

FILE HISTORY

US 5,940,510

PATENT: 5,940,510

INVENTORS: Curry, Stephen M.
Loomis, Donald W.
Bolan, Michael L.

TITLE: Transfer of valuable information between a
secure module and another module

APPLICATION
NO: US1996594975A

FILED: 31 JAN 1996

ISSUED: 17 AUG 1999

COMPILED: 12 JAN 2012

08/594975

Class	Subclass
380	25

ISSUE CLASSIFICATION

5940510

 5940510

UTILITY SERIAL NUMBER	08/594975	PATENT DATE	AUG 17 1999	PATENT NUMBER	
-----------------------	-----------	-------------	-------------	---------------	--

SERIAL NUMBER	FILING DATE	CLASS	SUBCLASS	GROUP ART UNIT	EXAMINER
			49	2766	White Soren Lofner

APPLICANTS

None
CW

None
CW

CERTIFICATE
 FEB 22 2000
OF CORRECTION

CPA

Foreign priority claimed 35 USC 119 conditions met	<input type="checkbox"/> yes <input checked="" type="checkbox"/> no <i>yes</i>	AS FILED	STATE OR COUNTRY	SHEETS DRWGS.	TOTAL CLAIMS	INDEP. CLAIMS	FILING FEE RECEIVED	ATTORNEY'S DOCKET NO.
Verified and Acknowledged	Examiner's initials	→						

ADDRESS

TITLE

U.S. DEPT. OF COMM./PAT. & TM—PTO-436L (Rev. 12-94)

PARTS OF APPLICATION FILED SEPARATELY		Applications Examiner	
NOTICE OF ALLOWANCE MAILED		CLAIMS ALLOWED	
<i>1-29-99</i>		Total Claims	Print Claim
		6	1
ISSUE FEE		DRAWING	
Amount Due	Date Paid	Sheets Drwg.	Figs. Drwg.
<i>1210.00</i>	<i>4/16/99</i>	8	7
Label Area		Print Fig.	3
		ISSUE BATCH NUMBER <i>040</i>	
		PREPARED FOR ISSUE	
<p><i>Salvatore Cangialosi</i> SALVATORE CANGIALOSI PRIMARY EXAMINER ART UNIT 222 Primary Examiner</p>			
<p>WARNING: The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.</p>			

Form PTO-436A (Rev. 8/92)

Formal Drawings (sheets) set

ISSUE FEE IN FILE

5,940,510

**TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND
ANOTHER MODULE**

Transaction History

Date	Transaction Description
2/23/1996	Initial Exam Team nn
4/1/1996	Notice Mailed--Application Incomplete--Filing Date Assigned
5/21/1996	Application Is Now Complete
6/27/1996	Application Captured on Microfilm
7/10/1996	Case Docketed to Examiner in GAU
8/18/1997	Non-Final Rejection
8/19/1997	Mail Non-Final Rejection
12/1/1997	Response after Non-Final Action
12/1/1997	Request for Extension of Time - Granted
12/10/1997	Date Forwarded to Examiner
2/17/1998	Final Rejection
2/19/1998	Mail Final Rejection (PTOL - 326)
6/11/1998	Request for Extension of Time - Granted
6/11/1998	Continuing Prosecution Application - Continuation (ACPA)
6/11/1998	Mail Express Abandonment (During Examination)
6/11/1998	Express Abandonment (during Examination)
6/11/1998	Amendment after Final Rejection
6/24/1998	Date Forwarded to Examiner
6/26/1998	Advisory Action (PTOL-303)
6/29/1998	Mail Advisory Action (PTOL - 303)
7/22/1998	Date Forwarded to Examiner
8/3/1998	Non-Final Rejection
8/10/1998	Mail Non-Final Rejection
11/16/1998	Response after Non-Final Action
11/20/1998	Date Forwarded to Examiner
11/25/1998	Case Docketed to Examiner in GAU
1/29/1999	Mail Notice of Allowance
1/29/1999	Notice of Allowance Data Verification Completed
1/29/1999	Mail Examiner's Amendment
1/29/1999	Examiner's Amendment Communication
2/11/1999	Preexamination Location Change
4/16/1999	Workflow - Drawings Finished
4/16/1999	Workflow - Drawings Matched with File at Contractor

4/16/1999	Issue Fee Payment Verified
4/16/1999	Workflow - Drawings Received at Contractor
4/16/1999	Workflow - Drawings Sent to Contractor
4/21/1999	Workflow - File Sent to Contractor
7/20/1999	Workflow - Complete WF Records for Drawings
7/26/1999	Application Is Considered Ready for Issue
8/9/1999	Issue Notification Mailed
8/17/1999	Recordation of Patent Grant Mailed
1/27/2000	Post Issue Communication - Certificate of Correction

08/594975

APPROVED FOR LICENSE

PATENT APPLICATION

INITIALS

08/594975



08594975

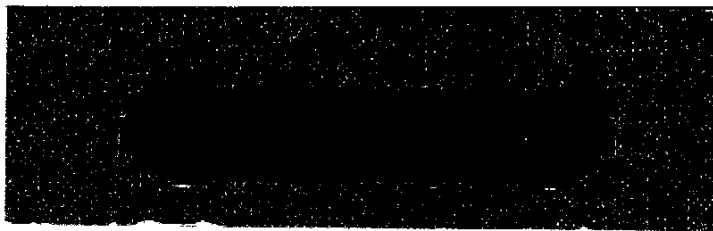
CONTENTS

Date Entered or Counted

Date Received or Mailed

Date Entered or Counted	Description	Date Received or Mailed
	1. Application _____ papers.	
	2. <i>Sturo Deal</i>	
	3. <i>Surcharge, Dec. Assignment</i>	<i>5-6-96</i>
<i>8/18</i>	4. <i>Rejection 3 mos</i>	<i>8-19-97</i>
	5. <i>Req Ext. Time</i> <i>Ext'd 05 mo.</i>	<i>12-1-97</i> <i>COF m/ 11-26-97</i>
	6. <i>Amndt A</i>	<i>12-1-97</i>
<i>2/17</i>	7. <i>3 months Final Rejection</i>	<i>2-19-98</i>
	8. <i>Req. Ext. Time</i>	<i>6-11-98</i> <i>Ext'd 11 mo</i>
	9. <i>Amndt B</i>	<i>6-11-98</i>
<i>6-26</i>	10. <i>Advisory Action</i>	<i>6/29/98</i>
<i>7/21/98</i>	11. <i>ext of time 3</i>	<i>6-11-98</i>
<i>7/21/98</i>	12. <i>119. in CPA 1.03(d)</i>	<i>6-11-98</i>
<i>8/13</i>	13. <i>Rej. (3 mos)</i>	<i>8/10/98</i>
<i>11/19</i>	14. <i>Amndt C</i>	<i>11-16-98</i> <i>COF m/ 11-9</i>
	15. <i>Notice of Allowance</i> <i>EX'S AMDT</i>	<i>1-29-99</i>
<i>7-20-99</i>	16. <i>8 mos</i>	<i>4-16-99</i>
	17. <i>Req for CO of C</i>	<i>10-21-99</i>
	18.	
	19.	
	20.	
	21.	
	22.	
	23.	
	24.	
	25.	
	26.	
	27.	
	28.	
	29.	
	30.	
	31.	
	32.	

(FRONT)



SEARCHED			
Class	Sub.	Date	Exmr.
380	49	8/17/97	dw
↓	24	7/20/98	aw
	23		
	25		
allow to stay		1/99	gpc

SEARCH NOTES		
	Date	Exmr.
APS Text Search 8/17/97	8/17/97	dw
↓	2/10/99	↓
	2/17/99	
	7/28/98	

INTERFERENCE SEARCHED			
Class	Sub.	Date	Exmr.
380	25,49	1/99	gpc

(RIGHT OUTSIDE)

PATENT NUMBER

ORIGINAL CLASSIFICATION

CLASS	SUBCLASS
380	25

APPLICATION SERIAL NUMBER

08/594,975

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)
380	49

APPLICANT'S NAME (PLEASE PRINT)

CURRY et al

IF REISSUE, ORIGINAL PATENT NUMBER

INTERNATIONAL CLASSIFICATION (INT. CL. 4)

H04L	9/00
------	------

GROUP ART UNIT

2746

ASSISTANT EXAMINER (PLEASE STAMP OR PRINT FULL NAME)

PRIMARY EXAMINER (PLEASE STAMP OR PRINT FULL NAME)

Salvatore Cangialosi

PTO 270 (10-84)

ISSUE CLASSIFICATION SLIP

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

Claim	Final	Original	Date
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			

Claim	Final	Original	Date
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			
61			
62			
63			
64			
65			
66			
67			
68			
69			
70			
71			
72			
73			
74			
75			
76			
77			
78			
79			
80			
81			
82			
83			
84			
85			
86			
87			
88			
89			
90			
91			
92			
93			
94			
95			
96			
97			
98			
99			
100			

SYMBOLS

- ✓ Rejected
- = Allowed
- (Through numeral) Canceled
- + Restricted
- N Non-elected
- I Interference
- A Appeal
- O Objected



US005940510A

United States Patent [19]

[11] Patent Number: 5,940,510

Curry et al.

[45] Date of Patent: *Aug. 17, 1999

[54] TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

[56] References Cited

U.S. PATENT DOCUMENTS

5,003,594	3/1991	Shinagawa	380/24
5,150,407	9/1992	Chan	380/4
5,189,700	2/1993	Blandsord	380/23
5,241,599	8/1993	Bellovin et al.	380/21
5,539,825	7/1996	Akiyama et al.	380/24
5,539,828	7/1996	Davis	380/50
5,546,463	8/1996	Caputo et al.	380/25
5,577,121	11/1996	Davis et al.	380/24
5,621,796	4/1997	Davis et al.	380/24
5,787,174	7/1998	Tuttle	380/23

[75] Inventors: Stephen M. Curry, Dallas; Donald W. Loomis, Coppell; Michael L. Bolan, Dallas, all of Tex.

[73] Assignee: Dallas Semiconductor Corporation, Dallas, Tex.

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—Jenkins & Gilchrist

[57] ABSTRACT

The present invention rotates to system, apparatus and method for communicating valuable data from a portable module to another module via an electronic device. More specifically, the disclosed system, apparatus and method are useful for enabling a user to fill a portable module with a cash equivalent and to spend the cash equivalent at a variety of locations. The disclosed system incorporates an encryption/decryption method.

[21] Appl. No.: 08/594,975

[22] Filed: Jan. 31, 1996

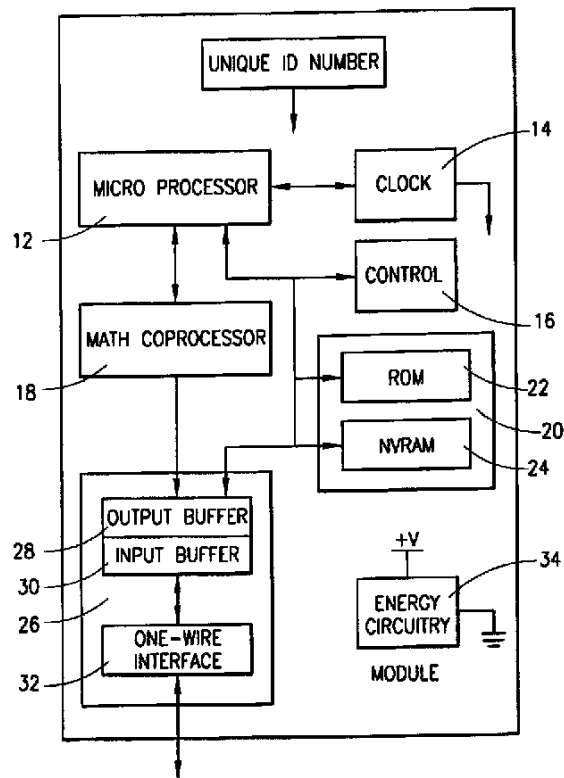
[51] Int. Cl.⁶ H04L 9/00

[52] U.S. Cl. 380/25; 380/49

[58] Field of Search 380/49, 24, 23, 380/25

6 Claims, 8 Drawing Sheets

108



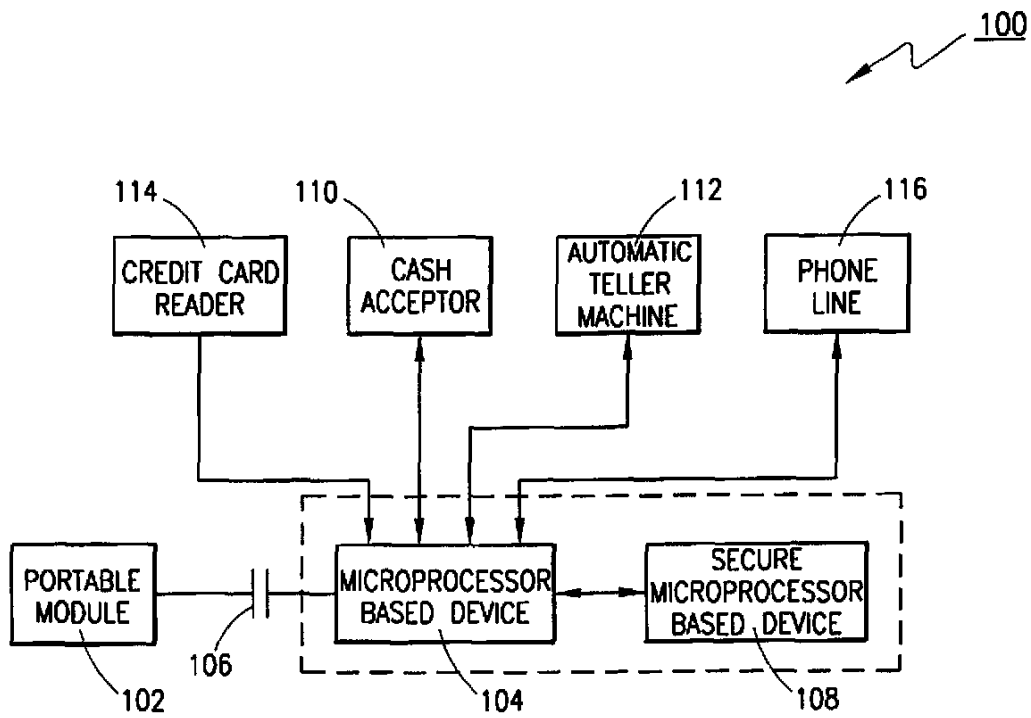


FIG. 1

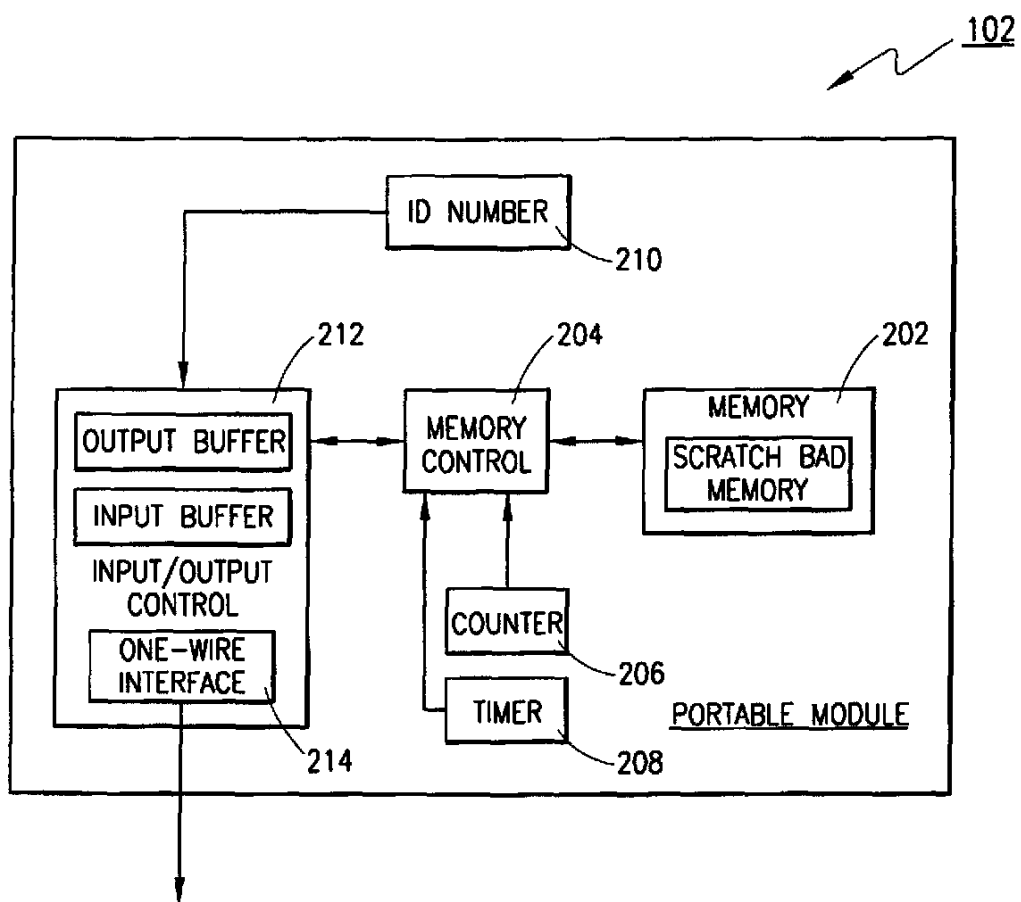


FIG. 2

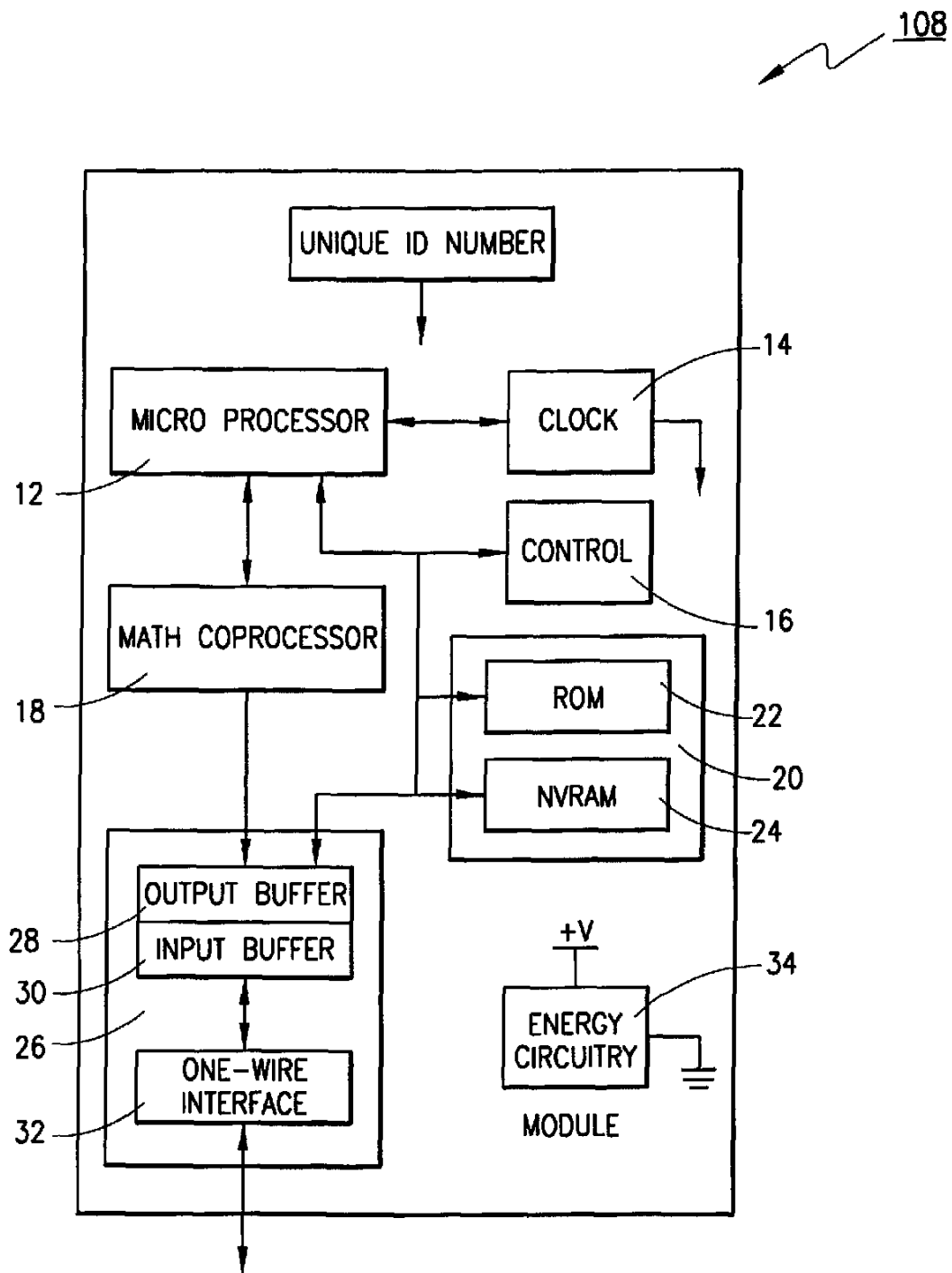
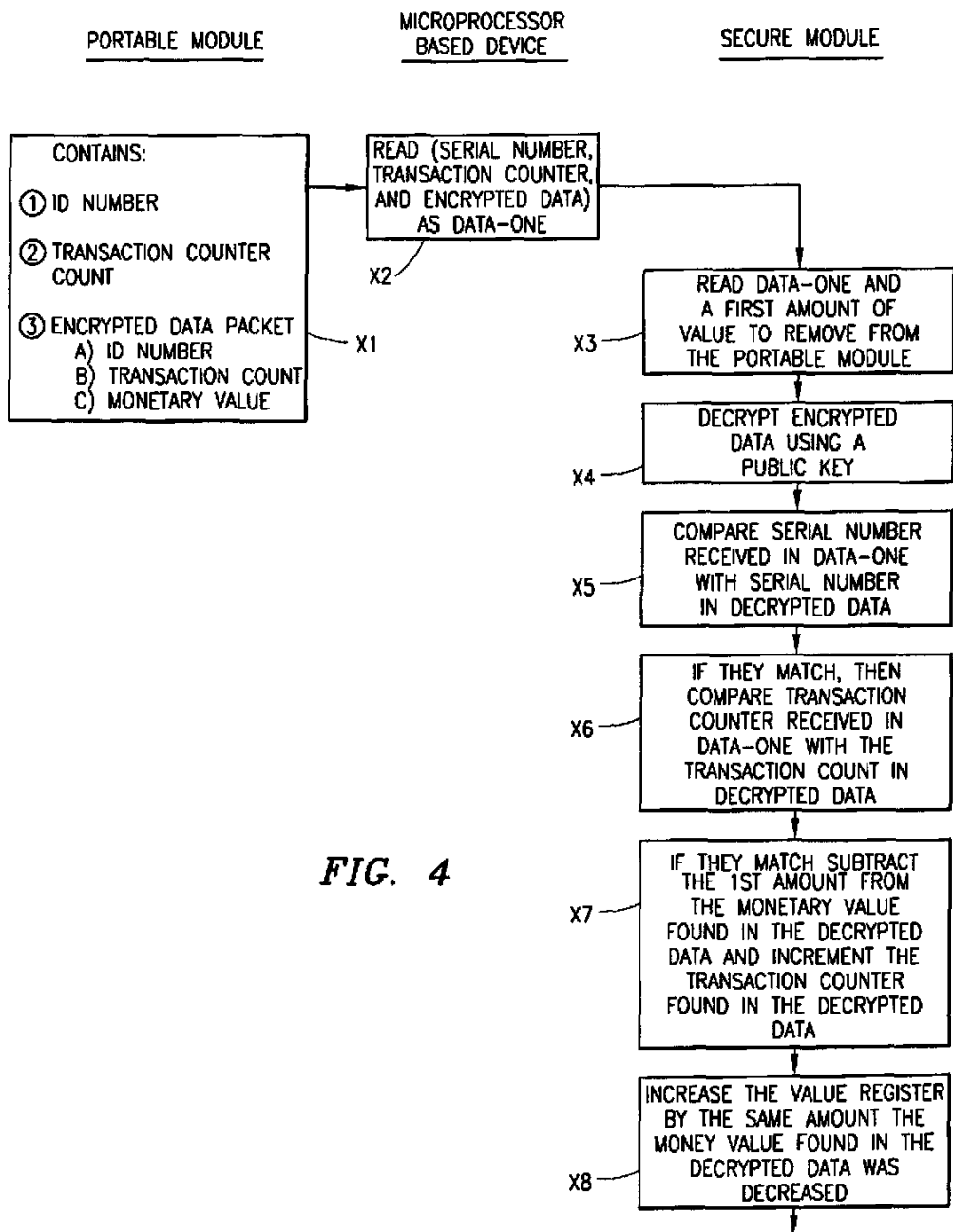


FIG. 3



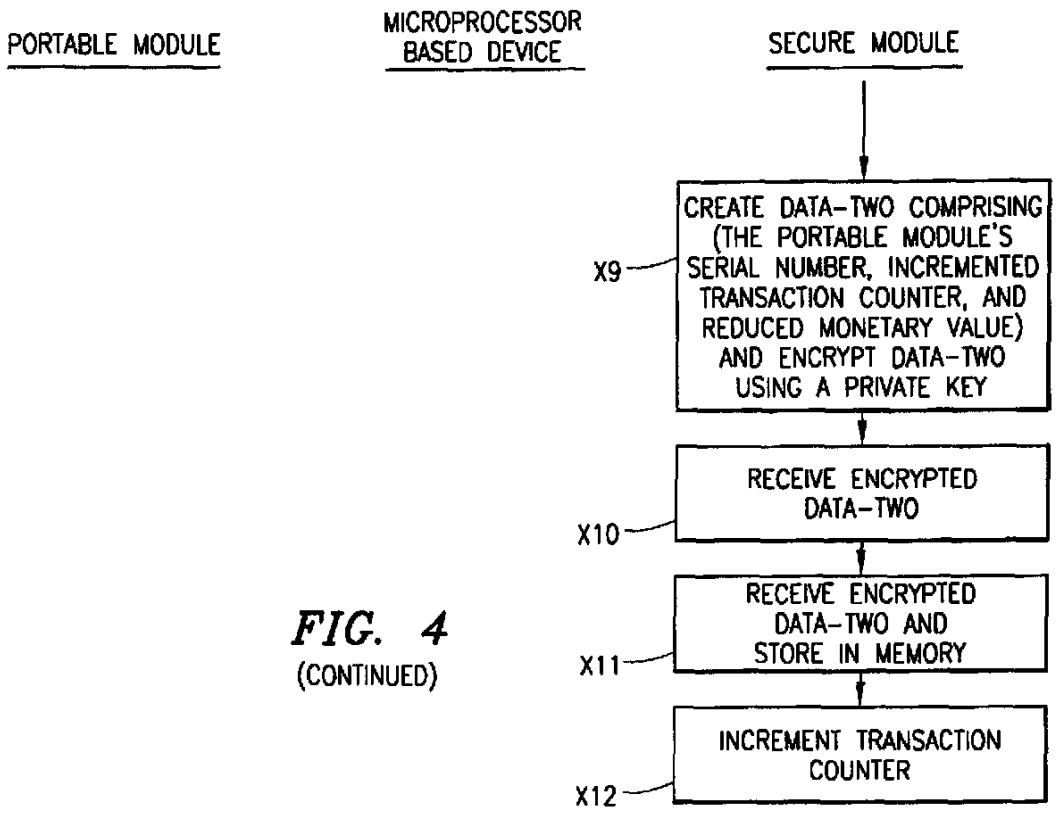


FIG. 4
(CONTINUED)

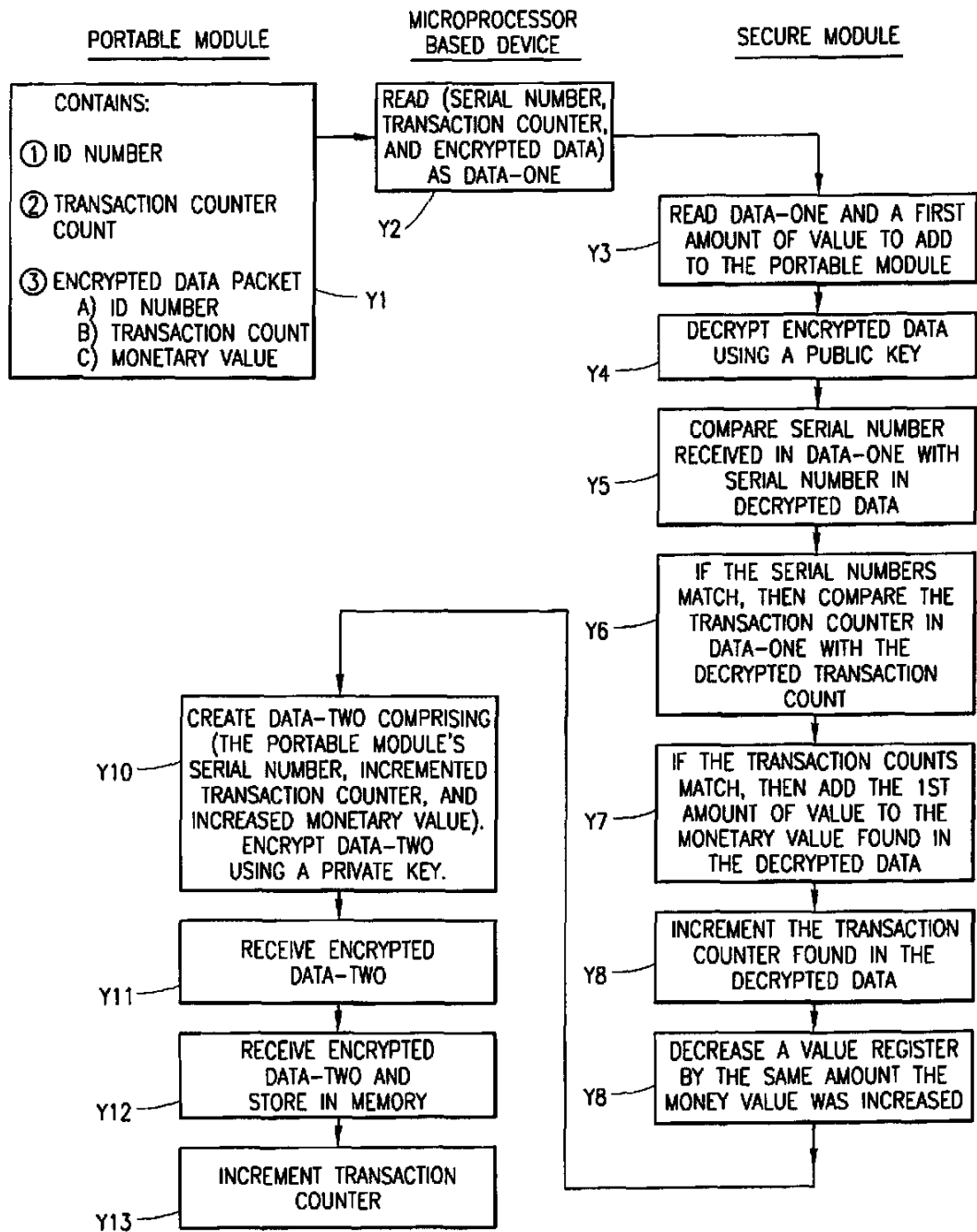


FIG. 5

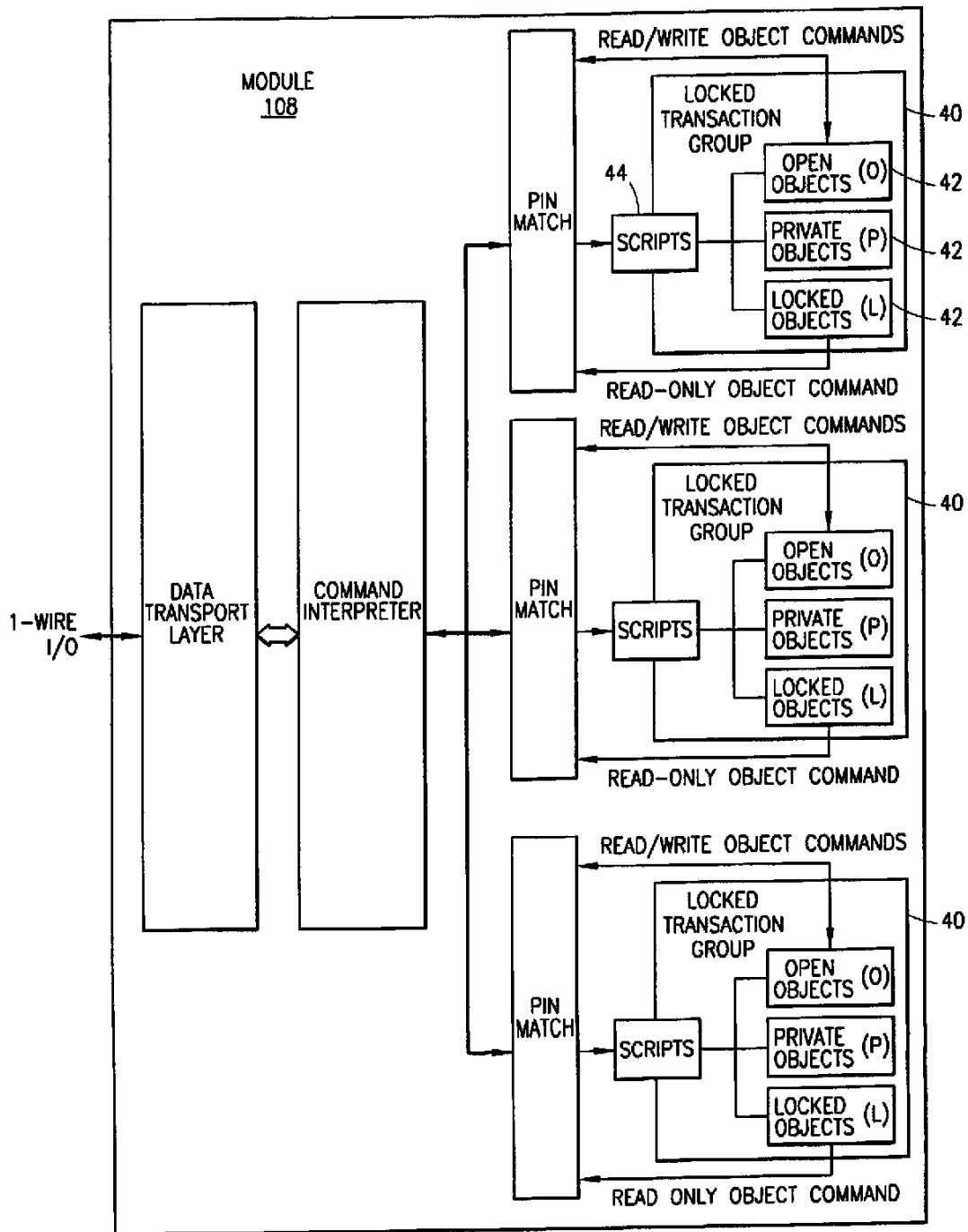


FIG. 6

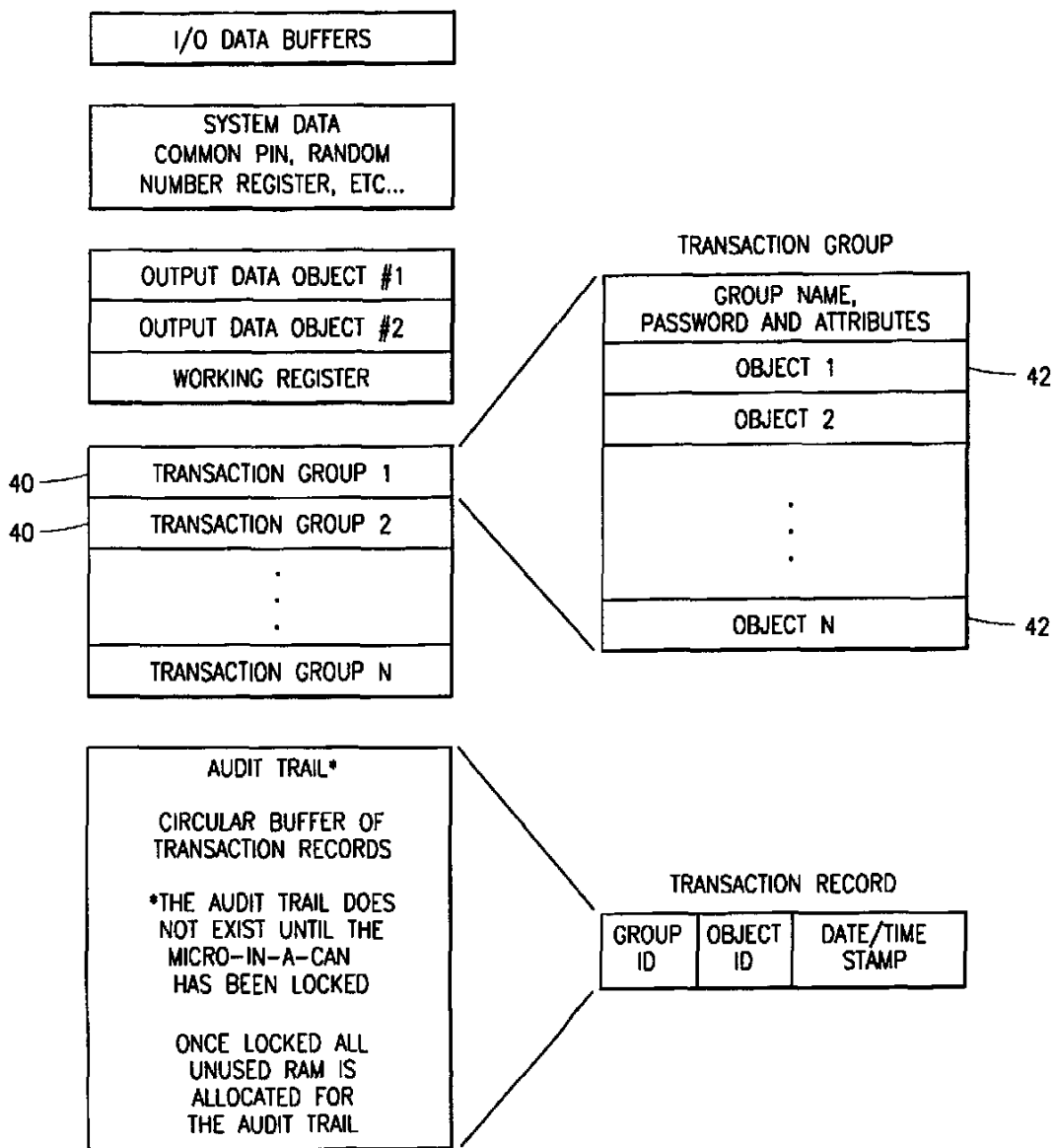


FIG. 7

**TRANSFER OF VALUABLE INFORMATION
BETWEEN A SECURE MODULE AND
ANOTHER MODULE**

**CROSS REFERENCE TO OTHER
APPLICATIONS**

The following applications of common assignee contains related subject matter and is hereby incorporated by reference:

Ser. No. 08/594,983, filed Jan. 31, 1996, entitled METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS; and

Ser. No. 08/595,014, filed Jan. 31, 1996, entitled METHOD, APPARATUS AND SYSTEM FOR TRANSFERRING UNITS OF VALUE.

