950143

ISSUE CLASSIFICATION	
Class	Subclass
380	24

[redacted]

BEST COPY

5805702

5805702

UTILITY SERIAL NUMBER	PATENT DATE	PATENT NUMBER
595014	SEP 08 1998	

SERIAL NUMBER	FILING DATE	CLASS	SUBCLASS	GROUP ART UNIT	EXAMINER
08/595,014	[illegible]	380	24	[illegible]2	White

APPLICANTS

STEPHEN A. [illegible], DALLAS, [illegible] TX;
CHRISTOPHER W. FOX, DALLAS, TX.

CONTINUING DATA*******************
VERIFIED PROVISIONAL APPLICATION NO. [illegible] 10/95

CW

FOREIGN/PCT APPLICATIONS**********
VERIFIED

CW

CERTIFICATE

APR 0 1999

CORRECTION

FOREIGN FILING LICENSE GRANTED 0[illegible]

Foreign priority claimed 35 USC 119 conditions met Verified and Acknowledged	□ yes ☒ no □ yes ☒ no CW Examiner's initials	AS FILED →	STATE OR COUNTRY	SHEETS DRWGS.	TOTAL CLAIMS	INDEP. CLAIMS	FILING FEE RECEIVED	ATTORNEY'S DOCKET NO.
			TX	8			[illegible]	2266-[illegible]

ADDRESS

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

TITLE

METHOD, APPARATUS, AND SYSTEM TO TRANSFER UNITS OF VALUE

U.S. DEPT. OF COMM./ PAT. & TM—PTO-436L (Rev.12-9

PARTS OF APPLICATION FILED SEPARATELY	Applications Examiner 10/3/95

NOTICE OF ALLOWANCE MAILED		CLAIMS ALLOWED	
10-2-97	Carmen D. White CW Assistant Examiner	Total Claims 15	Print Claim 1

ISSUE FEE			DRAWING		
Amount Due	Date Paid	THOMAS H. TARCZA SUPERVISORY PATENT EXAMINER GROUP 2200	Sheets Drwg.	Figs. Drwg.	Print Fig.
$1320	1-6-98		8	12	8

Label Area	Thomas H. Tarcza Primary Examiner PREPARED FOR ISSUE	ISSUE BATCH NUMBER 570

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.

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

ISSUE FEE IN FILE

PB

(FACE)

5,805,702

METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

Transaction History

Date	Transaction Description
2/15/1996	Initial Exam Team nn
3/18/1996	Notice Mailed--Application Incomplete--Filing Date Assigned
5/2/1996	Application Is Now Complete
6/3/1996	Application Captured on Microfilm
6/6/1996	Transfer Inquiry
6/10/1996	Case Docketed to Examiner in GAU
11/21/1996	Miscellaneous Incoming Letter
3/3/1997	Case Docketed to Examiner in GAU
7/18/1997	Restriction/Election Requirement
7/21/1997	Mail Restriction Requirement
9/8/1997	Response to Election / Restriction Filed
9/8/1997	Request for Extension of Time - Granted
9/24/1997	Date Forwarded to Examiner
10/2/1997	Mail Notice of Allowance
10/2/1997	Notice of Allowance Data Verification Completed
12/5/1997	Preexamination Location Change
1/6/1998	Mailroom Date of Drawing(s)
1/6/1998	Issue Fee Payment Verified
4/15/1998	Application Ordered to Match Drawing(s)
4/15/1998	Drawing(s) Received at Publications
5/20/1998	Application Received to Match Drawing(s)
7/1/1998	Drawing(s) Processing Completed
7/1/1998	Drawing(s) Matched to Application
8/3/1998	Issue Notification Mailed
9/8/1998	Recordation of Patent Grant Mailed
3/10/1999	Post Issue Communication - Certificate of Correction

08/595014

PATENT APPLICATION

08595014

APPROVED FOR LICENSE □

INITIALS ______

BEST COPY

CONTENTS

Date Entered or Counted			Date Received or Mailed
	1.	Application ______ papers.	
	2.	[illegible]	3/18/96
	3.	Dec, Surcharge, Add Fee	4-18-96
	4.	Req'd Cor. F. R.	6-10-96
	5.	Status Letter	10/24/96
	6.	Status Report	11/26/96
7-18	7.	3 month Restriction	7-21-97
	8.	Req. Ext. Time	9-8-97 [illegible]
	9.	Amdt A	9-8-97
	10.	Exr's Amdt / B	10-2-97
10/1	11.	P.T.O.-L-85	10-2-97
	12.	CPR	9/2/98
	13.	PTO GRANT SEP 08 1998	
	14.	Req for CofC R322	1-19-99
	15.		
	16.		
	17.		
	18.		
	19.		
	20.		
	21.		
	22.		
	23.		
	24.		
	25.		
	26.		
	27.		
	28.		
	29.		
	30.		
	31.		
	32.		

(FRONT)

STAPLE

☆U.S. GOVERNMENT PRINTING OFFICE 1997-422-215

PATENT NUMBER

ORIGINAL CLASSIFICATION

CLASS	SUBCLASS
380	24

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)			
25				

APPLICATION SERIAL NUMBER
08/595,014

APPLICANT'S NAME (PLEASE PRINT)
Steven M. Curry et. al.

