Apple Inc.

v.

Aire Technology Ltd.

IPR2022-01137, U.S. Patent No. 8,581,706

Patent Owner's Demonstrative Exhibits

October 2, 2023

Ex. 2013

Why Petition Fails

1. A POSITA would not be motivated to combine *Guthery* with *Nozawa* because the proposed combination contradicts *Guthery's* goal of tightly coupling the execution of applications with management of limited RAM memory. [Grounds 1, 2]

2. A POSITA would not be motivated to combine *Guthery* with *RFID Handbook* because the proposed combination leaves *Guthery's* RAM memory, which cannot be segmented, vulnerable to security risks. [Grounds 2, 4]

Grounds 1, 2: POSITA Would Not Combine *Guthery* & *Nozawa*

No Motivation to Combine *Guthery* with *Nozawa*

1. A method for contactless communication of a reading device with at least two communication-ready applications located on a portable data carrier, comprising the steps:

generating a first communication-readiness signal to the reading device for a first of the at least two applications, the communication-readiness signal comprising a first identification number which is assigned to the first of the at least two applications and indicates to the reading device the communication readiness of said first application, and

generating a second communication-readiness signal to the reading device for a second of the at least two applications, the second communication-readiness signal comprising a second identification number different from the first identification number, which is assigned to said second application and indicates to the reading device the communication readiness of said second application, and

storing information in a nonvolatile memory of the data carrier about which of the at least two applications was last selected for further communication by the reading device,

wherein the reading device selects for further communication one or more of the at least two applications via the identification numbers assigned to the applications.

'706 Patent (Ex. 1001), claim 1; *see also* claim 11.

Guthery's Goal of Managing Limited Resources

> A system and method is hereby disclosed for simultaneously communicating with multiple individual applications on a smart card. The system and method employs fixed-size data packets and tightly couples the execution of applications and thereby communication with them with efficient management of the smart card's limited RAM memory.

Guthery (Ex. 1005), 2:52-58.

> The primary purpose of the card manager **34** is to make the most efficient use of the limited RAM **14** in a smart card, the modest computational capabilities of the smart card and the relatively slow physical communication channel between the smart card and the outside world.

Guthery (Ex. 1005), 10:42-46.

Guthery's Utilizes One or Multiple Packets

> In one particular embodiment, all communication with the card manager **34** and hence with applications **32** on the smart card is formatted as packets of fixed number of bytes, e.g., sixteen bytes.

Guthery (Ex. 1005), 7:43-46.

> In addition, the high bit **54** of the second byte holds the value 1 to indicate that this packet is not the last packet of a series of packets comprising this data transfer. If the high bit **54** is 0, then this is last packet, and perhaps the only packet, of the data transfer. A sequence of packets with all but the last having the high bit **54** of the second byte set to 1 and the last packet having the bit **54** set to 0 is called a "packet chain."

Guthery (Ex. 1005), 7:58-65.

Guthery's Packet-by-Packet Control

> Upon receipt of a Request-to-Send packet **70**, the card manager **34** notifies each of the listed applications in turn that incoming data is available. The host then expects to receive a permission-to-send packet, described next, from each of these applications, when the application is ready to receive this data.

Guthery (Ex. 1005), 9:7-12.

> The card manager **34** adopts the convention that each application **32** is programmed to explicitly determine its own input, output and temporary storage memory requirements.

Guthery (Ex. 1005), 9:26-29.

> In one embodiment, the original request to send packet contains an indication of the size of the message, e.g., the total number of bytes that the host seeks to send to an application. Because packets are a fixed size, the application can determine how many packets to expect and therefore how many permissions to send it must grant to the host to receive the entire message.

Guthery (Ex. 1005), 12:65-13:4.

Guthery's Packet-by-Packet Control – cont'd

When an application's memory needs are satisfied, the application issues a Permission-to-Send packet **80**. The terminal or host computer must be in possession of such a packet in order to send data to the application. In one embodiment, one permission is required for each packet.

Guthery (Ex. 1005), 9:35-39.

A permission is needed from the application for each and every packet of a multi-packet request, because the application may be able to process the packets as they arrive. Thus, an application may require only one buffer or it may need to have a number of blocks sufficient to handle the entire request allocated at one time to process the request. Neither the sender for the operating system can know which of these two cases apply in any particular situation. Therefore, it is up to the smart-card application to strobe the packets onto the card one at a time.