BACKGROUND OF THE INVENTION

1. Technical Field of the Invention

The present invention relates to a method and system for transferring valuable information securely between a secure module and another module. More particularly, the present invention relates to transferring units of value between a microprocessor based secure module and another module used for carrying a monetary equivalent.

2. Description of Related Art

In the past the preferred means for paying for an item was cash. As our society has become more advanced, credit cards have become an accepted way to pay for merchandise or services. The payment is not a payment to the merchant, but instead is a credit given by a bank to the user that the merchant accepts as payment. The merchant collects money from the bank based on the credit. As time goes on, cash is used less and less, and money transfers between parties are becoming purely electronic.

Present credit cards have magnetic strips to identify the owner of the card and the credit provider. Some credit cards have electronic circuitry installed that identifies the credit card owner and the credit or service provider (the bank).

The magnetic strips installed in present credit cards do not enable the card to be used as cash. That is the modern credit card does not allow the consumer to buy something with the credit card and the merchant to receive cash at the time of the transaction. Instead, when the consumer buys something on credit, the merchant must later request that the bank pay for the item that the consumer bought. The bank then bills the consumer for the item that was bought.

Thus, there is a need for an electronic system that allows a consumer to fill an electronic module with a cash equivalent in the same way a consumer fills his wallet with cash. When the consumer buys a product or service from a merchant, the consumer's module can be debited and the merchant's cash drawer can be credited without any further transactions with a bank or service provider.

SUMMARY OF THE INVENTION

The present invention is an apparatus, system and method for communicating a cash equivalent electronically to and from a portable module. The portable module can be used as a cash equivalent when buying products and services in the market place.

The present invention comprises a portable module that can communicate to a secure module via a microprocessor based device. The portable module can be carried by a consumer, filled with electronic money at an add-money

station, and be debited by a merchant when a product or service is purchased by the consumer. As a result of a purchase, the merchant's cash drawer will indicate an increase in cash value.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be had by reference to the following Detailed Description when taken in conjunction with the accompanying Drawings wherein:

FIG. 1 depicts an exemplary system for transferring valuable information between a module and a secure device;

FIG. 2 is a block diagram of an embodiment of a portable module;

FIG. 3 is a block diagram of an embodiment of a microprocessor based module;

FIG. 4 is an exemplary technique for transferring valuable data securely into a portable module;

FIG. 5 is an exemplary technique for transferring valuable data securely out of a portable module;

FIG. 6 is an exemplary organization of the software and firmware within a secure microprocessor based device; and

FIG. 7 is an exemplary configuration of software and firmware within a secure microprocessor based device.

**DETAILED DESCRIPTION OF A PRESENTLY
PREFERRED EXEMPLARY EMBODIMENT**

FIG. 1 depicts a block diagram of an exemplary system 100 for transferring valuable information to and from a portable module. A portable module 102, which will be described in more detail later, communicates to a microprocessor based device 104. The portable module 102 may contain information that represents units of exchange or a currency equivalent. The microprocessor based device 104 can be any of an unlimited number of devices. For example, the microprocessor based device 104 could be a personal computer, an add-a-fare machine at a train or bus station (similar to those in today's District of Columbia metro stations), a turn style, a toll booth, a bank's terminal, a ride at a carnival, a washing machine at a Laundromat, a locking device, a mail metering device or any device that controls access, or meters a monetary equivalent, etc.

The means for communication 106 between the portable module 102 and the microprocessor based device 104 is preferably via a single wire or contact connection. The single wire connection 106 preferably incorporates a communication protocol that allows the portable module 102 and the microprocessor based device 104 to communicate in a bidirectional manner. Preferably the communication protocol is a one-wire protocol developed by Dallas Semiconductor. It is understood that the means for communicating 106 is not limited to a single wire connection. The communication means 106 could be multiple wires, a wireless communication system, infrared light, any electromagnetic means, a magnetic technique, or any other similar technique.

The microprocessor based device 104 is electrically connected to another microprocessor based device, which is preferably a secure device 108. The term secure device means that the device is designed to contain a secret code and the secret code is extremely difficult to learn. An example of a secure device 108 is explained later in this document.

The microprocessor based device 104 can be connected to a variety of other devices. Such devices include, but are not

limited to a cash acceptor 110, an automatic teller machine (ATM) 112, a credit card reader 114, and a phone line 116.

The cash acceptor 110 is adapted to receive cash in the form of currency, such as dollar bills or coins. The cash acceptor 110, preferably, determines the value of the accepted currency. The cash acceptor 110 communicates to the microprocessor based device 104 and informs the device 104 of how much currency has been deposited in the cash acceptor 110.

The cash acceptor 110 can also be a device which provides currency. That is, the cash acceptor 110 in response to a communication from the microprocessor based device 104, may provide a metered amount of currency to a person.

The credit card reader 114, and ATM 112 can also be attached to the microprocessor based device 104. The credit card reader 114 could be used to read a user's credit card and then, when authorized, either communicate to the microprocessor based device 104 that units of exchange need to be added to the portable module or that units of exchange need to be extracted from the portable module to pay for a good, service or credit card bill.

The ATM 112 may also be connected to the microprocessor based device. Via communications from the ATM 112, the microprocessor based device 104 can be informed that units of exchange need to be added or subtracted from the portable module 102.

Furthermore, it is also possible that the microprocessor based device 104 is connected to a phone line 116. The phone line may be used for a variety of things. Most importantly, the phone line may be used to allow the microprocessor based device 104 to communicate with a network of devices. Such telephonic communication may be for validating transactions or for aiding the accounting of transactions that are performed via the microprocessor based device's 104 aid. It is further understood that the phone line may be any of a vast variety of communication lines including wireless lines. Video, analog, or digital information may be communicated over the phone line 116.

FIG. 2 depicts a preferred exemplary portable module 102. The portable module 102 is preferably a rugged read/write data carrier that can act as a localized data base and be easily accessed with minimal hardware. The module can be incorporated in a vast variety of portable items which includes, but is not limited to a durable micro-can package that is highly resistant to environmental hazards such as dirt, moisture, and shock. The module can be incorporated into any object that can be articulated by a human or thing, such as a ring, bracelet, wallet, name tag, necklace, baggage, machine, robotic device, etc. Furthermore, the module 102 could be attached to a stationary item and the microprocessor based device 104 may be articulated to the portable module 102. For example, the module 102 may be attached to a piece of cargo and a module reader may be touched to or brought near the module 102. The module reader may be part of the microprocessor based device 104.

The portable module 102 comprises a memory 202 that is preferably, at least in part, nonvolatile memory for storing and retrieving vital information pertaining to the system to which the module 102 may become attached to. The memory 202 may contain a scratchpad memory which may act as a buffer when writing into memory. Data is first written to the scratchpad where it can be read back. After data has been verified, the data is transferred into the memory.

The module 102 also comprises a counter 206 for keeping track of the number of transactions the module has per-

formed (the number of times certain data in the memory of the module has been changed). A timer 102 may be provided in the module to provide the ability to time stamp transactions performed by the module. A memory controller 204 controls the reading and writing of data into and out of the memory 202.

The module also may comprise an identification number 210. The identification number preferably uniquely identifies the portable module from any other portable module.

An input/output control circuit 212 controls the data flow into and out of the portable module 102. The input/output control ("I/O") 212 preferably has an input buffer and an output buffer and interface circuitry 214. As stated above, the interface circuitry 214 is preferably a one-wire interface. Again, it is understood that a variety of technologies can be used to interface the portable module 102 to another electronic device. A single wire or single connection is preferred because the mechanics of making a complete connection is simplified. It is envisioned that a proximity/wireless communication technique is also a technique for communicating between the module 102 and another device. Thus, the interface circuit 214 can be a single wire, multiple wire, wireless, electromagnetic, magnetic, light, or proximity, interface circuit.

FIG. 3 depicts a block diagram of an exemplary secure microprocessor based device ("secure device") 108. The secure device circuitry can be a single integrated circuit. It is understood that the secure device 108 could also be a monolithic or multiple circuits combined together. The secure device 108 preferably comprises a microprocessor 12, a real time clock 14, control circuitry 16, a math coprocessor 18, memory circuitry 20, input/output circuitry 26, and an energy circuit 34.

The secure device 108 could be made small enough to be incorporated into a variety of objects including, but not limited to a token, a card, a ring, a computer, a wallet, a key fob, a badge, jewelry, a stamp, or practically any object that can be grasped and/or articulated by a user of the object. In the present system 100, the secure device 108 is preferably adapted to be a trusted certifying authority. That is the secure device 108 is a trusted computer. The secure device 108 comprises a numeric coprocessor 18 optimized for math intensive encryption. The BIOS is immune to alteration and is specifically designed for secure transactions. This secure device 108 is preferably encased in a durable, dirt, moisture and shock resistant stainless steel enclosure, but could be encased in wide variety of structures so long as specific contents of the secure device 108 are extremely difficult to decipher. The secure device 108. The secure device 108 may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device 108 and is not revealed under almost any circumstance. Furthermore, the secure module 108 is preferably designed to prevent discovery of the private key by an active self-destruction of the key upon wrongful entry.

The microprocessor 12 is preferably an 8-bit microprocessor, but could be 16, 32, 64 or any operable number of bits. The clock 14 provides timing for the module circuitry. There can also be separate clock circuitry 14 that provides a continuously running real time clock.

The math coprocessor circuitry 18 is designed and used to handle very large numbers. In particular, the coprocessor will handle the complex mathematics of RSA encryption and decryption or other types of math intensive encryption or decryption techniques.

The memory circuitry 20 may contain both read-only-memory and non-volatile random-access-memory.

Furthermore, one of ordinary skill in the art would understand that volatile memory, EPROM, SRAM and a variety of other types of memory circuitry might be used to create an equivalent device.

Control circuitry 16 provides timing, latching and various necessary control functions for the entire circuit.

An input/output circuit 26 enables bidirectional communication with the secure module 108. The input/output circuitry 26 preferably comprises at least an output buffer and an input buffer. For communication via a one-wire bus, one-wire interface circuitry can be included with the input/output circuitry 26. It is understood that the input/output circuitry 26 of the secure device 108 can be designed to operate on a single wire, a plurality of wires or any means for communicating information between the secure module 108 and the microprocessor based device 104.

An energy circuit 34 may be necessary to maintain stored information in the memory circuitry 20 and/or aid in powering the other circuitry in the module 108. The energy circuit 34 could consist of a battery, capacitor, R/C circuit, photo-voltaic cell, or any other equivalent energy producing circuit or means.

The firmware architecture of the secure module 108 and how it operates within the exemplary system for transferring valuable information, such as units of exchange or currency, between the secure module 108 and a portable module 102 will now be discussed. The secure module 108 provides encryption and decryption services for confidential data transfer through the microprocessor based device 104. The following examples are intended to illustrate a preferred feature set of the secure module 108 and to explain the services that the exemplary system 100 can offer. These applications and examples by no means limit the capabilities of the invention, but instead bring to light a sampling of its capabilities.

I. OVERVIEW OF THE PREFERRED SECURE MODULE 108 AND ITS FIRMWARE DESIGN

Referring to FIG. 3 again, the secure module 108 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, input and output buffers 28, 30 with a one-wire interface 32 for sending and receiving data, 32 Kbytes of ROM memory 22 with preprogrammed firmware, 8 Kbytes of NVRAM (non-volatile RAM) 24 for storage of critical data, and control circuitry 16 that enables the micro controller 12 to be powered up to interpret and act on the data placed in an input data object. The module 108 draws its operating power from a single wire, one-wire communication line. The micro controller 12, clock 14, memory 20, buffers 28, 30, one-wire front-end 32, modular exponentiation accelerator 18, and control circuitry 16 are preferably integrated on a single silicon chip and packaged in a stainless steel micro can using packaging techniques which make it virtually impossible to probe the data in the NVRAM 24 without destroying the data. Initially, most of the NVRAM 24 is available for use to support applications such as those described below. One of ordinary skill will understand that there are many comparable variations of the module design. For example, volatile memory might be used, or an interface other than a one-wire interface could be used.

The secure module 108 is preferably intended to be used first by a Service Provider who loads the secure module 108 with data to enable it to perform useful functions, and second by an End User who issues commands to the secure module 108 to perform operations on behalf of the Service

Provider for the benefit of the End User. For this reason, the secure module 108 offers functions to support the Service Provider in setting up the module for an intended application. It also offers functions to allow the End User to invoke the services offered by the Service Provider.

Each Service Provider can reserve a block of NVRAM memory to support its services by creating a transaction group 40 (refer to FIGS. 6 and 7). A transaction group 40 is simply a set of software objects 42 that are defined by the Service Provider. These objects 42 include both data objects (encryption keys, transaction counts, money amounts, date/time stamps, etc.) and transaction scripts 44 which specify how to combine the data objects in useful ways. Each Service Provider creates his own transaction group 40, which is independent of every other transaction group 40. Hence, multiple Service Providers can offer different services in the same module 108. The number of independent Service Providers that can be supported depends on the number and complexity of the objects 42 defined in each transaction group 40. Examples of some of the objects 42 that can be defined within a transaction group 40 are the following:

RSA Modulus	Clock Offset
RSA Exponent	Random SALT
Transaction Script	Configuration Data
Transaction Counter	Input Data
Money Register	Output Data
Destructor	

Within each transaction group 40 the secure module 108 will initially accept certain commands which have an irreversible effect. Once any of these irreversible commands are executed in a transaction group 40, they remain in effect until the end of the module's useful life or until the transaction group 40, to which it applies, is deleted from the secure module 108. In addition, there are certain commands which have an irreversible effect until the end of the module's life or until a master erase command is issued to erase the entire contents of the secure module 108. These commands will be discussed further below. These commands are essential to give the Service Provider the necessary control over the operations that can be performed by the End User. Examples of some of the irreversible commands are:

Privatize Object	Lock Object
Lock Transaction Group	Lock Micro-In-A-Can™

Since much of the module's utility centers on its ability to keep a secret, the Privatize command is a very important irreversible command.

Once the secure module 108, as a whole, is locked, the remaining NVRAM memory 24 is allocated for a circular buffer for holding an audit trail of previous transactions. Each of the transactions are identified by the number of the transaction group, the number of objects 42 within the specified group, and the date/time stamp.

The fundamental concept implemented by the firmware is that the Service Provider can store transaction scripts 44 in a transaction group 40 to perform only those operations among objects that he wishes the End User to be able to perform. The Service Provider can also store and privatize RSA key or keys (encryption keys) that allow the secure module 108 to "sign" transactions on behalf of the Service Provider, thereby guaranteeing their authenticity. By privatizing and/or locking one or more objects 42 in the trans-

action group 40, the Service Provider maintains control over what the secure module 108 is allowed to do on his behalf. The End User cannot add new transaction scripts 44 and is therefore limited to the operations on objects 42 that can be performed with the transaction scripts 44 programmed by the Service Provider.

II. USAGE MODELS OF THE SECURE MODULE 108 AND PORTABLE MODULE 102

This section presents practical applications of the system 100. Each of these applications is described in enough detail to make it clear why the secure module 108 and portable module 102 are important to the system application.

A. TRANSFERRING UNITS OF EXCHANGE OUT OF A PORTABLE MODULE 102

This section describes an example of how a portable module 102 and a secure module 108 operate in conjunction with the microprocessor based device 104 so that units of exchange can be securely transferred out of the portable module 102 and deposited into the secure module 108 and/or potentially communicated to at least one of the cash acceptor 110, ATM 112, credit card reader 114, or the phone line 116.

Referring to FIG. 4, initially the portable module 102 contains its ID number, a count within its transaction counter and an encrypted data packet stored in memory. Encrypted within the data packet is the portable modules ID number, the portable modules transaction count number, and the amount of value (the monetary value) of the portable module at the present time X1.

The user of the portable module touches, or somehow puts the portable module 102 into communication with the microprocessor based device 104. For explanation purposes, suppose the portable module 102 is being used as a token used to pay for a train fare. Thus, the microprocessor based device 104 could be, in this case, a turn style that allows the user to enter a train platform. The cost of entering the train platform is known by the microprocessor based device 104.

The microprocessor based device 104 reads the portable module's serial number, transaction count, and the encrypted data packet X2. This data could be referred to as a first data.

The microprocessor device 104 then provides the first data along with a first value, being the amount of value to be debited from the portable token (the train fare), to the secure module 108 X3. The secure module 108 decrypts the encrypted data found in the first data using a public key X4.

Next, the secure module 108 makes a few comparisons to make sure that the data received is good data and not counterfeit. The secure module 108 compares the serial number received in the first data with the decrypted serial number X5. If the two serial numbers match then the secure module 108 compares the transaction count received in the first data with the decrypted transaction count X6. If the two transaction counts match then the secure module is comfortable that the data received is not counterfeit data. It is understood that the comparisons can be done in any order.

Furthermore, there may have been a time stamp sent from the portable module 102. The time stamp may indicate a variety of things. One thing could be an indication of whether the portable module is still valid or the time stamp may further enable the secure module to decide if the data is or is not counterfeit.

Assuming all the data passed to the secure module 108 is determined to be valid data, the secure module 108 subtracts the first value, the train fare, from the monetary value of the portable module 102 X7. The decrypted transaction count is then incremented.

A register within the secure module 108 is increased by the amount of the first value, the train fare, so that the secure

module can keep an accounting of the amount of "money" it has collected X8. The secure module 108 creates a data packet, a second data, which comprises at least the portable module's serial number, the incremented transaction count, and the reduced monetary value of the portable module 102. The second data packet is then encrypted by the secure module 108 using a private key X9.

The microprocessor based device 104 receives the encrypted second data packet, passes the encrypted second data packet to the portable module 102 X10, and opens the turn style to let the module's user onto the train platform. The portable module 102 receives the encrypted second data packet and stores it in memory X11. The portable module also increments its transaction count indicating that another transaction has occurred X12.

Thus, the above description indicates how valuable information can be transferred between a portable insecure module 102 and a secure module 108 wherein there is a conservation of value. That is, no value is gained or lost. Value that was in the portable module 102 was decreased by the same amount value was added to the secure module 108. In the example provided, the decrease and increase in value was equal to a train fare. Such an increment or decrement can also be equal to an amount provided by an ATM, credit card transaction, cash acceptor, etc.

It is also understood that the insecure portable module 102 could be another secure module similar to the secure module in the system, but programed to act like a portable module 102.

B. TRANSFERRING UNITS OF EXCHANGE INTO THE PORTABLE MODULE 102

In this example, for simplicity, suppose the portable module does not have any monetary value and the user of the portable module wishes to "fill it up" with value. Suppose the user wishes to take cash out of an ATM machine and instead of pocketing the cash, the user wishes to put the cash value into the portable module 102.

Referring to FIG. 5, the portable module 102 contains its ID number, a transaction count and an encrypted data packet containing the portable module's ID number, transaction count and the monetary value of the portable module 102 Y1. The microprocessor based device 104, which in this example could be part of the ATM machine 112, receives the information contained in the portable module 102 when a communication is initiated between the portable module 102 and the microprocessor based device 104 Y2.

The microprocessor based device 104 passes the module's serial number, transaction count, and encrypted data packet as a first data packet to the secure module 108. The microprocessor based device also passes the amount of amount of monetary value to add to the portable module 102, as indicated by the ATM 112, to the secure module 108 Y3.

The secure module 108 decrypts the encrypted data passed to it using a public key Y4. The secure module 108 then makes a few comparisons to make sure that the data it has just received is valid and not counterfeit. The secure module 108 compares the serial number (ID number) received in the first data packet with the serial number (ID number) found in the decrypted data Y5. The secure module 108 also compares the transaction count passed the first data packet with the transaction count found in the decrypted data Y6. If the serial numbers and transaction counters match, then the secure module decides that the data received is valid and the secure module adds the monetary value, indicated by the ATM to the monetary value of the decrypted data Y7. The decrypted transaction count is incremented Y8. A register within the secure module may be decremented by the

same amount that the monetary value of the decrypted data was increased Y8.

The secure module 108 creates a second data packet, that contains the portable module's ID number, the incremented transaction counter and the increased monetary value. The second data packet is then encrypted using a private key Y10.

The microprocessor based device 104 reads the encrypted second data packet and sends it to the portable module 102 Y11. The portable module receives the encrypted second data packet and stores it in memory Y12. The portable module also advances its transaction counter Y13. The result being that the portable module now has the value of the cash withdrawn from the ATM 112. Furthermore, a record of the transaction may have been recorded and kept in the secure module, as well as by the bank that operates the ATM 112.

Exemplary Firmware Definitions for Use With the Secure Module		
Object	The most primitive data structure accepted by and operated on by the secure modules firmware. A list of valid objects and their definitions is provided in the next section.	20
Group	A self-contained collection of objects. An object's scope is restricted to the group of which it is a member.	25
Group ID	A number preferably between 0 and 255 representing a specific group.	
Object ID	A number preferably between 0 and 255 representing a specific object within a specific group.	30
Object Type	Preferably a 1-byte type specifier that describes a specific object.	
PIN	An alphanumeric Personal Identification number that is preferably eight bytes in length.	
Common PIN	The PIN that controls access to shared resources such as the audit trail. It is also used to control the host's ability to create and delete groups.	35
Group PIN	The PIN that controls access to operations specific to objects within a group	40
Audit Trail	A record of transactions occurring after the secure module has been locked.	
Locked Object	An object which has been locked by executing the lock object command. Once an object is locked it is not directly readable.	45
Private Object	An object which has been privatized by executing the privatize object command. Once an object is private, it is not directly readable or writable.	50
Locked Group	A group which has been locked using the locked group command. After a group has been locked it will not allow object creation.	
Composite Object	A combination of several objects. The individual objects inherit the attributes of the composite object.	55

Exemplary Object Definitions		
RSA Modulus	A large integer preferably of at most 1024 bits in length. It is the product of 2 large prime numbers that are each about half the number of bits in length of the desired modulus size. The RSA modulus is	65

-continued

Exemplary Object Definitions		
	used in the following equations for encrypting and decrypting a message M: Encryption: $C = M^e \pmod{N}$ (1) Decryption: $M = C^d \pmod{N}$ (2) where C is the cyphertext, d and e are the RSA exponents (see below) and N is the RSA modulus. Both e and d (shown in equations 1 and 2 above) are RSA exponents. They are typically large numbers but are smaller than the modulus (N). RSA exponents can be either private or public. When RSA exponents are created in the secure module, they may be declared as either. Once created an exponent may be changed from a public exponent to a private exponent. After an exponent has been made private, however, it will remain private until the transaction group 40 to which it belongs is destroyed.	
RSA Exponent	A transaction script is a series of instructions to be carried out by the secure module. When invoked the secure module firmware interprets the instructions in the script and places the results in the output data object (see below). The actual script is simply a list of objects. The order in which the objects are listed specifies the operations to be performed on the objects. transaction scripts 44 preferably may be as long as 128 bytes.	
Transaction Script	The transaction counter object is preferably 4 bytes in length and is usually initialized to zero when it is created. Every time a transaction script, which references this object, is invoked, the transaction counter increments by 1. Once a transaction counter has been locked it is read only and provides an irreversible counter.	
Transaction Counter	The money register object is preferably 4 bytes in length and may be used to represent money or some other form of credit. Once this object has been created, it must be locked to prevent a user from tampering with its value. Once locked the value of this object can be altered only by invoking a transaction script. A typical transaction group 40 which performs monetary transactions might have one script for withdrawals from the money register and one for deposits to the money register.	
Money Register	This object is preferably a 4 byte number which contains the difference between the reading of the secure module's real-time clock and some convenient time (e.g., 12:00 a.m., January 1, 1970). The true time can then be obtained from the secure module by adding the value of the clock offset to the real-time clock.	
Clock Offset	A SALT object is preferably 20 bytes in length and should be initialized with random data when it is created. When a host transmits a generate random SALT command, the secure module combines the previous SALT with the secure module's random number (produced preferably by	
SALT		60

-continued

Exemplary Object Definitions	
Configuration Data	randomly occurring power-ups) to generate a new random SALT. If the SALT object has not been privatized it may subsequently be read by issuing a read object command. This is a user defined structure with preferably a maximum length of 128 bytes. This object is typically used to store configuration information specific to its transaction group 40. For example, the configuration data object may be used to specify the format of the money register object (i.e., the type of currency it represents) Since this object has no pre-defined structure, it may never be used by a transaction object.
Input Data	An input data object is simply an input buffer with preferably a maximum length of 128 bytes. A transaction group may have multiple input objects. The host uses input data objects to store data to be processed by transaction scripts 44.
Output Data	The output data object is used by transaction scripts as an output buffer. This object is automatically created when the transaction group is created. It is preferably 512 bytes in length and inherits password protection from its group.
Random Fill	When the script interpreter encounters this type of object it automatically pads the current message so that its length is 1 bit smaller than the length of the preceding modulus. A handle to this object is automatically created when the transaction group is created. It is a private object and may not be read using the read object command.
Working Register	This object is used by the script interpreter as working space and may be used in a transaction script. A handle to this object is automatically created when the transaction group is created. It is a private object and may not be read using the read object command.
ROM Data	This object is automatically created when the transaction group is created. It is a locked object and may not be altered using the write object command. This object is 8 bytes and length and its contents are identical to the 8 by ROM data of the Micro-In-A-Can™.
PIN_TO_ERASE	00000001b (require PIN for Master Erase)
PIN_TO_CREATE	00000010b (require PIN for group creation)

Initially the secure module has a PIN (Personal Identification Number) of 0 (Null) and an option byte of 0. Once a PIN has been established it can only be changed by providing the old PIN or by a Master Erase. However, if the

PIN_TO_ERASE bit is set in the option byte, the PIN can only be changed through the set common PIN command. Possible error codes for the set common PIN command:

5	ERR_BAD_COMMON_PIN	(Common PIN match failed)
	ERR_BAD_PIN_LENGTH	(New PIN length > 8 bytes)
10	ERR_BAD_OPTION_BYTE	(Unrecognizable option byte)

For all commands described in this section, data received by the host will be in the form of a return packet. A return packet has the following structure:

15 Command status byte (0 if command successful, error code otherwise, 1 byte)

	Output data length	(Command output length, 2 bytes)
20	Output data	(Command output, length specified above).

Master Erase (02H)

25 Transmit data
02H, Common PIN
Receive data
CSB=0 if command was successful, ERR_BAD_COMMON_PIN otherwise
30 Output length=0
Output data=0

Notes:

35 If the LSB (least significant bit) of the PIN option is clear (i.e. PIN not required for Master Erase) then a 0 is transmitted for the Common PIN value. In general this text will always assume a PIN is required. If no PIN has been established a 0 should be transmitted as the PIN. This is true of the common PIN and group PINS (see below). If the PIN was correct the firmware deletes all groups (see below) and all objects within the groups. The common PIN and common PIN option byte are both reset to zero.

40 After everything has been erased the secure module transmits the return packet. The CSB is as described above. The output data length and output data fields are both set to 0.

Create Group (03H)

45 Transmit data
03H, Common PIN, Group name, Group PIN
50 Receive data
CSB=0 if command successful, appropriate error code otherwise
Output length=1 if successful, 0 otherwise
Output data=Group ID if successful, 0 otherwise

Notes:

55 The maximum group name length is 16 bytes and the maximum PIN length is eight bytes. If the PIN_TO_CREATE bit is set in the common PIN option byte and the PIN transmitted does not match the common PIN the secure module will set the OSC to ERR_BAD_COMMON_PIN. Possible error return codes for the create group command:

65	ERR_BAD_COMMON_PIN	(Incorrect common PIN)
	ERR_BAD_NAME_LENGTH	(If group name length > 16 bytes)

13

-continued

ERR_BAD_PIN_LENGTH	(If group PIN length > 8 bytes)	
ERR_MIAC_LOCKED	(The secure module has been locked)	5
ERR_INSUFFICIENT_RAM	(Not enough memory for new group)	

Set Group PIN (04H)

Transmit data 10
 04H, Group ID, old GPIN, new GPIN
 Receive data
 CSB=0 if command successful, appropriate error code otherwise
 Output length=0
 Output data=0

Notes:

The Group PIN only restricts access to objects within the group specified by the group ID transmitted in the command packet.

Possible error codes for the set group PIN command:

ERR_BAD_GROUP_PIN	(Group PIN match failed)	25
ERR_BAD_PIN_LENGTH	(New group PIN length > 8 bytes)	

Create Object (05H)

Transmit data 30
 05H, Group ID, Group PIN, Object type, Object attributes, Object data
 Receive data
 CSB=0 if command successful, appropriate error code otherwise 35
 Output length=1 if successful, 0 otherwise
 Output data=object ID if successful, 0 otherwise

Notes:

If the Create Object command is successful the secure module firmware returns the object's ID within the group specified by the Group ID. If the PIN supplied by the host was incorrect or the group has been locked by the Lock Group command (described below) the secure module returns an error code in the CSB. An object creation will also fail if the object is invalid for any reason. For example, if the object being created is an RSA modulus (type 0) and it is greater than 1024 bits in length. transaction script creation will succeed if it obeys all transaction scripts rules.

Possible error return codes for the create object command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)	
ERR_GROUP_LOCKED	(The group has been locked)	55
ERR_MIAC_LOCKED	(The secure module has been locked)	
ERR_INVALID_TYPE	(The object type specified is invalid)	
ERR_BAD_SIZE	(The objects length was invalid)	
ERR_INSUFFICIENT_RAM	(Not enough memory for new object)	60

Object types:

RSA modulus	0
RSA exponent	1
Money register	2
Transaction counter	3

14

-continued

Transaction script	4
Clock offset	5
Random SALT	6
Configuration object	7
Input data object	8
Output data object	9
Object Attributes:	

Locked	0000001b
Privatized	0000010b

Objects may also be locked and privatized after creation by using the Lock Object and Privatize Object commands described below.

Lock Object (06H)

Transmit data
 06H, Group ID, Group PIN, Object ID
 Receive data
 CSB=0 if command successful, appropriate error code otherwise
 Output length=0
 Output data=0

Notes:

If the Group ID, Group PIN and Object ID are all correct, the secure module will lock the specified object. Locking an object is an irreversible operation.

Possible error return codes for the lock object command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)	
ERR_GROUP_LOCKED	(The group has already been locked)	
ERR_MIAC_LOCKED	(The secure module has been locked)	
ERR_BAD_GROUP_ID	(Specified group does not exist)	35
ERR_BAD_OBJECT_ID	(Specified object does not exist)	

Privatize Object (07H)

Transmit data 40
 07H, Group ID, Group PIN, Object ID
 Receive data
 CSB=0 if successful, appropriate error code otherwise

Notes:

If the Group ID, Group PIN and Object ID were valid the object will be privatized. Privatized objects share all the properties of locked objects but are not readable. Privatized objects are only modifiable through transaction scripts. Note that locking a privatized object is legal, but has no meaning since object privatization is a stronger operation than object locking. Privatizing an object is an irreversible operation.

Possible error return codes for the privatize object command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)	
ERR_GROUP_LOCKED	(The group has already been locked)	55
ERR_MIAC_LOCKED	(The secure module has been locked)	
ERR_BAD_GROUP_ID	(Specified group does not exist)	60
ERR_BAD_OBJECT_ID	(Specified object does not exist)	

65 Make Object Destructable (08H)

Transmit data
 08H, Group ID, Group PIN, Object ID

Receive data

CSB=0 if successful, appropriate error code otherwise

Notes:

If the Group ID, Group PIN and Object ID were valid the object will be made destructable. If an object is destructable it becomes unusable by a transaction script after the groups destructor becomes active. If no destructor object exists within the transaction group the destructible object attribute bit has no affect. Making an object destructable is an irreversible operation.

Possible error return codes for the make object destructable command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_GROUP_LOCKED	(The group has already been locked)
ERR_MIAC_LOCKED	(The secure module has been locked)
ERR_BAD_GROUP_ID	(Specified group does not exist)
ERR_BAD_OBJECT_ID	(Specified object does not exist)

Lock Secure module (09H)

Transmit data

09H, Common PIN

Receive data

CSB=0 if successful, appropriate error code otherwise

Output length=2 if successful, 0 otherwise

Output data=audit trail size if successful, 0 otherwise

Notes:

If the host supplied Common PIN is correct and the secure module has not previously been locked, the command will succeed. When the secure module is locked it will not accept any new groups or objects. This implies that all groups are automatically locked. The RAM not used by the system or by groups will be used for an audit trail. There is no audit trail until the secure module has successfully been locked!

An audit trail record is six bytes long and has the following structure:

Group ID|Object ID|Date/Time stamp.

Once an audit trail has been established, a record of the form shown above will be stored in the first available size byte location every time a transaction script is executed. Note that since the secure module must be locked before the audit trail begins, neither the group ID nor any object ID is subject to change. This will always allow an application processing the audit trail to uniquely identify the transaction script that was executed. Once the audit trail has consumed all of its available memory, it will store new transaction records over the oldest transaction records.

Possible error codes for the lock secure module command:

ERR_BAD_COMMON_PIN	(Supplied common PIN was incorrect)
ERR_MIAC_LOCKED	(Secure module was already locked)

Lock Group (0AH)

Transmit data

0AH, Group ID, Group PIN

Receive data

CSB=0 if command successful, appropriate error code otherwise

Output length=0

Output data=0

Notes:

If the group PIN provided is correct the secure module BIOS will not allow further object creation within the specified group. Since groups are completely self-contained entities they may be deleted by executing the Delete Group command (described below).

Possible error return codes for the lock group command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_GROUP_LOCKED	(The group has already been locked)
ERR_MIAC_LOCKED	(The secure module has been locked)
ERR_BAD_GROUP_ID	(Specified group does not exist)

Invoke Transaction Script (0BH)

Transmit data

0BH, Group ID, Group PIN, Object ID

Receive data

CSB=0 if command successful, appropriate error code otherwise

Output length=1 if successful, 0 otherwise

Output data=estimated completion time

Notes:

The time estimate returned by the secure module is in sixteenths of a second. If an error code was returned in the CSB, the time estimate will be 0.

