington, D.C. 20231

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231

on April 11, 2000

Christy Wilson
Signature

Re:	Applicant(s):	Curry, et al.
	Serial No.:	09/041,19●
	Filed:	March 10, 1998
	Batch No.	G77
	NOA Mailed:	January 12, 2000
	For:	METHOD, APPARATUS, SYSTEM AND FIRMWARE F●R SECURE TRANSACTIONS
	D●cket No.:	206●1-00457C1

●ear Sir:

Transmitted for filing with the U.S. Patent and Trademark Office are the following documents for the above-referenced patent application:

1. Part B Issue Fee Transmittal
2. Letter to Official Draftsperson
3. 8 Sheets ●f F●rmal Drawings
4. Check in the amount of $1,240 00 for issue fee and soft copies
5. Acknowledgment Postcard

Please address all communications related to this to:

Roger L. Maxwell
Jenkens & Gilchrist, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799

In the event there is an under or over payment, please debit or credit our Deposit Acc●unt #10-0447.

Respectfully submitted,

W Stacy

Wayne O. Stacy
Registration No.45,125

LL

#17

LOC 7206

2-22-99

D●CKET NO.: 20661-457C1 **PATENT APPLICATION**

Issue Batch No.: S16/O24
Date of Not'ie
of Allowance : January 25, 1999
Serial No. : 09/041,190

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: Stephen M. Curry, *et al.*

Serial No.: 09/041,190 Group No.: 2766

Filed: March 10, 1998 Examiner: Gregory, B.

For: **Method, Apparatus, System and Firmware for Secure Transacti'ons**

Box Issue Fee
Assistant Commissioner
for Patents
Washington DC 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL
"EXPRESS MAIL" Mailing Label No._ EL274277998US
Date of Deposit: April 16 1999
I hereby certify that this paper or fee is being deposited with the U.S. Postal Service "Express Mall Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Applicat'ion, Washington, D.C. 20231
Type or Print Name: SUSAN MITCHELL
Susan E. Mitchell
Signature

ATTN: Official Draftsperson

Sir:

TRANSMITTAL LETTER TO OFFICIAL DRAFTSPERSON

Enclosed please find 8 sheet(s) of formal drawings relating to the above-identified patent application.

The enclosed drawings each bear the Issue Batch No., the date of the Notice of Allowance and Serial No. of the application on their reverse side.

In view of the above, the present applicati'on is believed to be in a condition ready for issuance.

Steven R. Greenfield
Steven R. Greenfield
Registration No. 38,166

Jenkens & Gilchrist, a Professional Corporation
1445 Ross Avenue, Ste. 3200
Dallas, Texas 75202-2799
214/855-4789
214/855-4300 FAX

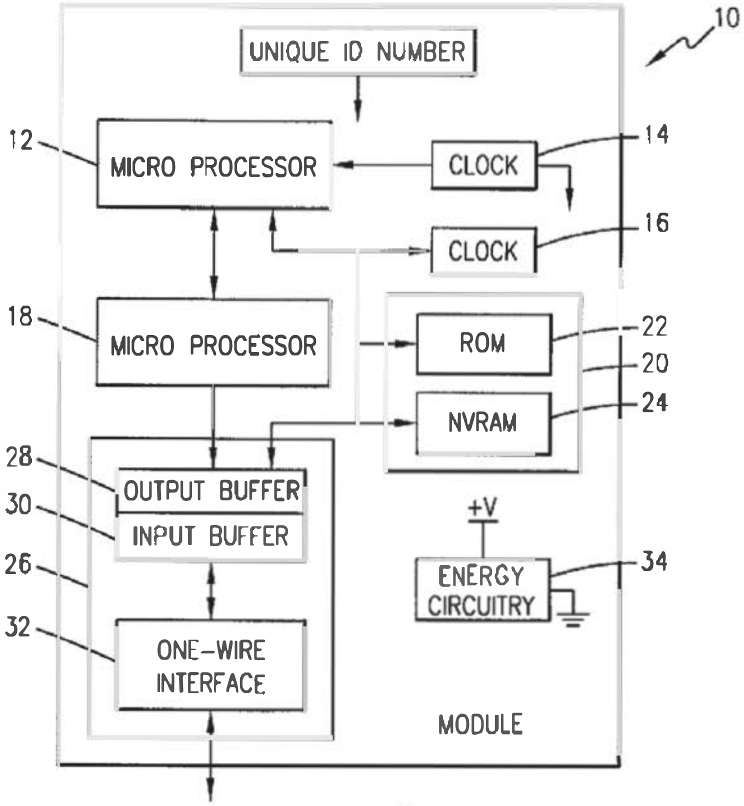

10
UNIQUE ID NUMBER
12
MICRO PROCESSOR
CLOCK
14
CLOCK
16
18
MICRO PROCESSOR
ROM
22
20
NVRAM
24
28
OUTPUT BUFFER
30
INPUT BUFFER
26
+V
ENERGY CIRCUITRY
34
32
ONE-WIRE INTERFACE
MODULE

FIG. 1

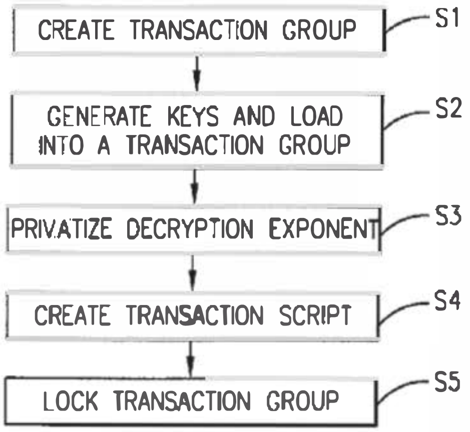

CREATE TRANSACTION GROUP
S1
GENERATE KEYS AND LOAD INTO A TRANSACTION GROUP
S2
PRIVATIZE DECRYPTION EXPONENT
S3
CREATE TRANSACTION SCRIPT
S4
LOCK TRANSACTION GROUP
S5

FIG. 2

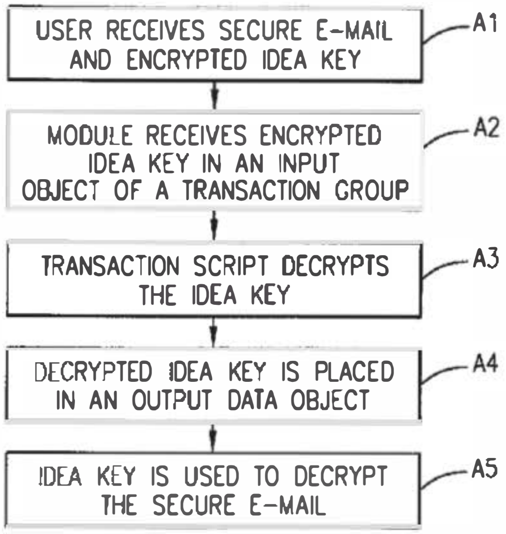

USER RECEIVES SECURE E-MAIL AND ENCRYPTED IDEA KEY
A1
MODULE RECEIVES ENCRYPTED IDEA KEY IN AN INPUT OBJECT OF A TRANSACTION GROUP
A2
TRANSACTION SCRIPT DECRYPTS THE IDEA KEY
A3
DECRYPTED IDEA KEY IS PLACED IN AN OUTPUT DATA OBJECT
A4
IDEA KEY IS USED TO DECRYPT THE SECURE E-MAIL
A5

FIG. 3

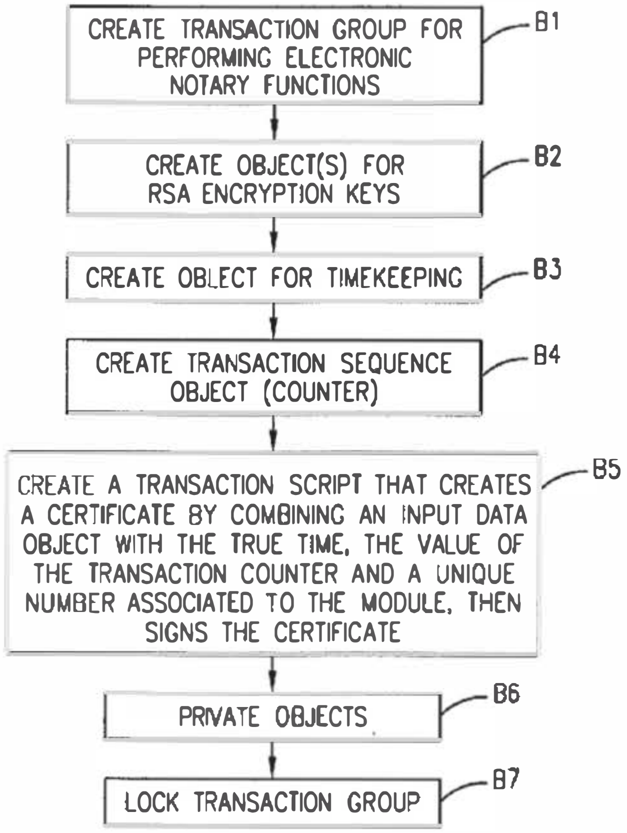

CREATE TRANSACTION GROUP FOR PERFORMING ELECTRONIC NOTARY FUNCTIONS
B1
CREATE OBJECT(S) FOR RSA ENCRYPTION KEYS
B2
CREATE OBLECT FOR TIMEKEEPING
B3
CREATE TRANSACTION SEQUENCE OBJECT (COUNTER)
B4
CREATE A TRANSACTION SCRIPT THAT CREATES A CERTIFICATE BY COMBINING AN INPUT DATA OBJECT WITH THE TRUE TIME, THE VALUE OF THE TRANSACTION COUNTER AND A UNIQUE NUMBER ASSOCIATED TO THE MODULE, THEN SIGNS THE CERTIFICATE
B5
PRIVATE OBJECTS
B6
LOCK TRANSACTION GROUP
B7

FIG. 4

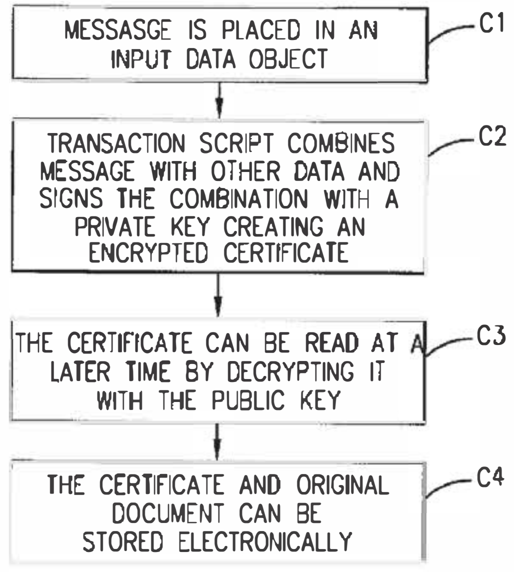

MESSASGE IS PLACED IN AN INPUT DATA OBJECT
C1
TRANSACTION SCRIPT COMBINES MESSAGE WITH OTHER DATA AND SIGNS THE COMBINATION WITH A PRIVATE KEY CREATING AN ENCRYPTED CERTIFICATE
C2
THE CERTIFICATE CAN BE READ AT A LATER TIME BY DECRYPTING IT WITH THE PUBLIC KEY
C3
THE CERTIFICATE AND ORIGINAL DOCUMENT CAN BE STORED ELECTRONICALLY
C4

FIG. 5

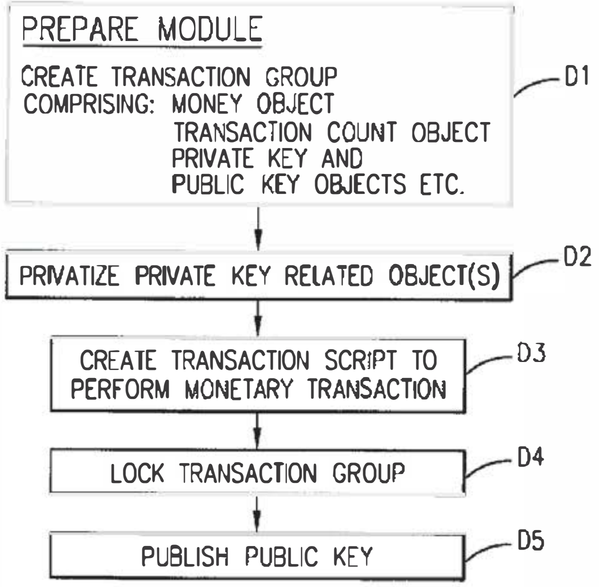

PREPARE MODULE
CREATE TRANSACTION GROUP COMPRISING: MONEY OBJECT
TRANSACTION COUNT OBJECT
PRIVATE KEY AND
PUBLIC KEY OBJECTS ETC.
D1
PRIVATIZE PRIVATE KEY RELATED OBJECT(S)
D2
CREATE TRANSACTION SCRIPT TO PERFORM MONETARY TRANSACTION
D3
LOCK TRANSACTION GROUP
D4
PUBLISH PUBLIC KEY
D5

FIG. 6

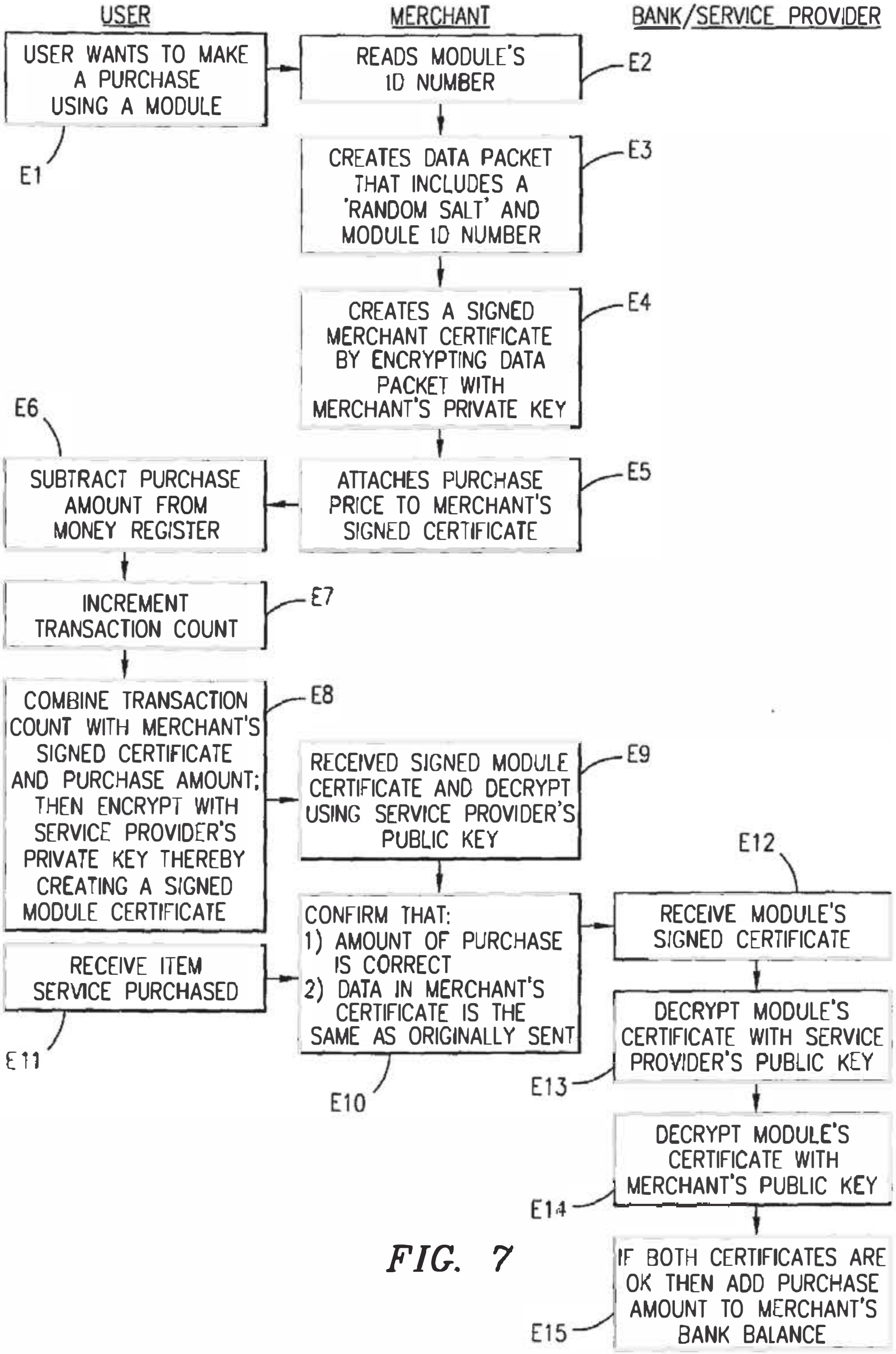

USER
MERCHANT
BANK/SERVICE PROVIDER
USER WANTS TO MAKE A PURCHASE USING A MODULE
E1
READS MODULE'S 1D NUMBER
E2
CREATES DATA PACKET THAT INCLUDES A 'RANDOM SALT' AND MODULE 1D NUMBER
E3
CREATES A SIGNED MERCHANT CERTIFICATE BY ENCRYPTING DATA PACKET WITH MERCHANT'S PRIVATE KEY
E4
ATTACHES PURCHASE PRICE TO MERCHANT'S SIGNED CERTIFICATE
E5
E6
SUBTRACT PURCHASE AMOUNT FROM MONEY REGISTER
INCREMENT TRANSACTION COUNT
E7
COMBINE TRANSACTION COUNT WITH MERCHANT'S SIGNED CERTIFICATE AND PURCHASE AMOUNT; THEN ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY THEREBY CREATING A SIGNED MODULE CERTIFICATE
E8
RECEIVED SIGNED MODULE CERTIFICATE AND DECRYPT USING SERVICE PROVIDER'S PUBLIC KEY
E9
CONFIRM THAT:
1) AMOUNT OF PURCHASE IS CORRECT
2) DATA IN MERCHANT'S CERTIFICATE IS THE SAME AS ORIGINALLY SENT
E10
RECEIVE ITEM SERVICE PURCHASED
E11
E12
RECEIVE MODULE'S SIGNED CERTIFICATE
DECRYPT MODULE'S CERTIFICATE WITH SERVICE PROVIDER'S PUBLIC KEY
E13
DECRYPT MODULE'S CERTIFICATE WITH MERCHANT'S PUBLIC KEY
E14
IF BOTH CERTIFICATES ARE OK THEN ADD PURCHASE AMOUNT TO MERCHANT'S BANK BALANCE
E15