IF REISSUE, ORIGINAL PATENT NUMBER

INTERNATIONAL CLASSIFICATION

H	0	4	L		9	/00
						/
						/
						/

GROUP ART UNIT
2202

ASSISTANT EXAMINER (PLEASE STAMP OR PRINT FULL NAME)
Carmen D. White

PRIMARY EXAMINER (PLEASE STAMP OR PRINT FULL NAME)
Thomas H. Tarcza

PTO 270
(REV. 5-91)

ISSUE CLASSIFICATION SLIP

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

Claim		Date								
Final	Original	5/7/97	9/30/97							
1	1	+	=							
2	2	+	=							
3	3	+	=							
4	4	+	=							
5	5	+	=							
6	6	+	=							
7	7	+	=							
8	8	+	=							
9	9	+	=							
10	10	+	=							
11	11	+	=							
12	12	+	=							
13	13	+	=							
14	14	+	=							
15	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									

SYMBOLS

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

Claim		Date							
Final	Original								
	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								

(LEFT INSIDE)

POSITION		ID NO.	DATE
CLASSIFIER		7	8-1-96
EXAMINER		290	3-11-96
TYPIST		330	5/18/ /
VERIFIER		315	5/21/96
CORPS CORR.			
SPEC. HAND			
FILE MAINT.			
DRAFTING			

INDEX OF CLAIMS

Claim		Date							
Final	Original	5/7/97	9/30/97						
1	1	+	=						
2	2	+	=						
3	3	+	=						
4	4	+	=						
5	5	+	=						
6	6	+	=						
7	7	+	=						
8	8	+	=						
9	9	+	=						
10	10	+	=						
11	11	+	=						
12	12	+	=						
13	13	+	=						
14	14	+	=						
15	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								

SYMBOLS

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

Claim		Date							
Final	Original								
	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								

[redacted]

SEARCHED

Class	Sub.	Date	Exmr.
380	23	4/23/97	CDW
	24		
	25		
	30		
364	717	↓	↓
	464.02		

INTERFERENCE SEARCHED

Class	Sub.	Date	Exmr.
380	24	9/30/97	CW

SEARCH NOTES

	Date	Exmr.
Aps Text Search	4/15/97	CW
	9/29/97	CW
	9/30/97	CW

(RIGHT OUTSIDE)

US005805702A

United States Patent [19]

Curry et al.

[11] **Patent Number: 5,805,702**

[45] **Date of Patent: Sep. 8, 1998**

[54] **METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE**

[75] Inventors: **Stephen M. Curry**, Dallas; **Donald W. Loomis**, Coppell; **Christopher W. Fox**, Dallas, all of Tex.

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

[21] Appl. No.: **595,014**

[22] Filed: **Jan. 31, 1996**

Related U.S. Application Data

[60] Provisional application No. 60/004,510, Sep. 29, 1995.

[51] **Int. Cl.**^{6} **H04L 9/00**

[52] **U.S. Cl.** **380/24**

[58] **Field of Search** 380/23, 24, 25, 380/30; 364/717, 464.02

[56] **References Cited**

U.S. PATENT DOCUMENTS

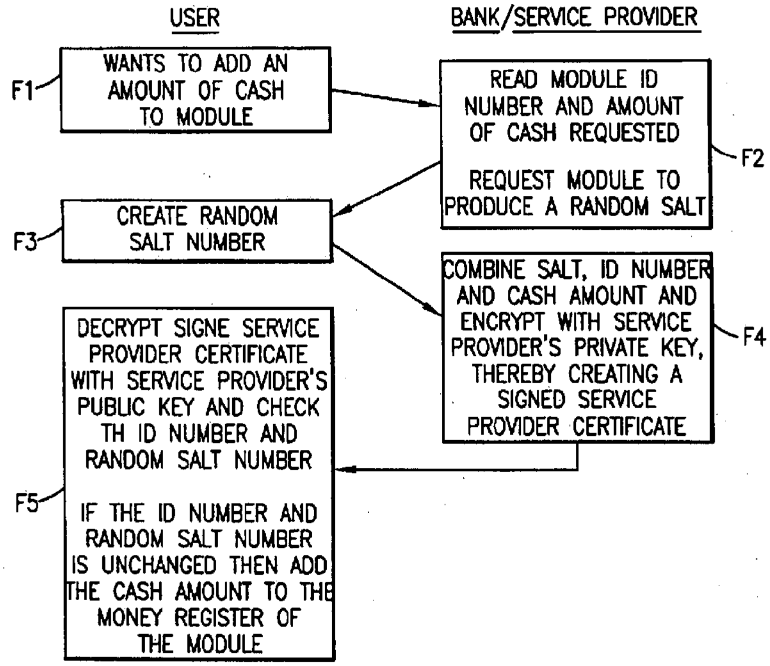
4,630,201	12/1986	White	364/408
5,077,792	12/1991	Herring	380/24
5,577,121	11/1996	Davis et al.	380/24

Primary Examiner—Thomas H. Tarcza
Assistant Examiner—Carmen D. White
Attorney, Agent, or Firm—Jenkens & Gilchrist

[57] **ABSTRACT**

The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing encrypted information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