Possible error return codes for the execution transaction script command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_BAD_GROUP_ID	(Specified group does not exist)
ERR_BAD_OBJECT_ID	(Script object did not exist in group)

Read Object (0CH)

Transmit data

0CH, Group ID, Group PIN, Object ID

Receive data

CSB=0 if command successful, appropriate error code otherwise

Output length=object length if successful, 0 otherwise

Output data=object data if successful, 0 otherwise

Notes:

If the Group ID, Group PIN and Object ID were correct, the secure module checks the attribute byte of the specified object. If the object has not been privatized the secure module will transmit the object data to the host. If the Group PIN was invalid or the object has been privatized the secure module will return a 0 in the output length, and data fields of the return packet.

Possible error codes for the read object command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_BAD_GROUP_ID	(Specified group does not exist)

-continued

ERR_BAD_OBJECT_ID	(Object did not exist in group)
ERR_OBJECT_PRIVATIZED	(Object has been privatized)

Write Object (ODH)
 Transmit data
 ODH, Group ID, Group PIN, Object ID, Object size, Object Data
 Receive data
 CSB=0 if successful, appropriate error code otherwise
 Output length=0
 Output data=0

Notes:
 If the Group ID, Group PIN and Object ID were correct, the secure module checks the attribute byte of the specified object. If the object has not been locked or privatized the secure module will clear the objects previous size and data and replace it with the new object data. Note that the object type and attribute byte are not affected.

Possible error codes for the write object command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_BAD_GROUP_ID	(Specified group does not exist)
ERR_BAD_OBJECT_ID	(Object did not exist in group)
ERR_BAD_OBJECT_SIZE	(Illegal object size specified)
ERR_OBJECT_LOCKED	(Object has been locked)
ERR_OBJECT_PRIVATIZED	(Object has been privatized)

Read Group Name (0EH)
 Transmit data
 0EH, Group ID
 Receive data
 CSB=0
 Output Length=length of group name
 Output data=group name

Notes:
 The group name length is a maximum of 16 bytes. All byte values are legal in a group name.

Delete Group (0FH)
 Transmit data
 0FH, Group ID, Group PIN
 Receive data
 CSB=0 if successful, appropriate error code otherwise
 Output length=0
 Output data=0

Notes:
 If the group PIN and group ID are correct the secure module will delete the specified group. Deleting a group causes the automatic destruction of all objects within the group. If the secure module has been locked the Delete Group command will fail.

Possible error codes for the delete group command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_BAD_GROUP_ID	(Specified group does not exist)

-continued

ERR_MIAC_LOCKED	(Secure module has been locked)
-----------------	---------------------------------

5 Get Command Status Info (10H)
 Transmit data
 10H
 Receive data
 CSB=0
 Output length=6
 Output data=secure module status structure (see below)
 Notes:
 This operation requires no PIN and never fails. The status structure is defined as follows:

Last command executed	(1 byte)
Last command status	(1 byte)
Time command received	(4 bytes)

20 Get Secure module Configuration Info (11H)
 Transmit data
 11H
 Receive data
 CSB=0
 Output length=4
 Output data=secure module configuration structure
 Notes:
 This operation requires no PIN and never fails. The configuration structure is defined as follows:

Number of groups	(1 byte)
Flag byte (see below)	(1 byte)
Audit trail size/Free RAM	(2 bytes)

The flag byte is the bitwise-or of any of the following values:
 00000001b (Secure module is locked)
 00000010b (Common PIN required for access)

Read Audit Trail Info (12H)
 Transmit data
 12H, Common PIN
 Receive data
 CSB=0 if command successful, appropriate error code otherwise
 Output length=audit trail structure size (5) if successful, 0 otherwise
 Output data=audit trail info structure if successful, 0 otherwise

Notes:
 If the transmitted Common PIN is valid and the secure module has been locked, it returns audit trail configuration information as follows:

Number of used transaction records (2 bytes)
 Number of free transaction records (2 bytes)
 A boolean specifying whether or not the audit trail rolled since previous read command (1 byte)
 Possible error codes for the read audit trail info command:
 ERR_BAD_COMMON_PIN (Common PIN was incorrect)
 ERR_MIAC_NOT_LOCKED (Secure module is not locked)

Read Audit Trail (13H)

Transmit data
 13H, Common PIN
 Receive data
 CSB=0 if command successful, appropriate error code otherwise
 Output length=# of new records * 6 if successful, 0 otherwise
 Output data=new audit trail records

Notes:

If the transmitted common PIN is valid and the secure module has been locked, it will transfer all new transaction records to the host.

Possible error codes for the read audit trail command:

ERR_BAD_COMMON_PIN	(Common PIN was incorrect)
ERR_MIAC_NOT_LOCKED	secure module is not locked

Read Group Audit Trail (14H)

Transmit data
 14H, Group ID, Group PIN
 Receive data
 CSB=0 if command successful, appropriate error code otherwise
 Output length=# or records for group * 6 if successful, 0 otherwise
 Output data=audit trail records for group

Notes:

This command is identical to the read audit trail command, except that only records involving the group ID specified in the transmit data are returned to the host. This allows transaction groups to record track their own activities without seeing other groups records.

Possible error codes for the read group audit trail command:

ERR_BAD_GROUP_ID	(Group ID does not exist)
ERR_BAD_GROUP_PIN	(Common PIN was incorrect)
ERR_MIAC_NOT_LOCKED	(The secure module is not locked)

Read Real Time Clock (15H)

Transmit data
 15H, Common PIN
 Receive data
 CSB=0 if the common PIN matches and ERR_BAD_COMMON_PIN otherwise
 Output length=4
 Output data=4 most significant bytes of the real time clock

Notes:

This value is not adjusted with a clock offset. This command is normally used by a service provider to compute a clock offset during transaction group creation.

Read Real Time Clock Adjusted (16H)

Transmit data
 16H, Group ID, Group PIN, ID of offset object
 Receive data
 CSB=0 if successful, appropriate error code otherwise
 Output length=4 if successful, 0 otherwise
 Output data=Real time clock+clock offset ID

Notes:

This command succeeds if the group ID and group PIN are valid, and the object ID is the ID of a clock offset. The secure module adds the clock offset to the current value of the 4 most significant bytes of the RTC and returns that value in the output data field. Note that a transaction script may be written to perform the same task and put the result in the output data object.

Possible error codes for the real time clock adjusted command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_BAD_GROUP_ID	(Specified group does not exist)
ERR_BAD_OBJECT_TYPE	(Object ID is not a clock offset)

Get Random Data (17H)

Transmit data
 17H, Length (L)
 Receive data
 CSB=0 if successful, appropriate error code otherwise
 Output length=L if successful, 0 otherwise
 Output data=L bytes of random data if successful

Notes:

This command provides a good source of cryptographically useful random numbers.

Possible error codes for the get random data command are:

ERR_BAD_SIZE (Requested number of bytes>128)

Get Firmware Version ID (18H)

Transmit data
 18H
 Receive data
 CSB=0
 Output length=Length of firmware version ID string
 Output data=Firmware version ID string

Notes:

This command returns the firmware version ID as a Pascal type string (length+data).

Get Free RAM (19H)

Transmit data
 19H
 Receive data
 CSB=0
 Output length=2
 Output data=2 byte value containing the amount of free RAM

Notes:

If the secure module has been locked the output data bytes will both be 0 indicating that all memory not used by transaction groups has been reserved for the audit trail.

Change Group Name (1AH)

Transmit data
 1AH, Group ID, Group PIN, New Group name
 Receive data
 CSB=0 if successful or an appropriate error code otherwise
 Output length=0
 Output data=0

Notes:

If the group ID specified exists in the secure module and the PIN supplied is correct, the transaction group name is replaced by the new group name supplied by the host. If a

21

group ID of 0 is supplied the PIN transmitted must be the common PIN. If it is correct, the secure module name is replaced by the new name supplied by the host.

Possible error codes for the change group name command:

ERR_BAD_GROUP_PIN	(Incorrect group PIN)
ERR_BAD_GROUP_ID	(Specified group does not exist)
ERR_BAD_NAME_LENGTH	(New group name > 16 bytes)

ERROR CODE DEFINITIONS

ERR_BAD_COMMAND (80H)

This error code occurs when the secure module firmware does not recognize the command just transmitted by the host.

ERR_BAD_COMMON_PIN (81H)

This error code will be returned when a command requires a common PIN and the PIN supplied does not match the secure module's common PIN. Initially the common PIN is set to 0.

ERR_BAD_GROUP_PIN (82H)

Transaction groups may have their own PIN, FIG. 6. If this PIN has been set (by a set group PIN command) it must be supplied to access any of the objects within the group. If the Group PIN supplied does not match the actual group PIN, the secure module will return the ERR_BAD_GROUP_PIN error code.

ERR_BAD_PIN_LENGTH (83H)

There are 2 commands which can change PIN values. The set group PIN and the set common PIN commands. Both of these require the new PIN as well as the old PIN. The ERR_BAD_PIN_LENGTH error code will be returned if the old PIN supplied was correct, but the new PIN was greater than 8 characters in length.

ERR_BAD_OPTION_BYTE (84H)

The option byte only applies to the common PIN. When the set common PIN command is executed the last byte the host supplies is the option byte (described in command section). If this byte is unrecognizable to the secure module, it will return the ERR_BAD_OPTION_BYTE error code.

ERR_BAD_NAME_LENGTH (85H)

When the create transaction group command is executed, one of the data structures supplied by the host is the group's name. The group name may not exceed 16 characters in length. If the name supplied is longer than 16 characters, the ERR_BAD_NAME_LENGTH error code is returned.

ERR_INSUFFICIENT_RAM (86H)

The create transaction group and create object commands return this error code when there is not enough heap available in the secure module.

ERR_MIAC_LOCKED (87H)

When the secure module has been locked, no groups or objects can be created or destroyed. Any attempts to create or delete objects will generate an ERR_MIAC_LOCKED error code.

22

ERR_MIAC_NOT_LOCKED (88H)

If the secure module has not been locked there is no audit trail. If one of the audit trail commands is executed this error code will be returned.

ERR_GROUP_LOCKED (89H)

Once a transaction group has been locked object creation within that group is not possible. Also the objects attributes and types are frozen. Any attempt to create objects or modify their attribute or type bytes will generate an ERR_GROUP_LOCKED error code.

ERR_BAD_OBJECT_TYPE (8AH)

When the host sends a create object command to the secure module, one of the parameters it supplies is an object type (see command section). If the object type is not recognized by the firmware it will return an ERR_BAD_OBJECT_TYPE error code.

ERR_BAD_OBJECT_ATTR (8BH)

When the host sends a create object command to the secure module, one of the parameters it supplies is an object attribute byte (see command section). If the object attribute byte is not recognized by the firmware it will return an ERR_BAD_OBJECT_ATTR error code.

ERR_BAD_SIZE (8CH)

An ERR_BAD_SIZE error code is normally generated when creating or writing an object. It will only occur when the object data supplied by the host has an invalid length.

ERR_BAD_GROUP_ID (8DH)

All commands that operate at the transaction group level require the group ID to be supplied in the command packet. If the group ID specified does not exist in the secure module it will generate an ERR_BAD_GROUP_ID error code.

ERR_BAD_OBJECT_ID (8EH)

All commands that operate at the object level require the object ID to be supplied in the command packet. If the object ID specified does not exist within the specific transaction group (also specified in the command packet) the secure module will generate an ERR_BAD_OBJECT_ID error code.

ERR_INSUFFICIENT_FUNDS (8FH)

If a script object that executes financial transactions is invoked and the value of the money register is less than the withdrawal amount requested an ERR_INSUFFICIENT_FUNDS error code will be returned.

ERR_OBJECT_LOCKED (90H)

Locked objects are read only. If a write object command is attempted and it specifies the object ID of a locked object the secure module will return an ERR_OBJECT_LOCKED error code.

ERR_OBJECT_PRIVATE (91H)

Private objects are not directly readable or writable. If a read object command or a write object command is attempted, and it specifies the object ID of a private object, the secure module will return an ERR_OBJECT_PRIVATE error code.

ERR_OBJECT_DESTROYED (92H)

If an object is destructible and the transaction group's destructor is active the object may not be used by a script. If a script is invoked which uses an object which has been destructed, an ERR_OBJECT_DESTROYED error code will be returned by the secure module.

The exemplary embodiment of the present invention is preferably placed within a durable stainless steel, token-like can. It is understood that an exemplary secure module can be placed in virtually any articulatable item. Examples of articulatable items include credit cards, rings, watches, wallets, purses, necklaces, jewelry, ID badges, pens, clipboards, etc.

The secure module 108 preferably is a single chip "trusted computer". By the word "trusted" it is meant that the computer is extremely secure from tampering by unwarranted means. The secure module incorporates a numeric coprocessor optimized for math intensive encryption. The BIOS is preferably immune to alteration and specifically designed for very secure transactions.

Each secure module can have a random "seed" generator with the ability to create a private/public key set. The private key never leaves the secure module and is only known by the secure module. Furthermore, discovery of the private key is prevented by active self-destruction upon wrongful entry into the secure module. The secure module can be bound to the user by a personal identification number (PIN).

When transactions are performed by the secure module 108 certificates of authentication are created by either or both the secure module and a system the secure module communicates with. The certificate can contain a variety of information. In particular, the certificate may contain:

- 1) who is the secure module user via a unique registration number and a certified public key.
- 2) when the transaction took place via a true-time stamping of the transaction.
- 3) where the transaction took place via a registered secure module interface site identification.
- 4) security information via uniquely serialized transactions and digital sign on message digests.
- 5) secure module status indicated as valid, lost, or expired.

Although a preferred embodiment of the method and apparatus of the present invention has been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiment disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

What is claimed is:

1. A system for communicating data securely, comprising:
 - a first portable module comprising:
 - a nonvolatile memory for storing a first data;
 - a first real time clock circuit for time stamping data transactions;
 - a counter for counting a transaction count;
 - an input/output circuit;
 - a substantially unique electronically readable identification number readable by said input/output circuit; and
 - a memory control circuit in electrical communication with said nonvolatile memory, said real time clock, said counter, and said input/output circuit;
 - a portable module reader that can be placed in communication with said first portable module, said portable module reader can be connected to a plurality of other devices;
 - a secure microcontroller based module in electronic communication with said portable module reader, said secure microcontroller comprising:
 - a microcontroller core;
 - a math coprocessor, in communication with said microcontroller core, for processing encryption calculations;
 - an energy circuit for storing energy;
 - a memory circuit connected to said microcontroller core;
 - a memory circuit in communication with said microcontroller core; and
 - a second real time clock circuit in communication with said microcontroller,
 said combination of said portable module reader and said secure microcontroller performing secure data transfers with said first portable module.
2. The system for communicating data securely of claim 1, wherein said plurality of other devices includes at least one of a credit card reader, a cash machine, an automatic teller machine, and a phone line.
3. The system for communicating data securely of claim 1, wherein said first data is a packet of encrypted data.
4. The system for communicating data securely of claim 1, wherein said first portable module communicates with said portable module reader via a single wire bus comprising a single bidirectional communication wire and a ground connection.
5. The system for communicating data securely of claim 1, wherein said first module can create random public/private key sets for encryption purposes.
6. The system for communicating data securely of claim 1, wherein said secure microcontroller can create random public/private key sets for encryption purposes.

* * * * *

T.W
7-9-96


PATENT APPLICATION SERIAL NO. 08/594975

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

DF70088 06/17/96 08594975 04-0031 070 101 20.00CH

RECEIVED BY THE PATENT AND TRADEMARK OFFICE
ON 06/17/96

TO-1556
(/87)

BAR CODE LABEL		U.S. PATENT APPLICATION			
					
SERIAL NUMBER		FILING DATE	CLASS	GROUP ART UNIT	
08/594,975		01/31/96	380	2202	
APPLICANT	STEPHEN M. CURRY, DALLAS, TX; DONALD W. LOOMIS, COPPELL, TX; MICHAEL L. BOLAN, DALLAS, TX. **CONTINUING DATA***** VERIFIED _____ **FOREIGN/PCT APPLICATIONS***** VERIFIED _____ FOREIGN FILING LICENSE GRANTED 06/19/96				
STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS	FILING FEE RECEIVED	ATTORNEY DOCKET NO.
TX	8	21	3	\$902.00	20661/429
ADDRESS	STEVEN R GREENFIELD JENKENS & GILCHRIST 3200 FOUNTAIN PLACE 1445 ROSS AVENUE DALLAS TX 75202-2799				
TITLE	TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE				
This is to certify that annexed hereto is a true copy from the records of the United States Patent and Trademark Office of the application which is identified above. By authority of the COMMISSIONER OF PATENTS AND TRADEMARKS					
Date	Certifying Officer				

08/594,975

Patent Application
Docket #20661/429



ABSTRACT OF THE DISCLOSURE

✓
The present invention relates to system, apparatus and method for communicating valuable data from a portable module to another module via an electronic device. More specifically, the disclosed system, apparatus and method are useful for enabling a user to fill a portable module with a cash equivalent and to spend the cash equivalent at a variety of locations. The disclosed system incorporates an encryption/decryption method.

5

10

08/594975

Patent Application
Docket #20661/429



CERTIFICATE OF MAILING BY EXPRESS MAIL	
"EXPRESS MAIL" Mailing Label No.	IB 885275721 US
Date of Deposit	January 31, 1996
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	JEANNE A. HOWARD
Signature	<i>Jeanne A Howard</i>

TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

CROSS REFERENCE TO OTHER APPLICATIONS

The following applications of common assignee contains related subject matter and is hereby incorporated by reference:

✓ 135
5/3/99

Serial No. ~~UNKNOWN~~ ^{08/594 983}, filed January 31, 1996, entitled METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS; and

✓ 136
5/3/99

Serial No. ~~UNKNOWN~~ ^{08/595 014}, filed January 31, 1996, entitled METHOD, APPARATUS AND SYSTEM FOR TRANSFERRING UNITS OF VALUE.

IPDAL 72906.1/20661-429



BACKGROUND OF THE INVENTION

Technical Field of the Invention

5 The present invention relates to a method and system for transferring valuable information securely between a secure module and another module. More particularly, the present invention relates to transferring units of value between a microprocessor based secure module and another module used for carrying a monetary equivalent.

Description of Related Art

10 In the past the preferred means for paying for an item was cash. As our society has become more advanced, credit cards have become an accepted way to pay for merchandise or services. The payment is not a payment to the merchant, but instead is a credit given by a bank to
15 the user that the merchant accepts as payment. The merchant collects money from the bank based on the credit. As time goes on, cash is used less and less, and money transfers between parties are becoming purely electronic.

Present credit cards have magnetic strips to identify the owner of the card and the credit provider. Some credit cards have electronic circuitry installed that identifies the credit card owner and the credit or
5 service provider (the bank).

The magnetic strips installed in present credit cards do not enable the card to be used as cash. That is the modern credit card does not allow the consumer to buy something with the credit card and the merchant to
10 receive cash at the time of the transaction. Instead, when the consumer buys something on credit, the merchant must later request that the bank pay for the item that the consumer bought. The bank then bills the consumer for the item that was bought.

15 Thus, there is a need for an electronic system that allows a consumer to fill an electronic module with a cash equivalent in the same way a consumer fills his wallet with cash. When the consumer buys a product or service from a merchant, the consumer's module can be

debited and the merchant's cash drawer can be credited without any further transactions with a bank or service provider.

SUMMARY OF THE INVENTION

5 The present invention is an apparatus, system and method for communicating a cash equivalent electronically to and from a portable module. The portable module can be used as a cash equivalent when buying products and services in the market place.

10 The present invention comprises a portable module that can communicate to a secure module via a microprocessor based device. The portable module can be carried by a consumer, filled with electronic money at an add-money station, and be debited by a merchant when a
15 product or service is purchased by the consumer. As a result of a purchase, the merchant's cash drawer will indicate an increase in cash value.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be had by reference to the following Detailed Description when
5 taken in conjunction with the accompanying Drawings wherein:

FIGURE 1 depicts an exemplary system for transferring valuable information between a module and a secure device;

10 FIGURE 2 is a block diagram of an embodiment of a portable module;

FIGURE 3 is a block diagram of an embodiment of a microprocessor based module;

15 FIGURE 4 is an exemplary technique for transferring valuable data securely into a portable module;

FIGURE 5 is an exemplary technique for transferring valuable data securely out of a portable module;

FIGURE 6 is an exemplary organization of the software and firmware within a secure microprocessor based device; and

FIGURE 7 is an exemplary configuration of software and firmware within a secure microprocessor based device.

DETAILED DESCRIPTION OF A PRESENTLY PREFERRED EXEMPLARY EMBODIMENT

FIGURE 1 depicts a block diagram of an exemplary system 100 for transferring valuable information to and from a portable module. A portable module 102, which will be described in more detail later, communicates to a microprocessor based device 104. The portable module 102 may contain information that represents units of exchange or a currency equivalent. The microprocessor based device 104 can be any of an unlimited number of

devices. For example, the microprocessor based device
104 could be a personal computer, an add-a-fare machine
at a train or bus station (similar to those in today's
District of Columbia metro stations), a turn style, a
5 toll booth, a bank's terminal, a ride at a carnival, a
washing machine at a Laundromat, a locking device, a mail
metering device or any device that controls access, or
meters a monetary equivalent, etc.

The means for communication 106 between the portable
10 module 102 and the microprocessor based device 104 is
preferably via a single wire or contact connection. The
single wire connection 106 preferably incorporates a
communication protocol that allows the portable module
102 and the microprocessor based device 104 to
15 communicate in a bidirectional manner. Preferably the
communication protocol is a one-wire protocol developed
by Dallas Semiconductor. It is understood that the means
for communicating 106 is not limited to a single wire
connection. The communication means 106 could be
20 multiple wires, a wireless communication system, infrared

light, any electro-magnetic means, a magnetic technique, or any other similar technique.

5 The microprocessor based device 104 is electrically connected to another microprocessor based device, which is preferably a secure device 108. The term secure device means that the device is designed to contain a secret code and the secret code is extremely difficult to learn. An example of a secure device 108 is explained later in this document.

10 The microprocessor based device 104 can be connected to a variety of other devices. Such devices include, but are not limited to a cash acceptor 110, an automatic teller machine (ATM) 112, a credit card reader 114, and a phone line 116.

15 The cash acceptor 110 is adapted to receive cash in the form of currency, such as dollar bills or coins. The cash acceptor 110, preferably, determines the value of the accepted currency. The cash acceptor 110

communicates to the microprocessor based device 104 and informs the device 104 of how much currency has been deposited in the cash acceptor 110.

5 The cash acceptor 110 can also be a device which provides currency. That is, the cash acceptor 110 in response to a communication from the microprocessor based device 104, may provide a metered amount of currency to a person.

10 The credit card reader 114, and ATM 112 can also be attached to the microprocessor based device 104. The credit card reader 114 could be used to read a user's credit card and then, when authorized, either communicate to the microprocessor based device 104 that units of exchange need to be added to the portable module or that
15 units of exchange need to be extracted from the portable module to pay for a good, service or credit card bill.

The ATM 112 may also be connected to the microprocessor based device. Via communications from the ATM 112, the microprocessor based device 104 can be

informed that units of exchange need to be added or subtracted from the portable module 102.

Furthermore, it is also possible that the microprocessor based device 104 is connected to a phone line 116. The phone line may be used for a variety of things. Most importantly, the phone line may be used to allow the microprocessor based device 104 to communicate with a network of devices. Such telephonic communication may be for validating transactions or for aiding the accounting of transactions that are performed via the microprocessor based device's 104 aid. It is further understood that the phone line may be any of a vast variety of communication lines including wireless lines. Video, analog, or digital information may be communicated over the phone line 116.

FIGURE 2 depicts a preferred exemplary portable module 102. The portable module 102 is preferably a rugged read/write data carrier that can act as a localized data base and be easily accessed with minimal

hardware. The module can be incorporated in a vast
variety of portable items which includes, but is not
limited to a durable micro-can package that is highly
resistant to environmental hazards such as dirt,
5 moisture, and shock. The module can be incorporated into
any object that can be articulated by a human or thing,
such as a ring, bracelet, wallet, name tag, necklace,
baggage, machine, robotic device, etc. Furthermore, the
module 102 could be attached to a stationary item and the
10 microprocessor based device 104 may be articulated to the
portable module 102. For example, the module 102 may be
attached to a piece of cargo and a module reader may be
touched to or brought near the module 102. The module
reader may be part of the microprocessor based device
15 104.

The portable module 102 comprises a memory 202 that is
preferably, at least in part, nonvolatile memory for
storing and retrieving vital information pertaining to
the system to which the module 102 may become attached
20 to. The memory 202 may contain a scratchpad memory which

may act as a buffer when writing into memory. Data is first written to the scratchpad where it can be read back. After data has been verified, the data is transferred into the memory.

5 The module 102 also comprises a counter 206 for keeping track of the number of transactions the module has performed (the number of times certain data in the memory of the module has been changed). A timer 102 may be provided in the module to provide the ability to time
10 stamp transactions performed by the module. A memory controller 204 controls the reading and writing of data into and out of the memory 202.

 The module also may comprise an identification number 210. The identification number preferably
15 uniquely identifies the portable module from any other portable module.

 An input/output control circuit 212 controls the data flow into and out of the portable module 102. The input/output control ("I/O") 212 preferably has an input
20 buffer and an output buffer and interface circuitry 214. As stated above, the interface circuitry 214 is

preferably a one-wire interface. Again, it is understood that a variety of technologies can be used to interface the portable module 102 to another electronic device. A single wire or single connection is preferred because the mechanics of making a complete connection is simplified. It is envisioned that a proximity/wireless communication technique is also a technique for communicating between the module 102 and another device. Thus, the interface circuit 214 can be a single wire, multiple wire, wireless, electromagnetic, magnetic, light, or proximity, interface circuit.

FIGURE 3 depicts a block diagram of an exemplary secure microprocessor based device ("secure device") 108. The secure device circuitry can be a single integrated circuit. It is understood that the secure device 108 could also be a monolithic or multiple circuits combined together. The secure device 108 preferably comprises a microprocessor 12, a real time clock 14, control circuitry 16, a math coprocessor 18, memory circuitry 20, input/output circuitry 26, and an energy circuit 34.

The secure device 108 could be made small enough to be incorporated into a variety of objects including, but not limited to a token, a card, a ring, a computer, a wallet, a key fob, a badge, jewelry, a stamp, or
5 practically any object that can be grasped and/or articulated by a user of the object. In the present system 100, the secure device 108 is preferably adapted to be a trusted certifying authority. That is the secure device 108 is a trusted computer. The secure device 108
10 comprises a numeric coprocessor 18 optimized for math intensive encryption. The BIOS is immune to alteration and is specifically designed for secure transactions. This secure device 108 is preferably encased in a durable, dirt, moisture and shock resistant stainless
15 steel enclosure, but could be encased in wide variety of structures so long as specific contents of the secure device 108 are extremely difficult to decipher. The secure device 108. The secure device 108 may have the ability to store or create a private/public key set,
20 whereby the private key never leaves the secure device 108 and is not revealed under almost any circumstance.

Furthermore, the secure module 108 is preferably designed to prevent discovery of the private key by an active self-destruction of the key upon wrongful entry.

5 The microprocessor 12 is preferably an 8-bit microprocessor, but could be 16, 32, 64 or any operable number of bits. The clock 14 provides timing for the module circuitry. There can also be separate clock circuitry 14 that provides a continuously running real time clock.

10 The math coprocessor circuitry 18 is designed and used to handle very large numbers. In particular, the coprocessor will handle the complex mathematics of RSA encryption and decryption or other types of math intensive encryption or decryption techniques.

15 The memory circuitry 20 may contain both read-only-memory and non-volatile random-access-memory. Furthermore, one of ordinary skill in the art would understand that volatile memory, EPROM, SRAM and a

variety of other types of memory circuitry might be used to create an equivalent device.

Control circuitry 16 provides timing, latching and various necessary control functions for the entire
5 circuit.

An input/output circuit 26 enables bidirectional communication with the secure module 108. The input/output circuitry 26 preferably comprises at least an output buffer and an input buffer. For communication
10 via a one-wire bus, one-wire interface circuitry can be included with the input/output circuitry 26. It is understood that the input/output circuitry 26 of the secure device 108 can be designed to operate on a single wire, a plurality of wires or any means for communicating
15 information between the secure module 108 and the microprocessor based device 104.

An energy circuit 34 may be necessary to maintain stored information in the memory circuitry 20 and/or aid

in powering the other circuitry in the module 108. The energy circuit 34 could consist of a battery, capacitor, R/C circuit, photo-voltaic cell, or any other equivalent energy producing circuit or means.

5 The firmware architecture of the secure module 108 and how it operates within the exemplary system for transferring valuable information, such as units of exchange or currency, between the secure module 108 and a portable module 102 will now be discussed. The secure
10 module 108 provides encryption and decryption services for confidential data transfer through the microprocessor based device 104. The following examples are intended to illustrate a preferred feature set of the secure module 108 and to explain the services that the exemplary system
15 100 can offer. These applications and examples by no means limit the capabilities of the invention, but instead bring to light a sampling of its capabilities.

I. OVERVIEW OF THE PREFERRED SECURE MODULE 108 AND ITS
FIRMWARE DESIGN

Referring to FIGURE 3 again, the secure module 108 preferably contains a general-purpose, 8051-compatible
5 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, input and output buffers 28, 30 with a one-wire interface 32 for sending and receiving
10 data, 32 Kbytes of ROM memory 22 with preprogrammed firmware, 8 Kbytes of NVRAM (non-volatile RAM) 24 for storage of critical data, and control circuitry 16 that enables the micro controller 12 to be powered up to interpret and act on the data placed in an input data
15 object. The module 108 draws its operating power from a single wire, one-wire communication line. The micro controller 12, clock 14, memory 20, buffers 28, 30, one-wire front-end 32, modular exponentiation accelerator 18, and control circuitry 16 are preferably integrated on a
20 single silicon chip and packaged in a stainless steel

micro can using packaging techniques which make it
virtually impossible to probe the data in the NVRAM 24
without destroying the data. Initially, most of the
NVRAM 24 is available for use to support applications
5 such as those described below. One of ordinary skill
will understand that there are many comparable variations
of the module design. For example, volatile memory might
be used, or an interface other than a one-wire interface
could be used.

10 The secure module 108 is preferably intended to be
used first by a Service Provider who loads the secure
module 108 with data to enable it to perform useful
functions, and second by an End User who issues commands
to the secure module 108 to perform operations on behalf
15 of the Service Provider for the benefit of the End User.
For this reason, the secure module 108 offers functions
to support the Service Provider in setting up the module
for an intended application. It also offers functions to
allow the End User to invoke the services offered by the
20 Service Provider.

Each Service Provider can reserve a block of NVRAM memory to support its services by creating a transaction group 40 (refer to FIGURES 6 and 7). A transaction group 40 is simply a set of software objects 42 that are defined by the Service Provider. These objects 42 include both data objects (encryption keys, transaction counts, money amounts, date/time stamps, etc.) and transaction scripts 44 which specify how to combine the data objects in useful ways. Each Service Provider creates his own transaction group 40, which is independent of every other transaction group 40. Hence, multiple Service Providers can offer different services in the same module 108. The number of independent Service Providers that can be supported depends on the number and complexity of the objects 42 defined in each transaction group 40. Examples of some of the objects 42 that can be defined within a transaction group 40 are the following:

	RSA Modulus	Clock Offset
	RSA Exponent	Random SALT
20	Transaction Script	Configuration Data

Transaction Counter	Input Data
Money Register	Output Data
Destructor	

5 Within each transaction group 40 the secure module
108 will initially accept certain commands which have an
irreversible effect. Once any of these irreversible
commands are executed in a transaction group 40, they
remain in effect until the end of the module's useful
life or until the transaction group 40, to which it
10 applies, is deleted from the secure module 108. In
addition, there are certain commands which have an
irreversible effect until the end of the module's life or
until a master erase command is issued to erase the
entire contents of the secure module 108. These commands
15 will be discussed further below. These commands are
essential to give the Service Provider the necessary
control over the operations that can be performed by the
End User. Examples of some of the irreversible commands
are:

Privatize Object	Lock Object
Lock Transaction Group	Lock Micro-In-A-Can™

5 Since much of the module's utility centers on its ability to keep a secret, the Privatize command is a very important irreversible command.

10 Once the secure module 108, as a whole, is locked, the remaining NVRAM memory 24 is allocated for a circular buffer for holding an audit trail of previous transactions. Each of the transactions are identified by the number of the transaction group, the number of objects 42 within the specified group, and the date/time stamp.

15 The fundamental concept implemented by the firmware is that the Service Provider can store transaction scripts 44 in a transaction group 40 to perform only those operations among objects that he wishes the End User to be able to perform. The Service Provider can also store and privatize RSA key or keys (encryption

keys) that allow the secure module 108 to "sign" transactions on behalf of the Service Provider, thereby guaranteeing their authenticity. By privatizing and/or locking one or more objects 42 in the transaction group 5 40, the Service Provider maintains control over what the secure module 108 is allowed to do on his behalf. The End User cannot add new transaction scripts 44 and is therefore limited to the operations on objects 42 that can be performed with the transaction scripts 44 10 programmed by the Service Provider.

II. USAGE MODELS OF THE SECURE MODULE 108 AND PORTABLE MODULE 102

This section presents practical applications of the system 100. Each of these applications is described in 15 enough detail to make it clear why the secure module 108 and portable module 102 are important to the system application.

A. TRANSFERRING UNITS OF EXCHANGE OUT OF A PORTABLE
MODULE 102

This section describes an example of how a portable
module 102 and a secure module 108 operate in conjunction
5 with the microprocessor based device 104 so that units of
exchange can be securely transferred out of the portable
module 102 and deposited into the secure module 108
and/or potentially communicated to at least one of the
cash acceptor 110, ATM 112, credit card reader 114, or
10 the phone line 116.

Referring to FIGURE 4, initially the portable module
102 contains its ID number, a count within its
transaction counter and an encrypted data packet stored
in memory. Encrypted within the data packet is the
15 portable modules ID number, the portable modules
transaction count number, and the amount of value (the
monetary value) of the portable module at the present
time X1.

The user of the portable module touches, or somehow puts the portable module 102 into communication with the microprocessor based device 104. For explanation purposes, suppose the portable module 102 is being used
5 as a token used to pay for a train fare. Thus, the microprocessor based device 104 could be, in this case, a turn style that allows the user to enter a train platform. The cost of entering the train platform is known by the microprocessor based device 104.

10 The microprocessor based device 104 reads the portable module's serial number, transaction count, and the encrypted data packet X2. This data could be referred to as a first data.

The microprocessor device 104 then provides the
15 first data along with a first value, being the amount of value to be debited from the portable token (the train fare), to the secure module 108 X3. The secure module 108 decrypts the encrypted data found in the first data using a public key X4.

Next, the secure module 108 makes a few comparisons to make sure that the data received is good data and not counterfeit. The secure module 108 compares the serial number received in the first data with the decrypted
5 serial number X5. If the two serial numbers match then the secure module 108 compares the transaction count received in the first data with the decrypted transaction count X6. If the two transaction counts match then the secure module is comfortable that the data received is
10 not counterfeit data. It is understood that the comparisons can be done in any order.

Furthermore, there may have been a time stamp sent from the portable module 102. The time stamp may indicate a variety of things. One thing could be an
15 indication of whether the portable module is still valid or the time stamp may further enable the secure module to decide if the data is or is not counterfeit.

Assuming all the data passed to the secure module 108 is determined to be valid data, the secure module 108

subtracts the first value, the train fare, from the monetary value of the portable module 102 X7. The decrypted transaction count is then incremented.

5 A register within the secure module 108 is increased by the amount of the first value, the train fare, so that the secure module can keep an accounting of the amount of "money" it has collected X8. The secure module 108 creates a data packet, a second data, which comprises at least the portable module's serial number, the
10 incremented transaction count, and the reduced monetary value of the portable module 102. The second data packet is then encrypted by the secure module 108 using a private key X9.

The microprocessor based device 104 receives the
15 encrypted second data packet, passes the encrypted second data packet to the portable module 102 X10, and opens the turn style to let the module's user onto the train platform. The portable module 102 receives the encrypted second data packet and stores it in memory X11. The

portable module also increments its transaction count indicating that another transaction has occurred X12.

Thus, the above description indicates how valuable information can be transferred between a portable
5 insecure module 102 and a secure module 108 wherein there is a conservation of value. That is, no value is gained or lost. Value that was in the portable module 102 was decreased by the same amount value was added to the secure module 108. In the example provided, the decrease
10 and increase in value was equal to a train fare. Such an increment or decrement can also be equal to an amount provided by an ATM, credit card transaction, cash acceptor, etc.