FIG. 7

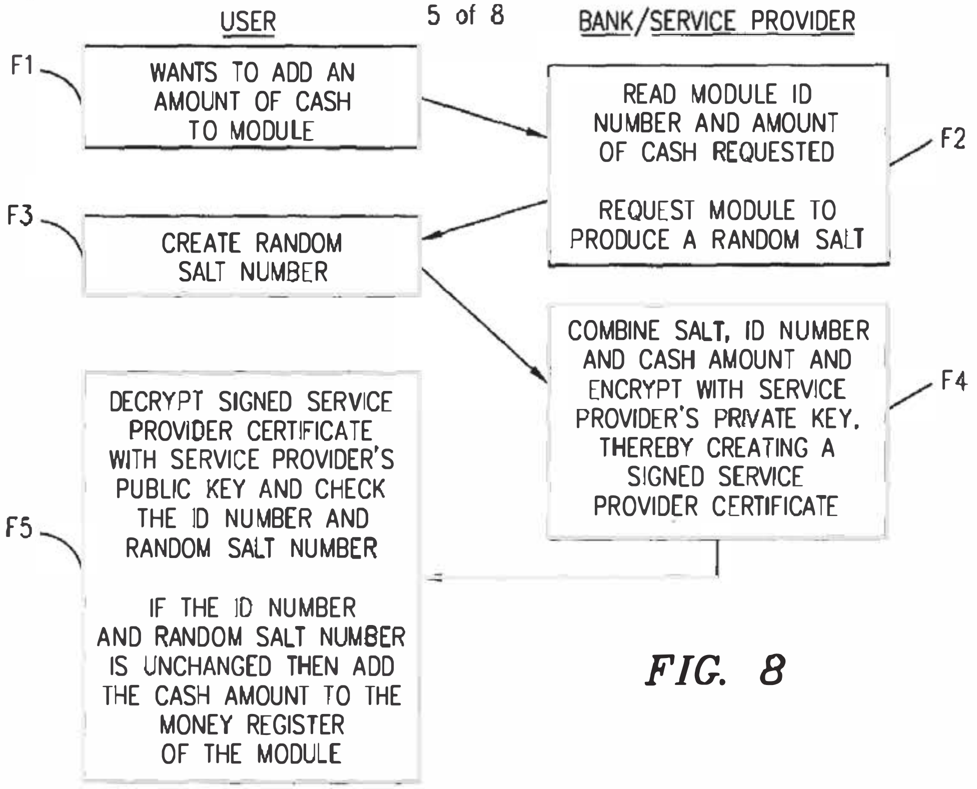

USER
BANK/SERVICE PROVIDER
F1
WANTS TO ADD AN AMOUNT OF CASH TO MODULE
READ MODULE ID NUMBER AND AMOUNT OF CASH REQUESTED
REQUEST MODULE TO PRODUCE A RANDOM SALT
F2
F3
CREATE RANDOM SALT NUMBER
COMBINE SALT, ID NUMBER AND CASH AMOUNT AND ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY, THEREBY CREATING A SIGNED SERVICE PROVIDER CERTIFICATE
F4
F5
DECRYPT SIGNED SERVICE PROVIDER CERTIFICATE WITH SERVICE PROVIDER'S PUBLIC KEY AND CHECK THE ID NUMBER AND RANDOM SALT NUMBER
IF THE ID NUMBER AND RANDOM SALT NUMBER IS UNCHANGED THEN ADD THE CASH AMOUNT TO THE MONEY REGISTER OF THE MODULE

FIG. 8

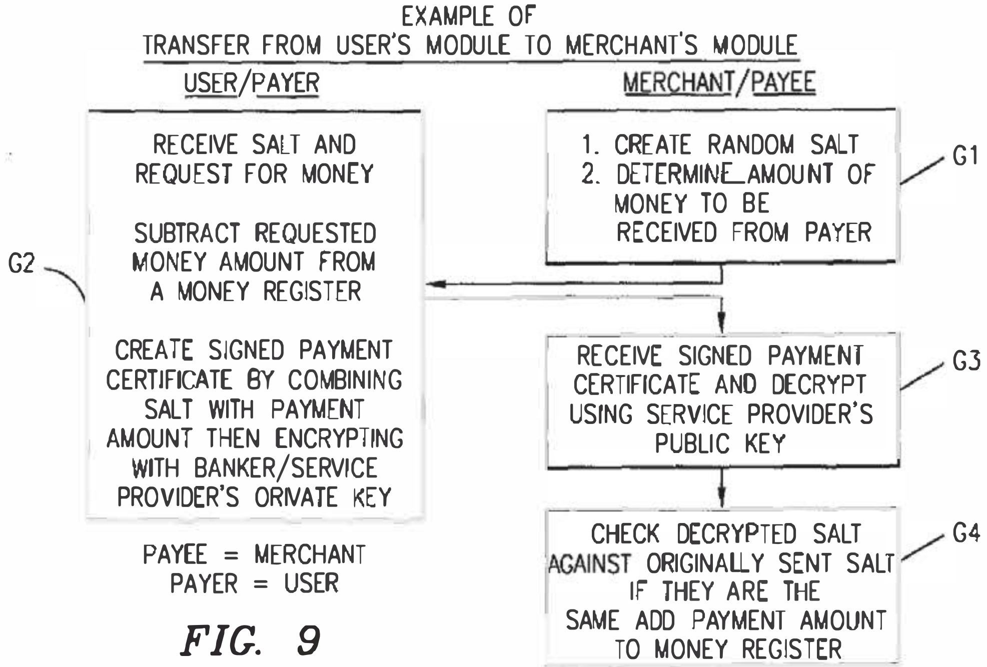

EXAMPLE OF
TRANSFER FROM USER'S MODULE TO MERCHANT'S MODULE
USER/PAYER
MERCHANT/PAYEE
1. CREATE RANDOM SALT
2. DETERMINE_AMOUNT OF MONEY TO BE RECEIVED FROM PAYER
G1
G2
RECEIVE SALT AND REQUEST FOR MONEY
SUBTRACT REQUESTED MONEY AMOUNT FROM A MONEY REGISTER
CREATE SIGNED PAYMENT CERTIFICATE BY COMBINING SALT WITH PAYMENT AMOUNT THEN ENCRYPTING WITH BANKER/SERVICE PROVIDER'S ORIVATE KEY
RECEIVE SIGNED PAYMENT CERTIFICATE AND DECRYPT USING SERVICE PROVIDER'S PUBLIC KEY
G3
CHECK DECRYPTED SALT AGAINST ORIGINALLY SENT SALT IF THEY ARE THE SAME ADD PAYMENT AMOUNT TO MONEY REGISTER
G4
PAYEE = MERCHANT
PAYER = USER

FIG. 9

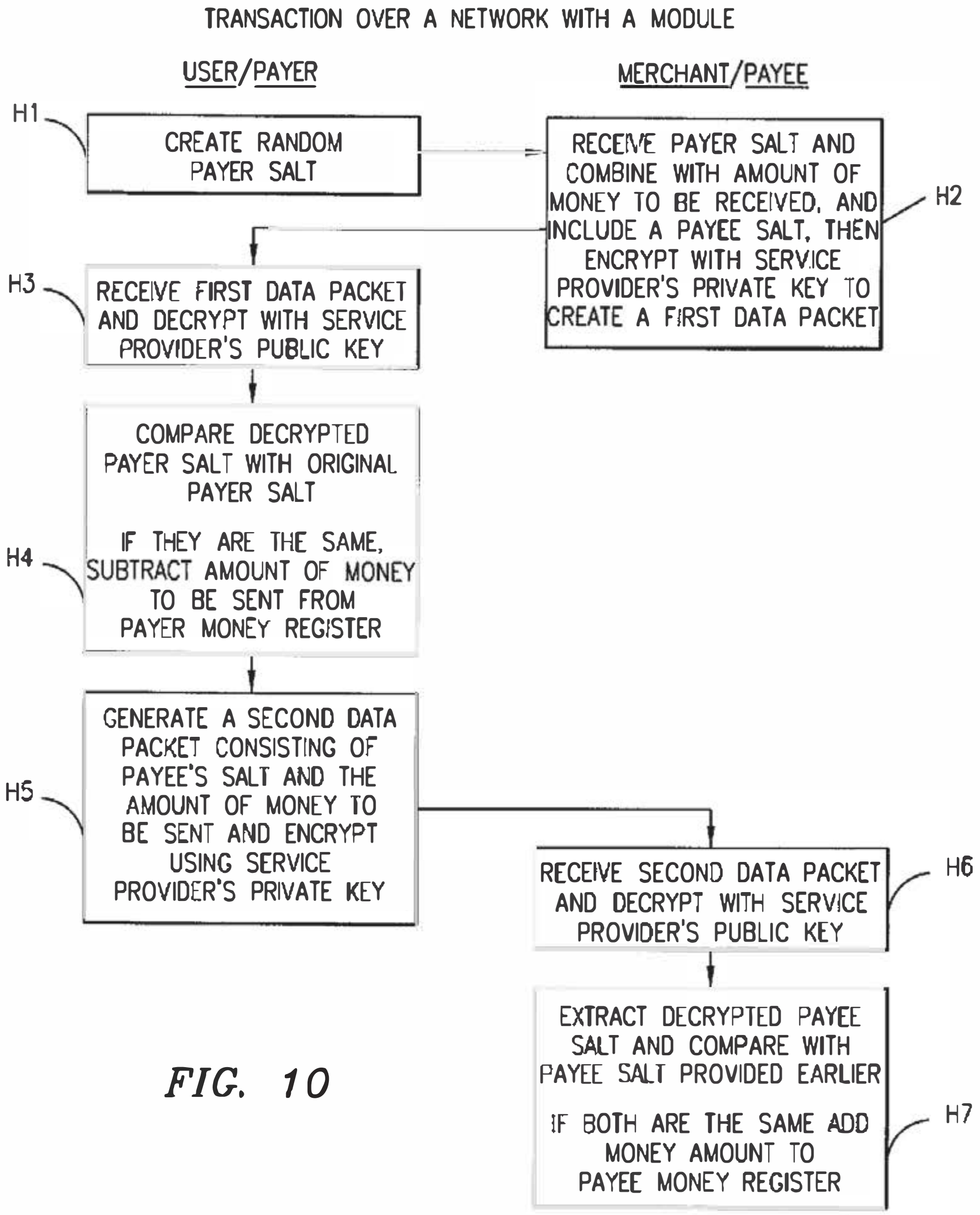

TRANSACTION OVER A NETWORK WITH A MODULE
USER/PAYER
MERCHANT/PAYEE
H1
CREATE RANDOM PAYER SALT
RECEIVE PAYER SALT AND COMBINE WITH AMOUNT OF MONEY TO BE RECEIVED, AND INCLUDE A PAYEE SALT, THEN ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY TO CREATE A FIRST DATA PACKET
H2
H3
RECEIVE FIRST DATA PACKET AND DECRYPT WITH SERVICE PROVIDER'S PUBLIC KEY
COMPARE DECRYPTED PAYER SALT WITH ORIGINAL PAYER SALT
IF THEY ARE THE SAME, SUBTRACT AMOUNT OF MONEY TO BE SENT FROM PAYER MONEY REGISTER
H4
GENERATE A SECOND DATA PACKET CONSISTING OF PAYEE'S SALT AND THE AMOUNT OF MONEY TO BE SENT AND ENCRYPT USING SERVICE PROVIDER'S PRIVATE KEY
H5
RECEIVE SECOND DATA PACKET AND DECRYPT WITH SERVICE PROVIDER'S PUBLIC KEY
H6
EXTRACT DECRYPTED PAYEE SALT AND COMPARE WITH PAYEE SALT PROVIDED EARLIER
IF BOTH ARE THE SAME ADD MONEY AMOUNT TO PAYEE MONEY REGISTER
H7