15 Claims, 8 Drawing Sheets


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

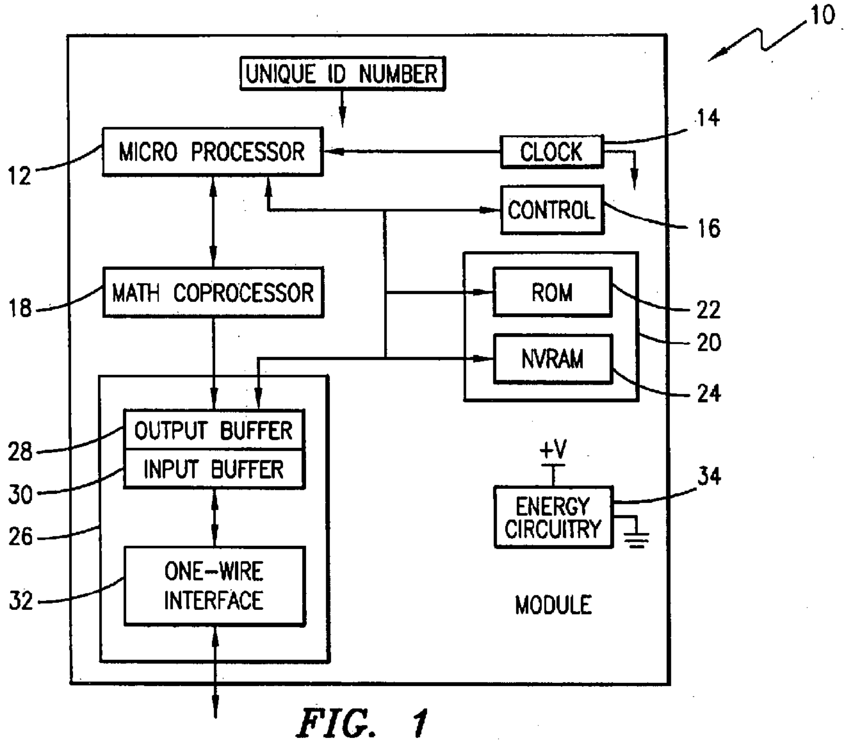

10
UNIQUE ID NUMBER
MICRO PROCESSOR
12
CLOCK
14
CONTROL
16
MATH COPROCESSOR
18
ROM
22
20
NVRAM
24
OUTPUT BUFFER
28
INPUT BUFFER
30
26
+V
ENERGY CIRCUITRY
34
ONE-WIRE INTERFACE
32
MODULE

FIG. 1

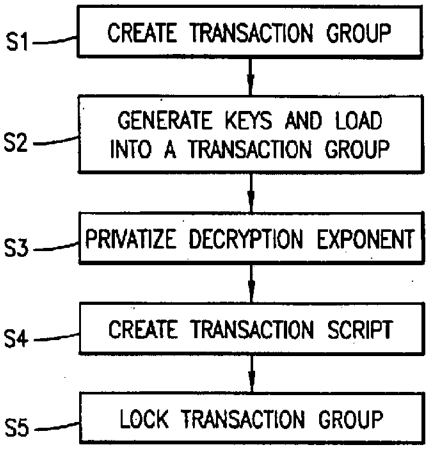

S1
CREATE TRANSACTION GROUP
S2
GENERATE KEYS AND LOAD INTO A TRANSACTION GROUP
S3
PRIVATIZE DECRYPTION EXPONENT
S4
CREATE TRANSACTION SCRIPT
S5
LOCK TRANSACTION GROUP

FIG. 2

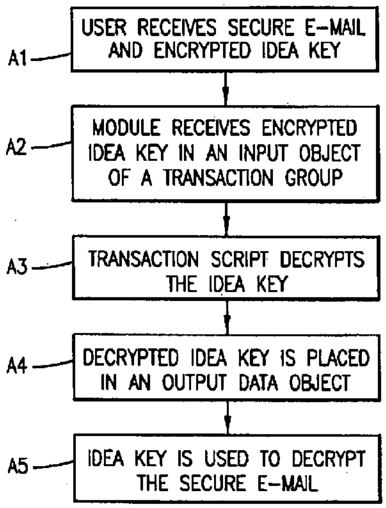

USER RECEIVES SECURE E-MAIL AND ENCRYPTED IDEA KEY
A1
MODULE RECEIVES ENCRYPTED IDEA KEY IN AN INPUT OBJECT OF A TRANSACTION GROUP
A2
TRANSACTION SCRIPT DECRYPTS THE IDEA KEY
A3
DECRYPTED IDEA KEY IS PLACED IN AN OUTPUT DATA OBJECT
A4
IDEA KEY IS USED TO DECRYPT THE SECURE E-MAIL
A5

FIG. 3

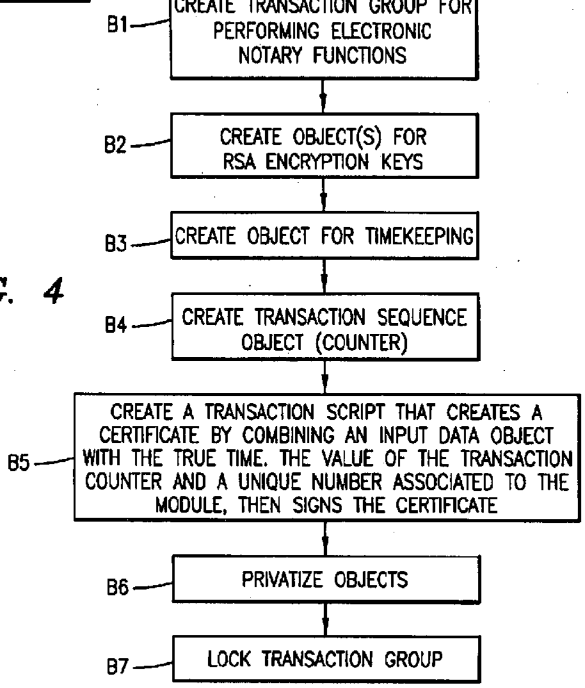

CREATE TRANSACTION GROUP FOR PERFORMING ELECTRONIC NOTARY FUNCTIONS
B1
CREATE OBJECT(S) FOR RSA ENCRYPTION KEYS
B2
CREATE OBJECT FOR TIMEKEEPING
B3
CREATE TRANSACTION SEQUENCE OBJECT (COUNTER)
B4
CREATE A TRANSACTION SCRIPT THAT CREATES A CERTIFICATE BY COMBINING AN INPUT DATA OBJECT WITH THE TRUE TIME.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