Guthery (Ex. 1005), 13:5-14.

Guthery's Exemplary Cases

- Executing single application with single packet input and single packet output; *see* Figs. 14A-14B.

FIG. **14** is a schematic diagram of a timeline **200**, with time going down, illustrating the operation of an embodiment of the present invention for the simple exemplary case of a host communicating with one application on the smart card.

Guthery (Ex. 1005), 12:17-22.

- Executing two applications simultaneously, each with single packet input and single packet output; *see* Figs. 15A-15D.

FIG. **15** is a schematic diagram of a timeline **300**, with time going down, illustrating the operation (steps **302**–**388**) of an embodiment of the present invention for an exemplary case of simultaneous communication between a host and two applications, Application M and Application N, on the smart card.

Guthery (Ex. 1005), 12:54-59.

Guthery's Exemplary Cases – cont'd

- Executing single application with single packet input and multiple packet output; *see* Figs. 16A-16B.

- Executing single application with multiple packet input and multiple packet output, where processing of the input packets only begins after all input packets have been received; *see* Figs. 17A-17C.

FIG. **16** is a schematic diagram of a timeline **400**, with time going down, illustrating the operation (steps **402–452**) of an embodiment of the present invention for an exemplary case of communication between a host and a single application that provides a multi-packet chained response.

Guthery (Ex. 1005), 12:60-64.

FIG. **17** is a schematic diagram of a timeline **800**, with time going down, illustrating the operation (steps **802–866**) of an embodiment of the present invention for an exemplary case of communication with a single application using a multi-packet input and multi-packet output where the entire message, comprising two packets is received before processing by the smart card. Thus, in this example, the application assembles the whole message before performing any processing. This is useful, for example, where the message is encrypted and the encryption depends on the whole message.

Guthery (Ex. 1005), 13:20-30.

Guthery's Exemplary Cases – cont'd

- Executing single application with multiple packet input and multiple packet output, where processing of the input packets begins after the first input packet has been received; *see* Figs. 18A-18D.

FIG. **18** is a schematic diagram of a timeline **900**, with time going down, illustrating the operation (steps **902–972**) of an embodiment of the present invention for an exemplary case of communication with a single application using a multi-packet input and multi-packet response, where message parts are processed by the smart card as they are received. Thus, in this example, the application needs only one buffer because the buffer can be reused to hold each new packet. This is useful, for example, where the application is handed several numbers to be stored.

Guthery (Ex. 1005), 13:43-52.

Guthery's "Embodiment"

- *Guthery's* ubiquitous use of "embodiment" refers to individual aspects or features of the "present invention."
- *Guthery* only discloses a preferred embodiment without an alternative embodiment.

Paper 22, Patent Owner's Sur-Reply at 6-9

No Motivation to Combine *Guthery* with *Nozawa*

- Petition proposes to modify *Guthery* with *Nozawa's* application tracking history to automatically select a particular application upon establishing a new connection with a host.
- Petition ***incorrectly*** asserts the benefit of efficiency gains.
- No efficiency gained because *Guthery* implements a tightly coupled scheduling regimen to efficiently utilize limited RAM.
- Not waiting to receive a Request-to-Send before selecting an application is detrimental to that scheduling regimen.

Paper 17, Patent Owner's Response at 11-15; Paper 22, Patent Owner's Sur-Reply at 1, 15, 16

No Motivation to Combine *Guthery* with *Nozawa*

- Without the Request-to-Send, *Guthery's* applications cannot determine:
  - the size of the message to be received from the host (slide 8)
  - the type of data to be received, e.g., encrypted, numbers for storage (slides 10, 11)
  - the number of buffers the application should request from the card manager (slide 7)
  - how to issue Permissions-to-Send (Figs. 17, 18)
- Modifying *Guthery's* Request-to-Send regimen does not reduce the number of initialization steps as Petitioner asserts.
- Destroys *Guthery's* objective of a tightly coupled scheduling regimen.