It is also understood that the insecure portable
15 module 102 could be another secure module similar to the secure module in the system, but programed to act like a portable module 102.

B. TRANSFERRING UNITS OF EXCHANGE INTO THE PORTABLE
MODULE 102

In this example, for simplicity, suppose the portable module does not have any monetary value and the user of the portable module wishes to "fill it up" with value. Suppose the user wishes to take cash out of an ATM machine and instead of pocketing the cash, the user wishes to put the cash value into the portable module 102.

Referring to FIGURE 5, the portable module 102 contains its ID number, a transaction count and an encrypted data packet containing the portable module's ID number, transaction count and the monetary value of the portable module 102 Y1. The microprocessor based device 104, which in this example could be part of the ATM machine 112, receives the information contained in the portable module 102 when a communication is initiated between the portable module 102 and the microprocessor based device 104 Y2.

The microprocessor based device 104 passes the module's serial number, transaction count, and encrypted data packet as a first data packet to the secure module 108. The microprocessor based device also passes the amount of amount of monetary value to add to the portable module 102, as indicated by the ATM 112, to the secure module 108 Y3.

The secure module 108 decrypts the encrypted data passed to it using a public key Y4. The secure module 108 then makes a few comparisons to make sure that the data it has just received is valid and not counterfeit. The secure module 108 compares the serial number (ID number) received in the first data packet with the serial number (ID number) found in the decrypted data Y5. The secure module 108 also compares the transaction count passed the first data packet with the transaction count found in the decrypted data Y6. If the serial numbers and transaction counters match, then the secure module decides that the data received is valid and the secure module adds the monetary value, indicated by the ATM to

the monetary value of the decrypted data Y7. The
decrypted transaction count is incremented Y8. A
register within the secure module may be decremented by
the same amount that the monetary value of the decrypted
5 data was increased Y8.

The secure module 108 creates a second data packet,
that contains the portable module's ID number, the
incremented transaction counter and the increased
monetary value. The second data packet is then encrypted
10 using a private key Y10.

The microprocessor based device 104 reads the
encrypted second data packet and sends it to the portable
module 102 Y11. The portable module receives the
encrypted second data packet and stores it in memory Y12.
15 The portable module also advances its transaction counter
Y13. The result being that the portable module now has
the value of the cash withdrawn from the ATM 112.
Furthermore, a record of the transaction may have been

recorded and kept in the secure module, as well as by the bank that operates the ATM 112.

Exemplary Firmware Definitions for Use With the Secure Module

- 5 **Object** The most primitive data structure accepted by and operated on by the secure modules firmware. A list of valid objects and their definitions is provided in the next section.
- 10 **Group** A self-contained collection of objects. An object's scope is restricted to the group of which it is a member.
- 15 **Group ID** A number preferably between 0 and 255 representing a specific group.

Object ID A number preferably between 0 and 255 representing a specific object within a specific group.

Object Type Preferably a 1-byte type specifier that describes a specific object.
5

PIN An alphanumeric Personal Identification number that is preferably eight bytes in length.

Common PIN The PIN that controls access to shared resources such as the audit trail. It is also used to control the host's ability to create and delete groups.
10

Group PIN The PIN that controls access to operations specific to objects within a group.
15

- Audit Trail** A record of transactions occurring after the secure module has been locked.
- 5 **Locked Object** An object which has been locked by executing the lock object command. Once an object is locked it is not directly readable.
- 10 **Private Object** An object which has been privatized by executing the privatize object command. Once an object is private, it is not directly readable or writable.
- 15 **Locked Group** A group which has been locked using the locked group command. After a group has been locked it will not allow object creation.

Composite Object A combination of several objects.
The individual objects inherit the
attributes of the composite object.

Exemplary Object Definitions

RSA Modulus

5 A large integer preferably of at most 1024 bits in length. It is the product of 2 large prime numbers that are each about half the number of bits in length of the desired modulus size. The RSA modulus is used in the following equations for encrypting and decrypting a message

10 M:

(1) Encryption: $C = M^e \pmod{N}$

(2) Decryption: $M = C^d \pmod{N}$

15 where C is the cyphertext, d and e are the RSA exponents (see below), and N is the RSA modulus.

RSA Exponent

5 Both e and d (shown in equations 1
and 2 above) are RSA exponents.
They are typically large numbers but
are smaller than the modulus (N).
10 RSA exponents can be either private
or public. When RSA exponents are
created in the secure module, they
may be declared as either. Once
created an exponent may be changed
15 from a public exponent to a private
exponent. After an exponent has
been made private, however, it will
remain private until the transaction
group 40 to which it belongs is
destroyed.

Transaction Script

20 A transaction script is a series of
instructions to be carried out by
the secure module. When invoked the
secure module firmware interprets
the instructions in the script and

5 places the results in the output
data object (see below). The actual
script is simply a list of objects.
The order in which the objects are
listed specifies the operations to
be performed on the objects.
transaction scripts 44 preferably
may be as long as 128 bytes.

10 **Transaction Counter** The transaction counter object is
preferably 4 bytes in length and is
usually initialized to zero when it
is created. Every time a
transaction script, which references
this object, is invoked, the
15 transaction counter increments by 1.
Once a transaction counter has been
locked it is read only and provides
an irreversible counter.

Money Register

5 The money register object is preferably 4 bytes in length and may be used to represent money or some other form of credit. Once this object has been created, it must be locked to prevent a user from tampering with its value. Once locked the value of this object can be altered only by invoking a transaction script. A typical transaction group 40 which performs monetary transactions might have one script for withdrawals from the money register and one for deposits to the money register.

10

15

Clock Offset

20 This object is preferably a 4 byte number which contains the difference between the reading of the secure module's real-time clock and some convenient time (e.g., 12:00 a.m.,

January 1, 1970). The true time can then be obtained from the secure module by adding the value of the clock offset to the real-time clock.

5 **SALT**

10

15

A SALT object is preferably 20 bytes in length and should be initialized with random data when it is created. When a host transmits a generate random SALT command, the secure module combines the previous SALT with the secure module's random number (produced preferably by randomly occurring power-ups) to generate a new random SALT. If the SALT object has not been privatized it may subsequently be read by issuing a read object command.

Configuration Data This is a user defined structure with preferably a maximum length of

5 128 bytes. This object is typically
used to store configuration
information specific to its
transaction group 40. For example,
the configuration data object may be
used to specify the format of the
money register object (i.e., the
type of currency it represents).
10 Since this object has no pre-defined
structure, it may never be used by a
transaction object.

Input Data

15 An input data object is simply an
input buffer with preferably a
maximum length of 128 bytes. A
transaction group may have multiple
input objects. The host uses input
data objects to store data to be
processed by transaction scripts 44.

Output Data

5

The output data object is used by transaction scripts as an output buffer. This object is automatically created when the transaction group is created. It is preferably 512 bytes in length and inherits password protection from its group.

Random Fill

10

15

When the script interpreter encounters this type of object it automatically pads the current message so that its length is 1 bit smaller than the length of the preceding modulus. A handle to this object is automatically created when the transaction group is created. It is a private object and may not be read using the read object command.

Working Register This object is used by the script interpreter as working space and may be used in a transaction script. A handle to this object is automatically created when the transaction group is created. It is a private object and may not be read using the read object command.

5

ROM Data This object is automatically created when the transaction group is created. It is a locked object and may not be altered using the write object command. This object is 8 bytes and length and its contents are identical to the 8 by ROM data of the Micro-In-A-Can™.

10

15

Preferred Secure module Firmware Command Set

Set Common PIN(01H)

Transmit (to secure module)

01H, old PIN, new PIN, PIN option byte

5 Receive data

 CSB (command status byte) = 0 if successful,
appropriate error code otherwise

 Output length = 0

 Output Data = 0

10 Notes:

 The PIN option byte may be the bitwise-or of any of
the following values:

 PIN_TO_ERASE 00000001b (require PIN for
Master Erase)

15 PIN_TO_CREATE 00000010b (require PIN for
group creation).

Initially the secure module has a PIN (Personal Identification Number) of 0 (Null) and an option byte of 0. Once a PIN has been established it can only be changed by providing the old PIN or by a Master Erase.
5 However, if the PIN_TO_ERASE bit is set in the option byte, the PIN can only be changed through the set common PIN command.

Possible error codes for the set common PIN command:

10	ERR_BAD_COMMON_PIN	(Common PIN match failed)
	ERR_BAD_PIN_LENGTH	(New PIN length > 8 bytes)
	ERR_BAD_OPTION_BYTE	(Unrecognizable option byte)

15 For all commands described in this section, data received by the host will be in the form of a return packet. A return packet has the following structure:

Command status byte (0 if command successful,
error code otherwise, 1 byte)

Output data length (Command output length, 2
bytes)

5 Output data (Command output, length
specified above).

Master Erase (02H)

Transmit data

02H, Common PIN

10 Receive data

CSB = 0 if command was successful,
ERR_BAD_COMMON_PIN otherwise

Output length = 0

Output data = 0

15 Notes:

If the LSB (least significant bit) of the PIN option
is clear (i.e. PIN not required for Master Erase) then a
*

0 is transmitted for the Common PIN value. In general
this text will always assume a PIN is required. If no
PIN has been established a 0 should be transmitted as the
PIN. This is true of the common PIN and group PINS (see
5 below). If the PIN was correct the firmware deletes all
groups (see below) and all objects within the groups.
The common PIN and common PIN option byte are both reset
to zero.

After everything has been erased the secure module
10 transmits the return packet. The CSB is as described
above. The output data length and output data fields are
both set to 0.

Create Group (03H)

Transmit data

15 03H, Common PIN, Group name, Group PIN

Receive data

CSB = 0 if command successful, appropriate
error code otherwise

Output length = 1 if successful, 0 otherwise

5 Output data = Group ID if successful, 0
otherwise

Notes:

The maximum group name length is 16 bytes and the
maximum PIN length is eight bytes. If the PIN_TO_CREATE
10 bit is set in the common PIN option byte and the PIN
transmitted does not match the common PIN the secure
module will set the OSC to ERR_BAD_COMMON_PIN.

Possible error return codes for the create group
command:

15 ERR_BAD_COMMON_PIN (Incorrect common PIN)
 ERR_BAD_NAME_LENGTH (If group name length > 16
bytes)

ERR_BAD_PIN_LENGTH (If group PIN length
> 8 bytes)

ERR_MIAC_LOCKED (The secure module has
been locked)

5 ERR_INSUFFICIENT_RAM (Not enough memory for
new group)

Set_Group_PIN (04H)

Transmit data

04H, Group ID, old GPIN, new GPIN

10 Receive data

CSB = 0 if command successful, appropriate
error code otherwise

Output length = 0

Output data = 0

Notes:

The Group PIN only restricts access to objects within the group specified by the group ID transmitted in the command packet.

5 Possible error codes for the set group PIN command:

ERR_BAD_GROUP_PIN (Group PIN match failed)

ERR_BAD_PIN_LENGTH (New group PIN length > 8 bytes)

10 Create Object (05H)

Transmit data

05H, Group ID, Group PIN, Object type, Object attributes, Object data

Receive data

15 CSB = 0 if command successful, appropriate error code otherwise

Output length = 1 if successful, 0 otherwise

Output data = object ID if successful, 0
otherwise

Notes:

5 If the Create Object command is successful the
secure module firmware returns the object's ID within the
group specified by the Group ID. If the PIN supplied by
the host was incorrect or the group has been locked by
the Lock Group command (described below) the secure
10 module returns an error code in the CSB. An object
creation will also fail if the object is invalid for any
reason. For example, if the object being created is an
RSA modulus (type 0) and it is greater than 1024 bits in
length. transaction script creation will succeed if it
15 obeys all transaction scripts rules.

Possible error return codes for the create object
command:

ERR_BAD_GROUP_PIN (Incorrect group PIN)

ERR_GROUP_LOCKED (The group has been
locked)
ERR_MIAC_LOCKED (The secure module has
been locked)
5 ERR_INVALID_TYPE (The object type
specified is invalid)
ERR_BAD_SIZE (The objects length
was invalid)
ERR_INSUFFICIENT_RAM (Not enough memory for
10 new object)

Object types: RSA modulus 0
RSA exponent 1
Money register 2
15 Transaction counter 3
Transaction script 4
Clock offset 5
Random SALT 6
Configuration object 7
20 Input data object 8
Output data object 9

Object Attributes:	Locked	00000001b
	Privatized	00000010b

Objects may also be locked and privatized after
creation by using the Lock Object and Privatize Object
5 commands described below.

Lock Object (06H)

Transmit data

06H, Group ID, Group PIN, Object ID

Receive data

10 CSB = 0 if command successful, appropriate
error code otherwise

Output length = 0

Output data = 0

Notes:

If the Group ID, Group PIN and Object ID are all correct, the secure module will lock the specified object. Locking an object is an irreversible operation.

5 Possible error return codes for the lock object
command:

	ERR_BAD_GROUP_PIN	(Incorrect group PIN)
	ERR_GROUP_LOCKED	(The group has already been locked)
10	ERR_MIAC_LOCKED	(The secure module has been locked)
	ERR_BAD_GROUP_ID	(Specified group does not exist)
	ERR_BAD_OBJECT_ID	(Specified object does not exist)

15

Privatize Object (07H)

Transmit data

07H, Group ID, Group PIN, Object ID

Receive data

CSB = 0 if successful, appropriate error code
otherwise

5 Notes:

If the Group ID, Group PIN and Object ID were valid
the object will be privatized. Privatized objects share
all the properties of locked objects but are not
readable. Privatized objects are only modifiable through
10 transaction scripts. Note that locking a privatized
object is legal, but has no meaning since object
privatization is a stronger operation than object
locking. Privatizing an object is an irreversible
operation.

15 Possible error return codes for the privatize object
command:

ERR_BAD_GROUP_PIN (Incorrect group PIN)

ERR_GROUP_LOCKED (The group has already
been locked)

ERR_MIAC_LOCKED (The secure module has
been locked)

5 ERR_BAD_GROUP_ID (Specified group does
not exist)

ERR_BAD_OBJECT_ID (Specified object does
not exist)

Make Object Destructable (08H)

10 Transmit data

08H, Group ID, Group PIN, Object ID

Receive data

CSB = 0 if successful, appropriate error code
otherwise

15 Notes:

If the Group ID, Group PIN and Object ID were valid
the object will be made destructable. If an object is
destructable it becomes unusable by a transaction script
after the groups destructor becomes active. If no

destructor object exists within the transaction group the destructible object attribute bit has no affect. Making an object destructable is an irreversible operation.

5 Possible error return codes for the make object destructable command:

	ERR_BAD_GROUP_PIN	(Incorrect group PIN)
	ERR_GROUP_LOCKED	(The group has already been locked)
10	ERR_MIAC_LOCKED	(The secure module has been locked)
	ERR_BAD_GROUP_ID	(Specified group does not exist)
	ERR_BAD_OBJECT_ID	(Specified object does not exist)

15 Lock Secure module (09H)

Transmit data

09H, Common PIN

Receive data

CSB = 0 if successful, appropriate error code
otherwise

Output length = 2 if successful, 0 otherwise

5 Output data = audit trail size if successful,
0 otherwise

Notes:

10 If the host supplied Common PIN is correct and the
secure module has not previously been locked, the command
will succeed. When the secure module is locked it will
not accept any new groups or objects. This implies that
all groups are automatically locked. The RAM not used by
the system or by groups will be used for an audit trail.
There is no audit trail until the secure module has
15 successfully been locked!

An audit trail record is six bytes long and has the
following structure:

Group ID | Object ID | Date/Time stamp.

Once an audit trail has been established, a record of the form shown above will be stored in the first available size byte location every time a transaction script is executed. Note that since the secure module must be locked before the audit trail begins, neither the group ID nor any object ID is subject to change. This will always allow an application processing the audit trail to uniquely identify the transaction script that was executed. Once the audit trail has consumed all of its available memory, it will store new transaction records over the oldest transaction records.

Possible error codes for the lock secure module command:

ERR_BAD_COMMON_PIN	(Supplied common PIN was incorrect)
ERR_MIAC_LOCKED	(Secure module was already locked)

Lock Group (0AH)

Transmit data

0AH, Group ID, Group PIN

Receive data

5 CSB = 0 if command successful, appropriate
error code otherwise

Output length = 0

Output data = 0

Notes:

10 If the group PIN provided is correct the secure
module BIOS will not allow further object creation within
the specified group. Since groups are completely self-
contained entities they may be deleted by executing the
Delete Group command (described below).

15 Possible error return codes for the lock group
command:

ERR_BAD_GROUP_PIN (Incorrect group PIN)
ERR_GROUP_LOCKED (The group has already
been locked)
ERR_MIAC_LOCKED (The secure module has
5 been locked)
ERR_BAD_GROUP_ID (Specified group does
not exist)

Invoke Transaction Script (OBH)

Transmit data
10 OBH, Group ID, Group PIN, Object ID

Receive data
CSB = 0 if command successful, appropriate
error code otherwise
Output length = 1 if successful, 0 otherwise
15 Output data = estimated completion time

Notes:

The time estimate returned by the secure module is in sixteenths of a second. If an error code was returned in the CSB, the time estimate will be 0.

5 Possible error return codes for the execution transaction script command:

ERR_BAD_GROUP_PIN (Incorrect group PIN)

ERR_BAD_GROUP_ID (Specified group does not exist)

10 ERR_BAD_OBJECT_ID (Script object did not exist in group)

Read Object (0CH)

Transmit data

0CH, Group ID, Group PIN, Object ID

15 Receive data

CSB = 0 if command successful, appropriate error code otherwise

Output length = object length if successful, 0
otherwise

Output data = object data if successful, 0
otherwise

5 Notes:

If the Group ID, Group PIN and Object ID were correct, the secure module checks the attribute byte of the specified object. If the object has not been privatized the secure module will transmit the object data to the host. If the Group PIN was invalid or the object has been privatized the secure module will return a 0 in the output length, and data fields of the return packet.

Possible error codes for the read object command:

15 ERR_BAD_GROUP_PIN (Incorrect group PIN)
 ERR_BAD_GROUP_ID (Specified group does
not exist)

ERR_BAD_OBJECT_ID (Object did not exist
in group)

ERR_OBJECT_PRIVATIZED (Object has been
privatized)

5 Write Object (ODH)

Transmit data

ODH, Group ID, Group PIN, Object ID, Object
size, Object Data

Receive data

10 CSB = 0 if successful, appropriate error code
otherwise

Output length = 0

Output data = 0

Notes:

15 If the Group ID, Group PIN and Object ID were
correct, the secure module checks the attribute byte of
the specified object. If the object has not been locked
or privatized the secure module will clear the objects

previous size and data and replace it with the new object data. Note that the object type and attribute byte are not affected.

Possible error codes for the write object command:

5	ERR_BAD_GROUP_PIN	(Incorrect group PIN)
	ERR_BAD_GROUP_ID	(Specified group does not exist)
	ERR_BAD_OBJECT_ID	(Object did not exist in group)
10	ERR_BAD_OBJECT_SIZE	(Illegal object size specified)
	ERR_OBJECT_LOCKED	(Object has been locked)
15	ERR_OBJECT_PRIVATIZED	(Object has been privatized)

Read Group Name (0EH)

Transmit data

0EH, Group ID

Receive data

5

CSB = 0

Output Length = length of group name

Output data = group name

Notes:

10 The group name length is a maximum of 16 bytes. All
byte values are legal in a group name.

Delete Group (0FH)

Transmit data

0FH, Group ID, Group PIN

Receive data

CSB = 0 if successful, appropriate error code
otherwise

Output length = 0

Output data = 0

5 Notes:

If the group PIN and group ID are correct the secure
module will delete the specified group. Deleting a group
causes the automatic destruction of all objects within
the group. If the secure module has been locked the

10 Delete Group command will fail.

Possible error codes for the delete group command:

ERR_BAD_GROUP_PIN (Incorrect group PIN)

ERR_BAD_GROUP_ID (Specified group does
not exist)

15 ERR_MIAC_LOCKED (Secure module has
been locked)

Get Command Status Info (10H)

Transmit data

10H

Receive data

5

CSB = 0

Output length = 6

Output data = secure module status structure

(see below)

Notes:

10

This operation requires no PIN and never fails. The status structure is defined as follows:

Last command executed	(1 byte)
Last command status	(1 byte)
Time command received	(4 bytes)

Get Secure module Configuration Info (11H)

Transmit data

11H

Receive data

5 CSB = 0
 Output length = 4
 Output data = secure module configuration
structure

Notes:

10 This operation requires no PIN and never fails. The
configuration structure is defined as follows:

Number of groups	(1 byte)
Flag byte (see below)	(1 byte)
Audit trail size/Free RAM	(2 bytes)

15 The flag byte is the bitwise-or of any of the
following values:

00000001b (Secure module is locked)

00000010b (Common PIN required for access)

Read Audit Trail Info (12H)

Transmit data

5 12H, Common PIN

Receive data

CSB = 0 if command successful, appropriate
error code otherwise

10 Output length = audit trail structure size (5)
if successful, 0 otherwise

Output data = audit trail info structure if
successful, 0 otherwise

Notes:

15 If the transmitted Common PIN is valid and the
secure module has been locked, it returns audit trail
configuration information as follows:

Number of used transaction records (2 bytes)

Number of free transaction records (2 bytes)

A boolean specifying whether or (1 byte)
not the audit trail rolled

5 since previous read command

Possible error codes for the read audit trail info
command:

ERR_BAD_COMMON_PIN (Common PIN was
incorrect)

10 ERR_MIAC_NOT_LOCKED (Secure module is not
locked)

Read Audit Trail (13H)

Transmit data

13H, Common PIN

15 Receive data

CSB = 0 if command successful, appropriate
error code otherwise

Output length = # of new records * 6 if
successful, 0 otherwise

5 Output data = new audit trail records

Notes:

If the transmitted common PIN is valid and the
secure module has been locked, it will transfer all new
transaction records to the host.

10 Possible error codes for the read audit trail
command:

ERR_BAD_COMMON_PIN (Common PIN was
incorrect)

ERR_MIAC_NOT_LOCKED secure module is not locked

Read Group Audit Trail (14H)

Transmit data

14H, Group ID, Group PIN

Receive data

5 CSB = 0 if command successful, appropriate
error code otherwise

 Output length = # of records for group * 6 if
successful, 0 otherwise

 Output data = audit trail records for group

10 Notes:

 This command is identical to the read audit trail
command, except that only records involving the group ID
specified in the transmit data are returned to the host.

15 This allows transaction groups to record track their own
activities without seeing other groups records.

 Possible error codes for the read group audit trail
command:

ERR_BAD_GROUP_ID (Group ID does not
exist)

ERR_BAD_GROUP_PIN (Common PIN was
incorrect)

5 ERR_MIAC_NOT_LOCKED (The secure module is
not locked)

Read Real Time Clock (15H)

Transmit data

15H, Common PIN

10 Receive data

CSB = 0 if the common PIN matches and
ERR_BAD_COMMON_PIN otherwise

Output length = 4

15 Output data = 4 most significant bytes of the
real time clock

Notes:

This value is not adjusted with a clock offset.
This command is normally used by a service provider to
compute a clock offset during transaction group creation.

5 Read Real Time Clock Adjusted (16H)

Transmit data

16H, Group ID, Group PIN, ID of offset object

Receive data

CSB = 0 if successful, appropriate error code

10 otherwise

Output length = 4 if successful, 0 otherwise

Output data = Real time clock + clock offset ID

Notes:

15 This command succeeds if the group ID and group PIN
are valid, and the object ID is the ID of a clock offset.
The secure module adds the clock offset to the current
value of the 4 most significant bytes of the RTC and

returns that value in the output data field. Note that a transaction script may be written to perform the same task and put the result in the output data object.

Possible error codes for the real time clock
5 adjusted command:

	ERR_BAD_GROUP_PIN	(Incorrect group PIN)
	ERR_BAD_GROUP_ID	(Specified group does not exist)
10	ERR_BAD_OBJECT_TYPE	(Object ID is not a clock offset)

Get Random Data (17H)

Transmit data

17H, Length (L)

Receive data

15 CSB = 0 if successful, appropriate error code
otherwise

Output length = L if successful, 0 otherwise
Output data = L bytes of random data if
successful

Notes:

5 This command provides a good source of
cryptographically useful random numbers.

Possible error codes for the get random data command
are:

ERR_BAD_SIZE (Requested number of bytes
10 > 128)

Get Firmware Version ID (18H)

Transmit data
18H

Receive data
15 CSB = 0

Output length = Length of firmware version ID
string

Output data = Firmware version ID string

Notes:

- 5 This command returns the firmware version ID as a
Pascal type string (length + data).

Get Free RAM (19H)

Transmit data

19H

- 10 Receive data

CSB = 0

Output length = 2

Output data = 2 byte value containing the
amount of free RAM

Notes:

If the secure module has been locked the output data bytes will both be 0 indicating that all memory not used by transaction groups has been reserved for the audit trail.

Change Group Name (1AH)

Transmit data

1AH, Group ID, Group PIN, New Group name

Receive data

10 CSB = 0 if successful or an appropriate error code otherwise

Output length = 0

Output data = 0

Notes:

15 If the group ID specified exists in the secure module and the PIN supplied is correct, the transaction group name is replaced by the new group name supplied by

the host. If a group ID of 0 is supplied the PIN transmitted must be the common PIN. If it is correct, the secure module name is replaced by the new name supplied by the host.

5 Possible error codes for the change group name
command:

 ERR_BAD_GROUP_PIN (Incorrect group PIN)

 ERR_BAD_GROUP_ID (Specified group does

not exist)

10 ERR_BAD_NAME_LENGTH (New group name > 16 bytes)

ERROR CODE DEFINITIONS

ERR_BAD_COMMAND (80H)

This error code occurs when the secure module
firmware does not recognize the command just transmitted
5 by the host.

ERR_BAD_COMMON_PIN (81H)

This error code will be returned when a command
requires a common PIN and the PIN supplied does not match
the secure module's common PIN. Initially the common PIN
10 is set to 0.

ERR_BAD_GROUP_PIN (82H)

Transaction groups may have their own PIN, FIGURE 6.
If this PIN has been set (by a set group PIN command) it
must be supplied to access any of the objects within the
15 group. If the Group PIN supplied does not match the

actual group PIN, the secure module will return the
ERR_BAD_GROUP_PIN error code.

ERR_BAD_PIN_LENGTH (83H)

There are 2 commands which can change PIN values.
5 The set group PIN and the set common PIN commands. Both
of these require the new PIN as well as the old PIN. The
ERR_BAD_PIN_LENGTH error code will be returned if the old
PIN supplied was correct, but the new PIN was greater
than 8 characters in length.

10 ERR_BAD_OPTION_BYTE (84H)

The option byte only applies to the common PIN.
When the set common PIN command is executed the last byte
the host supplies is the option byte (described in
command section). If this byte is unrecognizable to the
15 secure module, it will return the ERR_BAD_OPTION_BYTE
error code.

ERR_BAD_NAME_LENGTH (85H)

When the create transaction group command is executed, one of the data structures supplied by the host is the group's name. The group name may not exceed 16
5 characters in length. If the name supplied is longer than 16 characters, the ERR_BAD_NAME_LENGTH error code is returned.

ERR_INSUFFICIENT_RAM (86H)

The create transaction group and create object
10 commands return this error code when there is not enough heap available in the secure module.

ERR_MIAC_LOCKED (87H)

When the secure module has been locked, no groups or objects can be created or destroyed. Any attempts to
15 create or delete objects will generate an ERR_MIAC_LOCKED error code.

ERR_MIAC_NOT_LOCKED (88H)

If the secure module has not been locked there is no audit trail. If one of the audit trail commands is executed this error code will be returned.

5

ERR_GROUP_LOCKED (89H)

Once a transaction group has been locked object creation within that group is not possible. Also the objects attributes and types are frozen. Any attempt to create objects or modify their attribute or type bytes will generate an ERR_GROUP_LOCKED error code.

10

ERR_BAD_OBJECT_TYPE (8AH)

When the host sends a create object command to the secure module, one of the parameters it supplies is an object type (see command section). If the object type is not recognized by the firmware it will return an ERR_BAD_OBJECT_TYPE error code.

15

ERR_BAD_OBJECT_ATTR (8BH)

When the host sends a create object command to the secure module, one of the parameters it supplies is an object attribute byte (see command section). If the
5 object attribute byte is not recognized by the firmware it will return an ERR_BAD_OBJECT_ATTR error code.

ERR_BAD_SIZE (8CH)

An ERR_BAD_SIZE error code is normally generated when creating or writing an object. It will only occur
10 when the object data supplied by the host has an invalid length.

ERR_BAD_GROUP_ID (8DH)

All commands that operate at the transaction group level require the group ID to be supplied in the command
15 packet. If the group ID specified does not exist in the

secure module it will generate an ERR_BAD_GROUP_ID error code.

ERR_BAD_OBJECT_ID (8EH)

5 All commands that operate at the object level require the object ID to be supplied in the command packet. If the object ID specified does not exist within the specific transaction group (also specified in the command packet) the secure module will generate an ERR_BAD_OBJECT_ID error code.

10 ERR_INSUFFICIENT_FUNDS (8FH)

If a script object that executes financial transactions is invoked and the value of the money register is less than the withdrawal amount requested an ERR_INSUFFICIENT_FUNDS error code will be returned.

ERR_OBJECT_LOCKED (90H)

Locked objects are read only. If a write object command is attempted and it specifies the object ID of a locked object the secure module will return an
5 ERR_OBJECT_LOCKED error code.

ERR_OBJECT_PRIVATE (91H)

Private objects are not directly readable or writable. If a read object command or a write object command is attempted, and it specifies the object ID of
10 a private object, the secure module will return an ERR_OBJECT_PRIVATE error code.

ERR_OBJECT_DESTROYED (92H)

If an object is destructible and the transaction group's destructor is active the object may not be used
15 by a script. If a script is invoked which uses an object

which has been destructed, an ERR_OBJECT_DESTRUCTED error code will be returned by the secure module.

5 The exemplary embodiment of the present invention is preferably placed within a durable stainless steel, token-like can. It is understood that an exemplary secure module can be placed in virtually any articulatable item. Examples of articulatable items include credit cards, rings, watches, wallets, purses, necklaces, jewelry, ID badges, pens, clipboards, etc.

10 The secure module 108 preferably is a single chip "trusted computer". By the word "trusted" it is meant that the computer is extremely secure from tampering by unwarranted means. The secure module incorporates a numeric coprocessor optimized for math intensive
15 encryption. The BIOS is preferably immune to alteration and specifically designed for very secure transactions.

Each secure module can have a random "seed" generator with the ability to create a private/public key set. The private key never leaves the secure module and is only known by the secure module. Furthermore,
5 discovery of the private key is prevented by active self-destruction upon wrongful entry into the secure module. The secure module can be bound to the user by a personal identification number (PIN).

When transactions are performed by the secure module
10 108 certificates of authentication are created by either or both the secure module and a system the secure module communicates with. The certificate can contain a variety of information. In particular, the certificate may contain:

- 15
- 1) who is the secure module user via a unique registration number and a certified public key.
 - 2) when the transaction took place via a true-time stamping of the transaction.

- 3) where the transaction took place via a registered secure module interface site identification.
- 4) security information via uniquely serialized transactions and digital sign on message digests.
- 5) secure module status indicated as valid, lost, or expired.

Although a preferred embodiment of the method and apparatus of the present invention has been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiment disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

2
Segh,
A1

1 WHAT IS CLAIMED IS:

2 1. A system for communicating data securely,
3 comprising:

4 a first module for containing a first data;
5 an electronic system comprising a secure module,
6 said electronic system adapted to be able to communicate
7 with said first module.

1 2. The system of claim 1, wherein said first module
2 is a portable module.

1 3. The system of claim 1, wherein said first
2 module comprises a memory circuit for storing said first
3 data.

1 4. The system of claim 3, wherein said memory
2 circuit contains an encrypted data.

1 5. The system of claim 1, wherein said first
2 module comprises an identification means for identifying
3 said first module to said electronic system.

1 6. The system of claim 1, wherein said first
2 module comprises a counter for counting a number of
3 transactions said first module performed with said
4 electronic system.

Sub
B

1 7. The system of claim 6, wherein said number of
2 transactions represent the number of times a memory data
3 is changed in said module.

1 8. The system of claim 1, wherein said electronic
2 system is adapted to communicate with said first module
3 via a single conductive contact.

1 9. The system of claim 1, wherein said electronic
2 system is adapted to communicate with said first module
3 via a one-wire bus.

1 10. The system of claim 1, wherein said first
2 module is another secure module.

1 11. A system of claim 1, wherein said secure module
2 is adapted to receive said first data.

1 12. The system of claim 1, wherein said secure
2 module is adapted to receive said first data and create
3 a second data that contains at least one information that
4 was in said first data.

1 13. The system of claim 12, wherein said second
2 data is encrypted.

1 14. The system of claim 1, wherein said secure
2 module contains a substantially inaccessible private key
3 in memory portion of said secure module.

1 15. The system of claim 1, wherein said electronic
2 system is connected to at least one of a credit card
3 reader, a cash acceptor, a cash provider, an automatic
4 teller machine and a communication line.

1 16. A method for electronically transferring units
2 of exchange between a first module and a second module,
3 comprising the steps of:
4 a. initiating communication between said first
5 module and an electronic device;
6 b. passing a first value datum from said first
7 module to said electronic device;
8 c. passing said first value datum from said
9 electronic device to said second module;
10 d. performing a mathematical calculation on said
11 first value datum thereby creating a second value datum;
12 e. passing said second value datum from said
13 second module to said electronic device;
14 f. passing said second value datum from said
15 electronic device to said first module;
16 g. storing said second value datum in said first
17 module; and
18 h. discontinuing communication between said first
19 module and said electronic device.

1 17. The method of claim 16, wherein said first
2 value datum represents a monetary equivalent.

1 18. The method of claim 16, wherein said first
2 value datum is encrypted.

1 19. The method of claim 16, wherein said second
2 value datum is encrypted.

1 20. The method of claim 18, wherein the step of
2 performing a mathematical calculation comprises the steps
3 of:

4 m. decrypting said first value datum with a public
5 key thereby creating a decrypted value;

6 n. performing at least one of an addition function
7 and a subtraction function on said decrypted value
8 thereby creating a value result; and

9 o. encrypting said value result with a private key
10 thereby creating said second value datum.

- 1 21. wherein the step (b) of passing is performed
- 2 over at least a ~~single~~ conductive contact.

add
A2

add
B4

add
C1

**RULES 63 AND 67 (37 C.F.R. 1.63 and 1.67)
DECLARATION AND POWER OF ATTORNEY**

FOR UTILITY/DESIGN/CIP/PCT NATIONAL APPLICATIONS

As a named inventor, **STEPHEN M. CURRY, DONALD W. LOOMIS, and MICHAEL L. BOLAN**, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; and

I believe that I am the original, first and sole inventor (if only one name is listed above) or an original, first and joint inventor (if plural names are listed above) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE**, the specification of which: (mark only one)

- (a) is attached hereto.
- (b) was filed on _____ as Application Serial No. _____
- (c) was filed as PCT International Application No. PCT/_____ on _____ and was amended on _____ (if applicable).
- (d) was filed on _____ as Application Serial No. _____ and issued as Patent No. _____ on _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above or as allowed as indicated above.

I acknowledge the duty to disclose all information known to me to be material to the patentability of this application as defined in 37 CFR § 1.56. If this is a continuation-in-part (CIP) application, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose to the Office all information known to me to be material to patentability of the application as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this CIP application.

I hereby claim foreign priority benefits under 35 U.S.C. § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate filed by me or my assignee disclosing the subject matter claimed in this application and having a filing date (1) before that of the application

PATENT APPLICATION
DOCKET NO.: 20661/429

on which my priority is claimed or, (2) if no priority is claimed, before the filing date of this application:

PRIOR FOREIGN PATENTS

Number	Country	Month/Day/Year Filed	Date first laid- open or Published	Date patented or Granted	Priority Claimed	
					Yes	No
---	---	---	---	---	---	---
---	---	---	---	---	---	---

I hereby claim the benefit under 35 U.S.C. § 120/365 of any United States application(s) listed below and PCT international applications listed above or below:

PRIOR U.S. OR PCT APPLICATIONS

Application No. (series code/serial no.)	Month/Day/Year Filed	Status(pending, abandoned, patented)
---	---	---
---	---	---

I hereby appoint:

H. MATHEWS GARLAND, Reg. No. 19,129	P. WESTON MUSSELMAN, JR., Reg No. 31,644	STEVEN R. GREENFIELD, Reg. No. 38,166
THOMAS L. CANTRELL, Reg. No. 20,849	ROGER L. MAXWELL, Reg. No. 31,855	CRAIG A. HOERSTEN, Reg. No. 38,917
THOMAS L. CRISMAN, Reg. No. 24,846	JEFFERY E. BACON, Reg. No. 35,055	STUART D. DWORK, Reg. No. 31,103
STANLEY R. MOORE, Reg. No. 26,958	ANDRE M. SZUWALSKI, Reg. No. 35,701	
GERALD T. WELCH, Reg. No. 30,332	J. KEVIN GRAY, Reg. No. 37,141	

all of the firm of **JENKENS & GILCHRIST, P.C.**, 3200 Fountain Place, 1445 Ross Avenue, Dallas, Texas 75202-2799, as my attorneys and/or agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith, and to file and prosecute any international patent application filed thereon before any international authorities under the Patent Cooperation Treaty, and I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization who/which first sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct them in writing to the contrary.