FIG. 4

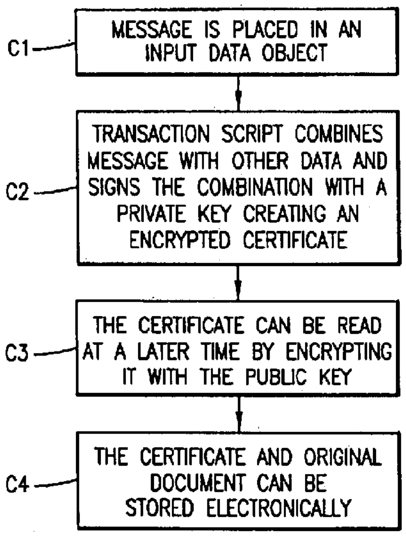

C1
MESSAGE IS PLACED IN AN INPUT DATA OBJECT
C2
TRANSACTION SCRIPT COMBINES MESSAGE WITH OTHER DATA AND SIGNS THE COMBINATION WITH A PRIVATE KEY CREATING AN ENCRYPTED CERTIFICATE
C3
THE CERTIFICATE CAN BE READ AT A LATER TIME BY ENCRYPTING IT WITH THE PUBLIC KEY
C4
THE CERTIFICATE AND ORIGINAL DOCUMENT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

FIG. 5

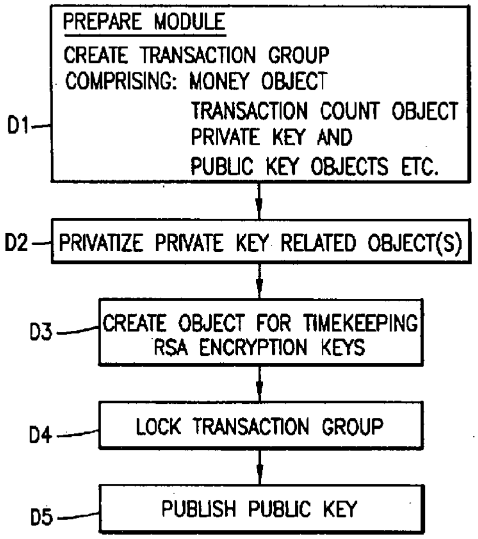

PREPARE MODULE
CREATE TRANSACTION GROUP
COMPRISING: MONEY OBJECT
TRANSACTION COUNT OBJECT
PRIVATE KEY AND
PUBLIC KEY OBJECTS ETC.
D1
D2
PRIVATIZE PRIVATE KEY RELATED OBJECT(S)
D3
CREATE OBJECT FOR TIMEKEEPING RSA ENCRYPTION KEYS
D4
LOCK TRANSACTION GROUP
D5
PUBLISH PUBLIC KEY