Paper 17, Patent Owner's Response at 11-15; Paper 22, Patent Owner's Sur-Reply at 1, 15, 16

No Motivation to Combine *Guthery* with *Nozawa*

- Petitioner points to Figs. 14-15 as limited to single packet communications.
- Petitioner ***incorrectly*** asserts that multiple packet capabilities are a different "embodiment" for *Guthery*.
  - In Figs. 14-18, *Guthery* gives "exemplary cases" to cover all options for either single or multiple packet scenarios in both input and output, not just single packets.
- Petitioner cannot "pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art."
  - *Application of Wesslau*, 353 F.2d 238, 241 (C.C.P.A. 1965).

Paper 22, Patent Owner's Sur-Reply at 1, 10-12

Grounds 2, 4: POSITA Would Not Combine *Guthery* & *RFID Handbook*

No Motivation to Combine *Guthery* with *Nozawa*

20. A contactlessly communicating portable data carrier, comprising at least two applications stored thereon and a communication device configured to control communication between a reading device and the at least two applications,

wherein the communication device is set up to generate communication-readiness signals to the reading device which in each case indicate to the reading device a communication readiness for one of the applications and comprise an identification number assigned to the corresponding communication-readiness application, and

wherein the data carrier is configured as an electronic device with a contactless interface for communication with a reading device and with a plurality of memories, each of the memories having no more than one of the at least two applications stored therein in each case.

'706 Patent, claim 20; *see also* claim 16.

No Motivation to Combine *Guthery* with *RFID Handbook*

- Petition proposes to modify *Guthery* with *RFID Handbook's* segmented EEPROM.
- EEPROM is not *Guthery's* only memory — *Guthery's* RAM cannot be segmented.
  - *Guthery's* RAM "is logically divided into several buffers [that] can be assigned to an application 32 according to the application's needs," *Guthery* at 7:12-15, Fig. 3.
  - The buffers are shared among applications to service all incoming and outgoing data.
- Petition ***incorrectly*** asserts that the proposed combination enhances security by "effectively isolating each application" because data communicated with the host is not isolated by application.
- POSITA would not have recognized any benefit from segmenting *Guthery's* EEPROM memory.

Paper 17, Patent Owner's Response at 1, 2, 17-19; Paper 22, Patent Owner's Sur-Reply at 1, 10-12

Contingent Motion to Amend

Substitute Claims

23. (Proposed substitute for claim 11) A contactlessly communicating portable data carrier, comprising at least two applications stored thereon and a communication device configured to control communication between a reading device and the at least two applications,

wherein the communication device is set up to generate communication-readiness signals to the reading device which in each case indicate to the reading device a communication readiness for one of the applications and comprise an identification number assigned to the corresponding communication-readiness application, ~~and~~

wherein after selection of one of the plurality of applications, subsequent communication between the reading device and the selected application takes place without requiring any further steps, and

wherein the communication device is set up to store information in a nonvolatile memory of the data carrier about which of the at least two applications last communicated with a reading device.

…

Paper 16, Patent Owner's Motion to Amend, Appendix A

Substitute Claims

23. (Proposed substitute for claim 11) A contactlessly communicating portable data carrier, comprising at least two applications stored thereon and a communication device configured to control communication between a reading device and the at least two applications,

wherein the communication device is set up ***to generate communication-readiness signals*** to the reading device which in each case indicate to the reading device a communication readiness for one of the applications and comprise an identification number assigned to the corresponding communication-readiness application, ~~and~~

wherein ***after selection*** of one of the plurality of applications, ***subsequent communication*** between the reading device and the selected application ***takes place without requiring any further steps***, and

wherein the communication device is set up to store information in a nonvolatile memory of the data carrier about which of the at least two applications last communicated with a reading device.