Please address all correspondence and direct all telephone calls to:

Steven R. Greenfield
Jenkins & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
214/855-4789
214/855-4300 (fax)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAMED INVENTOR(S)

1	STEPHEN M. CURRY		
	Full Name	Inventor's Signature	Date
	6646 Clearhaven Circle Dallas, TX 75248		USA
	Residence (city, state, country)		Citizenship
	6646 Clearhaven Circle Dallas, TX 75248 Post Office Address (include zip code)		

2	DONALD W. LOOMIS		
	Full Name	Inventor's Signature	Date
	316 Dakota Lane Coppell, TX 75019		USA
	Residence (city, state, country)		Citizenship
	316 Dakota Lane Coppell, TX 75019 Post Office Address (include zip code)		

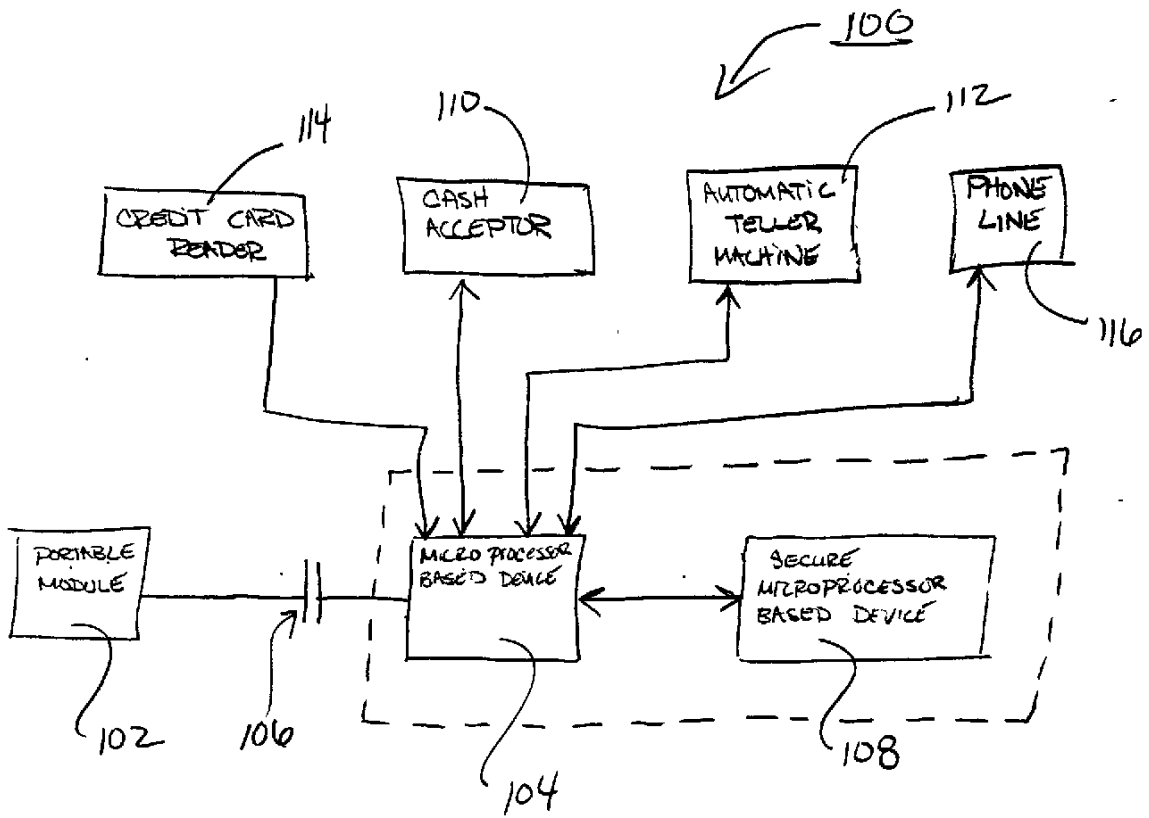
PATENT APPLICATION
DOCKET NO.: 20661/429

3	MICHAEL L. BOLAN		
	Full Name	Inventor's Signature	Date
	6214 Misty Trail Dallas, TX 75248		USA
	Residence (city, state, country)		Citizenship
	6214 Misty Trail Dallas, TX 75248		
	Post Office Address (include zip code)		

(FOR ADDITIONAL INVENTORS, check here ___ and add additional sheet for inventor information regarding signature, name, date, citizenship, residence and address)

200601-429

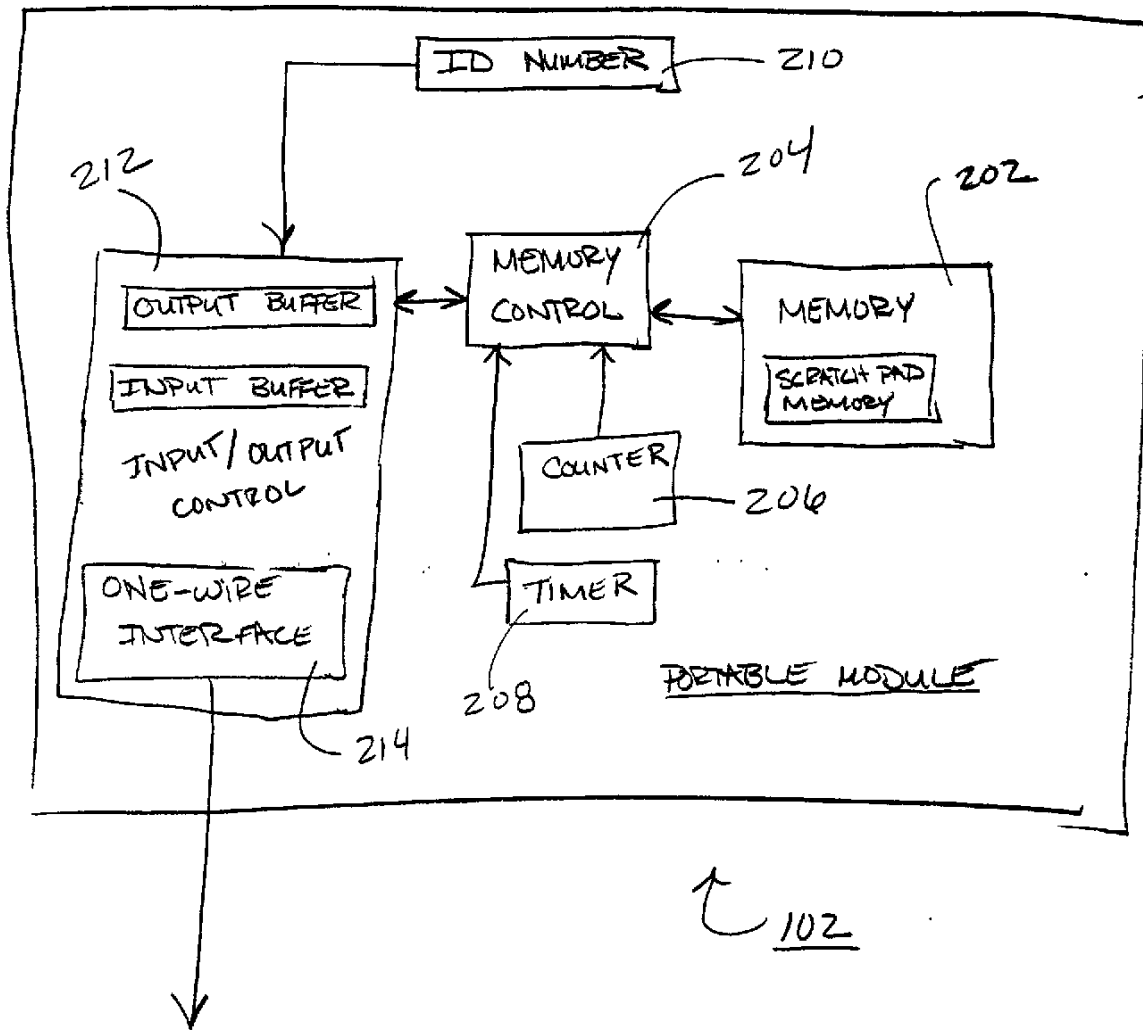
FIGURE 1



200601-429 08/594975

~~XXXXXXXXXX~~

FIGURE 2



20661-429

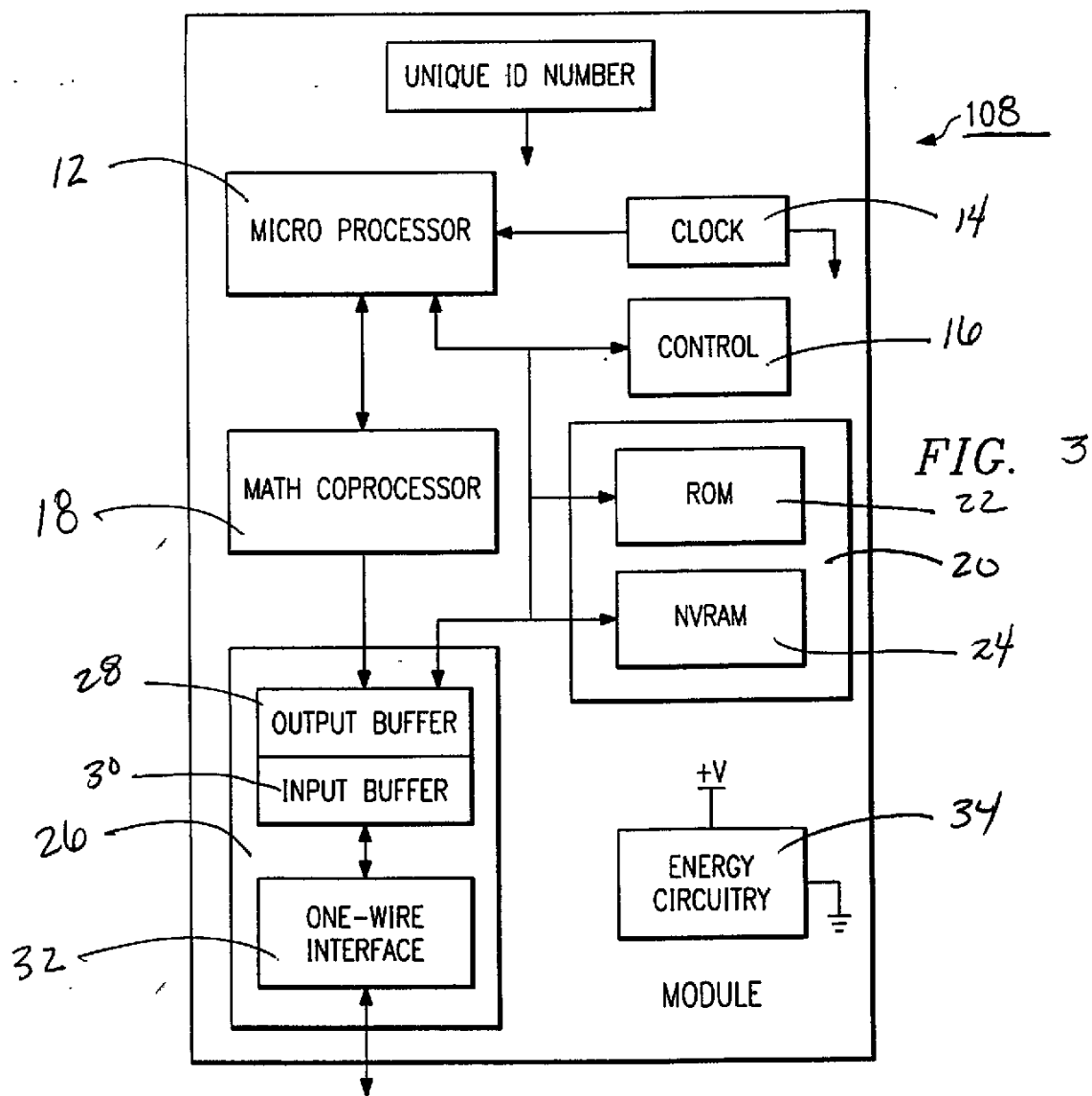


FIGURE 4

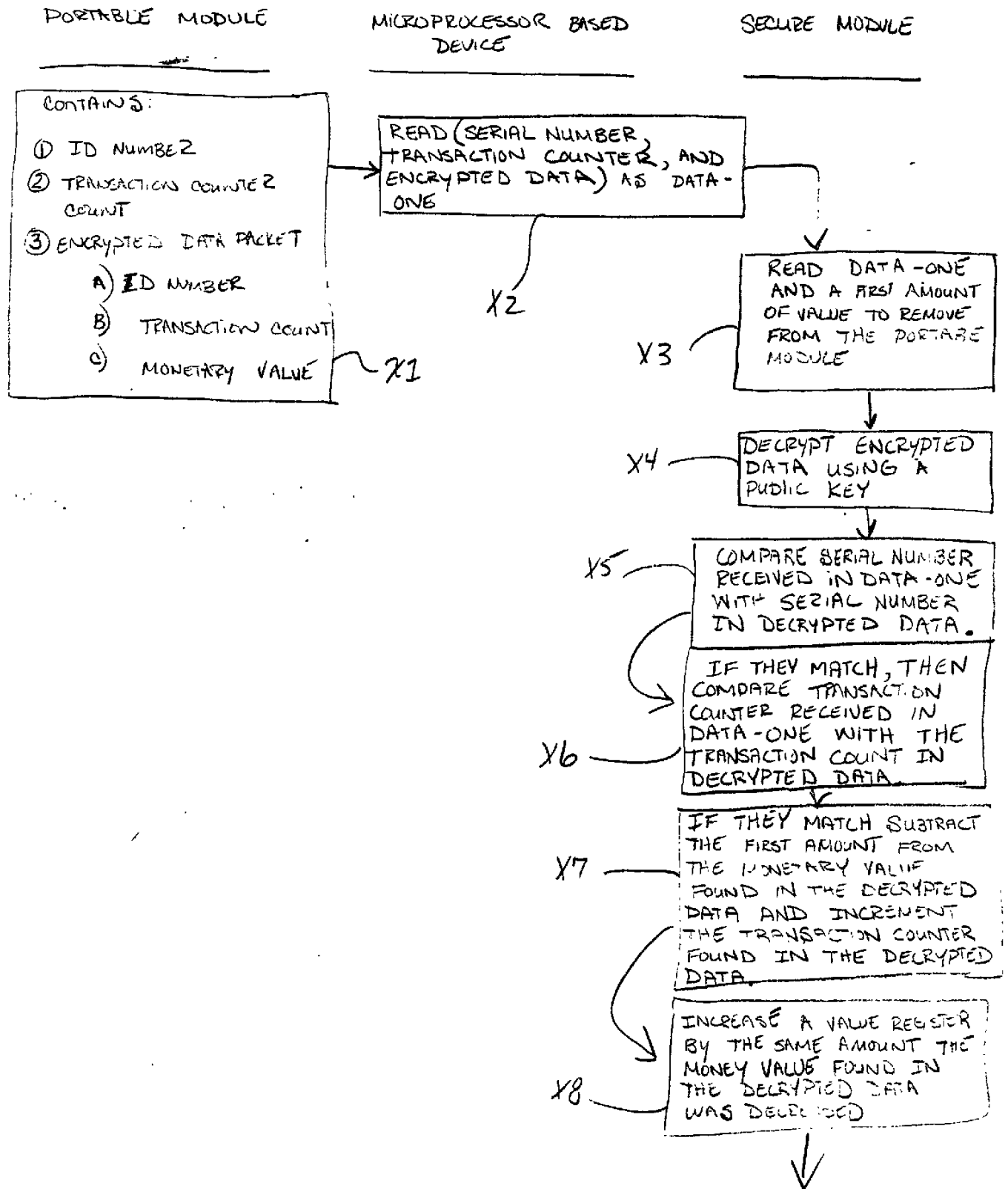


FIGURE 4 CONTINUED

200601-429

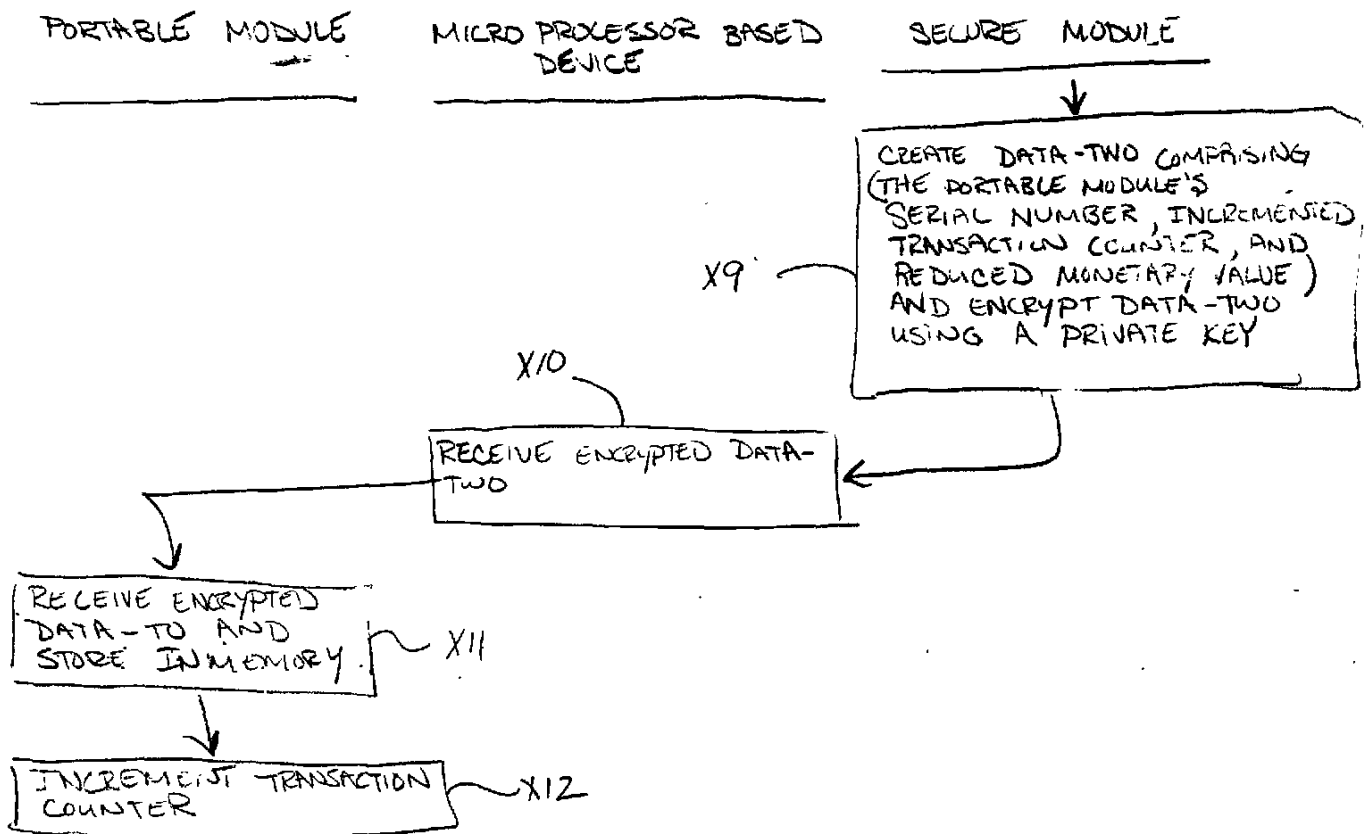
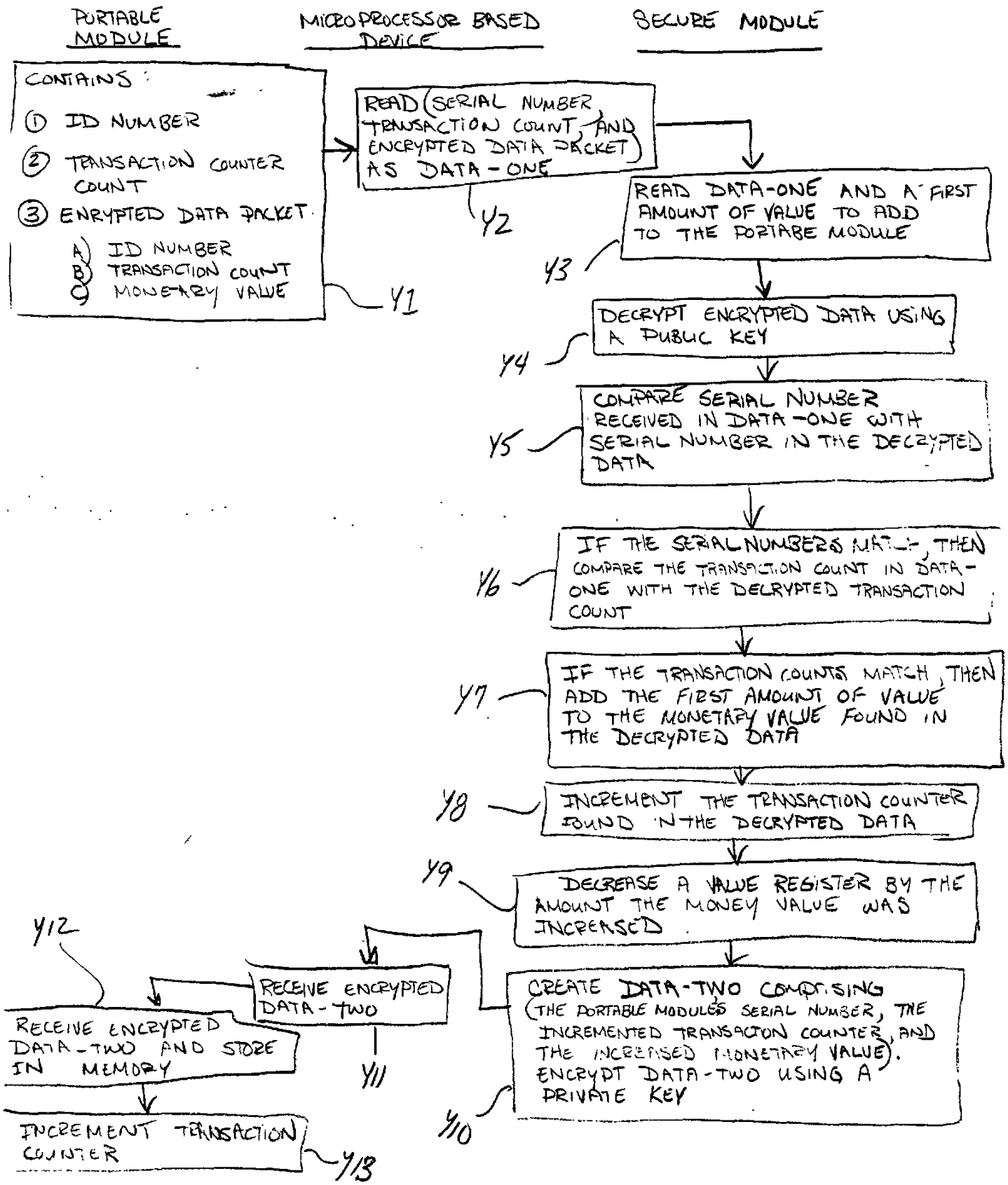


FIGURE 5



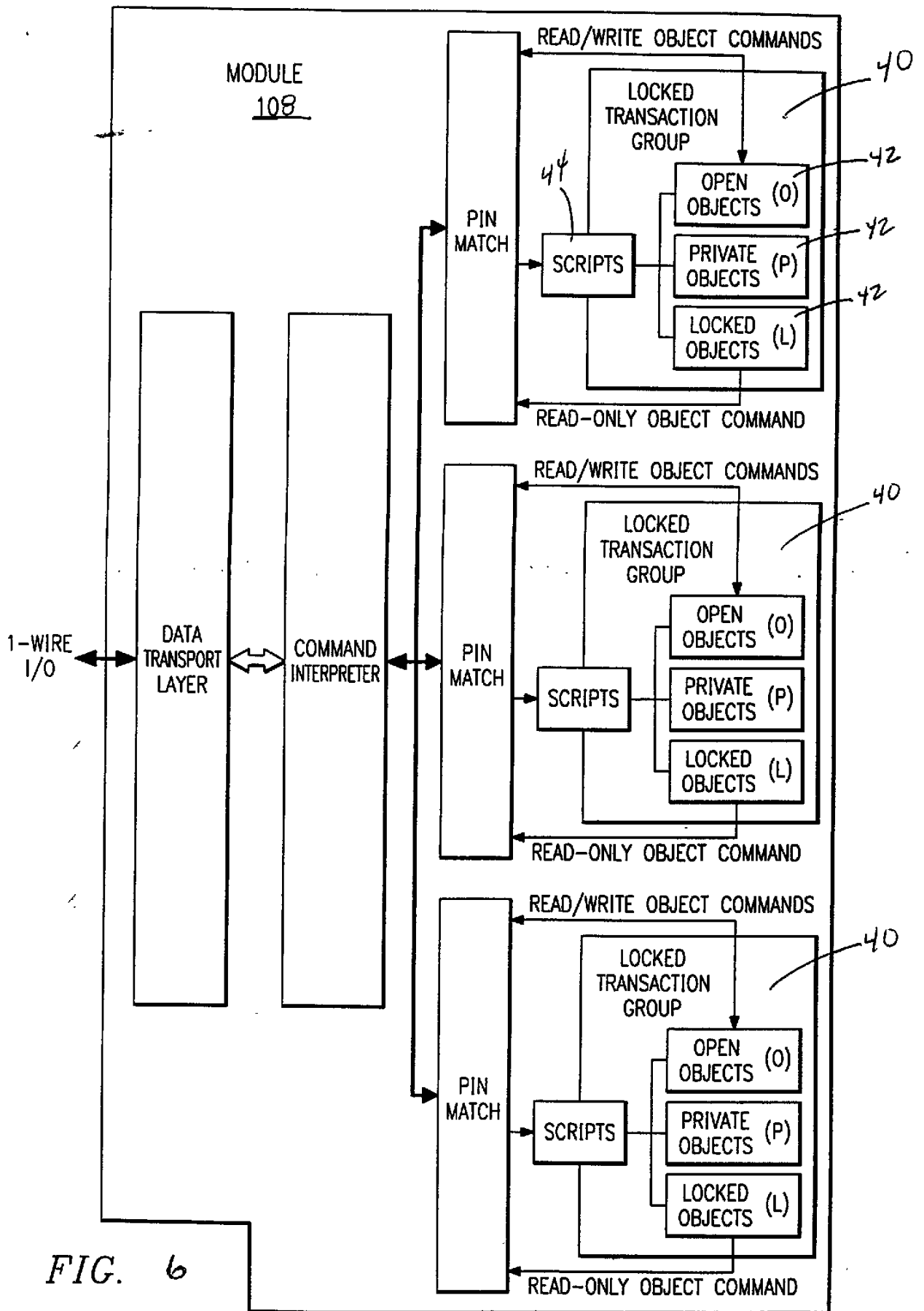
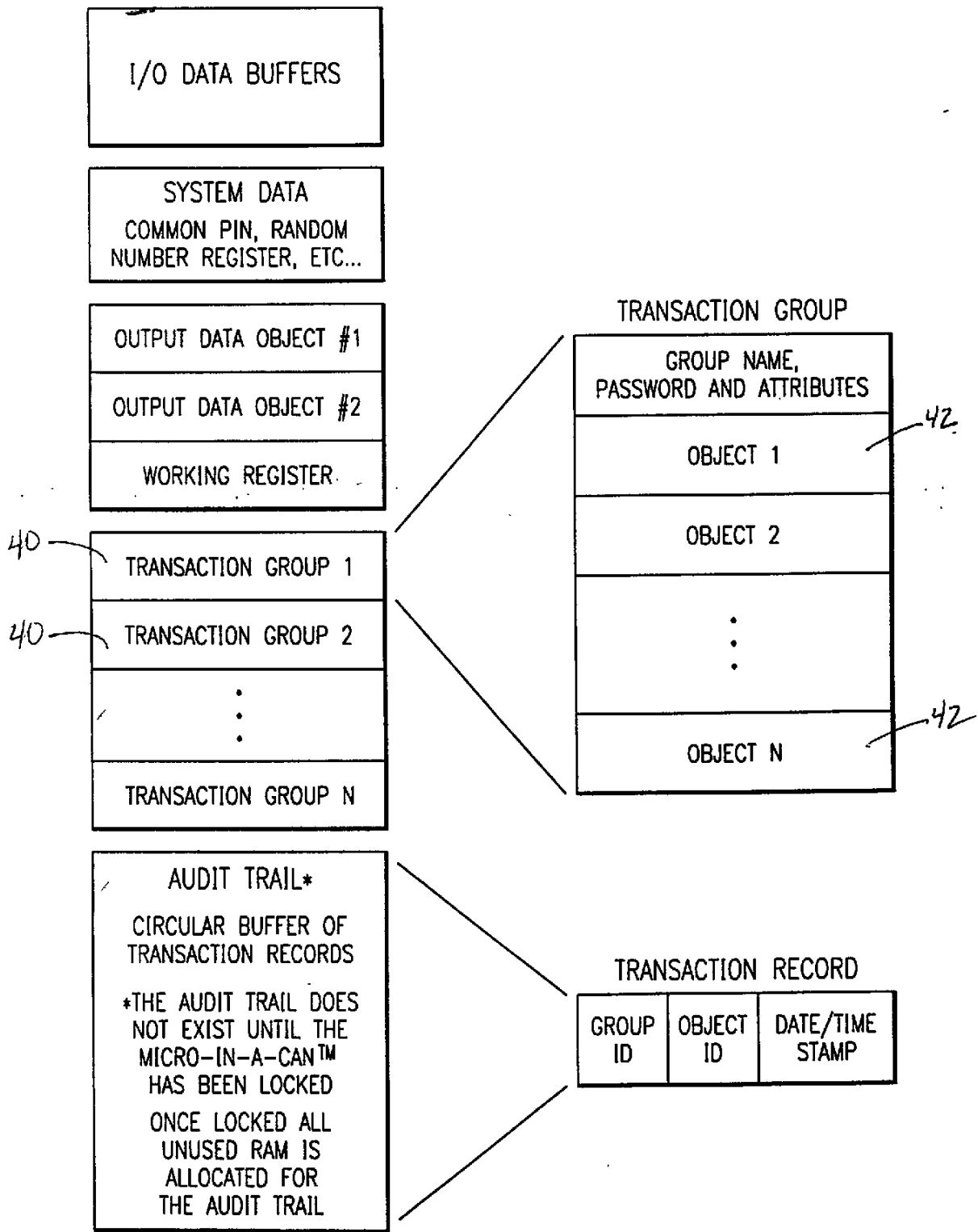


FIG. 6

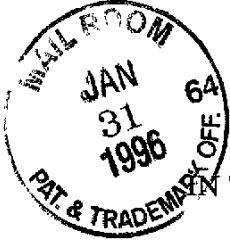
FIG. 7



8

08/594975

A



Patent Application
Docket No. 20661/429

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

⁻⁰⁰
STEPHEN M. CURRY, DONALD W. LOOMIS, and MICHAEL L. BOLAN

For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL	
"EXPRESS MAIL" Mailing Label No.	JB 885275721
Date of Deposit	January 31, 1996
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, Washington, D.C. 20231	
Type or Print Name	JEANNE A. HOWARD
Signature	<i>Jeanne A. Howard</i>

Dear Sir:

REQUEST FOR FILING A NATIONAL PATENT APPLICATION

Transmitted herewith for filing, please find the following:

- 1. Specification, claims and abstract of the above-referenced patent application having 97 pages.
- 2. 1 set(s) of drawing(s) (formal / informal).
- 3. Combined Declaration and Power of Attorney (signed unsigned).
- 3A. No filing fee, Oath, or Declaration is enclosed pursuant to 35 U.S.C. 53(d).
- 4. Information Disclosure Statement along with Form PTO-1449 and references.

IPDAL:73135.1/20661-429

___ 5. This is a: ___ CIP, ___ DIV, ___ CONT, or ___ substitute Application (MPEP 201.09) of Application Serial No. ___ filed ___; or, is a ___ reissue of U.S. Patent No. ___ filed on ___.

An extension to extend the life of the above prior Application to at least the date of filing hereof

(One box must be marked)

- (a) ___ is concurrently being filed in that prior Application,
(b) ___ was previously filed in that prior Application (check length of prior extension),
(c) ___ is not necessary for copendency (double check before X'ing this).

___ 6. Attached is an assignment to _____. Please return the recorded assignment to the undersigned. (NOTE: add recordal fee below).

___ 7. Priority is claimed under 35 U.S.C. § 119 based on filing in __(country)___.

	<u>Application No.</u>	<u>Filing Date</u>
(1)	___	___
(2)	___	___
(3)	___	___

___ (No.) Certified copy (copies) ___ are attached; or ___ were previously filed on ___.

___ 7.A. Priority is claimed under 35 U.S.C. § 119(e) based on Provisional Application Number ____, filed on ___.

___ 8. Attached: ___ (No.) verified statement(s) establishing "small entity" status under 37 CFR § 1.9 and 1.27.

X 9. Attached:

X Return Postcard
___ (Other)

___ 10. Preliminary Amendment:

Prior to a first Office Action, kindly amend the Application as follows:

11. The following Filing Fee calculation is based on the claims filed less any claims canceled by the Preliminary Amendment of Item 10.

BASIC FEE				SMALL ENTITY RATE	OR	LARGE ENTITY RATE	=	\$730.00
				\$365		\$730		\$730.00
	NUMBER FILED			NUMBER EXTRA				
TOTAL CLAIMS	<u>21</u>	-20	=	<u>1</u> (at least 0)	x 11	OR	x 22	= +\$22.00
INDEP. CLAIMS	<u>2</u>	-3	=	<u>0</u> (at least 0)	x 38	OR	x 76	= +\$0
If any <u>proper</u> multiple dependent claim (ignore improper) is present (Enter \$0.00 if this is a <u>reissue</u> application.)								
								+\$120 OR +\$240 = +\$0
If assignment is x'd (line 5), add recording fee \$40.00								+\$0
Attached is a Rule 47 Petition (inventor refuses to sign or cannot be reached) \$130								+\$0
TOTAL FILING FEE								= \$752.00

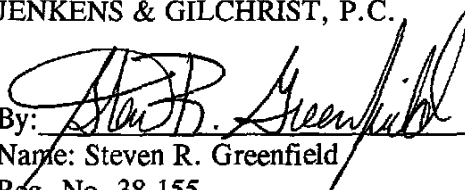
12. A check in the amount of \$ to cover the Filing Fee calculated in Item 11 is attached. Please charge any deficiency or credit any overpayment to Deposit Account No. 10-0447.
- X 13. Please charge **Dallas Semiconductor Corporation Deposit Account No. 04-0031** in the amount of **\$752.00** to cover the Filing Fee calculated in Item 11. This sheet is attached in duplicate.
- X 14. 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 **Dallas Semiconductor Corporation Deposit Account No. 04-0031**, for which purpose a **duplicate copy of this sheet is attached.***

Patent Application
Docket No. 20661/429

The Commissioner is not authorized to charge the issue fee until/unless an issue fee transmittal form is filed.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

By: 
Name: Steven R. Greenfield
Reg. No. 38,155

Date: January 31, 1996

Jenkins & Gilchrist, P.C.
1445 Ross Avenue
Suite 3200
Dallas, Texas 75202
(214) 855-4789
(214) 855-4300 (fax)

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 my Deposit Account No. 10-0447.

IPDAL: 73135.1 / 20661-429

4



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

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
--------------------	-------------	-----------------------	------------------------

06/594,975

01/31/96

CURRY

S

20661/429

0282/0401

JENKENS & GILCHRIST
 1445 ROSS AVENUE
 SUITE 3200
 DALLAS TX 75202

0000

DATE MAILED:

04/01/96

**NOTICE TO FILE MISSING PARTS OF APPLICATION
 FILING DATE GRANTED**

An Application Number and Filing Date have been assigned to this application. However, the items indicated below are missing. The required items and fees identified below must be timely submitted **ALONG WITH THE PAYMENT OF A SURCHARGE** for items 1 and 3-6 only of \$ 130.00 for large entities or \$ 65.00 for small entities who have filed a verified statement claiming such status. The surcharge is set forth in 37 CFR 1.16(e).