FIG. 6

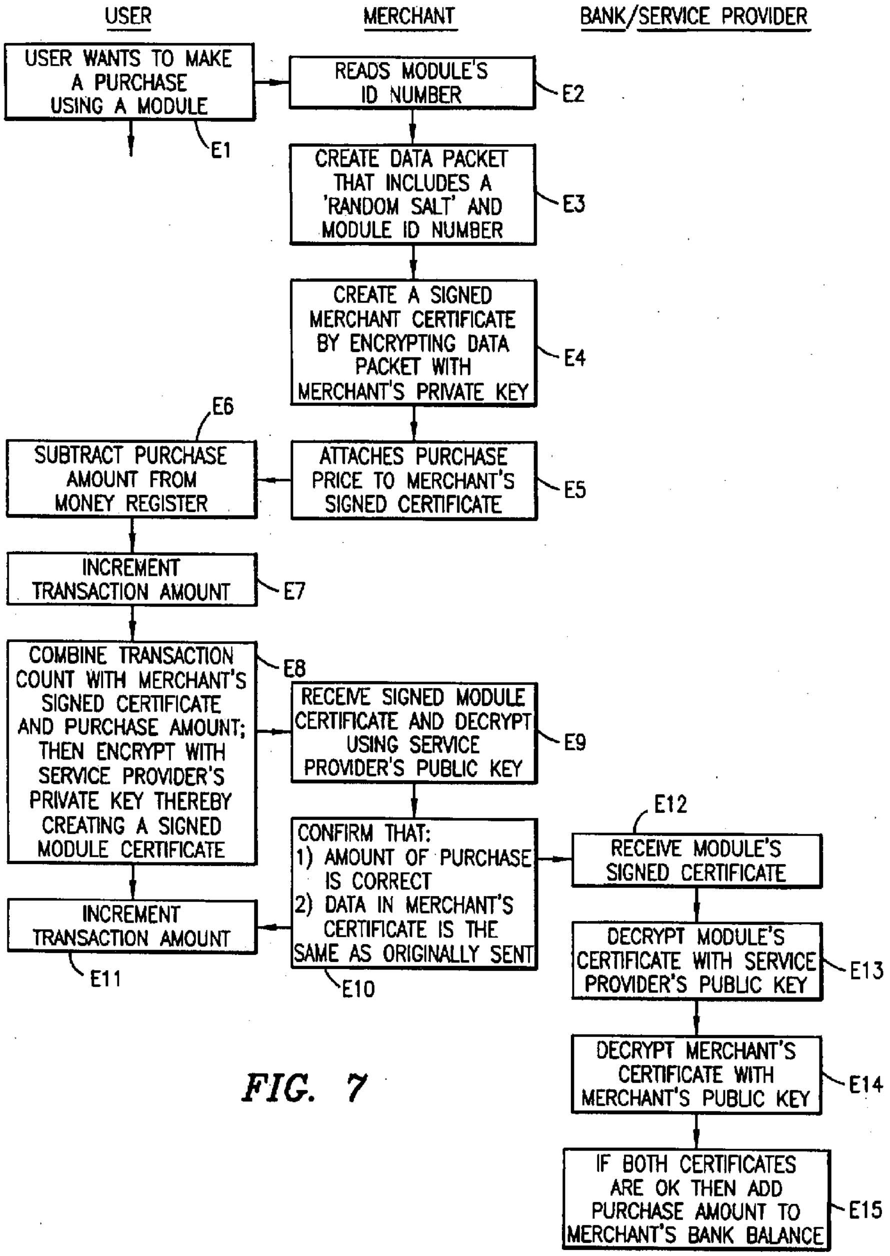

USER
MERCHANT
BANK/SERVICE PROVIDER
USER WANTS TO MAKE A PURCHASE USING A MODULE
E1
READS MODULE'S ID NUMBER
E2
CREATE DATA PACKET THAT INCLUDES A 'RANDOM SALT' AND MODULE ID NUMBER
E3
CREATE A SIGNED MERCHANT CERTIFICATE BY ENCRYPTING DATA PACKET WITH MERCHANT'S PRIVATE KEY
E4
ATTACHES PURCHASE PRICE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

FIG. 7

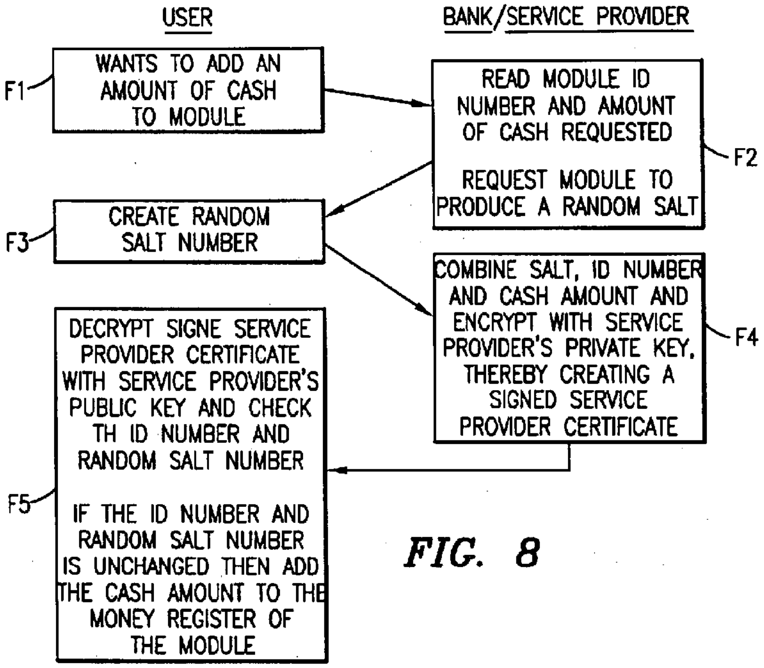

USER
BANK/SERVICE PROVIDER
WANTS TO ADD AN AMOUNT OF CASH TO MODULE
F1
READ MODULE ID NUMBER AND AMOUNT OF CASH REQUESTED
REQUEST MODULE TO PRODUCE A RANDOM SALT
F2
CREATE RANDOM SALT NUMBER
F3
COMBINE SALT, ID NUMBER AND CASH AMOUNT AND ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY, THEREBY CREATING A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