FIG. 10

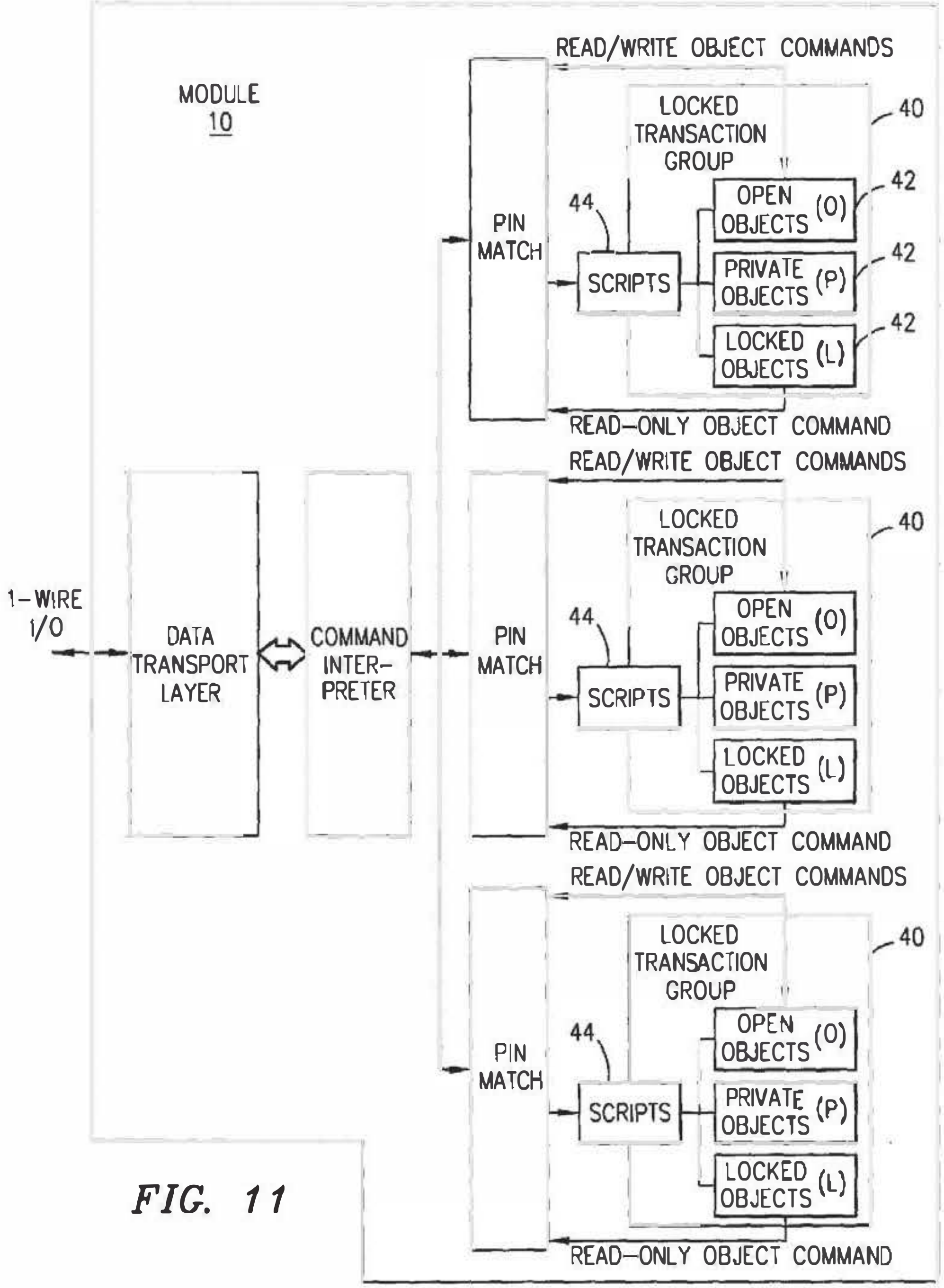

MODULE
10
1-WIRE
I/O
DATA
TRANSPORT
LAYER
COMMAND
INTER-
PRETER
READ/WRITE OBJECT COMMANDS
PIN
MATCH
LOCKED
TRANSACTION
GROUP
40
44
SCRIPTS
OPEN
OBJECTS
(O)
42
PRIVATE
OBJECTS
(P)
42
LOCKED
OBJECTS
(L)
42
READ-ONLY OBJECT COMMAND
READ/WRITE OBJECT COMMANDS
PIN
MATCH
LOCKED
TRANSACTION
GROUP
40
44
SCRIPTS
OPEN
OBJECTS
(O)
PRIVATE
OBJECTS
(P)
LOCKED
OBJECTS
(L)
READ-ONLY OBJECT COMMAND
READ/WRITE OBJECT COMMANDS
PIN
MATCH
LOCKED
TRANSACTION
GROUP
40
44
SCRIPTS
OPEN
OBJECTS
(O)
PRIVATE
OBJECTS
(P)
LOCKED
OBJECTS
(L)
READ-ONLY OBJECT COMMAND

FIG. 11

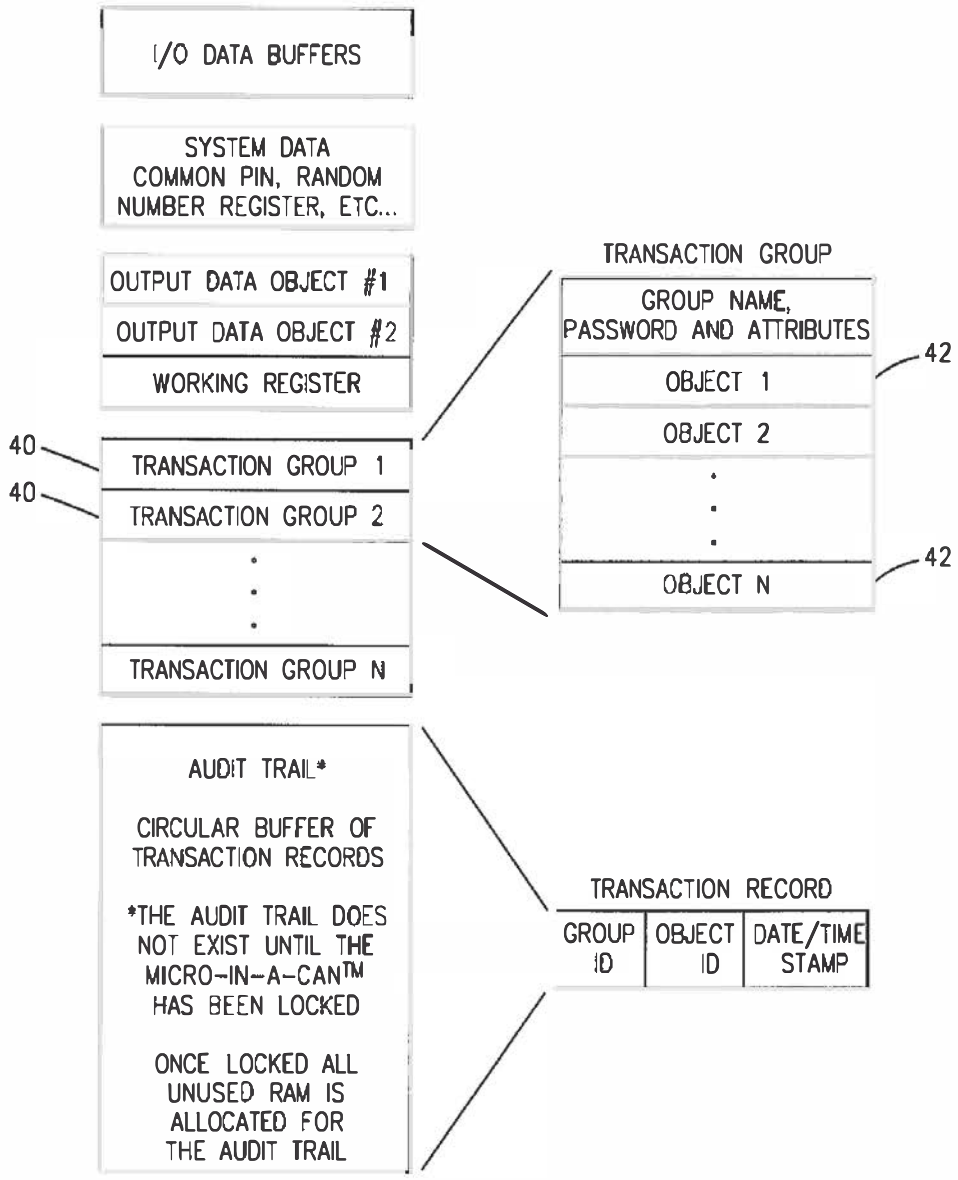

I/O DATA BUFFERS
SYSTEM DATA
COMMON PIN, RANDOM
NUMBER REGISTER, ETC...
OUTPUT DATA OBJECT #1
OUTPUT DATA OBJECT #2
WORKING REGISTER
40
TRANSACTION GROUP 1
40
TRANSACTION GROUP 2
TRANSACTION GROUP N
TRANSACTION GROUP
GROUP NAME,
PASSWORD AND ATTRIBUTES
42
OBJECT 1
OBJECT 2
OBJECT N
42
AUDIT TRAIL*
CIRCULAR BUFFER OF
TRANSACTION RECORDS
*THE AUDIT TRAIL DOES
NOT EXIST UNTIL THE
MICRO-IN-A-CAN™
HAS BEEN LOCKED
ONCE LOCKED ALL
UNUSED RAM IS
ALLOCATED FOR
THE AUDIT TRAIL
TRANSACTION RECORD
GROUP ID
OBJECT ID
DATE/TIME STAMP

FIG. 12

Jenkens & Gilchrist
A PROFESSIONAL CORPORATION

FOUNTAIN PLACE
1445 ROSS AVENUE, SUITE 3200
DALLAS, TX 75202

(214) 855-4500
TELECOPIER (214) 855-4300

AUSTIN, TEXAS
(512) 499-3800

HOUSTON, TEXAS
(713) 951-3300

SAN ANTONIO, TEXAS
(210) 308-3100

WASHINGTON, D.C.
(202) 326-1500

8#

WRITER'S DIRECT DIAL NUMBER
Steven R. Greenfield
(214) 855-4789

Box Issue Fee
Assistant Commissioner
for Patents
Washington DC 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. EL274277998US
Date of Deposit: April 16, 1999
I hereby certify that this paper or fee is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231

Type or Print Name. SUSAN MITCHELL
Susan Mitchell
Signature

Re:	Applicant(s):	Stephen M. Curry, *et al.*
	Serial No.:	09/041,190
	Filed:	March 10, 1998
	Batch No.	O24
	NOA Mailed:	February 19, 1999
	For:	Method, Apparatus, System and Firmware for Secure Transactions
	Docket No.:	20661-457C1

Dear Sir:

Transmitted for filing with the Patent and Trademark Office are the following documents for the above-referenced patent application:

1. Part B Issue Fee Transmittal
2. Letter to Official Draftsperson
3. 8 Sheets of Formal Drawings
4. Check in the amount of $1,240.00 for issue fee and soft copies
5. Acknowledgment Postcard

Please address all communications related to this to:

Steven R. Greenfield
Jenkens & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799

In the event there is an under or over payment, please debit or credit our Deposit Account #10-0447.

Respectfully submitted,

Steven R. Greenfield
Registration No. 38,166

#18
JL

PATENT APPLICATION
Docket No 20661-00457C1

Issue Batch No.:	G77
Date of Notice of Allowance:	January 12, 2000
Serial No.:	09/041,190

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: Curry, et al.

Serial No.: 09/041,190 Group No.: 3662

Filed: March 10, 1998 Examiner: B. Gregory

For: **METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS**

BOX ISSUE FEE
Assistant Commissioner for Patents
Washington, D.C. 20231

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231
on April 11, 2000
Christy Wilson
Signature

ATTN: Official Draftsperson

Sir:

TRANSMITTAL LETTER TO OFFICIAL DRAFTSPERSON

Enclosed please find 8 sheets of formal drawings relating to the above-identified patent application.

The enclosed drawings each bear the Issue Batch No. G77, the date of the Notice of Allowance January 12, 2000, and Serial No. 09/041,190 of the application on their reverse side.

In view of the above, the present application is believed to be in a condition ready for issuance.

Respectfully submitted,

JENKENS & GILCHRIST,
A Professional Corporation

W Stacy
Wayne O Stacy
Registration No.45,125

1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
214/855-4120
214/855-4300 FAX

6105013

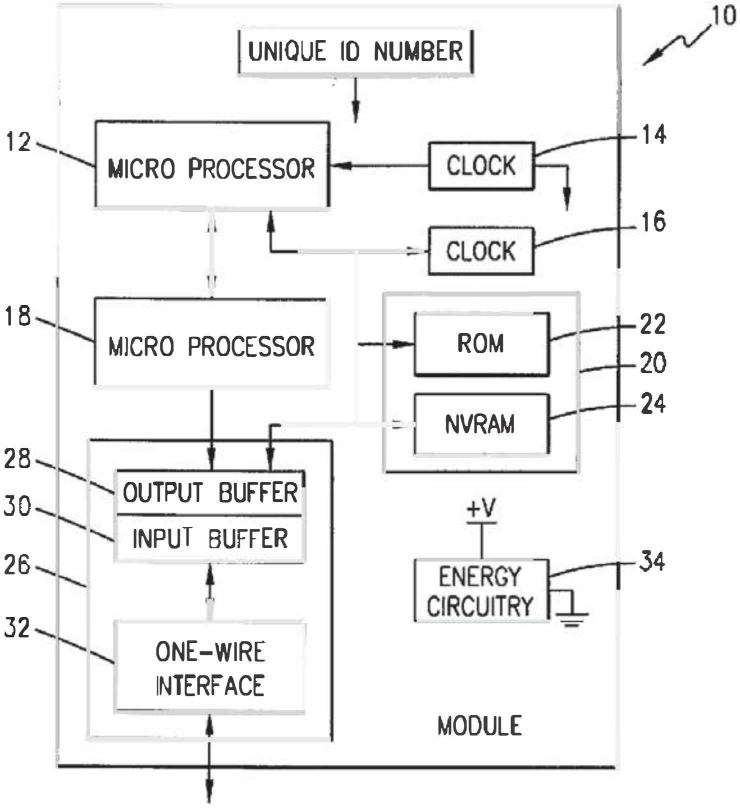


FIG. 1

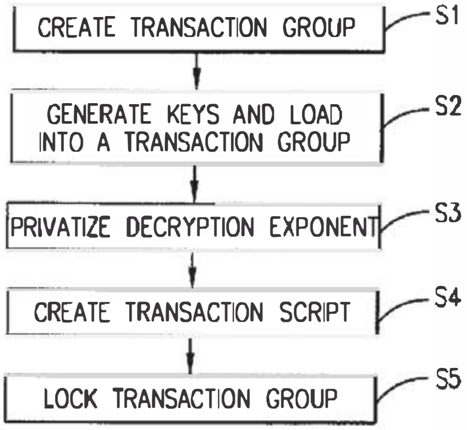

CREATE TRANSACTION GROUP
S1
GENERATE KEYS AND LOAD INTO A TRANSACTION GROUP
S2
PRIVATIZE DECRYPTION EXPONENT
S3
CREATE TRANSACTION SCRIPT
S4
LOCK TRANSACTION GROUP
S5

FIG. 2

FIG. 3

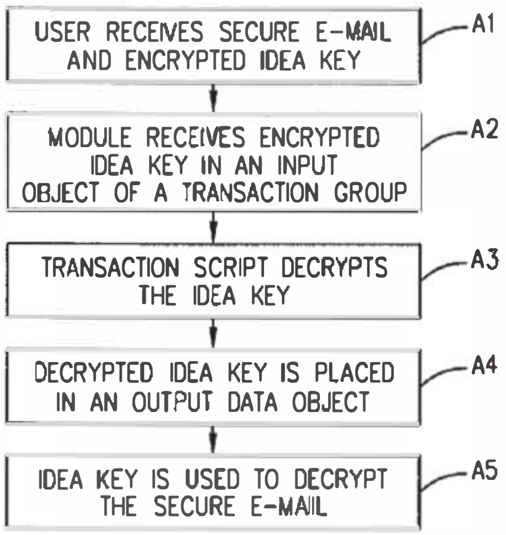
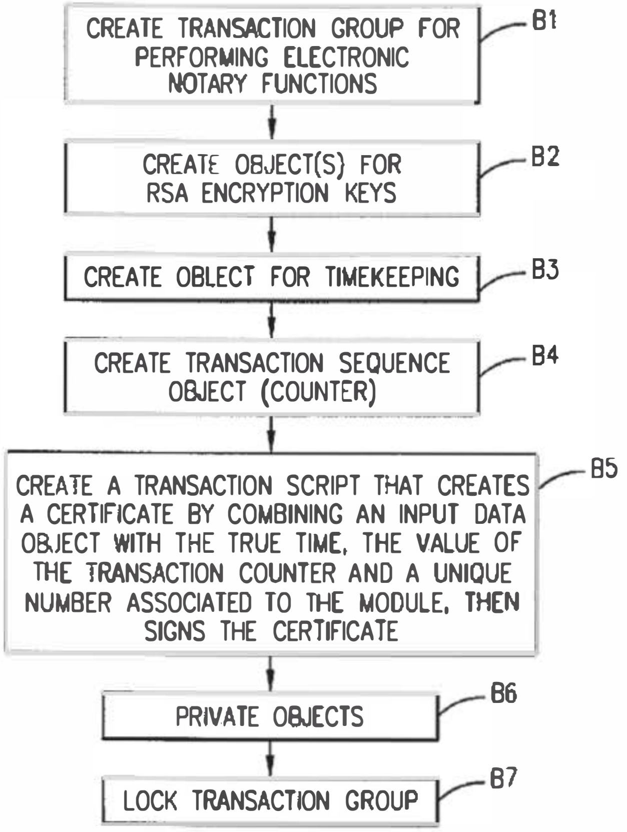

USER RECEIVES SECURE E-MAIL AND ENCRYPTED IDEA KEY
A1
MODULE RECEIVES ENCRYPTED IDEA KEY IN AN INPUT OBJECT OF A TRANSACTION GROUP
A2
TRANSACTION SCRIPT DECRYPTS THE IDEA KEY
A3
DECRYPTED IDEA KEY IS PLACED IN AN OUTPUT DATA OBJECT
A4
IDEA KEY IS USED TO DECRYPT THE SECURE E-MAIL
A5