If all required items on this form are filed within the period set below, the total amount owed by applicant as a large entity, small entity (verified statement filed), is \$ 150.00.

Applicant is given **ONE MONTH FROM THE DATE OF THIS LETTER, OR TWO MONTHS FROM THE FILING DATE** of this application, **WHICHEVER IS LATER**, within which to file all required items and pay any fees required above to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

1. The statutory basic filing fee is: missing insufficient. Applicant as a large entity small entity, must submit \$ 20.00 to complete the basic filing fee.
2. Additional claim fees of \$ _____ as a large entity, small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
3. The oath or declaration:
 - is missing.
 - does not cover the newly submitted items.

An oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date is required.
4. The oath or declaration does not identify the application to which it applies. An oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
5. The signature(s) to the oath or declaration is/are: missing; by a person other than the inventor or a person qualified under 37 CFR 1.42, 1.43, or 1.47. A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
6. The signature of the following joint inventor(s) is missing from the oath or declaration:

_____ An oath or declaration listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date, is required.
7. The application was filed in a language other than English. Applicant must file a verified English translation of the application and a fee of \$ _____ under 37 CFR 1.17(k), unless this fee has already been paid.
8. A \$ _____ processing fee is required since your check was returned without payment. (37 CFR 1.21(m)).
9. Your filing receipt was mailed in error because your check was returned without payment.
10. The application does not comply with the Sequence Rules. See attached Notice to Comply with Sequence Rules 37 CFR 1.821-1.825.
11. Other.

Direct the response to Box Missing Part and refer any questions to the Customer Service Center at (703) 308-1202.

A copy of this notice MUST be returned with the response.

OFFICE COPY

**RULES 63 AND 67 (37 C.F.R. 1.63 and 1.67)
DECLARATION AND POWER OF ATTORNEY**

#3

FOR UTILITY/DESIGN/CIP/PCT NATIONAL APPLICATIONS

As a named inventor, **STEPHEN M. CURRY, DONALD W. LOOMIS, and MICHAEL L. BOLAN**, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; and

I believe that I am the original, first and sole inventor (if only one name is listed above) or an original, first and joint inventor (if plural names are listed above) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE**, the specification of which: (mark only one)

- (a) is attached hereto.
- (b) was filed on January 31, 1996 as Application Serial No. 08/594,975.
- (c) was filed as PCT International Application No. PCT/____ on ____ and was amended on ____ (if applicable).
- (d) was filed on _____ as Application Serial No. _____ and issued as Patent No. _____ on _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above or as allowed as indicated above.

I acknowledge the duty to disclose all information known to me to be material to the patentability of this application as defined in 37 CFR § 1.56. If this is a continuation-in-part (CIP) application, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose to the Office all information known to me to be material to patentability of the application as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this CIP application.

I hereby claim foreign priority benefits under 35 U.S.C. § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate filed by me or my assignee disclosing the subject matter claimed in this application and having a filing date (1) before that of the application

PATENT APPLICATION
DOCKET NO.: 20661/00429

on which my priority is claimed or, (2) if no priority is claimed, before the filing date of this application:

PRIOR FOREIGN PATENTS

Number	Country	Month/Day/Year Filed	Date first laid-	Date	Priority Claimed	
			open or Published	patented or Granted	Yes	No
---	---	---	---	---	---	---
---	---	---	---	---	---	---

I hereby claim the benefit under 35 U.S.C. § 120/365 of any United States application(s) listed below and PCT international applications listed above or below:

PRIOR U.S. OR PCT APPLICATIONS

Application No. (series code/serial no.)	Month/Day/Year Filed	Status(pending, abandoned, patented)
---	---	---
---	---	---

I hereby appoint:

13
 H. MATHEWS GARLAND, Reg. No. 19,129 P. WESTON MUSSELMAN, JR., Reg. No. 31,644 STEVEN R. GREENFIELD, Reg. No. 38,166
 THOMAS L. CANTRELL, Reg. No. 20,849 ROGER L. MAXWELL, Reg. No. 31,855 CRAIG A. HOERSTEN, Reg. No. 38,917
 THOMAS L. CRISMAN, Reg. No. 24,846 JEFFERY E. BACON, Reg. No. 35,055 STUART D. DWORK, Reg. No. 31,103
 STANLEY R. MOORE, Reg. No. 26,958 ANDRE M. SZUWALSKI, Reg. No. 35,701
 GERALD T. WELCH, Reg. No. 30,332 J. KEVIN GRAY, Reg. No. 37,141

all of the firm of **JENKENS & GILCHRIST, P.C.**, 3200 Fountain Place, 1445 Ross Avenue, Dallas, Texas 75202-2799, as my attorneys and/or agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith, and to file and prosecute any international patent application filed thereon before any international authorities under the Patent Cooperation Treaty, and I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization who/which first sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct them in writing to the contrary.

Please address all correspondence and direct all telephone calls to:

Steven R. Greenfield
Jenkins & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
214/855-4789
214/855-4300 (fax)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAMED INVENTOR(S)

100

1	<u>STEPHEN M. CURRY</u> ✓	<i>Stephen M. Curry</i>	April 16, 1996
	Full Name	Inventor's Signature	Date
	6646 Clearhaven Circle Dallas, TX 75248		USA
	Residence (city, state, country)		Citizenship
	6646 Clearhaven Circle Dallas, TX 75248		
	Post Office Address (include zip code)		

200

2	<u>DONALD W. LOOMIS</u> ✓	<i>Donald W. Loomis</i>	April 16, 1996
	Full Name	Inventor's Signature	Date
	316 Dakota Lane Coppell, TX 75019		USA
	Residence (city, state, country)		Citizenship
	316 Dakota Lane Coppell, TX 75019		
	Post Office Address (include zip code)		



300

3	MICHAEL L. BOLAN	<i>Michael L Bolan</i>	7-18-98
	Full Name	Inventor's Signature	Date
	6214 Misty Trail Dallas, TX 75248		USA
	Residence (city, state, country)		Citizenship
	6214 Misty Trail Dallas, TX 75248 Post Office Address (include zip code)		

(FOR ADDITIONAL INVENTORS, check here ___ and add additional sheet for inventor information regarding signature, name, date, citizenship, residence and address)

Assignment Document

While copying your file we noticed that the Application Transmittal letter status that an assignment document was originally filed with this case.

At your request, we will attempt to obtain the assignment documents from the assignment branch located within the USPTO. Please note that additional charges will apply to this service.

Loc/0300



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

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
09/594,975	01/31/96	CURRY	S 20661/429

0282/0401

JENKENS & GILCHRIST
1445 ROSS AVENUE
SUITE 3200
DALLAS, TX 75202

0000

DATE MAILED: 04/01/96

**NOTICE TO FILE MISSING PARTS OF APPLICATION
FILING DATE GRANTED**

An Application Number and Filing Date have been assigned to this application. However, the items indicated below are missing. The required items and fees identified below must be timely submitted **ALONG WITH THE PAYMENT OF A SURCHARGE** for items 1 and 3-6 only of \$ 130.00 for large entities or \$ 65.00 for small entities who have filed a verified statement claiming such status. The surcharge is set forth in 37 CFR 1.16(e).

If all required items on this form are filed within the period set below, the total amount owed by applicant as a large entity, small entity (verified statement filed), is \$ 130.00.

Applicant is given **ONE MONTH FROM THE DATE OF THIS LETTER, OR TWO MONTHS FROM THE FILING DATE** of this application, **WHICHEVER IS LATER**, within which to file all required items and pay any fees required above to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

1. The statutory basic filing fee is: missing insufficient. Applicant as a large entity small entity, must submit \$ 20.00 to complete the basic filing fee.
2. Additional claim fees of \$ _____ as a large entity, small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
3. The oath or declaration:
 - is missing.
 - does not cover the newly submitted items.

An oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date is required.
4. The oath or declaration does not identify the application to which it applies. An oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
5. The signature(s) to the oath or declaration is/are: missing; by a person other than the inventor or a person qualified under 37 CFR 1.42, 1.43, or 1.47. A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
6. The signature of the following joint inventor(s) is missing from the oath or declaration:

_____ An oath or declaration listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date, is required.
7. The application was filed in a language other than English. Applicant must file a verified English translation of the application and a fee of \$ _____ under 37 CFR 1.17(k), unless this fee has already been paid.
8. A \$ _____ processing fee is required since your check was returned without payment. (37 CFR 1.21(m)).
9. Your filing receipt was mailed in error because your check was returned without payment.
10. The application does not comply with the Sequence Rules. See attached Notice to Comply with Sequence Rules 37 CFR 1.821-1.825.
11. Other.

Direct the response to Box Missing Part and refer any questions to the Customer Service Center



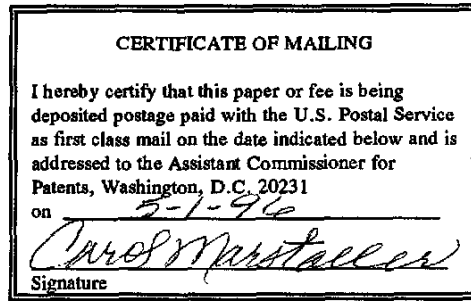
PATENT APPLICATION #3
DOCKET NO.: 20661-00429

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: §
Stephen M. Curry et al. §
Serial No.: 08/594,975 § Group No.: Not Yet Assigned §
Filed: January 31, 1996 § Examiner: Not Yet Assigned §

For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

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



TRANSMITTAL LETTER

Dear Sir:

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

- 1) Transmittal Letter (in duplicate);
- 2) Notice to File Missing Parts of Application (PTO-1533);
- 3) Declaration and Power of Attorney (signed);
- 4) Assignment (signed); and
- 5) 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.

___ No additional fee is required.

IPDAL:77842.1 20661-00429

PATENT APPLICATION
DOCKET NO.: 20661-00429

X The Fee for entering the attached Assignment, Declaration and Power of Attorney, and Notice to File Missing Parts of Application is calculated below:

	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST # PREVIOUSLY PAID FOR	PRESENT EXTRA	SMALL ENTITY RATE	LARGE ENTITY RATE
TOTAL CLAIMS	<u>21</u>	<u>21</u> (at least 20)	= <u>0</u> (at least 0)	x11 = <u>OR</u>	x22 = \$ <u> </u>
INDEP. CLAIMS	<u>2</u>	<u>3</u> (at least 3)	= <u>0</u> (at least 0)	x39 = <u>OR</u>	x78 = \$ <u>0</u>
FIRST PRESENTATION OF <u>PROPER</u> MULTIPLE DEPENDENT CLAIMS (leave blank if this is a <u>reissue</u> appln)				+125 = <u>OR</u>	+250 = \$ <u> </u>
	FEE FOR CLAIM AMENDMENTS				\$ <u> </u>
<u> </u>	IDS ATTACHED REQUIRES OFFICIAL FEE - ADD \$210 (RULE 1.97(c)) OR \$130 (RULE 1.97(d) PETITION)				\$ <u> </u>
<u>X</u>	Assignment Recordation Fee (\$40)				\$ <u>40</u>
<u> </u>	IF <u>TERMINAL DISCLAIMER</u> attached add Rule 20(d) Official Fee				\$55 (Small Entity) / \$110 (Large Entity) = \$ <u> </u>
<u>X</u>	Insufficient Filing Fees				\$ <u>20</u>
<u>X</u>	File <u>NOTICE TO FILE MISSING PARTS OF APPLICATIONS (PTO-1532) (\$130 - Large Entity)</u>				\$ <u>130</u>
<u> </u>	Petition is hereby made under 37 CFR 1.136(a) to extend the <u>original</u> 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	\$450		\$900	
	Four Months	\$700		\$1400	
	ADDITIONAL FEE FOR EXTENDED RESPONSE				\$ <u> </u>

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 \$190.00

 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.

X Please charge **Dallas Semiconductor Corporation Deposit Account No. 04-0031** in the amount of **\$190.00** to cover the TOTAL FEE. This sheet is attached in duplicate.

PATENT APPLICATION
DOCKET NO.: 20661-00429

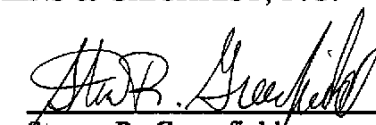
CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed herein or hereafter, and which are or may be required 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 Dallas Semiconductor Corporation Deposit Account No. 04-0031, 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
Registration No. 38,166

Dated: May 1, 1996

JENKENS & GILCHRIST, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202
Tel: 214/855-4789
Fax: 214/855-4300

*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 my Deposit Account No. 10-0447.



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/594,975	01/31/96	CURRY	S 20661/429

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

22M2/0819

EXAMINER

WHITE, C

ART UNIT	PAPER NUMBER
2202	#4

2202

DATE MAILED:

08/19/97

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

OFFICE ACTION SUMMARY

Responsive to communication(s) filed on January 31, 1996

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 D.C. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 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) 1-21 is/are pending in the application.

Of the above, claim(s) 16-21 is/are withdrawn from consideration.

Claim(s) _____ is/are allowed.

Claim(s) 1-15 is/are rejected.

Claim(s) _____ is/are objected to.

Claims 1-21 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 Reference 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 --

Art Unit: 2202

DETAILED ACTION

Restriction

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
 - I. Claims 1-15, drawn to a system for communicating data securely, classified in class 380, subclass 49.
 - II. Claims 16-21, drawn to a method for electronically transferring units of exchange between a first module and a second module, classified in class 380, subclass 49.
2. Inventions I and II are related as process and apparatus for its practice. The inventions are distinct if it can be shown that either: (1) the process as claimed can be practiced by another materially different apparatus or by hand, or (2) the apparatus as claimed can be used to practice another and materially different process. (MPEP § 806.05(e)). In this case the apparatus as claimed in Group I can be used to practice another and materially different process, such as the communication of data signals other than the value datum of Group II.
3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.
4. During a telephone conversation with Steven Greenfield on August 5, 1997, a provisional election was made without traverse to prosecute the invention of Group I (claims 1-15)-drawn to a system for communicating data securely. Affirmation of this election must be made by

Art Unit: 2202

applicant in responding to this Office action. Claims 16-21 have been withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

5. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a diligently-filed petition under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(h).

Drawings

6. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

Claim Rejections - 35 USC § 102

7. 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.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371© of this title before the invention thereof by the applicant for patent.

8. Claims 1-3 and 8-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Shinagawa.

Art Unit: 2202

Regarding claims 1-3 and 8-12, Shinagawa discloses all the elements of the claims (abstract and Fig. 1).

9. Claims 1-5 and 8-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Caputo.

Regarding claims 1-5 and 8-15, Caputo discloses a first module for containing a first data and an electronic system comprising a secure module, said electronic system adapted to be able to communicate with said first module (abstract and Figure 2).

10. Claims 1-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis ('796).

Regarding claims 1-15, Davis ('796) discloses all the elements of the claims (abstract, #608, Fig. 3, col. 12, lines 25-30).


Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Akiyama and Davis ('121) disclose a system for communicating data securely.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carmen White whose telephone number is (703) 305-4458.


Carmen White


THOMAS H. TARCZA
SUPERVISORY PATENT EXAMINER
GROUP 2200

TO SEPARATE, HOLD TOP AND BOTTOM EDGES, SNAP-APART AND DISCARD CARBON

FORM PTO-892 (REV. 2-92)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	SERIAL NO. 08/594,975	GROUPART UNIT 2202	ATTACHMENT TO PAPER NUMBER													
NOTICE OF REFERENCES CITED		APPLICANT(S) Stephen M. Curry et al															
U.S. PATENT DOCUMENTS																	
*	DOCUMENT NO.					DATE			NAME		CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE				
A	5	5	4	6	4	6	3	8	13	96	Caputo et al		380	25	7	12	94
B	5	0	0	3	5	9	4	3	26	91	Shinagawa		380	24			
C	5	5	7	7	1	2	1	11	19	96	Davis et al.		380	24	6	9	94
D	5	5	3	9	8	2	5	7	23	96	Akiyama et al.		380	24	11	21	94
E	5	6	2	1	7	9	6	4	15	97	Davis et al.		380	24	9	30	94
F																	
G																	
H																	
I																	
J																	
K																	
FOREIGN PATENT DOCUMENTS																	
*	DOCUMENT NO.					DATE			COUNTRY		NAME		CLASS	SUB-CLASS	PERTINENT SHTS. DWG. PP. SPEC.		
L																	
M																	
N																	
O																	
P																	
Q																	
OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)																	
R																	
S																	
T																	
U																	
EXAMINER William White					DATE 8/18/97												
Reference is not being furnished with this office action. Examining Procedure, section 707.05 (a.)																	

File History Report

Paper number _____ is missing from the United States Patent Trademark Office's copy of the file History. No additional information is available.

The following page(s) _____ of paper number _____ is/are missing from the United States Patent and Trademark Office's original copy of the file history. No additional information is available

The following checked item(s) below of paper number _____ is/are missing from the United States Patent and Trademark Office's original copy of the file history. No additional information is available

- PTO 1449
- PTO 892
- PTO 948
- PTO 1474
- Assignment
- Cover page

Additional comments: _____



Csp. 2202
3
Reg. Ext.

PATENT APPLICATION
DOCKET NO.: 20661-00429

Janie
Yrtd
01 mo.
Cyber

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of)
Curry et al.)
Serial No. 08/594,975)
Filed: January 31, 1996)
For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE)

Examiner: White
Group No.: 2202

RECEIVED
DEC 1997
GROUP 2200
1997-10-97

To The 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 *11-26-97*
Carol M. Mettler
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 August 19, 1997.
- 2) Acknowledgment Postcard.

12/10/1997 AHAYES 00000070 DAN:040031 06594975
01 FC:i15 110.00 CH

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.

No additional fee is required.

IPDAL:143191.1 20661-00429

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	<u>17</u>	- <u>21</u> (at least 20)	= <u>0</u> (at least 0)	x11 = <u>OR</u>	x22 = <u>\$ 0</u>
2. INDEP. CLAIMS	<u>3</u>	- <u>3</u> (at least 3)	= <u>0</u> (at least 0)	x41 = <u>OR</u>	x82 = <u>\$ 0</u>
3. FIRST PRESENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a reissue appln)				+130 = <u>OR</u>	+260 = <u>\$ 0</u>
4. TOTAL FEE FOR ADDED CLAIMS					<u>\$ 0</u>
5. _____ IDS ATTACHED REQUIRES OFFICIAL FEE - ADD \$230 (RULE 1.97(c)) OR \$130 (RULE 1.97(d) PETITION)					<u>\$ _____</u>
6. _____ IF <u>TERMINAL DISCLAIMER</u> attached add Rule 20(d) Official Fee				\$55 (Small Entity)	\$110 (Large Entity) <u>\$ _____</u>
7. _____ Petition is hereby made under 37 CFR 1.136(a) to extend the <u>original</u> due date to cover the date this response is filed for which the requisite fee is attached:					
			Small Entity	Large Entity	
	One Month	_____	\$ 55	<u>X</u> \$ 110	
	Two Months	_____	\$200	___ \$ 400	
	Three Months	_____	\$475	___ \$ 950	
	Four Months	_____	\$755	___ \$1,510	
	ADDITIONAL FEE FOR EXTENDED RESPONSE				<u>\$ 110.00</u>
8. TOTAL FEES					<u>\$ 110.00</u>

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.

9. _____ A check in the amount of \$ _____ is attached. Please charge any deficiency or credit any overpayment to Dallas Semiconductor Corporation Deposit Account No. 04-0031.
10. X Please charge Dallas Semiconductor Corporation Deposit Account No. 04-0031 in the amount of \$110.00 This sheet is attached in duplicate.

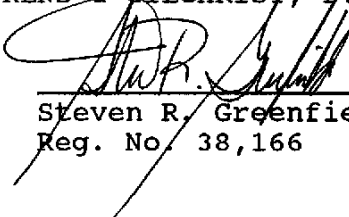
CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and may be required under 37 CFR 1.16-1.18 (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 Dallas Semiconductor Corporation Deposit Account No. 04-0031, 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
Reg. No. 38,166

Date: November 26 , 1997
Jenkins & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
Tel: (214) 855-4789
Fax: (214) 855-4300

*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.



Patent Application
Docket No. 20661-0000429

6/A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:

Curry et al.

Serial No.: 08/594,975

Filed: January 31, 1996

§
§
§
§
§
§
§

Examiner: *White, C.*

Group Art Unit: 2202

RECEIVED
DEC 10 1997
GROUP ID 2200

Coper
12-10-97

For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

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 <i>11-26-97</i>
Signature <i>Cathy M. White (C.M.W.)</i>

Dear Sir:

AMENDMENT

Responsive to the Official Action mailed on August 19, 1997, 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 delete claims 16-21 without prejudice.

Please amend the claims as follows:

1. (Amended) A system for communicating data securely, comprising:

A1
Sub B1
a first module for containing a first data, said first module comprising a real-time clock for time-stamping data transactions;

an electronic system comprising a secure module, said electronic system adapted to perform data transactions [be able to communicate] with said first module.

Please add the following new claims:

Sub B3
--22. A system for communicating data securely, comprising:

A2
a first module for containing a first data, said first module being able to create random private/public key sets for data encryption; and

an electronic system comprising a secure module, said electronic system adapted to perform data transactions with said first module.

~~23. A system for communicating data securely, comprising:~~

~~a first module for containing a first data, said first module comprising an energy storage device for maintaining a volatile memory circuit, said first data being stored in said volatile memory.--~~

REMARKS

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

Claims 1-15, 22 and 23 are pending in this application.

Claims 16-21 have been cancelled.

Regarding the Restriction

Applicants acknowledge the restriction required under 35 U.S.C. § 121. Applicants affirm the election of prosecuting group I, claims 1-15 which is drawn to a system for communicating data securely. Applicants have canceled and withdrawn claims 16-21 from further consideration by the Examiner.

In the Drawings

Applicants acknowledge that informal drawings have been provided for examination purposes only and will provide formal drawings when the application is allowed.

Regarding the § 102 Rejection

Claims 1-3 and 8-12 were rejected under 35 U.S.C. § 102(b) as being anticipated by Shinagawa.

Regarding claim 1, Applicants have amended claim 1 to require that the first module include a real-time clock for time-stamping

data transactions. The real-time clock is supported in the originally filed specification on pages 13, 15, 18, 22 and others. The real-time clock is also depicted at least in Figure 3. Applicants respectfully submit that Shinagawa does not teach, allude to or anticipate the use of a real-time clock in a module. Applicants further point out that Shinagawa could not operate with a real-time clock in the module because there is no disclosure of a power source within the module in order to power a real-time clock. Applicants respectfully submit that claim 1 is not anticipated by Shinagawa and requests that the § 102 rejection be withdrawn.

Regarding claims 2 and 3, these claims are directly dependent upon independent claim 1 and are not anticipated by Shinagawa for the same reasons as stated above with respect to claim 1. Applicants respectfully request that the § 102 rejection be withdrawn.

Regarding claim 8, this claim is also dependent upon independent claim 1 and is not anticipated for the same reasons as stated above with respect to claim 1. Furthermore, claim 8 requires that the electronic system communicates with the first module via a single conductive contact. Applicants respectfully submit that Shinagawa makes no mention of how many contacts are used between the IC card 2 and whatever device it is in contact with. Indeed, it appears from FIGURES 3A and 3B, that the IC card

2 has an 8 pin connection on its face, as is used in "smart cards", and not a single wire connection. Applicants respectfully submit that Shinagawa does not anticipate claim 8 for these reasons and respectfully requests that the § 102 rejection be withdrawn.

With respect to claim 9, this claim requires that the electronic system be adapted to communicate with the first module via a one-wire bus. Applicants respectfully submit that Shinagawa does not teach, allude to or anticipate the use of a one-wire bus in its disclosure. Applicants respectfully submit that a one-wire bus is a specific type of bus which bidirectionally transfers data on a single wire and a ground connection. For the reasons stated above, Applicants respectfully submit that claim 9 is not anticipated by Shinagawa and respectfully requests that the § 102 rejection be withdrawn.

Regarding claims 9, 10 and 11, these claims are directly dependent upon independent claim 1 and are therefore not anticipated by Shinagawa for the reasons stated above with respect to claim 1. Applicants respectfully request that the § 102 rejection be withdrawn.

Regarding claim 12, this claim requires that the secure module be able to receive a first data and thereby create a second data that contains at least one information that was in the first data. Conversely, Shinagawa teaches the passing of secret identification numbers between an IC card and a terminal, but does not teach,

allude to, or anticipate the passing of information from, for example, the IC card to the terminal such that the terminal uses a portion of the information and combines it with other data and passes that newly created information back to the IC card. Thus, Applicants respectfully submit that claim 12 is not anticipated by Shinagawa and further respectfully requests that the § 102 rejection be withdrawn.

Claims 1-5 and 8-15 were rejected under 35 U.S.C. § 102(e) as being anticipated by Caputo.

With respect to claim 1, as amended, this claim requires, among other things, that the first module comprises a real-time clock for time-stamping data transactions. Applicants respectfully submit that Caputo does not teach, allude to or render obvious the use of a real-time clock in the encryption/authenticating device 10 described in Caputo's specification. Applicants respectfully request that the § 102 rejection be withdrawn.

Regarding claims 2-5, these claims are either directly or indirectly dependent upon independent claim 1 and are therefore not anticipated by Caputo for the same reasons as stated above with respect to claim 1. Applicants respectfully request that the § 102 rejection be withdrawn.

Regarding claims 8 and 9, these claims require that the electronic system communicate with the first model via a single conductive contact or a one-wire bus, respectfully. Conversely,

Caputo requires the communication to take place over a telephone line which by definition includes a plurality of wires. Thus, Caputo does not anticipate claims 8 and 9. Furthermore, claims 8 and 9 are directly dependent upon independent claim 1 and are therefore not anticipated for the same reasons as stated above with respect to claim 1. Applicants respectfully request that the § 102 rejection be withdrawn.

Regarding claims 10 and 11, these claims are directly dependent upon independent claim 1 and are therefore not anticipated by Caputo for the same reasons as stated above with respect to claim 1. Applicants respectfully request that the § 102 rejection be withdrawn.

Regarding claims 12-15, these claims are also either directly or indirectly dependent upon claim 1 and are therefore not anticipated by Caputo for the same reasons as stated above with respect to claim 1. Applicants respectfully request that the § 102 rejection be withdrawn.

Claims 1-15 were rejected under 35 U.S.C. § 102(e) as being anticipated by Davis ('796).

Regarding claim 1, this claim requires, among other things, that the first module comprises a real-time clock for time-stamping data transactions. Applicants respectfully submit that Davis does not teach, allude to or anticipate such a real-time clock being included in the stored value card (SVC) 20. Applicants

respectfully submit that claim 1, as amended, is not anticipated by Davis and further requests that the § 102 rejection be withdrawn. Regarding claims 2-15, these claims are all either directly or indirectly dependent upon independent claim one and are therefore not anticipated by Davis for the same reasons as stated above with respect to claim 1. Applicants respectfully request that the § 102 rejection be withdrawn.

Furthermore, regarding claims 8 and 9, these claims require that there be either a single conductive contact or a one-wire bus, respectively. Applicants respectfully submit that Davis does not teach or allude to the use of a communication means using a single conductive contact or a one-wire bus. Applicants further submit that these are reasons that Davis does not anticipate claims 8 and 9.

With the above stated, Applicants respectfully request that the § 102 rejection be withdrawn and that all the claims are ready for allowance.

Regarding the New Claims

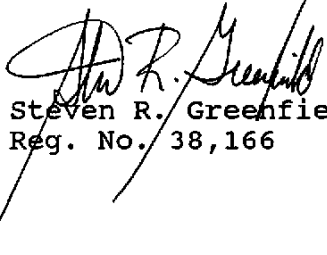
New claims 22 and 23 have been added. These claims claim novel aspects of the present invention that are believed to be worthy of patentability. Applicants respectfully request that these claims be examined and that an early Notice of Allowance is provided.

Patent Application
Docket No. 20661-0000429

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 26, 1997

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



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

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	CLASSIFICATION	OFFICE DOCKET NO.
08/594,975	01/31/98	CHRY		

PN52/0219

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

EXAMINER
 WHITE, C

ART UNIT: 3042
 PAPER NUMBER: 7

02/19/98

DATE MAILED:

This is a communication from the examiner in charge of your application.
 COMMISSIONER OF PATENTS AND TRADEMARKS

OFFICE ACTION SUMMARY

Responsive to communication(s) filed on December 1, 1997

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 D.C. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 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) 1-15 and 22-23 is/are pending in the application.
- Of the above, claim(s) 23 is/are withdrawn from consideration.
- Claim(s) _____ is/are allowed.
- Claim(s) 1-15 and 22 is/are rejected.
- Claim(s) _____ is/are objected to.
- Claim(s) 23 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

- Acknowledgment 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: _____

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

Attachment(s)

- Notice of Reference 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--

DETAILED ACTION

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:
 - I. Claims 1-15 and 22, drawn to a system for communicating data securely, comprising a first module and an electronic system, classified in class 380, subclass 49.
 - II. Claim 23, drawn to a system for communicating data securely, comprising a energy storage device, classified in class 365, subclass 229.
2. The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because Invention I does not require the energy storage device of Invention II. The subcombination has separate utility such as an energy storage device for maintaining a volatile memory circuit.
3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

Art Unit: 3642

4. Newly submitted claim 23 directed to an invention that is independent or distinct from the invention originally claimed for the following reasons: Claim 23 (Invention II above) and Invention I (claims 1-15 and 22) are related as combination and subcombination.

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claim 23 is withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Claim Rejections - 35 USC § 102

5. 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.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371© of this title before the invention thereof by the applicant for patent.

6. Claims 1-4 and 10-13 are rejected under 35 U.S.C. 102(b) as being anticipated by Blandford or Chan.

Regarding claims 1-4, and 10-13, Blandford or Chan discloses a first module for containing a first data, said first module comprising a real-time clock for time-stamping data transactions (Blandford-#13; Chan- #112); an electronic system comprising a secure module, said

Art Unit: 3642

electronic system adapted to perform data transactions (Blandford-fig. 1 and abstract; Chan- fig. 1 and abstract).

7. Claim 22 is rejected under 35 U.S.C. 102(b) as being anticipated by Bellovin.

Regarding claim 22, Bellovin discloses a first module for containing a first data, said first module being able to create random private/public key sets for data encryption; and an electronic system comprising a secure module, said electronic system adapted to perform data transactions with said first module (Fig. 6; col. 18, lines 17-18).

8. Claim 22 is rejected under 35 U.S.C. 102(e) as being anticipated by Davis ('828).

Regarding claim 22, Davis ('828) discloses all the elements of the claim (abstract; Fig. 6, step 135, step 115).

Claim Rejections - 35 USC § 103

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

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

10. Claims 1-3 and 8-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinagawa in view of Blandford or Chan.

Regarding claims 1-3 and 8-12, Shinagawa discloses all of the elements of the claims except the first module comprising a real-time clock (abstract and Fig. 1). Blandford or Chan discloses a real-time clock (Blandford-#13; Chan- #112). It would have been obvious to a person

Art Unit: 3642

of ordinary skill in the art to modify the invention of Shinagawa to include a real-time clock because it is well-known in the art to use real-time clocks for time stamping to increase the security of the authentication of data. Also, Shinagawa discloses the use of a bus for data communication that achieves all the functions of applicant's bus system; however, Shinagawa is silent on disclosing the specific type of bus used. It would have been obvious to a person of ordinary skill in the art to modify Shinagawa to include the specific type of bus, a one-wire bus, because it is well-known in the art to use many different types of buses for transporting data. Shinagawa is silent on the exact number of contacts used. However, Shinagawa further discloses the use of at least a single conductive contact to communicate data between the electronic system and the first module.

11. Claims 1-5 and 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo in view of Blandford or Chan.

Regarding claims 1-5 and 10-15, Caputo discloses all the elements of the claim except the use of a real-time clock (abstract and Figure 2). Blandford or Chan discloses a real-time clock (Blandford-#13; Chan- #112). Caputo is combinable with Blandford or Chan because they are from the same field of endeavor. It would have been obvious to a person of ordinary skill in the art to modify the invention of Caputo to include a real-time clock because it is well-known in the art to use real-time clocks for time stamping to increase the security of the authentication of data.

12. Claims 1-7 and 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('796) in view of Blandford or Chan.

Art Unit: 3642

Regarding claims 1-7 and 10-15, Davis ('796) discloses all the elements of the claim except the use of a real-time clock (abstract, #608, Fig. 3, col. 12, lines 25-30). Blandford or Chan discloses a real-time clock (Blandford-#13; Chan- #112). Davis ('796) is combinable with Blandford or Chan because they are from the same field of endeavor. It would have been obvious to a person of ordinary skill in the art to modify the invention of Davis ('796) to include a real-time clock because it is well-known in the art to use real-time clocks for time stamping to increase the security of authentication of data.

Examiner's Response to Applicant's Arguments

13. Applicant argues that the references cited in the examiner's office action dated, August 19, 1997, fail to disclose the use of a real-time clock, one-wire bus and communication via a single conductive contact. These features of applicant's invention have been discussed by examiner in the above claim rejections.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period

Serial Number: 08/594,975

Page 7

Art Unit: 3642

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carmen White whose telephone is (703) 305-4458.

CW

Carmen White

Thomas H. Tarcza

THOMAS H. TARCZA
SUPERVISORY PATENT EXAMINER
GROUP ~~200~~ 3640

FORM PTO-892 (REV. 2-92)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	SERIAL NO. 08/594,975	GROUP ART UNIT 3642	ATTACHMENT TO PAPER NUMBER
NOTICE OF REFERENCES CITED		APPLICANT(S) Curry et al.		

U.S. PATENT DOCUMENTS

*	DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
A	5150407	9/22/92	Chan	380	4	
B	5189700	2/23/93	Blandford	380	23	
C	5539828	7/23/94	Davis	380	50	5/31/94
D	5241599	8/31/93	Bellovin et al	380	21	
E						
F						
G						
H						
I						
J						
K						

FOREIGN PATENT DOCUMENTS

*	DOCUMENT NO.	DATE	COUNTRY	NAME	CLASS	SUB-CLASS	PERTINENT SHTS. DWG.	PP. SPEC.
L								
M								
N								
O								
P								
Q								

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

R	
S	
T	
U	

EXAMINER Carmen White	DATE 2/13/98
---------------------------------	------------------------

* A copy of this reference is not being furnished with this office action.
(See Manual of Patent Examining Procedure, section 707.05 (a).)



Corres. and Mail
BOX AF

PATENT APPLICATION
DOCKET NO.: 20661-0842

AF/GAU 3642.
Rep. Et. \$

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Curry et al.

Serial No. 08/594,975

Filed: January 31, 1996

Examiner: White, C.

Group No.: 3642

For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

RECEIVED
TECHNOLOGY CENTER 3600
JUN 17 AM 9:02
Htd
(1)ma
Cfa
6-21-98

RESPONSE UNDER 37 C.F.R. § 1.116
-- EXPEDITED PROCEDURE --
EXAMINING GROUP NUMBER: 3642

Assistant Commissioner
for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL
"EXPRESS MAIL" Mailing Label No. EMS59375217US
Date of Deposit: 6.11.98
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: Carol Marstaller
Signature: *Carol Marstaller*

RECEIVED
TECHNOLOGY CENTER 3600
JUN 23 AM 9:19

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 February 19, 1998.
- 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.

06/15/1998 RMGGT 00000087,000031,000008594975

01 FC:115 110.00 CH

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

_____ 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	<u>16</u>	- <u>21</u> (at least 20)	= <u>0</u> (at least 0)	x11 = OR	x22 = <u>\$ 0</u>
2. INDEP. CLAIMS	<u>1</u>	- <u>3</u> (at least 3)	= <u>0</u> (at least 0)	x41 = OR	x82 = <u>\$ 0</u>
3. FIRST PRESENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a reissue appln)				+130 = OR	+260 = <u>\$ 0</u>
4. TOTAL FEE FOR ADDED CLAIMS					<u>\$ 0</u>
5. _____ IDS ATTACHED REQUIRES OFFICIAL FEE - ADD \$230 (RULE 1.97(c)) OR \$130 (RULE 1.97(d) PETITION)					<u>\$ _____</u>
6. _____ IF <u>TERMINAL DISCLAIMER</u> attached add Rule 20(d) Official Fee				\$55 (Small Entity)	\$110 (Large Entity) <u>\$ _____</u>
7. _____ Petition is hereby made under 37 CFR 1.136(a) to extend the <u>original</u> due date to cover the date this response is filed for which the requisite fee is attached:					

	Small Entity	Large Entity
One Month	<u> </u> \$ 55	<u> x </u> \$ 110
Two Months	<u> </u> \$200	<u> </u> \$ 400
Three Months	<u> </u> \$475	<u> </u> \$ 950
Four Months	<u> </u> \$755	<u> </u> \$1,510

ADDITIONAL FEE FOR EXTENDED RESPONSE \$110.00

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.