FIG. 8

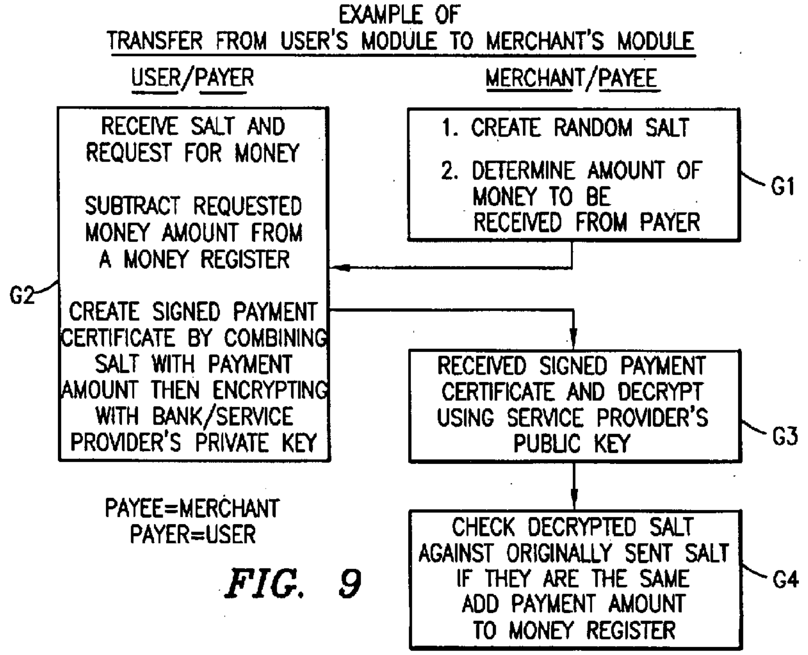

EXAMPLE OF
TRANSFER FROM USER'S MODULE TO MERCHANT'S MODULE
USER/PAYER
MERCHANT/PAYEE
1. CREATE RANDOM SALT
2. DETERMINE AMOUNT OF MONEY TO BE RECEIVED FROM PAYER
G1
RECEIVE SALT AND REQUEST FOR MONEY
SUBTRACT REQUESTED MONEY AMOUNT FROM A MONEY REGISTER
CREATE SIGNED PAYMENT CERTIFICATE BY COMBINING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

FIG. 9

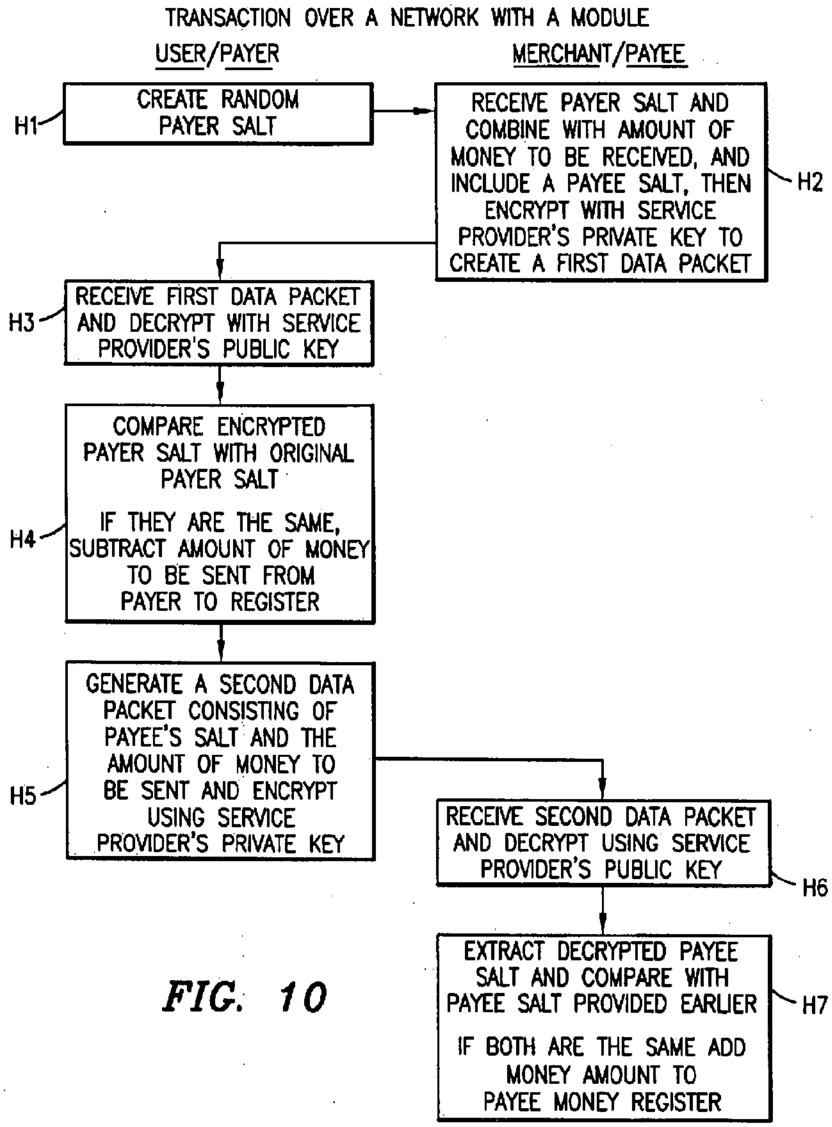

TRANSACTION OVER A NETWORK WITH A MODULE
USER/PAYER
MERCHANT/PAYEE
CREATE RANDOM PAYER SALT
H1
RECEIVE PAYER SALT AND COMBINE WITH AMOUNT OF MONEY TO BE RECEIVED, AND INCLUDE A PAYEE SALT, THEN ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY TO CREATE A FIRST DATA PACKET
H2
RECEIVE FIRST DATA PACKET AND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