FIG. 4


CREATE TRANSACTION GROUP FOR PERFORMING ELECTRONIC NOTARY FUNCTIONS
B1
CREATE OBJECT(S) FOR RSA ENCRYPTION KEYS
B2
CREATE OBLECT FOR TIMEKEEPING
B3
CREATE TRANSACTION SEQUENCE OBJECT (COUNTER)
B4
CREATE A TRANSACTION SCRIPT THAT CREATES A CERTIFICATE BY COMBINING AN INPUT DATA OBJECT WITH THE TRUE TIME, THE VALUE OF THE TRANSACTION COUNTER AND A UNIQUE NUMBER ASSOCIATED TO THE MODULE, THEN SIGNS THE CERTIFICATE
B5
PRIVATE OBJECTS
B6
LOCK TRANSACTION GROUP
B7

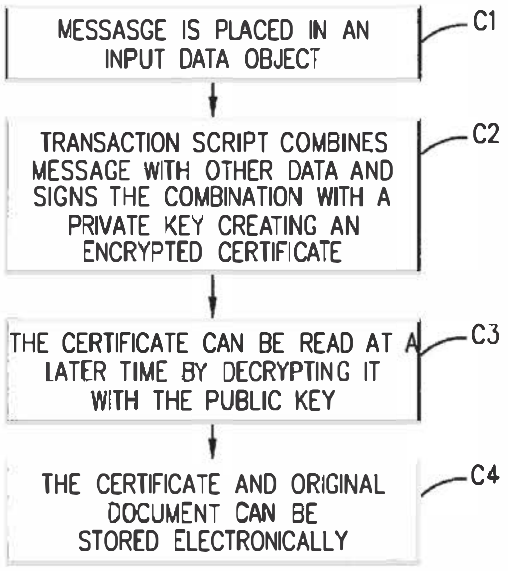

MESSASGE IS PLACED IN AN INPUT DATA OBJECT
C1
TRANSACTION SCRIPT COMBINES MESSAGE WITH OTHER DATA AND SIGNS THE COMBINATION WITH A PRIVATE KEY CREATING AN ENCRYPTED CERTIFICATE
C2
THE CERTIFICATE CAN BE READ AT A LATER TIME BY DECRYPTING IT WITH THE PUBLIC KEY
C3
THE CERTIFICATE AND ORIGINAL DOCUMENT CAN BE STORED ELECTRONICALLY
C4

FIG. 5

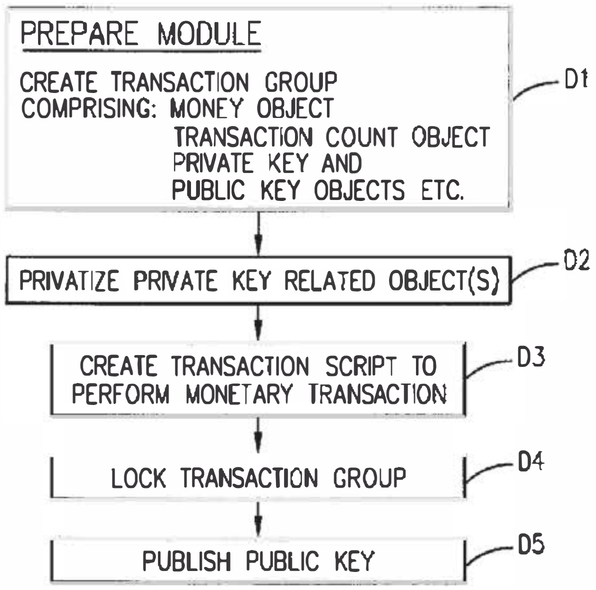

PREPARE MODULE
CREATE TRANSACTION GROUP COMPRISING: MONEY OBJECT
TRANSACTION COUNT OBJECT
PRIVATE KEY AND
PUBLIC KEY OBJECTS ETC.
D1
PRIVATIZE PRIVATE KEY RELATED OBJECT(S)
D2
CREATE TRANSACTION SCRIPT TO PERFORM MONETARY TRANSACTION
D3
LOCK TRANSACTION GROUP
D4
PUBLISH PUBLIC KEY
D5

FIG. 6

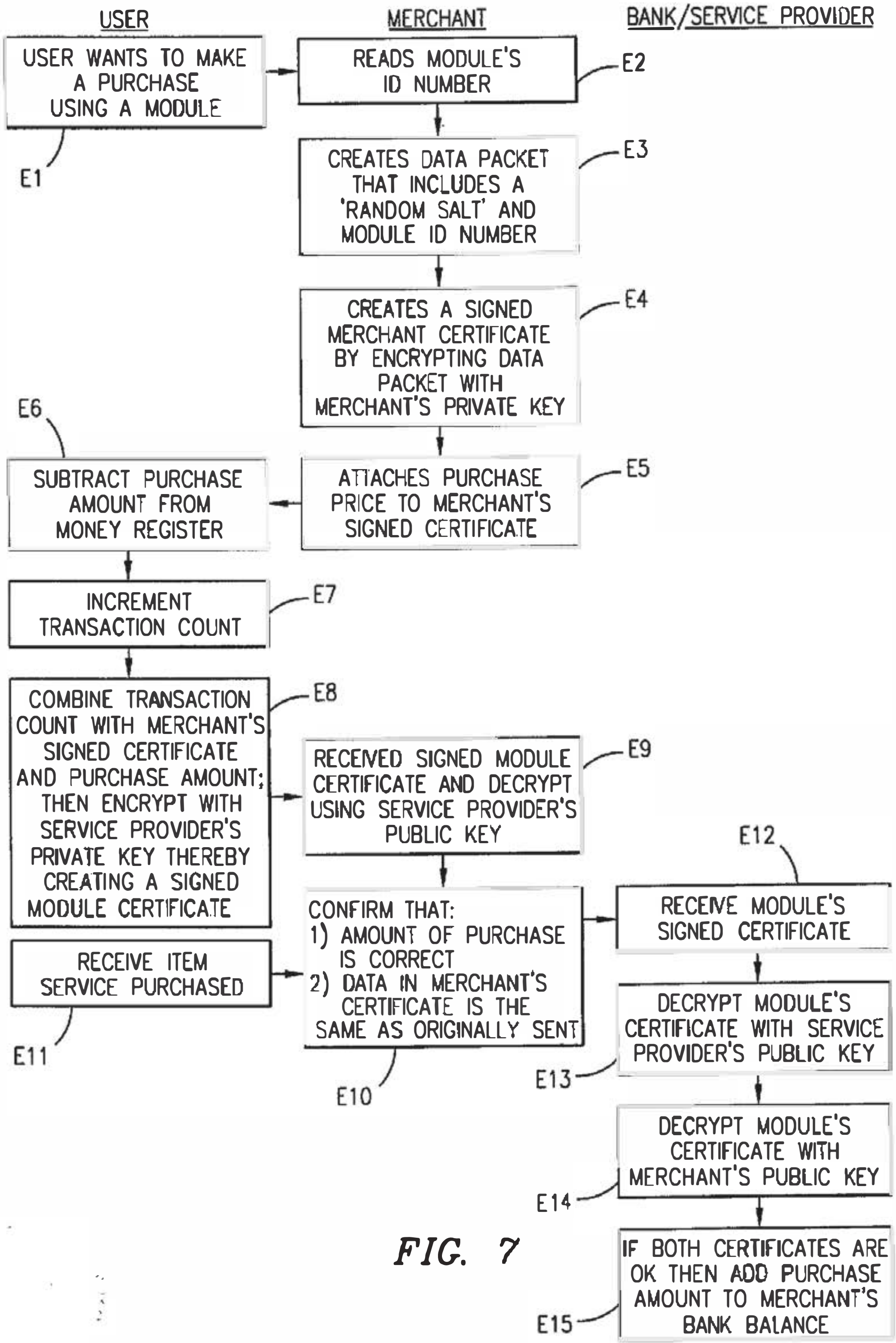

USER
MERCHANT
BANK/SERVICE PROVIDER
USER WANTS TO MAKE A PURCHASE USING A MODULE
E1
READS MODULE'S ID NUMBER
E2
CREATES DATA PACKET THAT INCLUDES A 'RANDOM SALT' AND MODULE ID NUMBER
E3
CREATES A SIGNED MERCHANT CERTIFICATE BY ENCRYPTING DATA PACKET WITH MERCHANT'S PRIVATE KEY
E4
ATTACHES PURCHASE PRICE TO MERCHANT'S SIGNED CERTIFICATE
E5
E6
SUBTRACT PURCHASE AMOUNT FROM MONEY REGISTER
INCREMENT TRANSACTION COUNT
E7
COMBINE TRANSACTION COUNT WITH MERCHANT'S SIGNED CERTIFICATE AND PURCHASE AMOUNT; THEN ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY THEREBY CREATING A SIGNED MODULE CERTIFICATE
E8
RECEIVED SIGNED MODULE CERTIFICATE AND DECRYPT USING SERVICE PROVIDER'S PUBLIC KEY
E9
E12
CONFIRM THAT: 1) AMOUNT OF PURCHASE IS CORRECT 2) DATA IN MERCHANT'S CERTIFICATE IS THE SAME AS ORIGINALLY SENT
RECEIVE MODULE'S SIGNED CERTIFICATE
RECEIVE ITEM SERVICE PURCHASED
E11
E10
DECRYPT MODULE'S CERTIFICATE WITH SERVICE PROVIDER'S PUBLIC KEY
E13
DECRYPT MODULE'S CERTIFICATE WITH MERCHANT'S PUBLIC KEY
E14
IF BOTH CERTIFICATES ARE OK THEN ADD PURCHASE AMOUNT TO MERCHANT'S BANK BALANCE
E15

FIG. 7

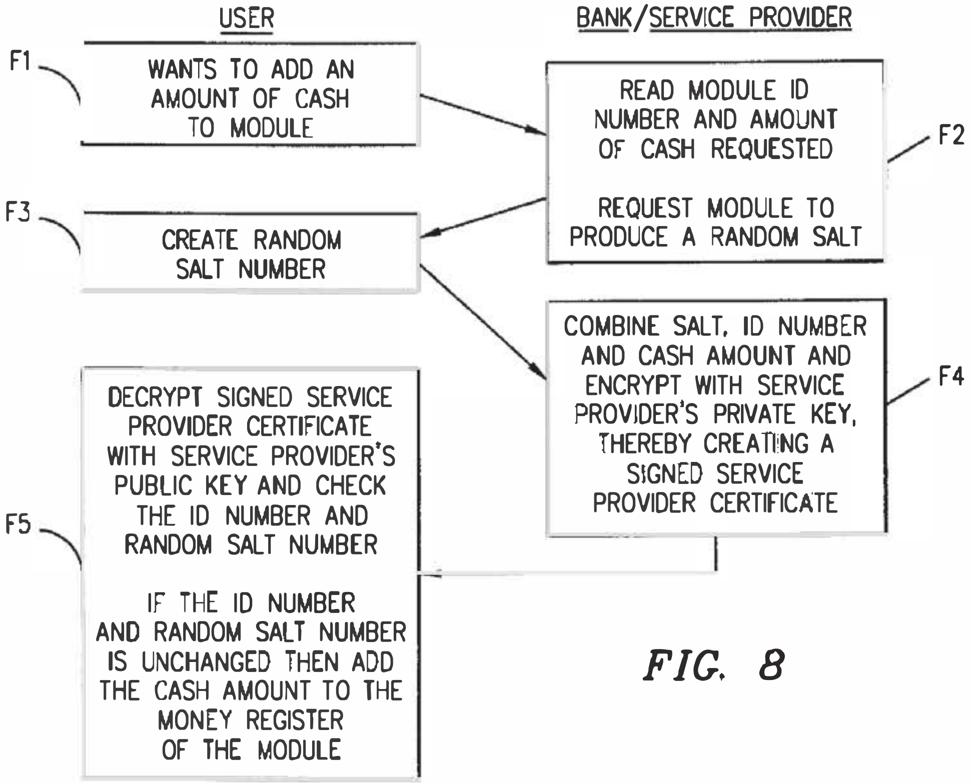

USER
BANK/SERVICE PROVIDER
F1
WANTS TO ADD AN AMOUNT OF CASH TO MODULE
READ MODULE ID NUMBER AND AMOUNT OF CASH REQUESTED
REQUEST MODULE TO PRODUCE A RANDOM SALT
F2
F3
CREATE RANDOM SALT NUMBER
COMBINE SALT, ID NUMBER AND CASH AMOUNT AND ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY, THEREBY CREATING A SIGNED SERVICE PROVIDER CERTIFICATE
F4
F5
DECRYPT SIGNED SERVICE PROVIDER CERTIFICATE WITH SERVICE PROVIDER'S PUBLIC KEY AND CHECK THE ID NUMBER AND RANDOM SALT NUMBER
IF THE ID NUMBER AND RANDOM SALT NUMBER IS UNCHANGED THEN ADD THE CASH AMOUNT TO THE MONEY REGISTER OF THE MODULE

FIG. 8

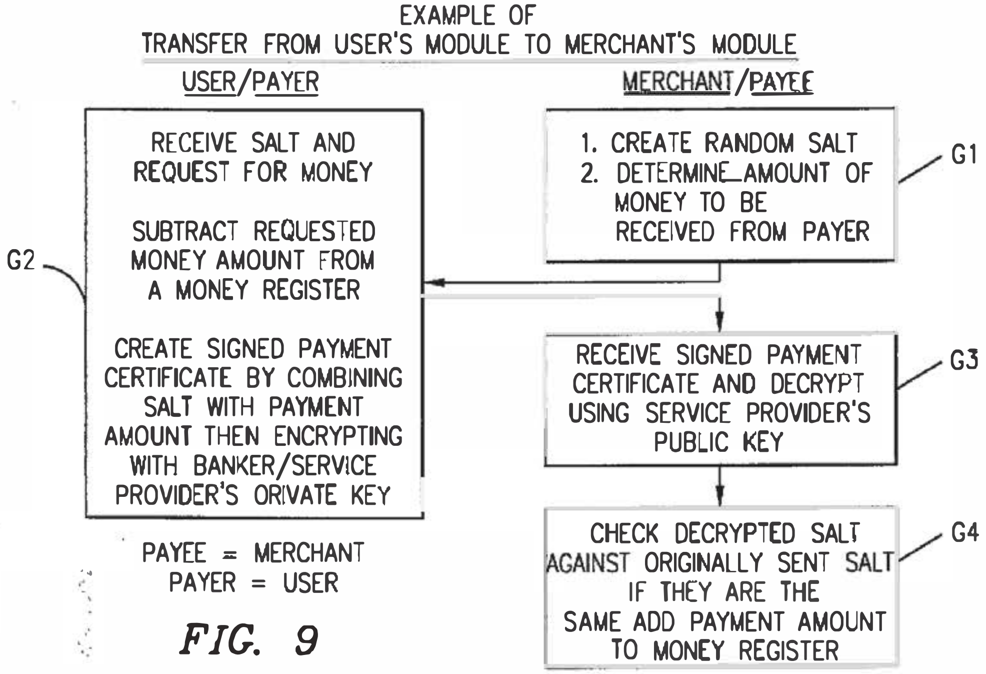

EXAMPLE OF
TRANSFER FROM USER'S MODULE TO MERCHANT'S MODULE
USER/PAYER
MERCHANT/PAYEE
1. CREATE RANDOM SALT
2. DETERMINE AMOUNT OF MONEY TO BE RECEIVED FROM PAYER
G1
G2
RECEIVE SALT AND REQUEST FOR MONEY
SUBTRACT REQUESTED MONEY AMOUNT FROM A MONEY REGISTER
CREATE SIGNED PAYMENT CERTIFICATE BY COMBINING SALT WITH PAYMENT AMOUNT THEN ENCRYPTING WITH BANKER/SERVICE PROVIDER'S ORIVATE KEY
RECEIVE SIGNED PAYMENT CERTIFICATE AND DECRYPT USING SERVICE PROVIDER'S PUBLIC KEY
G3
CHECK DECRYPTED SALT AGAINST ORIGINALLY SENT SALT IF THEY ARE THE SAME ADD PAYMENT AMOUNT TO MONEY REGISTER
G4
PAYEE = MERCHANT
PAYER = USER