…

Paper 16, Patent Owner Motion to Amend, Appendix A

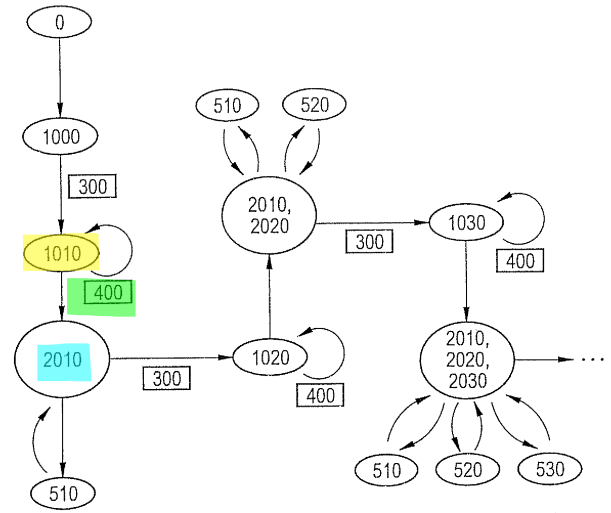
U.S. Patent No. 8,581,706

generate communication-readiness signals

selection of one of the plurality of applications

subsequent communication

FIG 2



Ex. 1002 at 313-314

U.S. Patent No. 8,581,706

[0021] The reading device selects an application for further communication by means of the identification number assigned to the application. The additional selection information optionally assigned to the application can also be used for selection by the reading device. An application selected for further communication is then assigned a session number dynamically by the reading device. Via said session number the application can be addressed uniquely during communication with the reading device. Upon addressing, the session number is so linked in the data carrier by the communication device with the identification number assigned to the application and optionally the additional selection information that the correct application is always addressed upon communication. When an application has been selected for further communication by the reading device, said communication takes place subsequently without requiring any further steps. An application selected for further communication by the reading device is thus then engaged in communication with the reading device.

Ex. 1002 at 290

U.S. Patent No. 8,581,706

[0035] Figure 2 shows a flow chart of a sequence of activities in a first embodiment of the inventive method. The numbers designate individual method steps and states of individual components. When the inventive data carrier 100, which at the onset is in the non-operational state 0, passes into the response field of a reading device 200, it becomes operational 1000 and receives a search signal 300 from the reading device 200. The communication device 70 of the data carrier 100 generates for a first application 10 a communication-readiness signal which comprises the identification number UID1 assigned to the application 10, 1010. Said signal is emitted by the data carrier, and the application 10 is selected for further communication by the reading device 200 in the course of the selection process 400 by means of an anti-collision method.

[0036] While or before the reading device 200 communicates with the application 10 of the data carrier 100, 2010, which it addresses via the session number CID1, 510, it emits further search signals 300, and the communication device 70 of the data carrier 100 generates for a second application 20 a communication-readiness signal comprising the identification number UID2, 1020, and the application 20 is selected for further communication by the reading device 200 in the course of the selection process 400. The reading device 200 is now engaged in communication with the two applications 10 and 20 in parallel, 2010, 2020, which are addressed via the session numbers CID1, 510, and CID2, 520.

[0037] The establishment of communication of the reading device 200 with the application 30 follows analogously by a search signal 300, a communication-readiness signal generated by the communication device 70, 1030, a selection step 400, so that the reading device 200 is finally communicating in parallel with the three applications 10, 20, 30, 510, 520, 530, addressed via the session numbers CID1, CID2, CIDn, 2010, 2020, 2030. As indicated, the method can continue with further applications in the same manner.