8. TOTAL FEES \$110.00

9. _____ A check in the amount of \$_____ is attached. Please charge any deficiency or credit any overpayment to Dallas Semiconductor Corporation Deposit Account No. 04-0031.

10. X Please charge Dallas Semiconductor Corporation Deposit Account No. 04-0031 in the amount of \$110.00 This sheet is attached in duplicate.

PATENT APPLICATION
DOCKET NO.: 20661-00429

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 Dallas Semiconductor Corporation Deposit Account No. 04-0031, 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
Reg. No. 38,166

Date: June 10, 1998
Jenkins & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
Tel: (214) 855-4789
Fax: (214) 855-4300

*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



[Handwritten signature]
Cofor
6-24-98

Patent Application
Docket No. 20661-00429

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:

CURRY ET AL
Serial No.: 08/594,975
Filed: JANUARY 31, 1996

§
§
§
§
§
§

Examiner: WHITE, C.
Group Art Unit: 3642

RECEIVED
TECHNOLOGY CENTER 3500
98 JUN 23 AM 9:19

For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

RESPONSE UNDER 37 C.F.R. § 1.116
-- EXPEDITED PROCEDURE --
EXAMINING GROUP NUMBER: 3642

Assistant Commissioner
for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL
"EXPRESS MAIL" Mailing Label No. EM550375217US
Date of Deposit: 6/10/98
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: Carol Marstaller
Carol Marstaller
Signature

Dear Sir:

AMENDMENT

Responsive to the Official Action mailed on February 19, 1998, reconsideration and allowance of the present application respectfully requested and believed to be appropriate in view of the following amendments and remarks:

RECEIVED
TECHNOLOGY CENTER 3500
98 JUN 23 AM 9:19

In the Claims:

Please cancel claim ~~6~~ and 23 without prejudice.

Please amend the claims as follows:

~~1. (Twice Amended) A system for communicating data securely, comprising:~~

~~a first module for containing a first data, said first module comprising a real-time clock for time-stamping data transactions and a counter for counting a number of transactions that said first module performs;~~

~~an electronic system comprising a secure module, said electronic system adapted to perform data transactions with said first module.~~

~~7. (Amended) The system of claim [6] 1, wherein said number of transactions represent the number of times a memory data is changed in said module.~~

~~22 (Amended) A system for communicating data securely, comprising:~~

~~a first module for containing a first data, said first module being able to create random private/public key sets for data encryption, said first module further comprising a counting~~

B3
~~circuitry for counting a number of transactions performed by said first module; and~~

an electronic system comprising a secure module, said electronic system adapted to perform data transactions with said first module.

Please add the following new claim.

BH
~~24. the system for communicating data securely of claim 22, wherein said first module further comprises [and] ^{an} energy storage device for maintaining a volatile memory circuit, said volatile memory circuit being for storing said created random private/public key sets.~~

REMARKS

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

Claims 1-5, 7-15, 22 and 24 are pending in this application.

Claims 6 and 23 have been canceled without prejudice.

Regarding the Restriction Requirement

Applicant has canceled claim 23. Applicant requests that Group I: Claims 1-15 and 22 be elected for prosecution.

Regarding the § 102 Rejection

Claims 1-4, and 10-13 were rejected under 35 U.S.C. § 102(b) for being anticipated by Blandford or Chan. Although applicant disagrees that both Blandford and Chan do not disclose the requisite real time clock, applicant has amended the claims to require that the module further require a counter for counting the number of transactions that the module performed. Applicant respectfully submits that none of the art cited anticipates such a counter for counting the number of transactions the module performed. Applicant submits that claim 1-4 and 1-13 are ready for allowance and requests that the §102 rejection be withdrawn.

Claim 22 was rejected under 35 U.S.C. § 102(b) for being anticipated by Bellovin and under §102(e) for being anticipated by Davis. Applicant has amended claim 22 to require that the first module further require a counting circuit for counting the number of transactions performed by said first module. Neither Bellovin nor Davis anticipate the novel idea of counting the transactions performed by the first module. Applicant respectfully requests that the §102 rejections be withdrawn and respectfully submits that claim 22 in ready for allowance.

Regarding the § 103 Rejections

Claims 1-3 and 8-12 were rejected under 35 U.S.C. § 103(a) for being rendered obvious by Shinagawa in view of Blandford or Chan.

Although applicant does not agree that Blandford or Chan teach or render obvious a real time clock as required by the present invention, applicant further indicates that there is no suggestion in any of the cited art to require the first module to count the number of transactions performed by the first module. The transaction counter circuitry is preferably irreversible and the count can be incorporated into the encrypted data to help thwart "replay" or counterfeiting. Applicant respectfully submits that the rejected claims require a counter for counting the number of transactions performed by the first module. Such a requirement is not taught alluded to or rendered obvious by the cited art. Applicant respectfully requests that the §103 rejection be withdrawn and that the claims 1-3 and 8-12 are ready for allowance.

Claims 1-5 and 1-15 were rejected under 35 U.S.C. §103(a) for being rendered obvious by Caputo in view of Blandford or Chan. Applicant disagrees with that Caputo can be combined with either of the other references because they are from the same field of endeavor. Applicant respectfully submits that there must be a suggestion to combine and there is no suggestion here. Furthermore, Applicant submits that Caputo, like the other cited art does not require that there be a counter for counting the number of transactions performed by the module. Applicant respectfully points out that the cited art does not teach, allude to, or render obvious the preset claims and requests that the

rejection be withdrawn. Applicant requests that claims 1-5 and 1-15 be moved toward allowance.


Claims 1-7 and 10-15 were rejected under 35 U.S.C. §103(a) for being rendered obvious by Davis in view of either Blandford or Chan. Applicant disagrees that Davis can be combined with either of the other cited references because they are from the same field of endeavor. Applicant respectfully submits that there must be a suggestion to combine and there is no suggestion here. Furthermore, Applicant submits that Davis, like the other cited art does not require that there be a counter for counting the number of transactions performed by the module. Therefore, Applicant respectfully points out that the cited art does not teach, allude to, or render obvious the preset claims and requests that the rejection be withdrawn. Applicant requests that claims 1-5 and 1-15 be moved toward allowance.

Patent Application
Docket No. 20661-00429

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: June 10, 1998

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



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

SERIAL NUMBER	FILED DATE	FIRST NAMED APPLICANT	ATTORNEY REG. NO.
08/594,975	01/31/96	CURRY	206617429

PM52/0629

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

EXAMINER	
WHITE, C	
ART UNIT	PAPER NUMBER
2766	
DATE MAILED: 06/29/98	

#10

Below is a communication from the EXAMINER in charge of this application

COMMISSIONER OF PATENTS AND TRADEMARKS

ADVISORY ACTION

THE PERIOD FOR RESPONSE:

- a) is extended to run _____ or continues to run 3 months from the date of the final rejection
- b) expires three months from the date of the final rejection or as of the mailing date of this Advisory Action, whichever is later. In no event however, will the statutory period for the response expire later than six months from the date of the final rejection.

Any extension of time must be obtained by filing a petition under 37 CFR 1.136(a), the proposed response and the appropriate fee. The date on which the response, the petition, and the fee have been filed is the date of the response and also the date for the purposes of determining the period of extension and the corresponding amount of the fee. Any extension fee pursuant to 37 CFR 1.17 will be calculated from the date of the originally set shortened statutory period for response or as set forth in b) above.

Appellant's Brief is due in accordance with 37 CFR 1.192(a).

Applicant's response to the final rejection, filed June 11, 1998 has been considered with the following effect, but it is not deemed to place the application in condition for allowance:

1. The proposed amendments to the claim and /or specification will not be entered and the final rejection stands because:
- a. There is no convincing showing under 37 CFR 1.116(b) why the proposed amendment is necessary and was not earlier presented.
- b. They raise new issues that would require further consideration and/or search. (See Note).
- c. They raise the issue of new matter. (See Note).
- d. They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal.
- e. They present additional claims without cancelling a corresponding number of finally rejected claims.

NOTE: Applicant's amendment to the independent claims, ^{is the source of} ~~is~~ a new argument for patentability, which applicant has raised. This would require further consideration by examiner.

2. Newly proposed or amended claims _____ would be allowed if submitted in a separately filed amendment cancelling the non-allowable claims.
3. Upon the filing an appeal, the proposed amendment will be entered will not be entered and the status of the claims will be as follows:

Claims allowed: _____
 Claims objected to: _____
 Claims rejected: 1-15 and 22

However;

Applicant's response has overcome the following rejection(s): _____

4. The affidavit, exhibit or request for reconsideration has been considered but does not overcome the rejection because it would require further consideration

5. The affidavit or exhibit will not be considered because applicant has not shown good and sufficient reasons why it was not earlier presented.

The proposed drawing correction has has not been approved by the examiner.

Other Examiner - Carmen White
(703) 305-4458

THOMAS H. TARCZA
 SUPERVISORY PATENT EXAMINER
 GROUP 2200

11



#11 ext of time
7/24/98
tooky

Patent Application
Docket No. 20661-00429

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Curry, et al.) Group Art Unit: 2766
Serial No.: 08/594,975) Examiner: White, C.
Filed: January 31, 1996)

98 JUL 20 AM 8:21
RECEIVED
GROUP 2400

For: Transfer of Valuable Information Between a Secure Module and Another Module

Assistant Commissioner
for Patents
Washington DC 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL
"EXPRESS MAIL" Mailing Label No. E1053138828US
Date of Deposit: July 10, 1998
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 of Print Name: CAROL MARSTADLER
<i>Carol Marstadler</i> Signature

PETITION FOR EXTENSION OF TIME

Dear Sir:

Petition is hereby made under 37 C.F.R. 1.136(a) for a two (2) month(s) extension in which to extend the time for response to the Office Action mailed June 10, 1998. If this petition is granted, the response period will extend to and through July 19, 1998. A one-month extension of \$110.00 was paid at the time of the filing of the response. Please charge \$290.00 to Dallas Semiconductor Corporation's Deposit Account No. 04-0031 for the remainder of the \$400.00 owed for a two-month extension.

Respectfully submitted,

By:

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

07/16/1998 ZABDELLA 00000028 040031 08594975

01 FC:116 290.00 CH
Date: July 10, 1998

JENKENS & GILCHRIST, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202
(214) 855-4789
(214) 855-4300

IPDAL:172052.1 20661-00429

Please type a plus sign (+) inside this box [+]

G W 27 7/21/98 #12 continued time

PTO/SB/29 (12/97) Approved for use through 09/30/00. OMB 0651-0032 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.

**CONTINUED PROSECUTION APPLICATION (CPA)
REQUEST TRANSMITTAL**

Submit an original, and a duplicate for fee processing.
(Only for Continuation or Divisional applications under 37 CFR 1.53(d))

CHECK BOX, if applicable
 DUPLICATE

Address to: Assistant Commissioner for Patents Box CPA Washington, D.C. 20231	Attorney Docket No.	20661-00429
	First Named Inventor	Stephen M. Curry
	Express Mail Label No.	EL053138828US
	Total Pages	2

This is a request for a continuation or divisional application under 37 CFR 1.53(d), (continued prosecution application (CPA)) of prior application number 08/594,975, filed on January 31, 1996, entitled "Transfer of Valuable Information Between a Secure Module and Another Module".

NOTES

FILING QUALIFICATIONS: The prior application identified above must be a nonprovisional application that is either: (1) complete as defined by 37 CFR 1.51(b) and filed on or after June 8, 1995, or (2) the national stage of an international application in compliance with 35 U.S.C. 371 and filed on or after June 8, 1995.

C-I-P NOT PERMITTED: A continuation-in-part application cannot be filed as a CPA under 37 CFR 1.53(d), but must be filed under 37 CFR 1.53(b).

EXPRESS ABANDONMENT OF PRIOR APPLICATION: The filing of this CPA will be construed to include a waiver of confidentiality by the applicant under 35 U.S.C. 122 to the extent that any member of the public who is entitled under the provisions of 37 CFR 1.14 to access to, copies of, or information concerning, the prior application may be given similar access to, copies of, or similar information concerning, the other application or applications in the file jacket.

35 U.S.C. 120 STATEMENT: In a CPA, no reference to the prior application is needed in the first sentence of the specification and none should be submitted. If a sentence referencing the prior application is submitted, it will not be entered. A request for a CPA is the specific reference required by 35 U.S.C. 120 and to every application assigned the application number identified in such request, 37 CFR 1.78(a).

1. Enter the unentered Amendment previously filed on June 10, 1998 under 37 CFR 1.116 in the prior nonprovisional application.
2. A preliminary Amendment is enclosed.
3. This application is filed by fewer than all the inventors named in the prior application, 37 CFR 1.53(d)(4).
 - a. DELETE the following inventor(s) named in the prior nonprovisional application:

 - b. The inventor(s) to be deleted are set forth on a separate sheet attached hereto.
4. A new power of attorney or authorization of agent (PTO/SB/81) is enclosed.
5. Information Disclosure Statement (IDS) is enclosed:
 - a. PTO-1449
 - b. Copies of IDS Citations

RECEIVED
 98 JUL 20 AM 8:27
 GROUP 2700

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box CPA, Washington, D.C. 20231.

07/22/1998 TCOLEY 00000001 040031 08594975

01 FC:131 IPDAL:17199010061-00429

Please type a plus sign (+) inside this box [+]

PTO/SB/29 (12/97)
 Approved for use through 09/30/00. OMB 0651-0032
 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.

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
TOTAL CLAIMS (37 CFR 1.16(c))		16 - 20 =	0	x \$ 22 =	\$ _____
INDEPENDENT CLAIMS (37 CFR 1.16(b))		1 - 3 =	0	x \$ 32 =	\$ _____
MULTIPLE DEPENDENT CLAIMS (if applicable) (37 CFR 1.16(d))				+ \$ _____ =	
				BASIC FEE (37 CFR 1.16(a))	\$ _____
				Total of above Calculations =	\$ _____
Reduction by 50% for filing by small entity (Note 37 CFR 1.9, 1.27, 1.28).					- _____
				TOTAL =	\$ -0-

6. Small entity status;
- a. A small entity statement is enclosed.
 - b. A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.
 - c. is no longer claimed.
7. The Commissioner is hereby authorized to credit overpayments or charge the following fees to **Deposit Account No. 10-0447**:
- a. Fees required under 37 CFR 1.16.
 - b. Fees required under 37 CFR 1.17.
 - c. Fees required under 37 CFR 1.18.
8. A check in the amount of \$ _____ .00 is enclosed.
9. Other: Please charge \$290.00 to Deposit Account 04-0031 for the two month extension minus what was already paid for a one month extension.

NOTE: *The prior application's correspondence address will carry over to this CPA UNLESS a new correspondence address is provided below.*

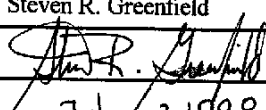
10. NEW CORRESPONDENCE ADDRESS

Customer Number or Bar Code Label Or New correspondence address below

(Insert Customer No. Or Attach bar code label here)

NAME				
ADDRESS				
CITY		STATE:	ZIP CODE	
COUNTRY		TELEPHONE	FAX	

11. SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

NAME	Steven R. Greenfield	Reg. No. 38,166
SIGNATURE		
DATE	July 13, 1998	

(Page 2 of 2)



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

(Handwritten mark)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/594,975	01/31/96	CURRY	206617429

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

LM02/0810

EXAMINER

WHITE, C

ART UNIT	PAPER NUMBER
2766	

DATE MAILED: 08/10/98 ¹³

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

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	08/594,975	Applicant(s)	Curry et al.
Examiner	Carmen White	Group Art Unit	2766

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

Period for Response

A SHORTENED STATUTORY PERIOD FOR RESPONSE IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a response be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for response is specified above, such period shall, by default, expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to respond within the set or extended period for response will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

- Responsive to communication(s) filed on June 11, 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.

Disposition of Claims

- Claim(s) 1-5, 7-15, 22 and 24 is/are pending in the application.
Of the above claim(s) _____ is/are withdrawn from consideration.
- Claim(s) _____ is/are allowed.
- Claim(s) 1-5, 7-15, 22 and 24 is/are rejected.
- Claim(s) _____ is/are objected to.
- Claim(s) _____ are subject to restriction or election requirement.

Application Papers

- See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.
- The proposed drawing correction, filed on _____ is approved disapproved.
- The drawing(s) filed on _____ is/are objected to by the Examiner.
- 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 (a)-(d)

- Acknowledgment 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: _____.

Attachment(s)

- Information Disclosure Statement(s), PTO-1449, Paper No(s) _____
- Notice of References Cited, PTO-892
- Notice of Draftsperson's Patent Drawing Review, PTO-948
- Interview Summary, PTO-413
- Notice of Informal Patent Application, PTO-152
- Other _____

Office Action Summary

Art Unit: 2766

DETAILED ACTION

Continued Prosecution Application

1. The request filed on July 13, 1998, for a Continued Prosecution Application (CPA) under 37 CFR 1.53(d) based on parent Application No. 08/594,975 is acceptable and a CPA has been established. An action on the CPA follows.

Claim Rejections - 35 USC § 103

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

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

3. Claims 1-5 and 7-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('121) or Davis ('796) in view of Blandford or Chan.

Regarding claims 1-5, 7-8 and 10-15, Davis ('121) or Davis ('796) discloses a first module for containing a first data, said first module comprising a counter for counting a number of transactions that said first module performs; and an electronic system comprising a secure module, said electronic system adapted to perform data transactions with said first module (Davis ('121)- Figure 3A, #328, and col. 11, lines 44-57; Davis ('796)- Fig. 7, #700, and col. 11, lines 38-41). Davis ('121) or Davis ('796) fails to disclose the first module comprising a real-time

Art Unit: 2766

clock for time-stamping data transactions. Blandford or Chan discloses the use of a real-time clock for time-stamping data transactions (Blandford- Fig. 1 and abstract; Chan- Fig. 1 and abstract). Blandford or Chan is combinable with Davis ('121) or Davis ('796) because they are from the similar area pertaining to data security in communication systems. It would have been obvious to a person of ordinary skill in the art to combine the time-stamping of Blandford or Chan with Davis ('796) or Davis ('121) because it is well-known in the art to use counters to keep track of transaction data.

Regarding claim 9, Davis ('121) or Davis ('796) in view of Blandford or Chan discloses the elements as explained above. Davis ('121) or Davis ('796) fails to disclose the type of bus used to transfer information from the first module to the secure module. It would have been obvious to a person of ordinary skill in the art to modify Davis ('121) or Davis ('796) to include the use of a specific type of bus for data transfer because it is well-known in the art to use many different types of buses for transporting data.

4. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('828) or Bellovin in view of Davis ('121) or Davis ('796).

Regarding claim 22, Davis ('828) or Bellovin discloses a first module for containing a first data, said first module being able to create random private/public key sets for data encryption; and an electronic system comprising a secure module, said electronic system adapted to perform data transactions with said first module (Bellovin- Fig. 6 and col. 18, lines 17-18; Davis ('828) -abstract, Fig. 6, step 135, and step 115). Davis ('828) or Bellovin fails to disclose a

Art Unit: 2766

counter for counting the number of transactions. Davis ('121) or Davis ('796) discloses a counter (see the above claim rejection). Davis ('121) or Davis ('796) is combinable with Davis ('828) or Bellovin because they are from the similar area pertaining to data security in communication systems. It would have been obvious to a person of ordinary skill in the art to combine the use of a counter of Davis ('121) or Davis ('796) with Davis ('828) or Bellovin because it is well-known in the art to use counters to keep track of transaction data.

5. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('828) in view of Davis ('121) or Davis ('796), as applied to claim 22 above, and further in view of Tuttle.

Regarding claim 24, Davis ('828) in view of Davis ('121) or Davis ('796) discloses the elements as explained above. Although Davis ('828) discloses storing random private/public key sets in a non-volatile memory circuit, Davis ('828) fails to disclose the use of a volatile memory circuit to store random private/public key sets. Tuttle discloses the storage of data in volatile memory and an energy storage device for maintaining a volatile memory (col. 4, lines 25-30). Tuttle is combinable with Davis ('828) because they are from the similar area pertaining to data security in communication systems. It would have been obvious to a person of ordinary skill in the art to modify the invention of Davis ('828) to include the use of volatile memory as disclosed by Tuttle because it is well-known in the art to store data in a volatile memory.

Examiner's Response to Applicant's Remarks

6. Applicant submits that the prior art, which was cited by the examiner in the prior office action, fails to teach a counter for counting the number of transactions performed by the first

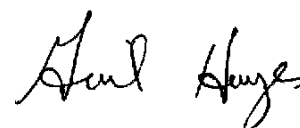
Art Unit: 2766

module. Examiner has addressed this claim element in the above claim rejections. Applicant, further asserts that there is no suggestion to combine Davis ('796) with Blandford or Chan. Examiner has provided the motivation for combining the prior art in the above claim rejections.

Information on How to Contact USPTO

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carmen White whose telephone number is (703) 305-4458. Examiner can be reached during the hours of 8:30 am and 5:00 pm, Monday-Friday. If attempts to reach the examiner are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711.


Carmen White



GAIL O. HAYES
SUPERVISORY PATENT EXAMINER
GROUP 2700

FORM PTO-892 (REV. 2-92)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	SERIAL NO. 08/594,975	GROUPART UNIT 2766	ATTACHMENT TO PAPER NUMBER
NOTICE OF REFERENCES CITED		APPLICANT(S) Curry et al.		

U.S. PATENT DOCUMENTS

*	DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
A	5787174	7-28-98	Tuttle	380	23	11/2/95
B						
C						
D						
E						
F						
G						
H						
I						
J						
K						

FOREIGN PATENT DOCUMENTS

*	DOCUMENT NO.	DATE	COUNTRY	NAME	CLASS	SUB-CLASS	PERTINENT SHTS. DWG	PP. SPEC.
L								
M								
N								
O								
P								
Q								

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

R	
S	
T	
U	

EXAMINER Carmen White	DATE 7-28-98
--------------------------	-----------------

* A copy of this reference is not being furnished with this office action.
(See Manual of Patent Examining Procedure, section 707.05 (a).)



#14/C
11/19/98

Patent Application
Docket No. 20661-00429

TCOLEY

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

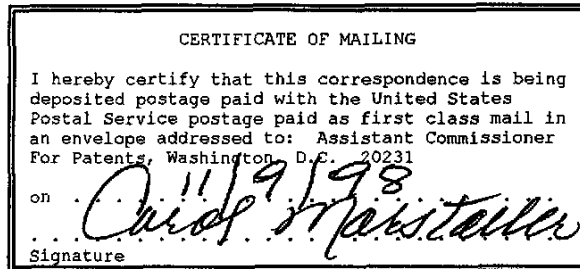
In the Application of:

Curry et al.
Serial No.: 08/594,975
Filed: January 31, 1996

§
§
§ Examiner: White, C.
§
§ Group Art Unit: 2766
§
§

For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

Assistant Commissioner For
Patents
Washington, D.C. 20231



Dear Sir:

AMENDMENT

Responsive to the Official Action mailed on August 10, 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 claims ~~1-5, 7-15, 22 and 24~~, without prejudice.

11/20/1998 TCOLEY 00000003 100447 08594975
01 FC:103 54.00 CH

Please add the following new claims:

1 --~~25.1~~ A system for communicating data securely,
2 comprising:
3 a first portable module comprising:
4 a nonvolatile memory for storing a first data;
5 a first real time clock circuit for time stamping
6 data transactions;
7 a counter for counting a transaction count;
8 an input/output circuit;
9 a substantially unique electronically readable
10 identification number readable by said input/output circuit; and
11 a memory control circuit in electrical communication
12 with said nonvolatile memory, said real time clock, said counter,
13 and said input/output circuit;
14 a portable module reader that can be placed in
15 communication with said first portable module, said portable module
16 reader can be connected to a plurality of other devices;
17 a secure microcontroller based module in electronic
18 communication with said portable module reader, said secure
19 microcontroller comprising:
20 a microcontroller core;
21 a math coprocessor, in communication with said
22 microcontroller core, for processing encryption calculations;
23 an energy circuit for storing energy;

24 a memory circuit connected to said microcontroller core;
25 a memory circuit in communication with said
26 microcontroller core; and
27 a second real time clock circuit in communication with
28 said microcontroller,
29 said combination of said portable module reader and said
30 secure microcontroller performing secure data transfers with said
31 first portable module.

1 26. The system for communicating data securely, ^{of claim 25} wherein said
2 plurality of other devices includes at least one of a credit card
3 reader, a cash machine, an automatic teller machine, and a phone
4 line.

1 27. The system for communicating data securely, ^{of claim 25} wherein said
2 first data is a packet of encrypted data.

1 28. The system for communicating data securely, ^{of claim 25} wherein said
2 first portable module communicates with said portable module reader
3 via a single wire bus comprising a single bidirectional
4 communication wire and a ground connection.

1 ^S 29. The system for communicating data securely¹ wherein said
2 first module can create random public/private key sets for
3 encryption purposes. ^{of claim 25 1}

1 ⁶ 30. The system for communicating data securely¹ wherein said
2 secure microcontroller can create random public/private key sets
3 for encryption purposes.-- ^{of claim 25 1}

REMARKS

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

Claims 25-30 are pending in this application.

Claims 1-5, 7-15, 22 and 24 have been canceled without prejudice.

Regarding the § 103 Rejection

Claims 1-5, 7-15, 22 and 24 were all rejected for various reasons under 35 U.S.C. § 103 for being rendered obvious by the cited art. Applicant has canceled these claims thereby rendering these rejections moot.

Regarding the New Claims

Applicant has added new claims 25-30 because they are believed to contain novel aspects of the present invention worthy of a patent. Applicant notes that new independent claim 25 claims a system for communicating data securely. The system requires a first portable module, a portable module reader, and a secure microcontroller. The portable module comprises memory for storing data, real time clock, a counter for counting transactions and an input/output circuit along with a substantially unique electronically readable identification number which can be provided via the input/output circuit. The portable module reader can be placed in communication with the first portable module. The portable module reader can be connected to a variety of devices as discussed in the application.

A secure microcontroller based module can be placed in an electronic communication with the portable module reader. The secure microcontroller comprises among other things, a microcontroller core and a math co-processor circuit. The math co-processor circuit greatly enhances the speed for which the secure microcontroller can process encrypted calculations.

The system for communicating data securely, as discussed in the specification, allows a user to carry the portable module and install digital money equivalents into the module and spend or cash

the portable digits at locations that have a portable module reader.

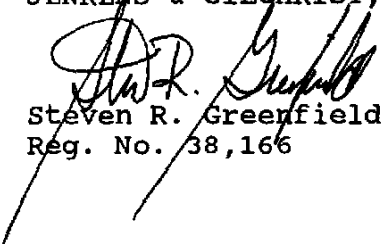
Applicant respectfully points out that none of the art cited to date, includes a system as claimed in the present application, and in particular, does not include a secure microcontroller having a dedicated math co-processor combined therewith such that secure communications can be provided between the portable module reader and the first portable module. Applicant further points out that none of the art cited teaches the advantages of combining a real time clock and a counter, along with a substantially unique electronically readable identification number found in the first portable module when creating certificates. Applicant further indicates that the present invention is an improvement over other systems for communicating data securely. Applicant believes that the present invention is not anticipated or rendered obvious by any of the cited art. Applicant respectfully submits that the new claims are ready for allowance.

Patent Application
Docket No. 20661-00429

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 8, 1998

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

SEM 2766



PATENT APPLICATION
DOCKET NO.: 20661-00429

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:

Curry et al.

Serial No.: 08/594,975 ✓

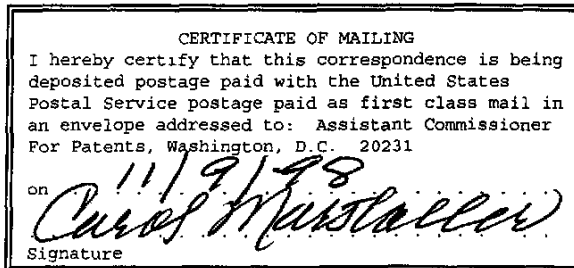
Filed: January 31, 1996 ✓

§
§
§
§
§
§

RECEIVED
NOV 18 1998
Examiner: White, Group 2700
Group Art Unit: 2766 ✓

For: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE

Assistant Commissioner For
Patents
Washington, D.C. 20231



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 August 10, 1998.
- 2) Acknowledgment Postcard.

IPDAL:187186.1 20661-00429

_____ 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.

XX No additional fee is required.

RECEIVED

NOV 18 1993

Group 2700

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	<u>6</u>	(at least 20)	= <u>0</u> (at least 0)	x11 = <u>OR</u>	x22 = \$ <u>0</u>
2. INDEP. CLAIMS	<u>6</u>	<u>3</u> (at least 3)	= <u>3</u> (at least 0)	x41 = <u>OR</u>	x82 = \$ <u>0</u>
3. FIRST PRESENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a <u>reissue</u> appln)				+130 = <u>OR</u>	+260 = \$ <u>0</u>
4. TOTAL FEE FOR ADDED CLAIMS					\$ <u>0</u>
5. _____ IDS ATTACHED REQUIRES OFFICIAL FEE - ADD \$230 (RULE 1.97(c)) OR \$130 (RULE 1.97(d)) PETITION)					\$ _____
6. _____ IF <u>TERMINAL DISCLAIMER</u> attached add Rule 20(d) Official Fee				\$55 (Small Entity)	\$110 (Large Entity) \$ _____
7. _____ <u>Petition is hereby made</u> under 37 CFR 1.136(a) to extend the <u>original</u> 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

PATENT APPLICATION
DOCKET NO.: 20661-00429

Four Months _____ \$755 _____ \$1,510

ADDITIONAL FEE FOR EXTENDED RESPONSE \$ 0

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** \$ 0

9. _____ A check in the amount of \$_____ 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 Jenkins & Gilchrist Deposit Account No. 10-0447 for which purpose a duplicate copy of this sheet is attached.*

PATENT APPLICATION
DOCKET NO.: 20661-00429

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
Reg. No. 38,166

Date: Nov 8, 1998
Jenkins & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
Tel: (214) 855-4789
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	ATTORNEY DOCKET NO
---------------	-------------	-----------------------	--------------------

DEVIN K. BRIDGEMAN
 JENNIFER W. HATHROBT
 300 MOUNTAIN PLACE
 1445 RUSSELL AVENUE
 WASHINGTON, DC 20002-7799

11/16/98

EXAMINER
 CAROL L. DOLAN

ART UNIT
 2781

PAPER NUMBER
 #15
 01/20/99

DATE MAILED:

NOTICE OF ALLOWABILITY

PART I.

- 1 This communication is responsive to 11/16/98
- 2 All the 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 sent in due course
- 3 The allowed claims are 25-30
- 4 The drawings filed on _____ are acceptable.
- 5 Acknowledgment is made of the claim for priority under 35 U.S.C 119. The certified copy has [] been received. [] not been received [] been filed in parent application Serial No _____, filed on _____
- 6 Note the attached Examiner's Amendment
- 7 Note the attached Examiner Interview Summary Record, PTOL-413.
- 8 Note the attached Examiner's Statement of Reasons for Allowance.
- 9 Note the attached NOTICE OF REFERENCES CITED, PTO-892.
- 10 Note the attached INFORMATION DISCLOSURE CITATION, PTO-1449.

PART II.

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

- 1 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
- 2 APPLICANT MUST MAKE THE DRAWING CHANGES INDICATED BELOW IN THE MANNER SET FORTH ON THE REVERSE SIDE OF THIS PAPER.
 - a Drawing informalities are indicated on the NOTICE RE PATENT DRAWINGS, PTO-948, attached hereto or to Paper No. 4 CORRECTION IS REQUIRED
 - b The proposed drawing correction filed on _____ has been approved by the examiner. CORRECTION IS REQUIRED.
 - c Approved drawing corrections are described by the examiner in the attached EXAMINER'S AMENDMENT. CORRECTION IS REQUIRED
 - d Formal drawings are now REQUIRED

Any response to this letter should include in the upper right hand corner, the following information from the NOTICE OF ALLOWANCE AND ISSUE FEE DUE: ISSUE BATCH NUMBER, DATE OF THE NOTICE OF ALLOWANCE, AND SERIAL NUMBER.

Attachments:

- Examiner's Amendment
- Examiner Interview Summary Record, PTOL-413
- Reasons for Allowance
- Notice of References Cited PTO-892
- Information Disclosure Citation, PTO-1449
- Notice of Informal Application, PTO-152
- Notice re Patent Drawings, PTO-948
- Listing of Bonded Draftsmen
- Other

Salvatore Cangialosi
SALVATORE CANGIALOSI
PRIMARY EXAMINER
ART UNIT 222

Serial Number: 08/594,975

-2-

Art Unit: 2746

Part III EXAMINER'S AMENDMENT

1. An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 C.F.R. § 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the Issue Fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Steven R. Greenfield on 1/28/99.

The application has been amended as follows:

In claim 26, line 1, the following has been inserted after "data securely",

--of claim 25--.

In claim 27, line 1, the following has been inserted after "data securely",

--of claim 25--.

In claim 28, line 1, the following has been inserted after "data securely",

--of claim 25--.

In claim 29, line 1, the following has been inserted after "data securely",

--of claim 25--.

In claim 30, line 1, the following has been inserted after "data securely",

--of claim 25--.


Serial Number: 08/594,975

-3-

Art Unit: 2746

Any comments considered necessary by applicant must be submitted no later than the payment of the Issue Fee and to avoid processing delays should preferably accompany the Issue Fee.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Salvatore Cangialosi whose telephone number is (703) 305-1837.


**SALVATORE CANGIALOSI
PRIMARY EXAMINER
ART UNIT 222**

sac

January 28, 1999



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

27

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

1. This notice is being mailed to you because you have been selected for allowance of your application. 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.

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
08/11/80	01/11/86	106	ANDREW A. GILL	7/20/89
First Named Applicant	MOTOROLA CORPORATION, 1300 NORTH CHERRY STREET, CHICAGO, ILLINOIS 60610			

TITLE OF INVENTION: SYSTEMS AND METHODS FOR TRANSMITTING AND RECEIVING DATA IN A WIRELESS COMMUNICATIONS SYSTEM

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
08/11/80	01/11/86	106	UTILITY	NO	\$1,200.00	10/20/89

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

PTOL-85 (REV. 10-96) Approved for use through 06/30/99. (0651-0033)

PART B—ISSUE FEE TRANSMITTAL

Complete and mail this form, together with applicable fees, to: **Box ISSUE FEE
Assistant Commissioner for Patents
Washington, D.C. 20231**

FILING 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.

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.

Suzanne Mitchell (Depositor's name)
Suzanne Mitchell (Signature)
April 16, 1999 (Date)

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

INDEPENDENT SCIENTIFIC
CORPORATION
2000 FOUNTAIN PLACE
DALLAS, TEXAS 75242-1799



APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
08/194,701	01/20/96	106	CAHVAL/15, 3	7/16 01/20/99
First Named Applicant	JENKENS & GILCHRIST			

TITLE OF INVENTION: SYSTEMS AND METHODS FOR NETWORK AND DEVICE MODULES AND METHODS

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
08/194,701	0800-0401, 000	000	UTILITY	NO	\$1210.00	12/29/98

- 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.
- 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 Jenkins & 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, Texas

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

Individual corporation or other private group entity government

- The following fees are enclosed (make check payable to Commissioner of Patents and Trademarks):
 - Issue Fee
 - Advance Order - # of Copies 10
- 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) *[Signature]* (Date) 4/16/99

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 ZABD011 00000051 08594975

01 FC:142 1210.00 DP
02 FC:361 30.00 DP

Byrd 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.