FIG. 9

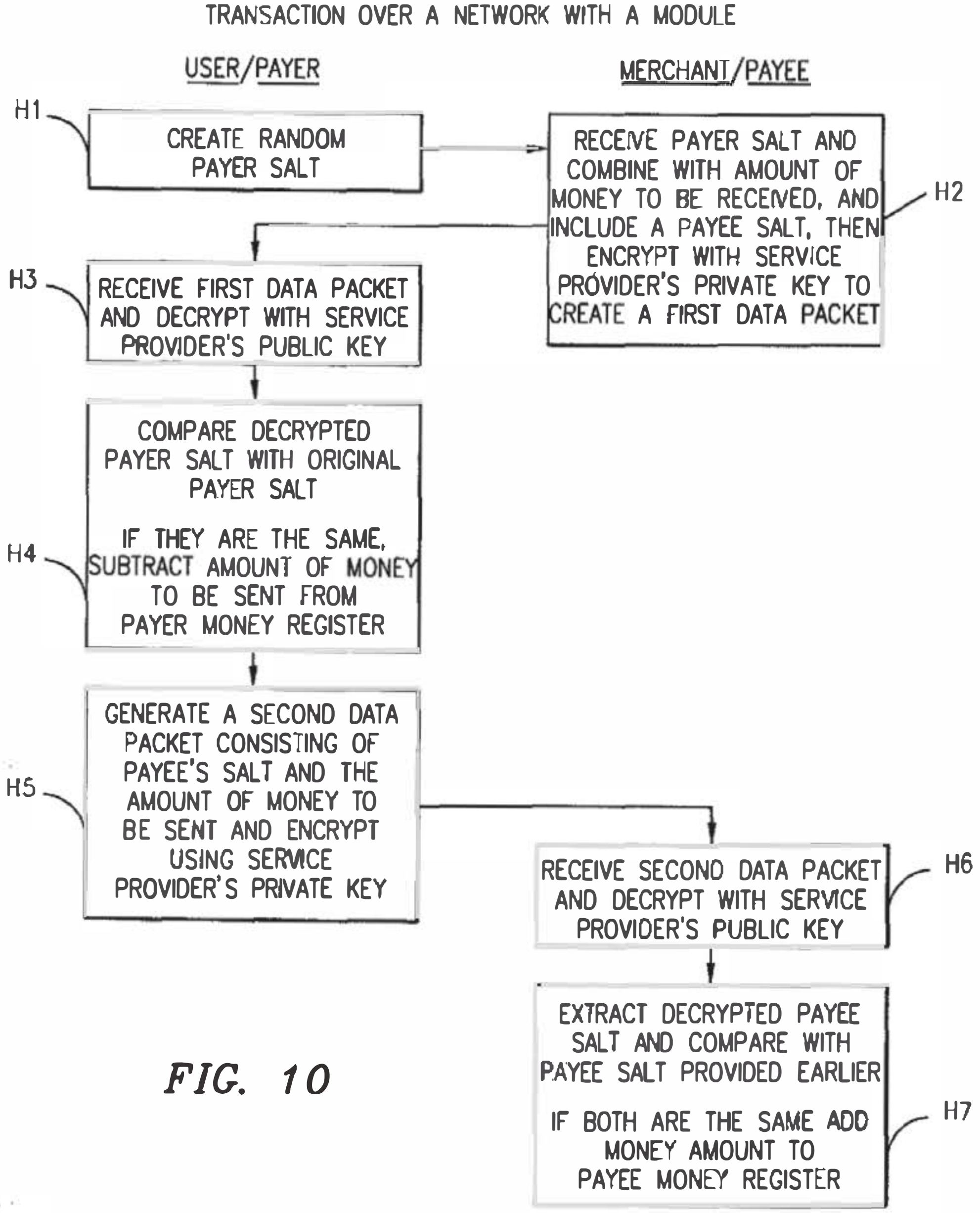

TRANSACTION OVER A NETWORK WITH A MODULE
USER/PAYER
MERCHANT/PAYEE
H1
CREATE RANDOM PAYER SALT
RECEIVE PAYER SALT AND COMBINE WITH AMOUNT OF MONEY TO BE RECEIVED, AND INCLUDE A PAYEE SALT, THEN ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY TO CREATE A FIRST DATA PACKET
H2
H3
RECEIVE FIRST DATA PACKET AND DECRYPT WITH SERVICE PROVIDER'S PUBLIC KEY
COMPARE DECRYPTED PAYER SALT WITH ORIGINAL PAYER SALT
IF THEY ARE THE SAME, SUBTRACT AMOUNT OF MONEY TO BE SENT FROM PAYER MONEY REGISTER
H4
GENERATE A SECOND DATA PACKET CONSISTING OF PAYEE'S SALT AND THE AMOUNT OF MONEY TO BE SENT AND ENCRYPT USING SERVICE PROVIDER'S PRIVATE KEY
H5
RECEIVE SECOND DATA PACKET AND DECRYPT WITH SERVICE PROVIDER'S PUBLIC KEY
H6
EXTRACT DECRYPTED PAYEE SALT AND COMPARE WITH PAYEE SALT PROVIDED EARLIER
IF BOTH ARE THE SAME ADD MONEY AMOUNT TO PAYEE MONEY REGISTER
H7

FIG. 10

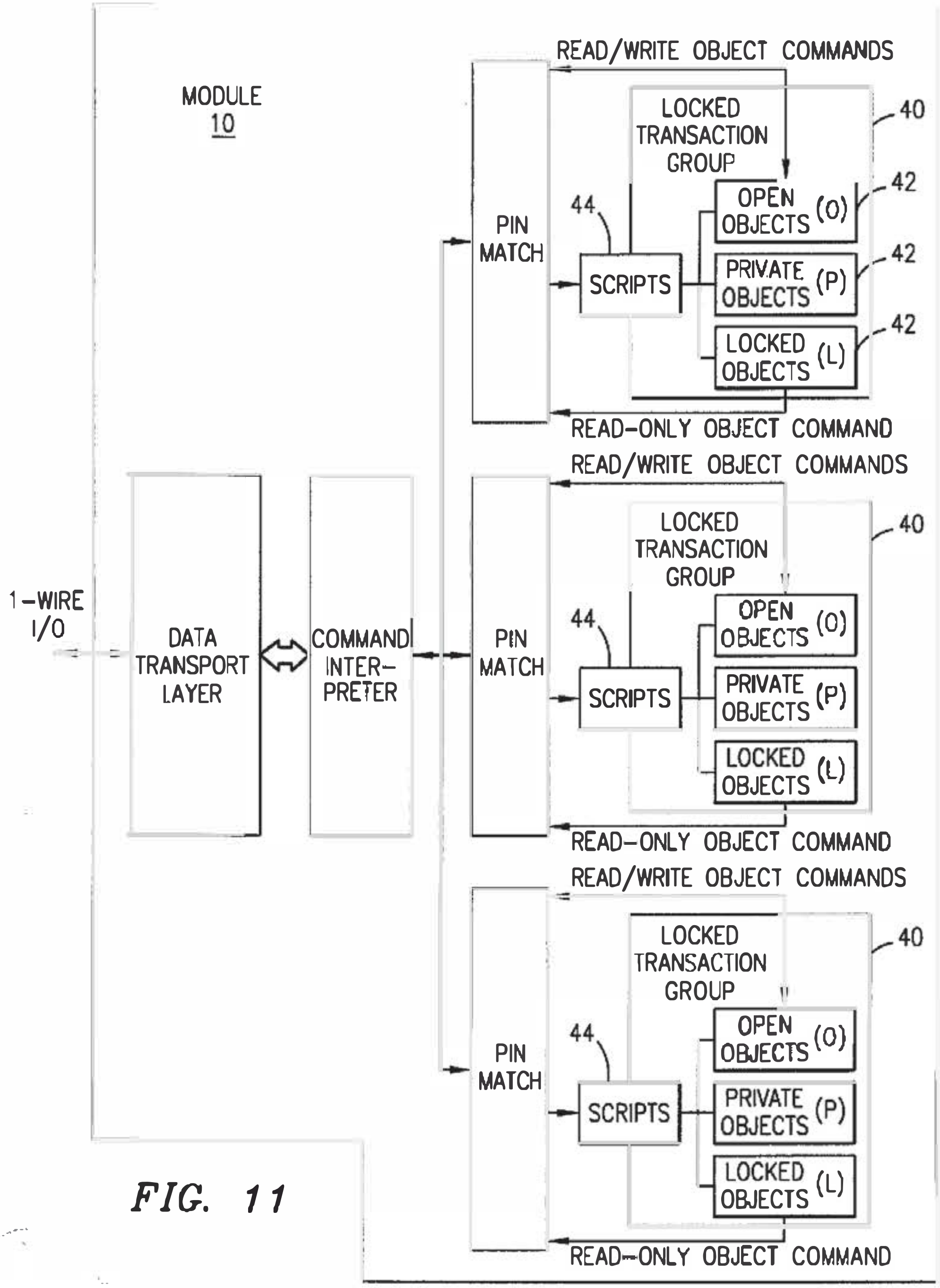

MODULE
10
1-WIRE
I/O
DATA
TRANSPORT
LAYER
COMMAND
INTER-
PRETER
READ/WRITE OBJECT COMMANDS
PIN
MATCH
LOCKED
TRANSACTION
GROUP
40
42
44
OPEN
OBJECTS
(O)
SCRIPTS
PRIVATE
OBJECTS
(P)
42
LOCKED
OBJECTS
(L)
42
READ-ONLY OBJECT COMMAND
READ/WRITE OBJECT COMMANDS
PIN
MATCH
LOCKED
TRANSACTION
GROUP
40
44
OPEN
OBJECTS
(O)
SCRIPTS
PRIVATE
OBJECTS
(P)
LOCKED
OBJECTS
(L)
READ-ONLY OBJECT COMMAND
READ/WRITE OBJECT COMMANDS
PIN
MATCH
LOCKED
TRANSACTION
GROUP
40
44
OPEN
OBJECTS
(O)
SCRIPTS
PRIVATE
OBJECTS
(P)
LOCKED
OBJECTS
(L)
READ-ONLY OBJECT COMMAND

FIG. 11

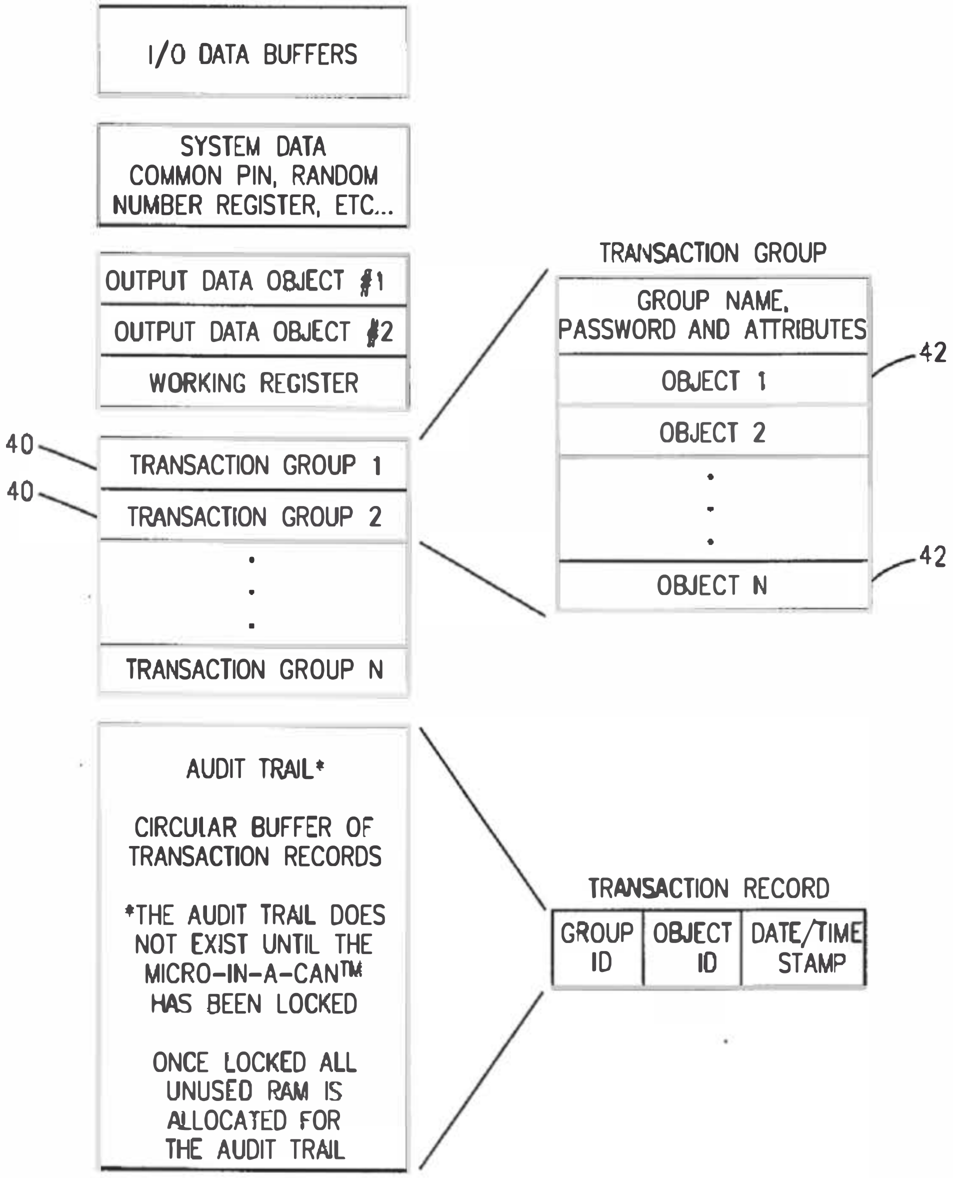

I/O DATA BUFFERS
SYSTEM DATA
COMMON PIN, RANDOM
NUMBER REGISTER, ETC...
OUTPUT DATA OBJECT #1
OUTPUT DATA OBJECT #2
WORKING REGISTER
40
TRANSACTION GROUP 1
40
TRANSACTION GROUP 2
TRANSACTION GROUP N
TRANSACTION GROUP
GROUP NAME,
PASSWORD AND ATTRIBUTES
42
OBJECT 1
OBJECT 2
42
OBJECT N
AUDIT TRAIL*
CIRCULAR BUFFER OF
TRANSACTION RECORDS
*THE AUDIT TRAIL DOES
NOT EXIST UNTIL THE
MICRO-IN-A-CAN™
HAS BEEN LOCKED
ONCE LOCKED ALL
UNUSED RAM IS
ALLOCATED FOR
THE AUDIT TRAIL
TRANSACTION RECORD
GROUP
ID
OBJECT
ID
DATE/TIME
STAMP

FIG. 12

Docket No. 20661-00457USC1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:		)		
Curry, et al.		)		
		)		
U.S. Patent No.:	6,105,013	)	Examiner:	Gregory, B.
		)		
Issued:	8/29/00	)	Group Art Unit:	3662

For: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

Box Certificate of Correction
Commissioner of Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING

I hereby certify that this paper or fee is being deposited with the U.S. Postal Service as first class mail on the date indicated below and is addressed to: Box Certificate of Correction, Assistant Commissioner of Patents, Washington, D.C. 20231

Date 6-15-01

Julie Lipton
Signature

Attention: Decision and Certificate of Correction Branch of the Patent Issue Division

REQUEST FOR CERTIFICATE OF CORRECTION OF PATENT
(37 CFR 1.322(a))

Attached in duplicate is Form PTO-1050 with at least one copy being suitable for printing.

The exact location where the errors occur in the patent and where the matter appears correctly in the application file are:

Patent	Application File
Column 3, line 8	Page 8, lines 10-11 of the originally filed application
Column 14, line 18	Page 53, line 4 of the originally filed application
Column 19, line 49	Page 75, line 17 of the originally filed application
Column 27, line 40	Page 108, line 1 of the originally filed application
Column 28, line 24	Page 111, line 8 of the originally filed application
Column 29, line 12	Page 114, line 7 of the originally filed application
Column 29, line 24	Page 115, line 1 of the originally filed application

Errors are typographical errors of the Patent and Trademark Office (as indicated above).