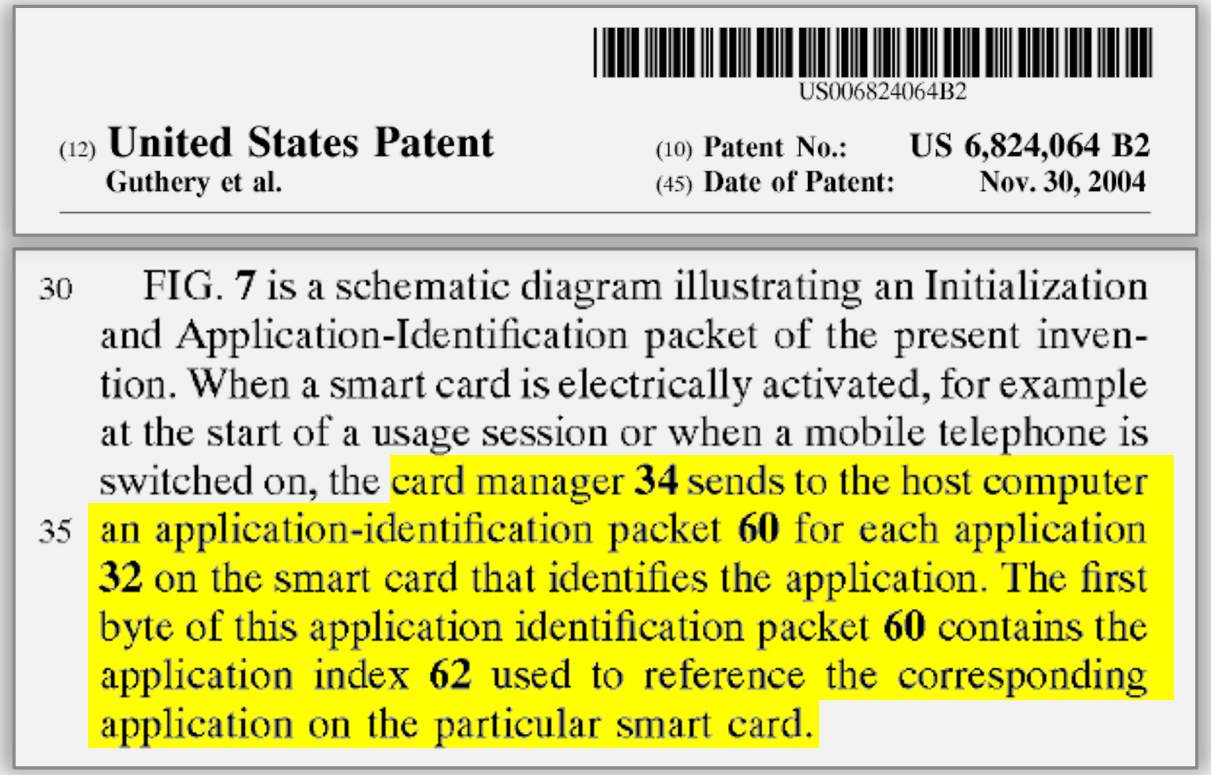
Ex. 1002 at 295-296

U.S. Patent No. 8,581,706

[0043] For the reading device 200 there is also the possibility of briefly switching off the magnetic field to then, if data carriers without their own energy supply are involved, after their restart (power-on reset) select a new data carrier in the response field. According to the invention, the communication device 70 of the data carrier 100 can be set up to store in a nonvolatile memory of the data carrier 100 information about which of the applications 10, 20, 30 last communicated with the reading device 200, which of the applications 10, 20, 30 already completed active communication with the reading device 200, and the like. With the help of such information it is then possible e.g. to generate a communication-readiness signal first for an application 10, 20, 30 that did not communicate with the reading device 200 last, in order e.g. to prevent the same application 10, 20, 30 from always being served first and other applications 10, 20, 30 from possibly having to put up with long waiting periods or not being executed at all. It is also possible, however, to first generate a communication-readiness signal for that application 10, 20, 30 with which the reading device 200 actively communicated last, in order for example to bring to an end a data communication that was commenced but not completed.

Ex. 1002 at 297-298

U.S. Patent No. 6,824,064 (Guthery)



US006824064B2

(12) **United States Patent**
Guthery et al.

(10) **Patent No.: US 6,824,064 B2**
(45) **Date of Patent: Nov. 30, 2004**

FIG. **7** is a schematic diagram illustrating an Initialization and Application-Identification packet of the present invention. When a smart card is electrically activated, for example at the start of a usage session or when a mobile telephone is switched on, the card manager **34** sends to the host computer an application-identification packet **60** for each application **32** on the smart card that identifies the application. The first byte of this application identification packet **60** contains the application index **62** used to reference the corresponding application on the particular smart card.

Ex. 1005 at 8:30-39

U.S. Patent No. 6,824,064 (Guthery)

FIG. **8** is a schematic diagram illustrating a Request-to-Send packet **70** of the present invention. A Request-to-Send packet **70** is sent from the host computer to the card and addressed to the card manager **34**, i.e., the application index **72** is 0. The packet type field holds a Request-to-Send value **74**. The packet's data comprises a list **76** of applications for which packets are waiting on the host side. The list **76** is terminated by a null byte **78**, and possibly followed by one or more filler bytes **99**.