FIG. 10

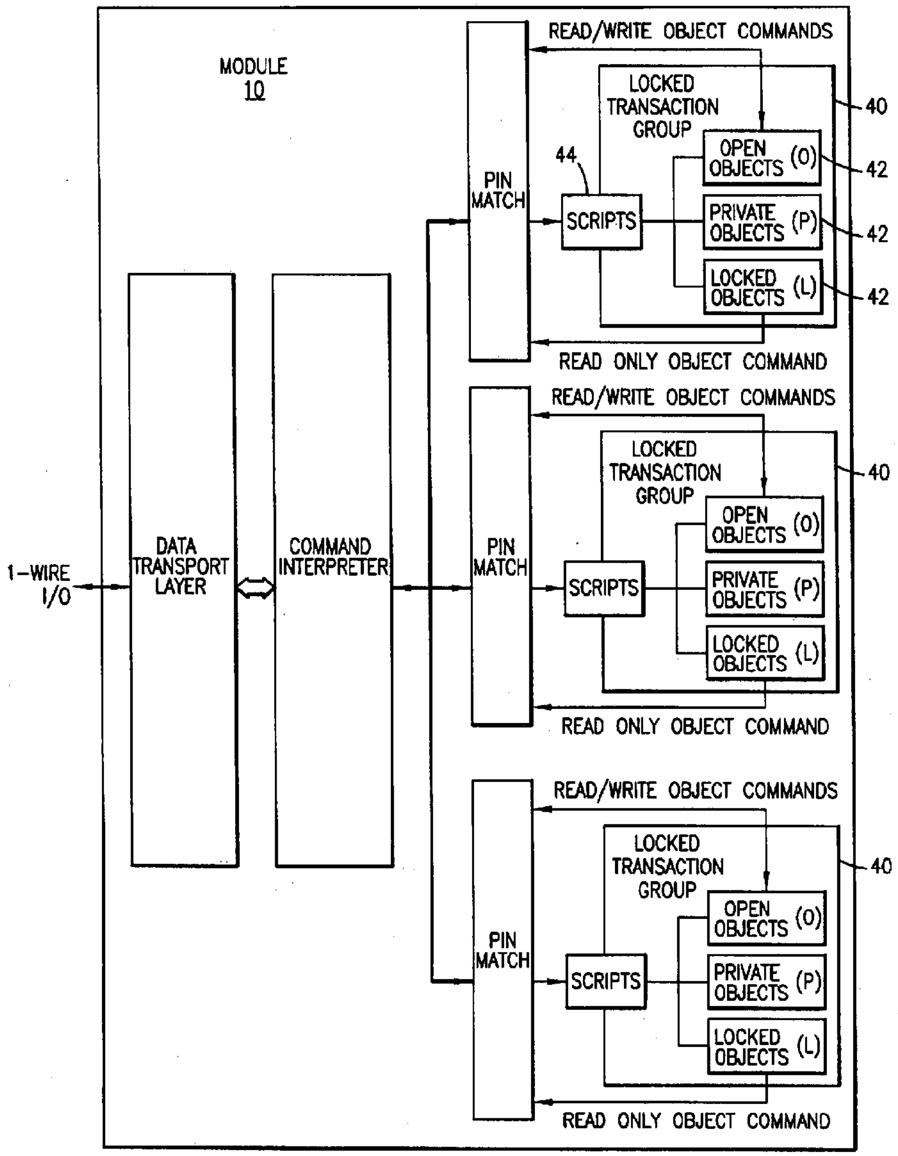

MODULE
10
1-WIRE
I/O
DATA
TRANSPORT
LAYER
COMMAND
INTERPRETER
PIN
MATCH
READ/WRITE OBJECT COMMANDS
LOCKED
TRANSACTION
GROUP
40
44
SCRIPTS
OPEN
OBJECTS (O)
42
PRIVATE
OBJECTS (P)
42
LOCKED
OBJECTS (L)
42
READ ONLY OBJECT COMMAND
PIN
MATCH
READ/WRITE OBJECT COMMANDS
LOCKED
TRANSACTION
GROUP
40
SCRIPTS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