Please send the Certificate of Correction to:

Roger L. Maxwell
Jenkens & Gilchrist, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799

Assignee: Dallas Semiconductor Corporation

Roger L. Maxwell
Assignee's Attorney
Reg. No. 31,855

/ / Assignment recorded on
Reel/Frame:

/_/ Recordal of assignment attached

PTO/SB/44 (08-00)
Approved for use through 09/30/2000. OMB 0651-0033
U.S Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO :	6,105,013
DATED :	August 15, 2000
INVENTOR(S) :	Curry et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 3, line 8	Replace "photovoltaic" With -- photo-voltaic --
Column 14, line 18	Replace "FIPS" With -- FIBS --
Column 19, line 49	Replace "COMMON PIN" With -- COMMON_PIN --
Column 27, line 40	Replace "Chance" With -- Change --
Column 28, line 24	Replace "BAD OPTION BYTE" With -- BAD_OPTION_BYTE --
Column 29, line 12	Replace "BAD SIZE" With -- BAD_SIZE --
Column 29, line 24	Replace "BAD OBJECT ID" With -- BAD_OBJECT_ID --

MAILING ADDRESS OF SENDER:

Roger L. Maxwell
1445 Ross Avenue
Suite 3200
Dallas, Texas 75202-2799
20661-00457USC1

PATENT NO. 6,105,013

No. of additional copies

⇨ 1 of 1

Burden Hour Statement: This form is estimated to take 1.0 hour 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 TO: Assistant Commissioner for Patents, Washington, DC 20231.

PTO/SB/44 (08-00)
Approved for use through 09/30/2000. OMB 0651-0033
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.

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO : 6,105,013
DATED : August 15, 2000
INVENTOR(S) : Curry et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 3, line 8	Replace "photovoltaic" With -- photo-voltaic --
Column 14, line 18	Replace "FIPS" With -- FIBS --
Column 19, line 49	Replace "COMMON PIN" With -- COMMON_PIN --
Column 27, line 40	Replace "Chance" With -- Change --
Column 28, line 24	Replace "BAD OPTION BYTE" With -- BAD_OPTION_BYTE --
Column 29, line 12	Replace "BAD SIZE" With -- BAD_SIZE --
Column 29, line 24	Replace "BAD OBJECT ID" With -- BAD_OBJECT_ID --

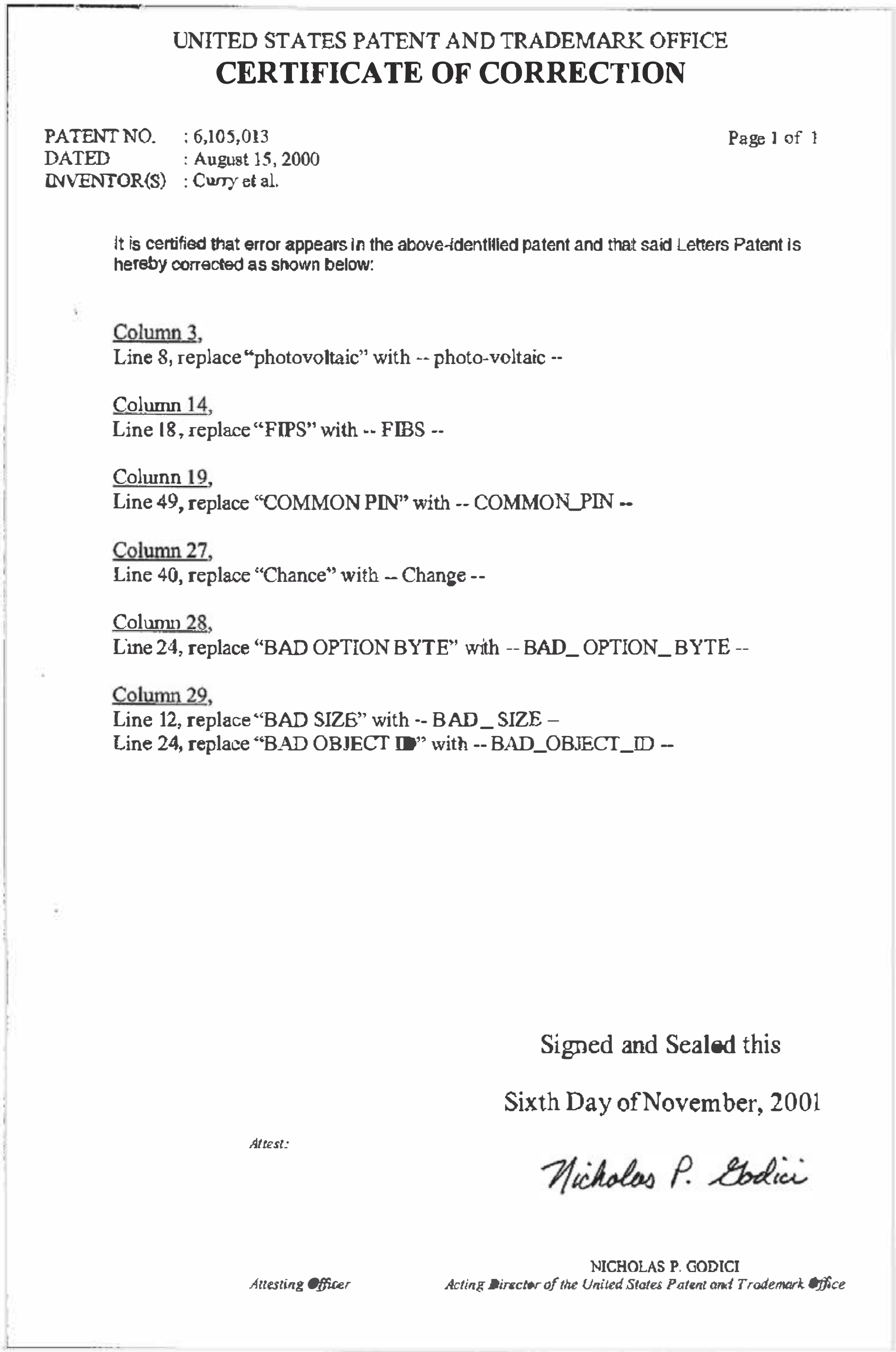
MAILING ADDRESS OF SENDER:

Roger L. Maxwell
1445 Ross Avenue
Suite 3200
Dallas, Texas 75202-2799
20661-00457USC1

PATENT NO. 6,105,013

No. of additional copies
⇨ 1 of 1

Burden Hour Statement: This form is estimated to take 1.0 hour 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 TO: Assistant Commissioner for Patents, Washington, DC 20231.



UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,105,013
DATED : August 15, 2000
INVENTOR(S) : Curry et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 3,
Line 8, replace "photovoltaic" with -- photo-voltaic --

Column 14,
Line 18, replace "FIPS" with -- FIBS --

Column 19,
Line 49, replace "COMMON PIN" with -- COMMON_PIN --

Column 27,
Line 40, replace "Chance" with -- Change --

Column 28,
Line 24, replace "BAD OPTION BYTE" with -- BAD_ OPTION_ BYTE --

Column 29,
Line 12, replace "BAD SIZE" with -- BAD_ SIZE –
Line 24, replace "BAD OBJECT ID" with -- BAD_OBJECT_ID --

Signed and Sealed this

Sixth Day of November, 2001

Attest:

Nicholas P. Godici

Attesting Officer

NICHOLAS P. GODICI
Acting Director of the United States Patent and Trademark Office

#19

Jenkens & Gilchrist

A PROFESSIONAL CORPORATION

1445 Ross Avenue
Suite 3200
Dallas, Texas 75202

(214) 855-4500
Facsimile (214) 855-4300

www.jenkens.com

Austin, Texas
(512) 499-3800

Chicago, Illinois
(312) 425-3900

Houston, Texas
(713) 951-3300

Los Angeles, California
(310) 820-8800

New York, New York
(212) 704-6000

San Antonio, Texas
(210) 246-5000

Washington, D.C.
(202) 326-1500

Roger L. Maxwell
(214) 855-4787
rmaxwell@jenkens.com

Box Certificate of Correction
Commissioner of Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING

I hereby certify that this paper or fee is being deposited with the U.S. Postal Service as first class mail on the date indicated below and is addressed to: Box Certificate of Correction, Assistant Commissioner of Patents, Washington, D.C. 20231

Date 6-15-01

Signature

Re: Applicant(s): Curry, et al.
U.S. Patent No.: 6,105,013
Issued: August 15, 2000
For: METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS
Docket No.: 20661-00457USC1

Dear Sir or Madam:

Transmitted for filing with the Patent and Trademark Office are the following documents for the above-referenced patent:

1. Request for Certificate of Correction of Patent to correct typographical errors in the patent, which does not introduce any new matter;
2. Form PTO-1050 (in duplicate); and
3. an acknowledgment postcard.

Please address all related communication to:

Roger L. Maxwell
Jenkens & Gilchrist, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799

In the event there is an under or over-payment, please debit or credit our Deposit Account #10-4447.

Respectfully submitted,

Roger L. Maxwell
Reg. No. 31,855

RLM/cg
Enclosures

RAM Fee History Query

Revenue Accounting and Management

Name/Number: 09041190 Total Records Found: 6

Start Date: Any Date End Date: Any Date

Accounting Date	Sequence Num.	Tran Type	Fee Code	Fee Amount	Mailroom Date	Payment Method
03/18/1998	00000051	1	101	$790.00	03/10/1998	DA 040031
11/09/1998	00000143	1	115	$110.00	11/09/1998	OP
04/20/1999	00000076	1	142	$1,210.00	04/16/1999	OP
04/20/1999	00000077	1	561	$30.00	04/16/1999	OP
09/16/1999	00000008	1	142	-$1,210.00	04/16/1999	OP
09/16/1999	00000009	1	561	-$30.00	04/16/1999	OP

RAM Fee History Query

Revenue Accounting and Management

Name/Number: 09041190   Total Records Found: 4

Start Date: Any Date   End Date: Any Date

Accounting Date	Sequence Num.	Tran Type	Fee Code	Fee Amount	Mailroom Date	Payment Method
03/18/1998	00000051	1	101	$790.00	03/10/1998	DA 040031
1 1/09/1998	00000143	1	115	$110.00	11/09/1998	OP
04/20/1999	00000076	1	142	$1,210.00	04/16/1999	OP
04/20/1999	00000077	1	561	$30.00	04/16/1999	OP

```
     (FILE 'USPAT' ENTERED AT 16:27:53 ON 29 JUL 1998)
L1         2972 S (380*23 OR 380*24 OR 380*25 OR 235*379 OR 235*380)/CCLS
L2        14706 S (DATA(W)CARRIER OR CARD# OR SMARTCARD#)/TI,AB
L3        16592 S L1 OR L2
L4         2517 S L3 AND MICROPROCESSOR#
L5           90 S L4 AND (COPROCESSOR# OR CO(W)PROCESSOR#)
L6        13038 S ENCRYPT? OR ENCIPHER? OR SCRAMBL? OR CRYPTO?
L7        15536 S 380*?/CCLS OR L6
L8           30 S L5 AND L7

     FILE 'JPOABS' ENTERED AT 16:31:35 ON 29 JUL 1998
L9        32366 S DATA(W)CARRIER OR CARD# OR SMARTCARD#
L10         313 S L9 AND MICROPROCESSOR#
L11           0 S L10 AND (COPROCESSOR# OR CO(W)PROCESSOR#)
L12        2714 S L6
L13           5 S L10 AND L12

     FILE 'USPAT' ENTERED AT 16:33:36 ON 29 JUL 1998
```

PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 1997

Application or Docket Number 09/041190

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY TYPE □		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE	FEE		RATE	FEE
BASIC FEE	▨	▨	▨	395.00	OR	▨	790.00
TOTAL CLAIMS	9 minus 20 =	*	x$11=		OR	x$22=	
INDEPENDENT CLAIMS	1 minus 3 =	*	x41=		OR	x82=	
MULTIPLE DEPENDENT CLAIM PRESENT			+135=		OR	+270=	
			TOTAL		OR	TOTAL	790

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
Total	* Same	Minus	**	=	x$11=		OR	x$22=	
Independent	*	Minus	***	=	x41=		OR	x82=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+135=		OR	+270=	
					TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1)		(Column 2)	(Column 3)					
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
Total	* 18	Minus	** 20	= —	x$11=		OR	x$22=	
Independent	* 2	Minus	*** 3	= —	x41=		OR	x82=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+135=		OR	+270=	
					TOTAL ADDIT. FEE	—	OR	TOTAL ADDIT. FEE	—

19

AMENDMENT C

	(Column 1)		(Column2)	(Column 3)					
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
Total	* 18	Minus	* 20	= —	x$11=		OR	x$22=	
Independent	* 2	Minus	*** 3	= —	x41=		OR	x82=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+135=		OR	+270=	
					TOTAL ADDIT. FEE	—	OR	TOTAL ADDIT. 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.

*U.S. Government Printing Office 1987 - 430-371/69194

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/15471

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G07F19/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 458 306 A (TOSHIBA) 27 November 1991 see abstract; claims; figures 1-7 ---	1,4
Y X A	EP 0 186 981 A (IBM) 9 July 1986 see abstract; claims; figures 1-7 ---	1,4 21 8,9,13
Y	EP 0 194 839 A (TOSHIBA) 17 September 1986 see abstract; claims; figures see page 9, line 1 - page 15, line 24 see page 18, line 26 - page 19, line 23 ---	1,2, 6-10, 12-14, 17,18

-/--

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle 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" 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 documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

2

Date of the actual completion of the international search 21 March 1997	Date of mailing of the international search report 02. 04. 97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer David, J

Ir _ RNATIONAL SEARCH REPORT

International Application No
PCT/US 96/15471

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 44 06 602 A (DEUTSCHE BUNDESPOST TELEKOM) 7 September 1995	1,2, 6-10, 12-14, 17,18
A	see the whole document ---	4,21
A	EP 0 294 248 A (ELECTRONIQUE SERGE DASSAULT) 7 December 1988 see the whole document ---	1-3,6-9, 12-20
A	EP 0 624 014 A (A.M. FISCHER) 9 November 1994 see abstract; claims; figures ---	1,4,5,22
A	EP 0 337 185 A (SPA SYSPATRONIC) 18 October 1989 ---	
A	WO 93 08545 A (JONHIG) 29 April 1993 ---	
A	EP 0 172 670 A (TECHNION RESEARCH & DEVELOPMENT) 26 February 1986 -----	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 96/15471

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0458306 A	27-11-91	JP 4033085 A	04-02-92
EP 0186981 A	09-07-86	G8 2168514 A	18-06-86
		DE 3585439 A	02-04-92
		JP 61139878 A	27-06-86
		US 4731842 A	15-03-88
EP 0194839 A	17-09-86	JP 6091526 8	14-11-94
		JP 62000140 A	06-01-87
		US 4862501 A	29-08-89
DE 4406602 A	07-09-95	NONE	
EP 0294248 A	07-12-88	FR 2615638 A	25-11-88
		DE 3887207 D	03-03-94
		DE 3887207 T	26-05-94
		ES 2048211 T	16-03-94
EP 0624014 A	09-11-94	US 5422953 A	06-06-95
		AU 666424 8	08-02-96
		AU 5778194 A	17-11-94
		CA 2120665 A	06-11-94
		JP 7254897 A	03-10-95
EP 0337185 A	18-10-89	AT 123347 T	15-06-95
		DE 58909263 D	06-07-95
		ES 2072870 T	01-08-95
		US 4985921 A	15-01-91
WO 9308545 A	29-04-93	AT 145744 T	15-12-96
		AU 663739 8	19-10-95
		AU 2888692 A	21-05-93
		BR 9205416 A	17-05-94
		CA 2098481 A	17-04-93
		DE 69215501 D	09-01-97
		EP 0567610 A	03-11-93
		JP 6503913 T	28-04-94
		PL 299825 A	18-04-94
		US 5440634 A	08-08-95

IN ꞮNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 96/15471

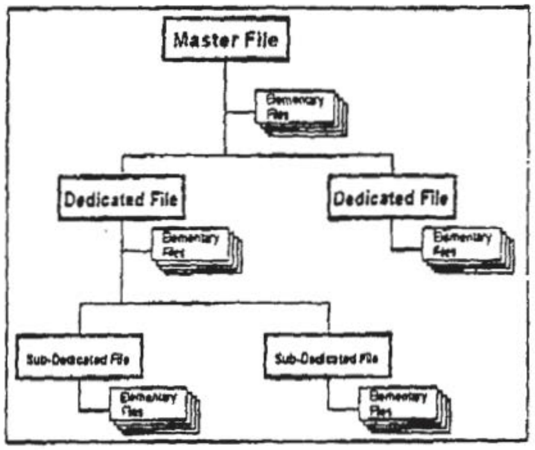
Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0172670 A	26-02-86	JP 61094177 A	13-05-86

CP8® PRODUCTS

CRYPTO CARD

The Bull CP8 Crypto Card has unique cryptographic functionalities and conforms to the latest work of ISO on operating system standardisation.