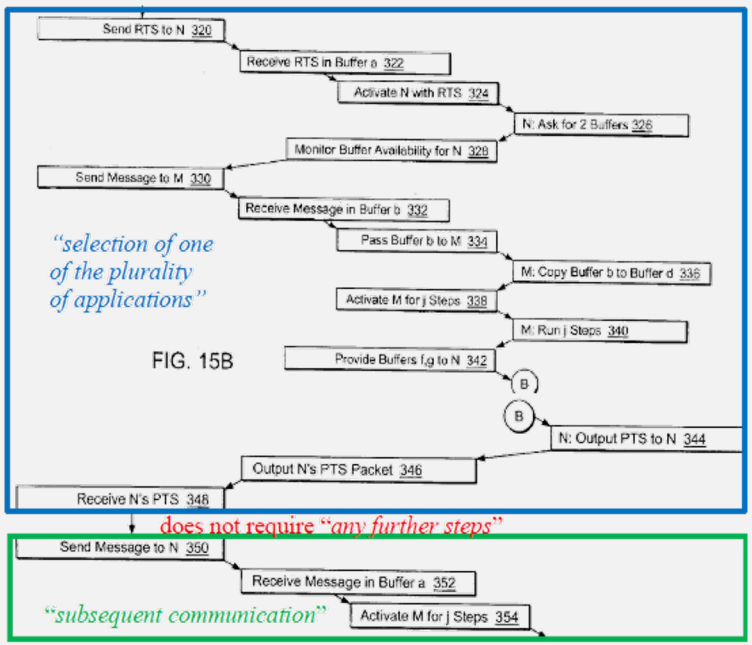
Upon receipt of a Request-to-Send packet **70**, the card manager **34** notifies each of the listed applications in turn that incoming data is available. The host then expects to receive a permission-to-send packet, described next, from each of these applications, when the application is ready to receive this data.

FIG. **9** is a schematic diagram of a Permission-to-Send packet **80** of the present invention. The first byte contains the application index **82** of the application sending the packet **80**. The second byte contains the Permission-to-Send packet type **84**.

Ex. 1005 at 8:65-9:17.

U.S. Patent No. 6,824,064 (Guthery)

"Card manager sends application index…"



Ex.1005, Figs. 15B and 15C (partial, annotated); Ex.1026, ¶ 27.

Ex. 1005 at 8:30-39; Paper 19, Pet. Opp. to Motion to Amend at 15

U.S. Patent No. 6,824,064 (Guthery)

FIG. **15** is a schematic diagram of a timeline **300**, with time going down, illustrating the operation (steps **302–388**) of an embodiment of the present invention for an exemplary case of simultaneous communication between a host and two applications, Application M and Application N, on the smart card.

Ex. 1005 at 12:53-59, 10:6-12, 10:26-31

Substitute Claims

24. (Proposed substitute for claim 12) The data carrier according to claim ~~1~~ 23, wherein the communication device is set up to emit, upon new contacting of a reading device with the data carrier, a communication-readiness signal first for one of the at least two applications that is different from the application designated by the stored information,

wherein the communication device is set up to uniquely address the one or more of the least two applications with a receiving device, and

wherein communication between the reading device and the uniquely addressed application takes place subsequently without requiring any further steps after the communication-readiness signals are generated.

Paper 16, Patent Owner's Motion to Amend, Appendix A

Substitute Claims

25. (Proposed substitute for claim 18) A contactlessly communicating portable data carrier, comprising at least two applications stored thereon and a communication device configured to control communication between a reading device and the at least two applications,

wherein the communication device is set up to generate communication-readiness signals to the reading device which in each case indicate to the reading device a communication readiness for one of the applications and comprise an identification number assigned to the corresponding communication-readiness application,

wherein after selection of one of the plurality of applications, subsequent communication between the reading device and the selected application takes place without requiring any further steps, and

wherein the data carrier is configured as a security module in a device comprising a communication device configured for contactless communication, the security module having software configured to communicate contactlessly via the communication device of the device.

Paper 16, Patent Owner's Motion to Amend, Appendix A

Substitute Claims

26. (Proposed substitute for Claim 20) A contactlessly communicating portable data carrier, comprising at least two applications stored thereon and a communication device configured to control communication between a reading device and the at least two applications,

wherein the communication device is set up to generate communication-readiness signals to the reading device which in each case indicate to the reading device a communication readiness for one of the applications and comprise an identification number assigned to the corresponding communication-readiness application,

wherein after selection of one of the plurality of applications, subsequent communication between the reading device and the selected application takes place without requiring any further steps, and

wherein the data carrier is configured as an electronic device with a contactless interface for communication with a reading device and with a plurality of memories, each of the memories having no more than one of the at least two applications stored therein in each case.

Paper 16, Patent Owner's Motion to Amend, Appendix A