RECEIVED
APR 23 1999

TRANSMIT THIS FORM WITH FEE
Publishing Division
Corres/Allowed Files (07)
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Jenkins & Gilchrist
A PROFESSIONAL CORPORATION

05 C 5 76 B#

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

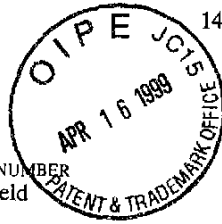
(214) 855-4500
TELECOPIER (214) 855-4300

AUSTIN, TEXAS
(512) 499-3800

HOUSTON, TEXAS
(713) 951-3300

SAN ANTONIO, TEXAS
(210) 308-3100

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



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. EL274278018US
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 C.F.R. 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231
Susan E. Mitchell
Signature: SUSAN E MITCHELL

Re: Applicant(s): Stephen M. Curry, et al.
Serial No.: 08/594,975
Filed: January 31, 1996
Batch No. 040
NOA Mailed: January 29, 1999
For: Transfer of Valuable Information Between a Secure Module and Another Module
Docket No.: 20661-00429

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

Please address all communications related to this to:

Steven R. Greenfield
Jenkins & 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 #10-0447.

RECEIVED
APR 23 1999
Publishing Division
Corresponding Files (07)

Respectfully submitted,

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

IPDAL:211582.1 20661-00429

DOCKET NO.: 236 A-00429

PATENT APPLICATION



Issue Batch No.: 040
Date of Notice of Allowance : January 29, 1999
Serial No. : 08/594,975

7530
2700
4/23/99
SF94
16
ZE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: Curry, et al.

Serial No.: 08/594,975

Group No.: 2746

Filed: January 31, 1996

Examiner: Cangialosi, S.

For: **Transfer of Valuable Information Between a Secure Module and Another Module**

BOX ISSUE FEE
Assistant Commissioner
for Patents
Washington DC 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL
"EXPRESS MAIL" Mailing Label No. EL274278018US
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 C.F.R. 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231
<i>Susan E. Mitchell</i>
Signature: SUSAN E MITCHELL

ATTN: Official Draftsperson

Dear 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., the date of the Notice of Allowance and Serial No. 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.

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

Steven R. Greenfield

Steven R. Greenfield
Registration No. 38,166

RECEIVED

APR 23 1999

Publishing Division
Corres/Allowed Files (07)

5940510

1/8

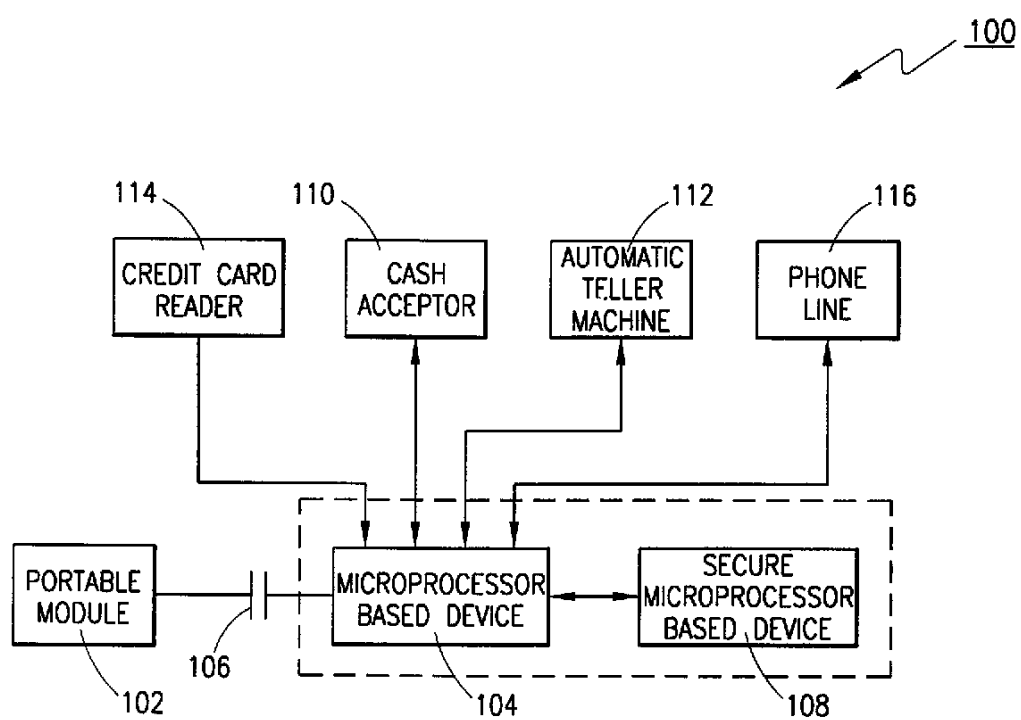


FIG. 1

102

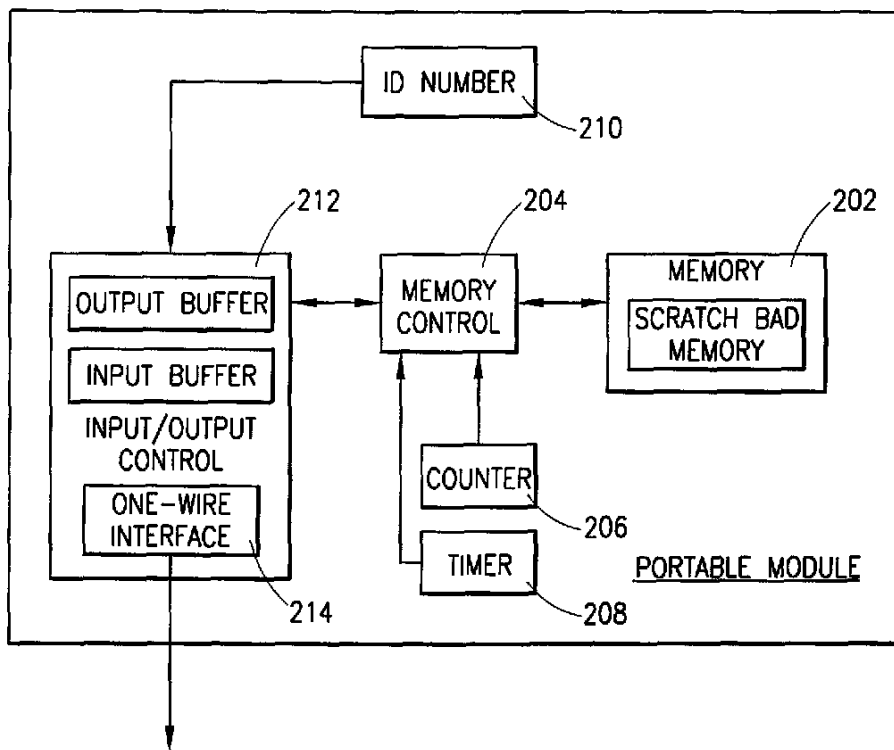


FIG. 2

108

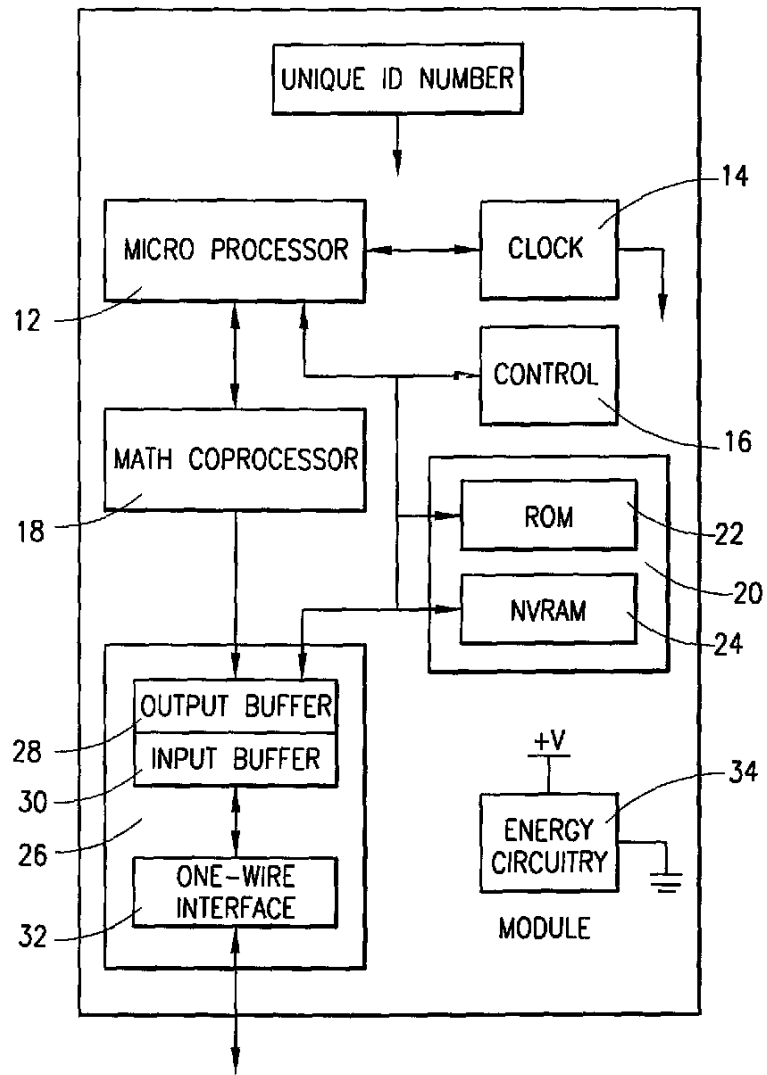


FIG. 3

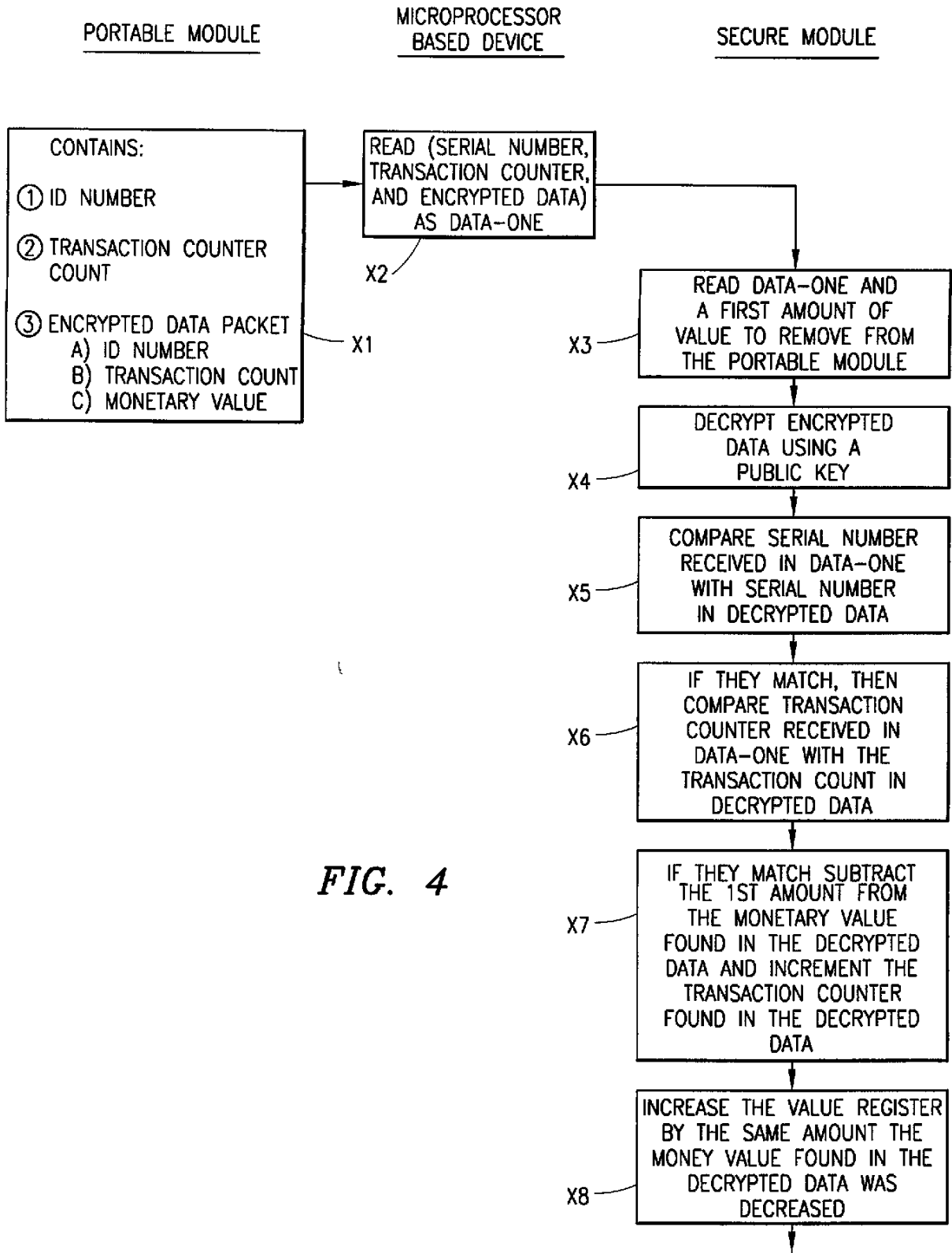


FIG. 4

PORTABLE MODULE

MICROPROCESSOR
BASED DEVICE

SECURE MODULE

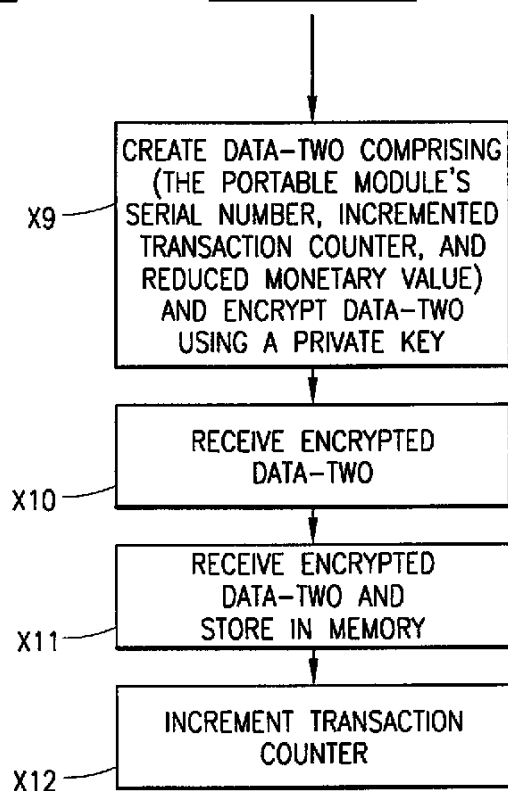


FIG. 4
(CONTINUED)

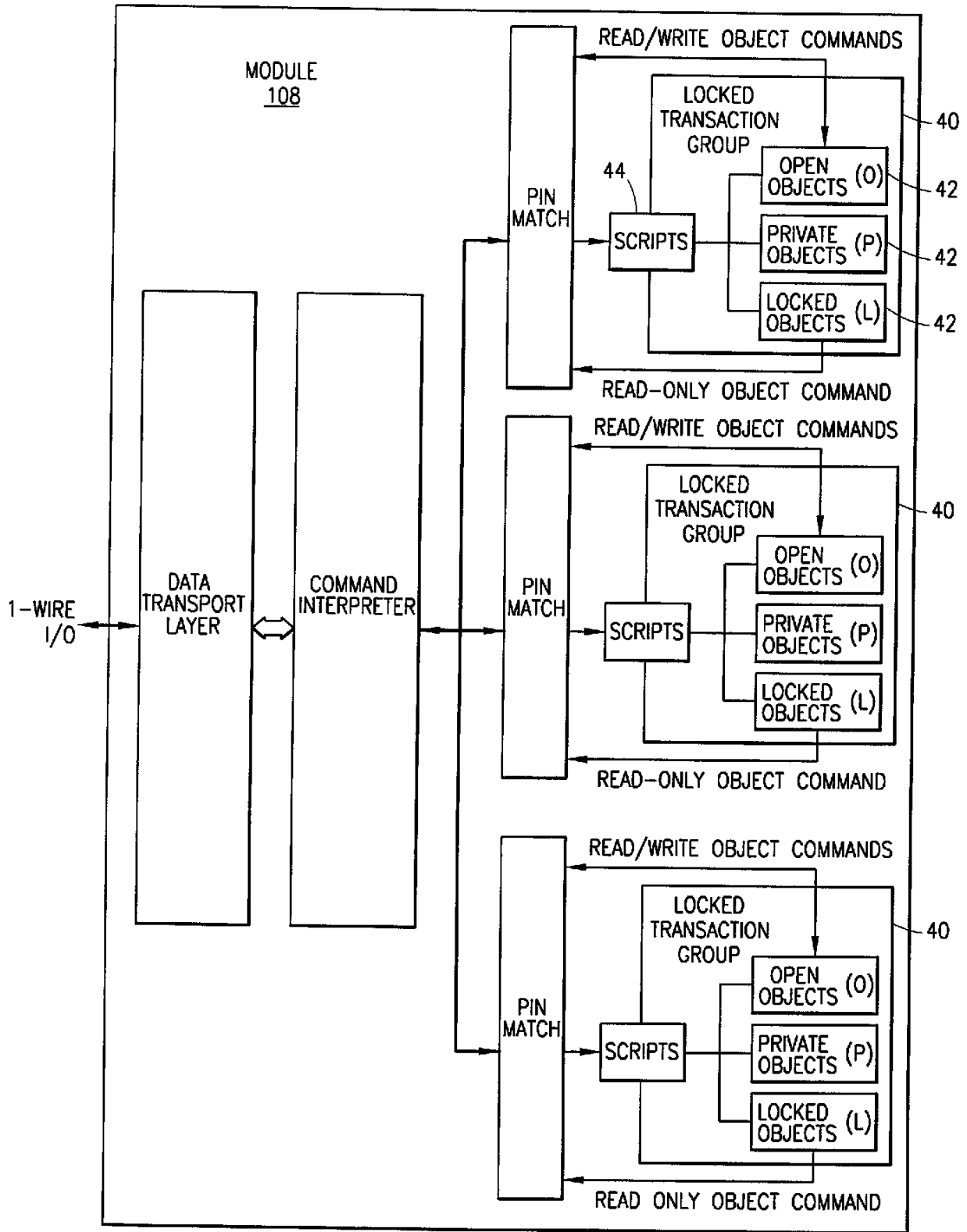


FIG. 6

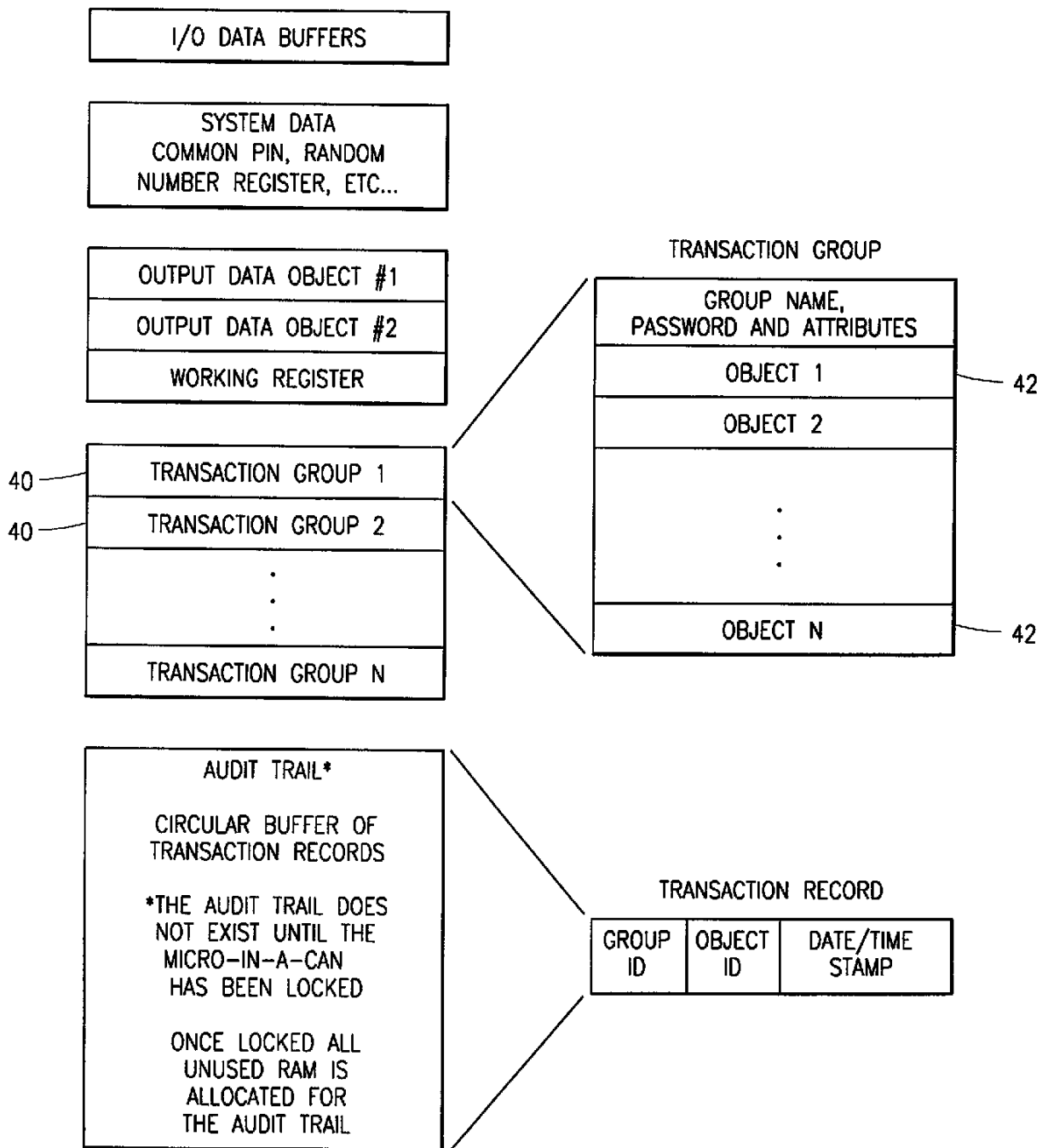


FIG. 7

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Number: 5,940,510
Issued: Aug. 17, 1999
Name of Patentee: Curry et al.
Title of Invention: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE
MODULE AND ANOTHER MODULE

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

CERTIFICATE OF MAILING	
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box Certificate of Correction Assistant Commissioner of Patents Washington, D.C. 20231	
on	29 September 1999
Signature	P. Guardiola
Printed Name	P. Guardiola

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:

<u>Patent</u>	<u>Application File</u>
Item [57], line 1	Page 97, line 2

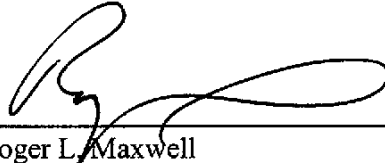
LW

The errors are printing errors by the Patent and Trademark Office and, accordingly, should be corrected without fee from applicant.

Please send the Certificate of Correction to:

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

Assignee: Dallas Semiconductor Corporation



Roger L. Maxwell
Assignee's Attorney
Reg. No. 34,746

/ X / Assignment recorded on
Reel/Frame 8029/0098 *et seq.*

/ ___ / Recordal of assignment attached

Jenkins & 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

WRITER'S DIRECT DIAL NUMBER

Roger L. Maxwell
(214) 855-4787

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

CERTIFICATE OF MAILING	
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box Certificate of Correction Assistant Commissioner of Patents Washington, D.C. 20231	
on	29 September 1999
Signature	P. Guardiola
Printed Name	P. Guardiola

Re: Patent No.: 5,940,510
Issued: Aug. 17, 1999
Title: TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER
MODULE
Inventor: Curry et al.

Dear Sir or Madam:

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

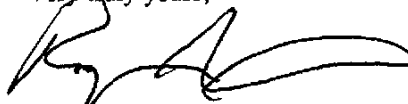
1. Request for Certificate of Correction of Patent to correct typographical errors in the patent, which does not introduce any new matter;
2. Form PTO-1050 (in duplicate); and
3. An acknowledgement postcard.

Please address all related communications to:

Roger L. Maxwell
Jenkins & 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 #10-0447. This letter is being filed in duplicate to facilitate processing.

Very truly yours,



Roger L. Maxwell
Reg. No. 34,746

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 1997

Application or Docket Number

08/594975

CLAIMS AS FILED - PART I

(Column 1) (Column 2)

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	16 minus 20 = *	—
INDEPENDENT CLAIMS	2 minus 3 = *	—
MULTIPLE DEPENDENT CLAIM PRESENT		

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

SMALL ENTITY TYPE

OR OTHER THAN SMALL ENTITY

RATE	FEE	OR	RATE	FEE
	395.00	OR		790.00
x\$11=		OR	x\$22=	
x41=		OR	x82=	
+135=		OR	+270=	
TOTAL		OR	TOTAL	

CLAIMS AS AMENDED - PART II

(Column 1) (Column 2) (Column 3)

AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	* 6	Minus	** 20	=
Independent	* 6	Minus	*** 3	= 3
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY

OR OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
x\$11=		OR	x\$22=	
x41=		OR	x82=	228 ⁰⁰
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	228 ⁰⁰

(Column 1) (Column 2) (Column 3)

AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
x\$11=		OR	x\$22=	
x41=		OR	x82=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

(Column 1) (Column 2) (Column 3)

AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
x\$11=		OR	x\$22=	
x41=		OR	x82=	
+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.

PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 1995

Application or Docket Number

594975

CLAIMS AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	21 minus 20 = *	1
INDEPENDENT CLAIMS	3 minus 3 = *	
MULTIPLE DEPENDENT CLAIM PRESENT		

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

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
	375.00	OR		750.00
x\$11=		OR	x\$22=	27
x39=		OR	x78=	
+125=		OR	+250=	
TOTAL		OR	TOTAL	777

CLAIMS AS AMENDED - PART II

AMENDMENT A	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR		
Total	* 17	Minus ** 21	=	-
Independent	* 3	Minus *** 3	=	-
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDI-TIONAL FEE		RATE	ADDI-TIONAL FEE
x\$11=		OR	x\$22=	
x39=		OR	x78=	
+125=		OR	+250=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR		
Total	* 16	Minus ** 21	=	-
Independent	* 2	Minus *** 3	=	-
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDI-TIONAL FEE	RATE	ADDI-TIONAL FEE
x\$11=		OR	x\$22=
x39=		OR	x78=
+125=		OR	+250=
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE

AMENDMENT C	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR		
Total	*	Minus **	=	
Independent	*	Minus ***	=	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDI-TIONAL FEE	RATE	ADDI-TIONAL FEE
x\$11=		OR	x\$22=
x39=		OR	x78=
+125=		OR	+250=
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.

MPI Family Report (Family Bibliographic and Legal Status)

In the MPI Family report, all publication stages are collapsed into a single record, based on identical application data. The bibliographic information displayed in the collapsed record is taken from the latest publication.

Report Created Date: 2012-01-12

Name of Report:

Number of Families: 1

Comments:

Table of Contents

1.	US5940510A 19990817 DALLAS SEMICONDUCTOR US	
	Transfer of valuable information between a secure module and another module	1

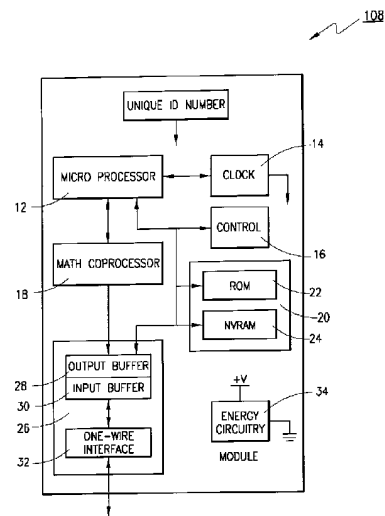


Family1**2 records in the family.****US5940510A 19990817****(ENG) Transfer of valuable information between a secure module and another module****Assignee:** DALLAS SEMICONDUCTOR US**Inventor(s):** CURRY STEPHEN M US ; LOOMIS DONALD W US ; BOLAN MICHAEL L US**Application No:** US 59497596 A**Filing Date:** 19960131**Issue/Publication Date:** 19990817

Abstract: (ENG) The present invention relates to system, apparatus and method for communicating valuable data from a portable module to another module via an electronic device. More specifically, the disclosed system, apparatus and method are useful for enabling a user to fill a portable module with a cash equivalent and to spend the cash equivalent at a variety of locations. The disclosed system incorporates an encryption/decryption method.

Priority Data: US 59497596 19960131 A Y;**IPC (International Class):** G07F00710; G07F00708**ECLA (European Class):** G07F00708C2B; G07F00710D4E**US Class:** 705065; 705076; 713173**Publication Language:** ENG**Filing Language:** ENG**Agent(s):** Jenkins & Gilchrist**Examiner Primary:** Cangialosi, Salvatore**US Post Issuance:**

--US Certificate of Correction: 20000222

Assignments Reported to USPTO:**Reel/Frame:** 08029/0098 **Date Signed:** 19960416 **Date Recorded:** 19960506**Assignee:** DALLAS SEMICONDUCTOR CORPORATION 4401 S. BELTWOOD PARKWAY DALLAS TEXAS 75244**Assignor:** CURRY, STEPHEN M.; LOOMIS, DONALD W.; BOLAN, MICHAEL L.**Corres. Addr:** JENKENS & GILCHRIST, P.C. STEVEN R. GREENFIELD, P.C 1445 ROSS AVENUE SUITE 3200 DALLAS, TX 75202-2799**Brief:** ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).**Reel/Frame:** 21253/0637 **Date Signed:** 20080610 **Date Recorded:** 20080717**Assignee:** MAXIM INTEGRATED PRODUCTS, INC. 120 SAN GABRIEL DRIVE SUNNYVALE CALIFORNIA 94086**Assignor:** DALLAS SEMICONDUCTOR CORPORATION

Corres. Addr: NORTH WEBER & BAUGH LLP ATTN: MICHAEL V. NORTH 2479 E. BAYSHORE RD, SUITE 707 PALO ALTO, CA 94303

Brief: MERGER

Legal Status:

Date	+/-	Code	Description
19960506	()	AS	New owner name: DALLAS SEMICONDUCTOR CORPORATION, TEXAS; : ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNORS:CURRY, STEPHEN M.;LOOMIS, DONALD W.;BOLAN, MICHAEL L.;REEL/FRAME:008029/0098;SIGNING DATES FROM 19960416 TO 19960418;
20000222	()	CC	CERTIFICATE OF CORRECTION
20021220	()	FPAY	Year of fee payment: 4;
20070302	()	FPAY	Year of fee payment: 8;
20070302	()	SULP	Year of fee payment: 7;
20080307	()	REMI	New owner name: MAXIM INTEGRATED PRODUCTS, INC., CALIFORNIA; : MERGER;ASSIGNOR:DALLAS SEMICONDUCTOR CORPORATION;REEL/FRAME:021253/0637; Effective date: 20080610;
20110321	()	REMI	

US5949880A 19990907

(ENG) Transfer of valuable information between a secure module and another module

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; BOLAN MICHAEL L US

Application No: US 97879897 A

Filing Date: 19971126

Issue/Publication Date: 19990907

Abstract: (ENG) The present invention relates to system, apparatus and method for communicating valuable data from a portable module to another module via an electronic device. More specifically, the disclosed system, apparatus and method are useful for enabling a user to fill a portable module with a cash equivalent and to spend the cash equivalent at a variety of locations. The disclosed system incorporates an encryption/decryption method.

Priority Data: US 97879897 19971126 A N; US 59497596 19960131 A 3 Y;

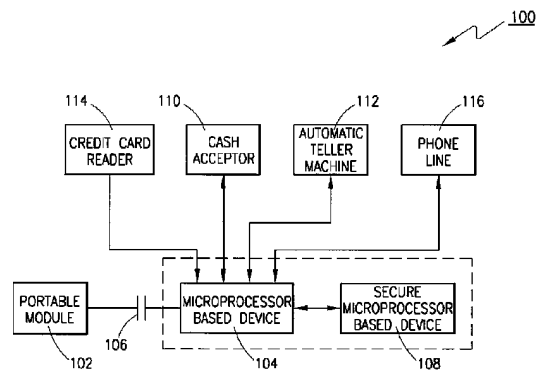
Related Application(s): 08/594975 19960131 US PENDING

IPC (International Class): G07F00710; G07F00708

ECLA (European Class): G07F00708C2B; G07F00710D4E

US Class: 705066; 705039; 705042; 705065

Publication Language: ENG



Filing Language: ENG

Agent(s): Jenkins & Gilchrist

Examiner Primary: Tarcza, Thomas H.

Examiner Assistant: White, Carmen D.

US Post Issuance:

--US Certificate of Correction: 20000425 20000425 a Certificate of Correction was issued for this patent

Assignments Reported to USPTO:

Reel/Frame: 06462/0935 **Date Signed:** 19930315 **Date Recorded:** 19930316

Assignee: MIDAS REX PNEUMATIC TOOLS, INC. 3001 RACE STREET FORT WORTH TEXAS 76111

Assignor: BARBER, FOREST C., JR., EXECUTOR OF ESTATE OF FOREST C. BARBER, M.D.; BARRETT, CARON HELEN BARRETT, CARON HELEN I., EXECUTORS OF ESTATE OF FOREST C. BARBER, M.D.

Corres. Addr: JAMES E. BRADLEY FELSMAN, BARDLEY, GUNTER & DILLON, LLP 2600 CONTINENTAL PLAZA 777 MAIN STREET FORT WORTH, TX 76102

Brief: ASSIGNMENT OF ASSIGNORS INTEREST.

Reel/Frame: 08847/0336 **Date Signed:** 19971110 **Date Recorded:** 19971124

Assignee: MURATA MANUFACTURING CO., LTD. NAGAOKAKYO-SHI 26-10, 2-CHOME, TENJIN KYOTO 617 JAPAN

Assignor: SHIMOE, KAZUNOBU

Corres. Addr: GRAHAM & JAMES LLP ALBERT L. JACOBS, JR. INTELLECTUAL PROPERTY GROUP 885 THIRD AVENUE NEW YORK, NY 10022

Brief: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Reel/Frame: 21253/0637 **Date Signed:** 20080610 **Date Recorded:** 20080717

Assignee: MAXIM INTEGRATED PRODUCTS, INC. 120 SAN GABRIEL DRIVE SUNNYVALE CALIFORNIA 94086

Assignor: DALLAS SEMICONDUCTOR CORPORATION

Corres. Addr: NORTH WEBER & BAUGH LLP ATTN: MICHAEL V. NORTH 2479 E. BAYSHORE RD, SUITE 707 PALO ALTO, CA 94303

Brief: MERGER

Legal Status:

Date	+/-	Code	Description
19930316	()	AS	New owner name: MIDAS REX PNEUMATIC TOOLS, INC., TEXAS; : ASSIGNMENT OF ASSIGNORS INTEREST.;ASSIGNORS:BARBER, FOREST C., JR., EXECUTOR OF ESTATE OF FOREST C.BARBER, M.D.;BARRETT, CARON HELEN I., EXECUTORS OF ESTATE OF FOREST C. BARBER, M.D.;REEL/FRAME:006462/0935; Effective date: 19930315;
19971124	()	AS	New owner name: MURATA MANUFACTURING CO., LTD., JAPAN; : ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNOR:SHIMOE, KAZUNOBU;REEL/FRAME:008847/0336; Effective date: 19971110;



20000425	()	CC	CERTIFICATE OF CORRECTION
20021225	()	FPAY	Year of fee payment: 4;
20070302	()	FPAY	Year of fee payment: 8;
20080717	()	AS	New owner name: MAXIM INTEGRATED PRODUCTS, INC., CALIFORNIA; : MERGER;ASSIGNOR:DALLAS SEMICONDUCTOR CORPORATION;REEL/FRAME:021253/0637; Effective date: 20080610;
20110411	()	REMI	



USPTO Maintenance Report

Patent Bibliographic Data		01/12/2012 11:56 AM			
Patent Number:	5940510	Application Number:	08594975		
Issue Date:	08/17/1999	Filing Date:	01/31/1996		
Title:	TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER M				
Status:	4th, 8th and 12th year fees paid		Entity:	Large	
Window Opens:	N/A	Surcharge Date:	N/A	Expiration:	N/A
Fee Amt Due:	Window not open	Surchg Amt Due:	Window not open	Total Amt Due:	Window not open
Fee Code:					
Surcharge Fee Code:					
Most recent events (up to 7):	08/15/2011 08/15/2011 03/21/2011 08/05/2010 08/05/2010 03/07/2007 03/02/2007	11.5 yr surcharge- late pmt w/in 6 mo, Large Entity. Payment of Maintenance Fee, 12th Year, Large Entity. Maintenance Fee Reminder Mailed. Payor Number Assigned. Payer Number De-assigned. Maintenance Fee Reminder Mailed. Payment of Maintenance Fee, 8th Year, Large Entity. --- End of Maintenance History ---			
Address for fee purposes:	NORTH WEBER & BAUGH LLP 2479 E. BAYSHORE ROAD SUITE 707 PALO ALTO CA 94303				