This multi-directory and multi-file card is particularly interesting for its high security, flexibility and capability of evolving. The users of this card will benefit from the numerous security and cryptographic functions in symmetric and asymmetric cryptography.



Memory organisation

Conforming to the latest works in ISO, the card operating system manages the user memory as a tree of directories on three levels. The root directory is called the Master File and is mandatory. Each directory supports a number of Elementary Files which can be of four different types (secret, access control, public or working files). These files differ in their contents and the way they may be accessed. Each Elementary file is optional.

Flexibility

Directories and files may be added at any time during the active life of the card. They may also be invalidated to end their use. There is no limitation to the number of directories and files.

Specifications

This new Crypto Card of Bull CP8 has a 20 Kbits EEPROM memory. It also includes a co-processor and very large size of ROM and RAM memories for the best performances.

Cryptographic functionalities

Crypto Card has specific cryptographic commands for its different algorithm: DES, RSA and Zero-Knowledge. The following functionalities can be performed:

- Authentication with DES, RSA or Zero-Knowledge
- Ciphering with DES, RSA
- Signature with DES (MAC), RSA
- Secured key exchange with RSA

Security

Independence & Control system

Each directory may be independently protected, providing it has its own control system which consists of :

- a set of keys and codes in their respective secret files
- an access control file
- a number of protection parameters

Cardholder codes

The PIN code (Personal Identification Number) is the main cardholder code. A correct PIN opens rights for all the directories present in the card.
An AID code (Alternate IDentification) is dedicated to one directory. A correct submission opens rights for that directory only.

Issuer keys

The primary Issuer Key IK is an essential key of the control system. It is used to gain access to various files and also to unblock the directory's access control file, create new directories/files or invalidate them.

The four Secondary Keys SK0 to SK3 are used to protect working files for writing and reading. The four Erase Keys EK0 to EK3 are used to protect working files for erasing.

Protections

When protections are definable (for working files), they specify a combination of cardholder codes and issuer keys.

DES algorithm

All Keys, security and cryptographic procedures can operate with the DES algorithm which is a public, reversible and symmetricalalgorithm.

Cryptographic calculation keys

The four Authentication keys AK0 to AK3 are used to calculate certificates (cryptograms returned by the card) which may serve as signatures of internal data or to authenticate the card.

The card supports keys dedicated to MAC calculation (Message Authentication Code), used to sign external messages: MAC Generation Keys, GK. Verification Keys, VK, or for both operations, GVK.

The KEXK key is dedicated to key exchanges with RSA algorithm.

Asymmetric algorit ms

The Crypto Card includes RSA, Zero-Knowledge with both public and secret keys. RSA algorithm can be performed on 512 bits keys in less than 0.3s in the card without using the "Chinese Reminders" theorem and therefore giving the highest level of security.

Data structure

Words

The card operating system manages data in blocks of four bytes called words. The user will write a word or erase a group of words. Data may be read byte per byte.
The 32 bits of a word are all usable as information bits.

Validation

When a word is correctly written in memory, it is automatically "validated" by the operating system. This operation consists of writing a bit outside user memory. An incorrectly written word will not be validated and will be signalled as such. Validation also makes overwriting impossible.

The validation of information in the card is a feature unique to Bull CP8 cards.

Validation is very important to guarantee data integrity.

Elementary Files

Secret files

Reading	: forbidden
Writing	: protected
Erasing	: forbidden

A secret file contains a key or a code. It will only be accessed by the operating system for verification.

Working files

Reading	: definable protection
Writing	: definable protection
Erasing	: definable protection

These files contain the application information.

Access control files

Reading	: free
Writing	: forbidden
Erasing	: forbidden

These files managed by the operating system are used to memorise the results of key or code verifications.

Public files

Reading	: free
Writing	: protected
Erasing	: forbidden

These files contain non confidential information such as the serial number of the card.

File creation

Creating a file (or a directory) consists of writing its descriptive header. This header contains all the information necessary for the file management :

- level, type, identifier
- length of file
- protection attributes

Logical addressing

Data stored in a file is addressable relatively to the beginning of that file which must first be selected.

Commands

General purpose commands

Read n bytes
Write one word
Erase n words
Search for profile
Create directory or file
Select directory or file
Read result

Security commands

Generate random number
Submit PIN or AID in clear or encrypted text
Submit key in encrypted text
Secure-write/create/erase
Invalidate directories/files
Write lock

Symmetric cryptographic commands

Calculate certificate
Generate temporary key
Generate MAC
Verify MAC
DES Cipher/Decipher

Specific asymmetric cryptographic commands and performances

Start Zero Knowledge Authentication
Compute Zero-Knowledge Authentication Message

Select RSA public Key
Provide public exponent
Provide Modulus
Select RSA secret key

Make RSA public calculus
Make RSA secret calculus
Chain secret-public RSA calculus

For asymmetric cryptography, the following operations can be performed very quickly making of the Bull CP8 Crypto Card the fastest cryptographic ISO card on the market:

RSA Secret Key Calculation (512bits key)	500ms
RSA Public Key Calculation (512bits key)	130ms
RSA Secret-Public Keys chained Calculation (Authentic encryption)	530ms
DES Key exchange using RSA chained calculation	560ms
Card authentication with Zero-Knowledge Guillou-Quisquater mechanism	330ms

(times calculated at 3.57MHz ISO standard clock frequency, including data exchange at 9600bps ISO standard communication speed)

Environment

Security Modules

To ensure complete security, Bull CP8 has developed Security Modules which are unbreakable safes for the keys of the system. They are programmed to execute the cryptographic functions associated with the cards

Key generation

Bull CP8 proposes services for applications where security is of prime importance :

-creation of keys as half secrets
-creation of mother cards
-personalisation of Security Modules

Personalisation

Bull CP8 proposes for the personalisation of Crypto Card a software called GenerICC, which runs on PC compatibles in a Microsoft WINDOWS 3.0 environment.

GenerICC can be used to determine the card structure, to define the information to be captured, to enter the data which can change from one card to another.

Hardware devices

Bull CP8 proposes a range of connectors, reader/writers, Security Processors, OEM products, all complying with ISO standards and which are compatible with Crypto Card.

Libraries

To help the application developer, Bull CP8 proposes libraries to interface Crypto Cards in different environments (DOS, WINDOWS, OS2, MAC, UNIX) with its range of hardware devices :

-DRIVER to drive the readers
-TBLIB to use the functions of the Crypto Card simply and efficiently for its general purpose functionalities

Compatibility

The Crypto Card is compatible with industry standard TB family of cards for its general purpose and basic security commands. **Therefore all applications running with TB cards can be adapted to the new Crypto Card.**

Specifications

Chip

Technology : HCMOS
CPU : 8 bits

The maker guarantees the following specifications :
Data integrity : 10 years
Write/arase cycles : 10 000

Complete card

Operating temperature :
-30to +60°C

Relative humidity : up to 80% (non condensing, range 10 to 30°C)

Standards/protocols

The Crypto Card strictly comply with the ISO 7816-1,2,3 standards and also to the working draft ISO 7816-4.
It communicates using the half duplex character mode protocol at a speed of 9600 bps, as defined in the ISO 7816-3 standard.

This document gives outline information only. It represents no legal obligation on the part of the [illegible] and may be [illegible] without notice
All trademarks [illegible]
Bull CP8 [illegible]

FRANCE: Bull CP8 - 68, route de Versailles - B.P. 45 - 78430 LOUVECIENNES
Tél.: 33 (1) 3902 44 00 - Fax: 33 (1) 3902 4402

U.S.A. : M.C.T.I. - 15851 North Dallas Parkway - Suite 500 - DALLAS, TX 75248
Tél.: 1 (214) 770 5503 - Fax: 1 (214) 239 7138

PP 023J A01 - October 93 Bull CP8 1993 - DACTYL FRANCE

SGS-THOMSON MICROELECTRONICS

ST16CF54

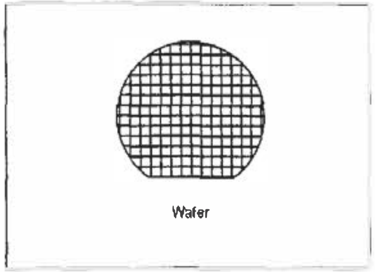
CMOS MCU BASED SAFEGUARDED SMARTCARD IC WITH MODULAR ARITHMETIC PROCESSOR

ADVANCE DATA

- 8 BIT ARCHITECTURE CPU
- 16K BYTES of ROM, SECTORS COMBINATIVE
- 352 BYTES of RAM
- 4K BYTES of EEPROM, SECTORS COMBINATIVE:
  - Highly reliable CMOS EEPROM Technology
  - 10 Years Data Retention
  - 100k Erase/Write Cycles Endurance
  - Protected one time programmable block (32 or 64 bytes)
  - Separate Write and Erase cycle for fast "1" programming
  - 1 to 32 bytes block Erase or Write single cycle programming
- MODULAR ARITHMETIC PROCESSOR
  - Fast modulo N multiplication, squanng and calculation of MONTGOMERY constants.
  - Software selec able operand length (256/512 bit)
  - Double operand operation (1024 bit)
- SERIAL ACCESS, ISO 7816-3 COMPATIBLE
- SINGLE 5V ± 10% SUPPLY VOLTAGE
- POWER SAVING IDLE MODE
- 5 MHz INTERNAL OPERATING FREQUENCY
- VERY HIGH SECURITY FEATURES
- 6 PINS CONTACT ASSIGNMENT as for ISO7816-2
- E.S.D. PROTECTION GREATER than 5000V
- SOFTWARE SUPPORT OPTION, CHIP-MANAGER
  - Standard-Manager
  - Crypto-Manager

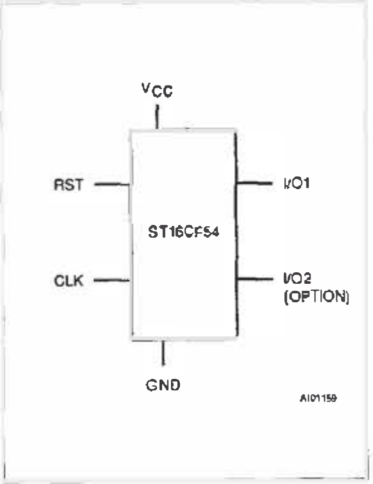
Table 1. Signal Names

CLK	Clock
RST	Reset
I/O1	Data Input / Output
I/O2	Data Input / Output (Option)
V_{cc}	Supply Voltage
GND	Ground



- FAST CRYPTATION PROCESSING
  - 66ms RSA Signature
  - 100ms DSS Signature
  - 200ms DSS Authentification

Figure 1. Logic Diagram



This is advance information on a new product now in development or undergoing evaluation. Details are subjets to change without notice

DESCRIPTION

The ST16CF54, a member of the ST16XYZ family devices, is a serial access microcontroller especially designed for very large volume and cost competitive smartcards applications, where high performance Public Key Algorithms will be implemented, to cut down initiallization and communication costs and to increase security.

Its internal Modular Arithmetic Processor is designed to speed up cryptographic calculations using Public Key Algorithms. It processes modular multiplications and squaring on 256/512 bit operands or a double operand of 1024 bits. The ST16CF54 is based on an SGS-THOMSON 8 bit CPU core including on-chip memories. 352 bytes of RAM, 16K bytes of ROM and 4K of EEPROM.

Both ROM and EEPROM memories can be configured into two sectors. Access rules from any memory section (sector) to any other are setup by User's defined Memory Access Control Matrix.

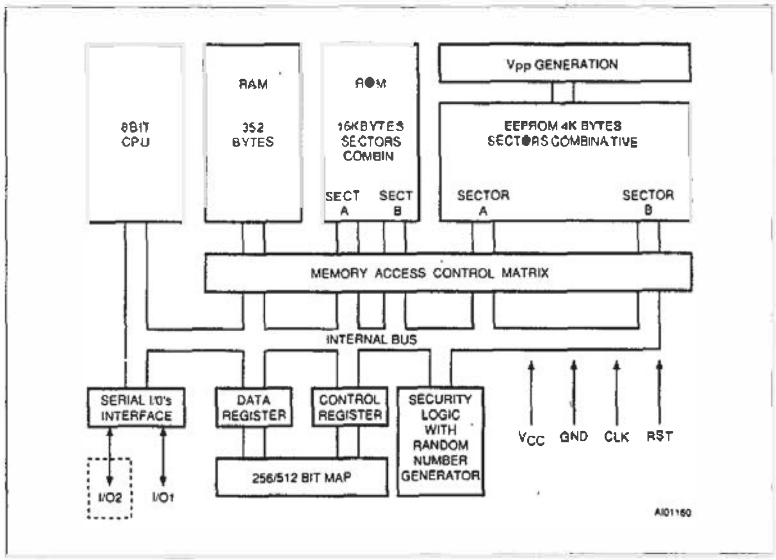
It is manufactured using the high reliable SGS-THOMSON 1μm CMOS EEPROM technology.

As all the other ST16XYZ family members, it is fully compatible with the ISO standards for smartcards applications.

Software development and firmware (ROM code/options) generation can be done with the ST16S-EMU development system.

The ST16CF54 can be delivered in 5 inches sawn or unsawn, 180μm or 280μm thickness wafers.

Figure 2. Block Diagram



STANDARD-MANAGER and CRYPTO-MANAGER

The ST16CF54 Manager is an executable code in accordance to the SGS-THOMSON Chip Manager concept, implemented on the ST16CF54 MCU based Smartcard IC. It includes standard commands and cryptographic related commands. It allows easy access to ST16CF54 memories and Modular Arithmetic Processor (MAP) registers:

- through an extensive set of commands,
- through a ROM crypto library located in the system ROM, containing a various set of functions for handling the MAP registers and mathematical/cryptographic calculations.

The ST16CF54 Manager is designed to reduce the time required for the fabrication of any ROM-masked product, using or not cryptographic functions, and to offer the user direct entry to the application, as well as giving easy access to the ST16CF54 product for evaluation.

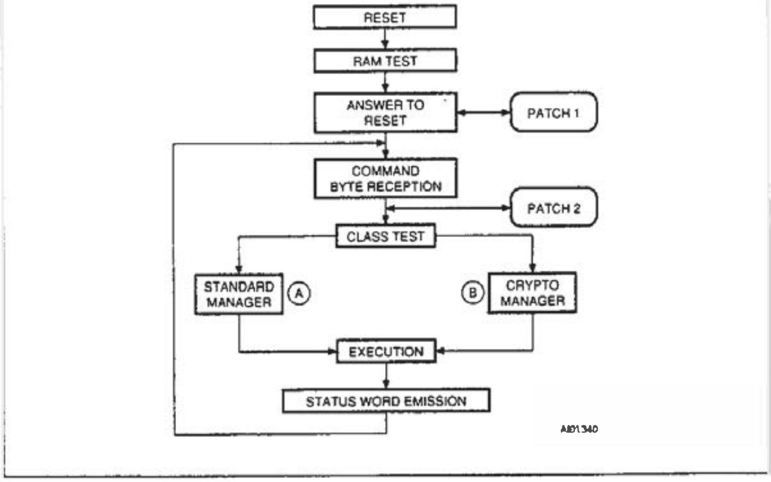
Patch 1 and patch 2 allow modification of the Manager behaviour using some EEPROM tables or subroutines for modifying the Answer To Reset or the received commands.

MANAGER FEATURES

In addition to the standard commands, compatible with ISO 7816-3 standard protocols, the user may set/reset a few controls of the ST16CF54 Manager. These functional modifications are:

- ISO protocol selection inverted or direct convention.
- Output selection: I/O1 or I/O2.
- I/O input: polling or interrupt from stand-by.
- I/O baud rate selection, allowing high baud rate with slow clocks.
- CLK frequency selection, allowing high baud rate with slow clocks.
- Security register management.
- Patches: conditional extension branch

Figure 3. ST16CF54 Manager Flowchart



A - ST16CF54 STANDARD-MANAGER SET OF COMMANDS

Standard commands (class 80h)

D0h WRITE:	Write N bytes in EEPROM.
D2h OV_WRITE:	Over write N bytes in EEPROM.
D4h WRT_RAM:	Write N bytes in RAM or registers.
C0hERASE:	Erase N bytes from EEPROM.
C2h ERA_FEW:	Erase a few bytes from EEPROM.
B2hRD_EEP:	Read N bytes from EEPROM.
B4h RD_RAM:	Read N bytes from RAM or registers.
B6h RD_SERIAL_NB:	Read the 6 first bytes from EEPROM.
E2h CHK_EEP:	Checksum of an EEPROM block.
E4h CHK_ALL:	Checksum of the whole EEPROM
30hEEP_IN:	Execute a subroutine in EEPROM (with incoming parameters).
32h EEP_OUT:	Execute a subroutine in EEPROM (with outgoing parameters).

ROM subroutines for the ST16CF54 Standard-Manager

Some subroutines may be called from EEPROM, allowing the User to rely on the Manager code for low level operations: I/O handling, EEPROM programming or erasing...

B - ST16CF54 CRYPTO-MANAGER SET OF COMMANDS

Crypto-commands (class 88h or 8Ch)

02h:	RFU
12h:	RFU
22h MOV:	Move data from I/O or MAP register or memory to I/O or MAP register or memory.
32h CALC_H:	Calculate H the first Montgomery constant.
34h CALC_J0:	Calculate J0 the second Montgomery constant.
36h CALC_P(B.A)N:	Calculate a P-field modular multiplication.
38h CALC_P(B B)N:	Calculate a P-field modular square.
3Ah:	RFU
3Ch:	RFU
3Eh CALC_B^E_mod_N:	Calculate a modular exponentiation.
42h:	RFU
52hCALC_RN:	Calculate a random number.

Advanced crypto-commands (class 8Ch):

72h:	RFU
74h:	RFU
76h:	RFU
78h:	RFU
7Ah:	RFU

ROM subroutines for the ST16CF54 Crypto-Manager

The Crypto-Manager library contains a large set of functions for handling the MAP registers, loading/unloading data, calculating simple or more complex mathematical expressions, and executing some cryptographic algorithms.

Data and parameters may be passed to and from the functions using several addressing schemes. All features are controlled by the exhaustive and modificable set of crypto commands mentioned above.

Information furnished is believed to be accurate and reliable. However, SGS-THOMSON Microelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SGS-THOMSON Microelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. SGS-THOMSON Microelectronics products are not authorized for use as critical components in life support devices or systems without express written approval of SGS-THOMSON Microelectronics.

Bull CP8 Patents

SGS-THOMSON Microelectronics GROUP OF COMPANIES
Australia - Brazil - China - France - Germany - Hong Kong - Italy - Japan - Korea - Malaysia - Malta - Morocco - The Netherlands - Singapore - Spain - Sweden - Switzerland - Taiwan - Thaialnd - United Kingdom - U.S.A.

SGS-THOMSON
MICROELECTRONICS

ST16xF74

CMOS CRYPTO-COMPUTER FAMILY

ADVANCE DATA

- 8 BIT ARCHITECTURE CPU
- 20K BYTES of ROM
- 608 BYTES oF RAM
- 4K BYTES of EEPROM SECTORS COMBINATIVE:
  - Highly reliable CMOS EEPROM Technology
  - 10 Years Data Retention
  - 100K Erase/Write Cycles Endurance
  - Protected one time programmable block (32 or 64 bytes)
  - Separate Write and Erase cycle for fast "1" programming
  - 1 to 32 bytes block Erase or Write single cycle programming
- SINGLE 5V ± 10% SUPPLY VOLTAGE
- SOPHISTICATED HIGH SECURITY FEATURES
- PROGRAMMABLE 8 BIT PARALLEL HOST BUS INTERFACE
- FIVE I/0 PORTS
  - Two 8 bit ports
  - One 4 bit por
  - Two serial ports
- MODULAR ARITHMETIC PROCESSOR
  - Fast modulo N addition, subtraction, multiplication, exponentiation and calculation of MONTGOMERY constants
  - Software selectable operand length (256/512 bit)
  - Double operand operation (1024 bit)
- REAL RANDOM NUMBER GENERATOR (can generate secret keys on board)
- OPTIONAL DES ACCELERATOR

PQFP64

- 64 PIN POFP PACKAGE
- 512 BIT RSA SIGNATURES with 5MHz EXTERNAL CLOCK in 17ms

DESCRIPTION

The ST16xF74 is a family of safeguarded 8 bit MCU, especially designed for large volume and cost competitive smartcard terminals applications where high performance Public Key Algorithm are implemented, and Secret Keys are generated on board.

Its internal Modular Arithmetic Processor is designed to speed up cryptographic calculation using Public Key Algorithms. It can process modular addition, subtraction and exponentiation on 256/512 bit operands or 1024 bit double operand.

The optional DES Accelerator speeds up the necessary permutation specified by the NIST DEA standards.

The ST16xF74 is based on the SGS-THOMSON ST16XYZ family of 8 bit MCU.

Product Variance

ST16KF74	All fea ies
ST16LF74	All features except DES accelerator
ST16MF74	All features except parallel I/O ports
ST16NF74	All features except DES accelerator and parallel I/O ports

This is advance information on a new product now in development or undergoing evaluation. Details are subjets to change without notice.

_SCRIPTION (cont'd)

On-chip memones include: 608 bytes of RAM, 16K bytes of ROM and 4K bytes of EEPROM. The EEPROM can be configured into any of the following sector conbinations:

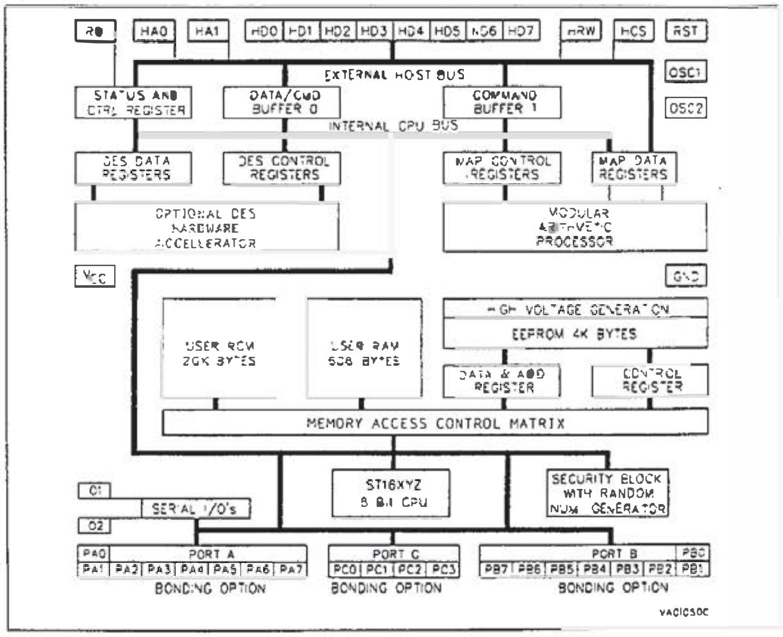
Sector A	Sector B
0	4096
512	3584
1024	3072
2048	2048

.s manulactured using the high reliable SGS-THOMSON 1μm CMOS EEPROM technology.

Software development and firmware (ROM code/options) generation can be done with the SGS-THOMSON ST16XYZ-EMU development system.

The ST16xF74 can be delivered in 64 pin POFP.

Figure 1. Block Diagram



Information furnished is believed to be accurate and reliable. However, SGS-THOMSON Microelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SGS-THOMSON Microelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. SGS-THOMSON Microelectronics products are not authorized for use as critical components in life support devices or systems without express written approval of SGS-THOMSON Microelectronics.

Bull CP8 Patents

SGS-THOMSON Microelectronics GROUP OF COMPANIES
Australia - Brazil - France - Germany - Hong Kong - Italy - Japan - Korea - Malaysia - Malta - Morocco - The Netherlands -
Singapore - Spain - Sweden - Switzerland - Taiwan - Thailand - United Kingdom - U.S.A.

STT Wire Formats and Protocols

version 0.902

5 Oct 1995

1. Introduction

STT (Secure Transaction Technology) is a protocol provided by Microsoft and Visa International to the financial and technical communities for review and comment. Comments on this specification are welcome. Please email comments to STT@microsoft.com

STT is desgned to handle secure payment with bank cards over insecure data transaports like the Internet.The protocol requires only reliable message transport, such as TCP. It features strong, export-approved DES encryption of financial information, direct RSA (TM) encryption of bank card account numbers, and mandatory authentication of all participants, including clients, for reduced financial risk. [1]

IMPORTANT NOTE

This document covers the International Version of the STT protocol, which includes DES encryption of all financial data, **direct RSA encryption of bank card account numbers**, and 40-bit RC4 encryption of the purchasing order form contents and receipt. A US/Canada version of the protocol with **triple-DES** encryption of the order, receipt, and all financial data and direct RSA encryption of bank card account numbers will be documented and published in the near future.

STT is independent of other authentication and privacy protocols. An implementation of STT is being developed by Microsoft and an authentication trust hierarchy will be operated by VISA. Implementation plans and schedules are not covered in this document. This document is a terse technical companion to a much more thoroughgoing exposition of STT for general audiences.

This document presents protocols and message formats for version 1.0 of STT. Protocols are the conditions under which messages are sent. Message formats are presented as they appear "on the wire". The purpose of this document is to facilitate implementation of interoperable STT applications. The target audience is software developers. Section 9 presents the protocols and earlier sections cover formats. All formats are little-endian, favoring performance on Intel X86 and compatible platforms, which make up the majority of the installed base of personal computers. All objects are byte-packed: pad bytes are explicitly denoted.

Encrypted messages are shown in their plaintext forms. A separate section explains STT's use of bulk data symmetric-key cryptography. STT uses RSA public-key cryptography (PKC) to protect bank card numbers and bulk data encryption keys and for digital signatures. Message-creating software should construct plaintext messages, then sign and encrypt them, in that order, as described in detail below. Message-reading software should decrypt, verify signatures, then parse plaintext.

STT Version 1 character string data is ANSI. STT may support UNICODE or other multibyte character sets in future versions.

Note on Randomness

STT uses cryptographic algorithms and globally unique IDs (GUIDs) that require truly random information, as opposed to mere pseudorandom information. STT-compliant implementations shall take advantage of as much physically random information as is available on their platforms. Truly random information must be noise from the world external to the strictly deterministic parts of the machine. The best source of such noise is direct human interaction with the machine. Some information may be collected in real time by asking the user, for example, to type for a while or move the cursor around randomly. This is the preferred method for implementations of STT, though it is recognized that it trades off against user interface concerns. Other information may have accumulated over the lifetime of the machine as users create and delete files, processes, install and remove software, and so on. The following list is a small fraction of the amount of random information that systems programmers can access. The "true entropy" of these sources ranges from high, for those sources that change rapidly in time, to low, for those sources that do not or are likely to be the same from one machine to the next.

- □ the number of files on any mounted hard disks
- □ the numbers of files in each directory, recursively
- □ the amount of free space on each disk
- □ the amount of free space in each free block in every file system free chain
- □ the system time
- □ high-precision clocks on the system board and peripherals
- □ the cursor or mouse pointer location
- □ accumulated physical state information in keyboard input buffers, i/o service queues, video drivers
- □ any performance measurement instrumentation, such as cache miss counts and rates, processor utilization statistics, memory statistics, scheduler statistics, file system statistics, etc.
- □ the state of main memory and peripheral memory on the bus, such as video cards, including such information as the number of heaps, the number of free blocks in each heap, the addresses and sizes of each free block, selected data bits in various memory buffers, the number of items on the clipboard, and so on
- □ the number of tasks in the OS scheduling queue, their task ids, their code base addresses and sizes
- □ customization information, such as the current screen saver name, color specifications for windows.

environment variables, lists of installed software, initialization scripts (like autoexec.bat, win.ini, system.ini, etc., on Microsoft Windows platforms)

□ screen state information, such as the sizes and locations of all windows, the sizes of overlapping and obscured regions

All such data should be melded through a mixing and compression function, such as MD5 or SHA, so that correlations from run to run or boot to boot will be destroyed. XOR is not an adequate mixing function. since it allows reversal of the addition of noise. STT-compliant software shall seed pseudorandom number generators with physically random information and shall frequently update the seed with physically random information. STT-compliant software shall also use seeds of at least 160 bits. See Internet RFC 1750 for general information on randomness.

2. Type Hierarchy and Notation

STT messages are made up of data objects, or just objects. Data objects are instances of data types. Data types include Atoms and Low-Level Composites. A meta-data type called a TLV serves both as a grouping construct and to define higher-level types.

Objects are written in Cambridge Prefix Notation with the type first, followed by an optional literal value and an optional symbolic name that might be used in expository text or later definitions to refer to the object. So, for example, a Byte called bFoo is written as follows:

```
(BYTE bFoo)
```

A BYTE object not needing a name would be written

```
(BYTE)
```

or, where unambiguous, as

```
BYTE
```

Cambridge Prefix Notation also denotes ordered collections or sequences of objects. On the wire, these objects appear in time order; in memory, they appear as byte-packed concatenations. So, for example, A BYTE called bFoo followed by a CString called customerName and DWORD called dwCount is written as follows:

```
((BYTE    bFoo)
 (CString customerName)
 (DWORD   dwCount))
```

If these objects did not need names, the same sequence would be written

```
((BYTE) (CString) (DWORD))
```

A fixed-length array or stream of N objects of type X has type X[N], a pseudo-C notation. So, for example, the type of an array of BYTEs of length cb is written

```
BYTE[cb]
```

The optional value field is written as a numeric or string constant, as in

```
(WORD 0x1234)
```

or

```
   (BYTE[4] "RSA1")
```

denoting a BYTE array holding a character string, or in

```
   (BYTE[4] 0x23 rgbFoo)
```

denoting a BYTE array named rgbFoo and filled with repititions of 0x23.

Complexity is built by defining new types. So, for example, the expression

```
   (define-type BOGEY
     ((BYTE     bFoo)
      (CString customerName)
      (DWORD    dwCount)))
```

gives the name BOGEY to the sequence shown. In later expressions, BOGEY may be used as a stand-in expression for the sequence, shortening the notation and removing redundancy with its concomitant possibility for error. Define-type also admits some automated consistency checks on the notation.

Comments inline to the Cambridge Notation are preceded by semicolons.

3. Atoms

The following are the plaintext formats of STT's data atomic data types.

```
   BYTE: 8-bit unsigned integer.

   WORD: 16-bit unsigned integer, low-order byte first on the wire
      (or, in memory, at lower byte address).  STT writes the number
      of bytes in a WORD as the symbolic constant cbW, which equals 2.

   DWORD: 32-bit unsigned integer, low-order WORD first.  STT writes
      the number of bytes in a DWORD as the symbolic constant cbDW,
      which equals 4.

   QWORD: 64-bit unsigned integer, low DWORD followed by high DWORD.

   DECFLOAT: decimal floating point.  This atom type is reserved for
      future versions of STT.

   RSA1KE: RSA encryption of a 128-byte quantity under a 1024-bit
      modulus.

   RSA.75KE: RSA encryption of a 96-byte quantity under a 768-bit
      modulus.

   RSA.5KE: RSA encryption of a 64-byte quantity under a 512-bit
      modulus.

   CString: character count followed by string data (ANSI chars).
      Character count is contained in either a byte, 3 bytes, or 7
      bytes, as follows:

      1.  If the first byte is between 0 and 0xFE, inclusive, this is
          the character count.
```