FIG. 11

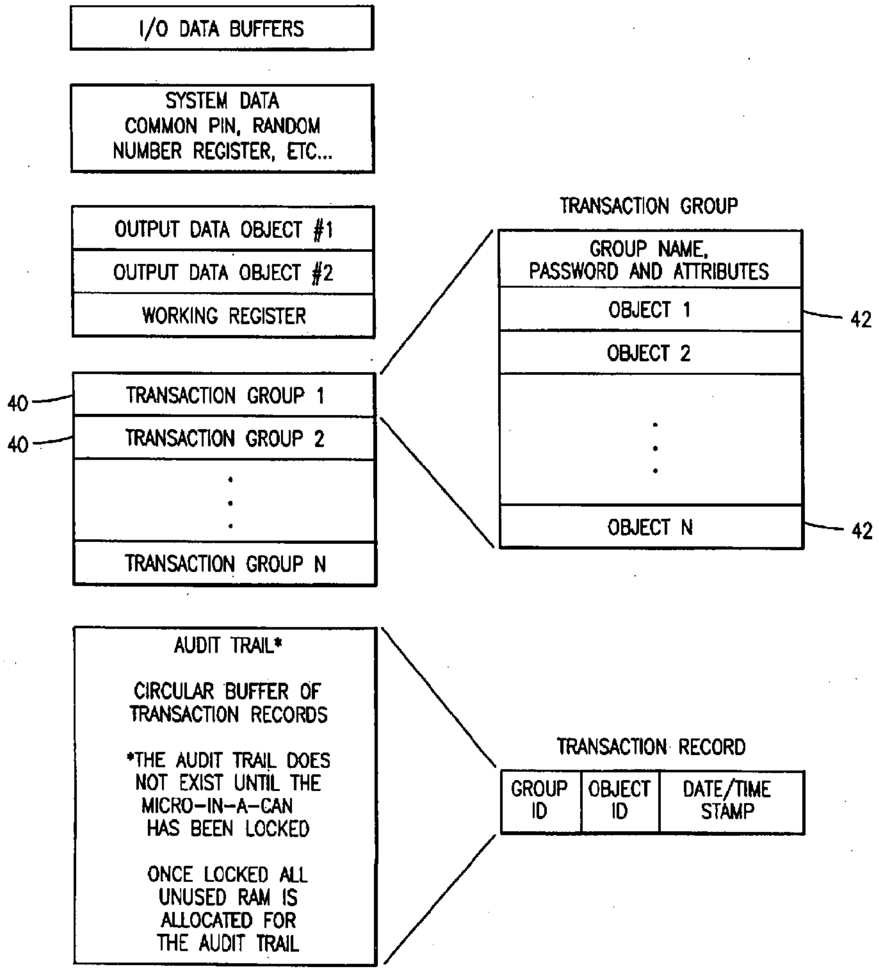

I/O DATA BUFFERS
SYSTEM DATA
COMMON PIN, RANDOM
NUMBER REGISTER, ETC...
OUTPUT DATA OBJECT #1
OUTPUT DATA OBJECT #2
WORKING REGISTER
40
TRANSACTION GROUP 1
40
TRANSACTION GROUP 2
TRANSACTION GROUP N
TRANSACTION GROUP
GROUP NAME,
PASSWORD AND ATTRIBUTES
OBJECT 1
42
OBJECT 2
OBJECT N
42
AUDIT TRAIL*
CIRCULAR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

FIG. 12

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, apparatus and system for transferring money or its equivalent electronically. In particular, in an electronic module based system, the module can be configured to provide at least secure data transfers or to authorize monetary transactions.

2. Description of Related Art

Presently, credit cards that have a magnetic strip associated with them, are a preferred monetary transaction medium in the market place. A card user can take the card to an automatic cash machine, a local store or a bank and make monetary transactions. In many instances the card is used via a telephone interface to make monetary exchanges. The magnetic strip card is used to help identify the card and user of the card. The card provides a relatively low level of security for the transfer. Regardless, the card enables a card holder to buy products, pay debts and make monetary exchanges between separate bank accounts.

Improvements have been made to the magnetic strip card. There have been cards created with microcircuits instead of magnetic strips. In general the microcircuit, like a magnetic strip, is used to enable a card-reader to perform a transaction.

SUMMARY OF THE INVENTION

The present invention is an apparatus, system and method for communicating encrypted information between a preferably portable module and a service provider's equipment. The invention comprises a module, that has a unique identification, that is capable of creating a random number, for example, a SALT, and passing the random number, along with, for example, a request to exchange money, to a service provider's equipment. The service provider's equipment may in return encrypt the random number with a private or public key (depending on the type of transaction), along with other information and pass the encrypted information back to the module as a signed certificate. The module, upon receiving the signed certificate, will decrypt the certificate with a public or private key (depending on the type of transaction) and compare the decrypted number with the original random number. Furthermore, if the numbers are the same then the transaction that was requested may be deemed secure and thereby proceeds. The module is capable of time stamping and storing in memory information about the transaction for later review.

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 is a block diagram of an embodiment of a module;

FIG. 2 is an exemplary process for creating a transaction group;

FIG. 3 is an exemplary technique for receiving an E-mail message;

FIG. 4 is an exemplary technique for preparing a module for notary functions;

FIG. 5 is an exemplary technique for using the module as a notary;

FIG. 6 is an exemplary technique for preparing a module to perform a money transaction;

FIG. 7 is an exemplary technique for performing a money transaction using a module;

FIG. 8 is an exemplary technique for performing a money transaction using a module;

FIG. 9 is an exemplary technique for performing a money transaction using a module;

FIG. 10 is an exemplary technique for passing data over a network;

FIG. 11 is an exemplary organization of the software and firmware within a module; and

FIG. 12 is an exemplary configuration of software and firmware within a module.

DETAILED DESCRIPTION OF A PRESENTLY PREFERRED EXEMPLARY EMBODIMENT

FIG. 1 depicts a block diagram of an exemplary module **10** that incorporates an exemplary embodiment of the present invention. The module circuitry can be a single integrated circuit. It is understood that the module **10** could also be on multiple integrated or descrete element circuits combined combined together. The module **10** 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.

The module **10** 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, badge, jewelry, stamp, or practically any object that can be grasped and/or articulated by a user of the object.

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.

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 could 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 module **10**. The input/output circuitry **26** preferably comprises at least an output buffer **28** and an input buffer. For communication via a one-wire bus, one-wire interface circuitry **32** can be included with the input/output circuitry **26**.

An energy circuit **34** may be necessary to maintain the memory circuitry **20** and/or aid in powering the other circuitry in the module **10**. The energy circuit **34** could consist of a battery, capacitor, R/C circuit, photovoltaic cell, or any other equivalent energy producing circuit or means.

The firmware architecture of a preferred embodiment of a secure transaction module and a series of sample applications using the module **10** will now be discussed. These examples are intended to illustrate a preferred feature set of the module **10** and to explain the services that the module offers. These applications by no means limit the capabilities of the invention, but instead bring to light a sampling of its capabilities.

I. OVERVIEW OF THE PREFERRED MODULE AND ITS FIRMWARE DESIGN

The module **10** preferably contains a general-purpose, 8051-compatible micro controller **12** or a reasonably similar product, a continuously running real-time clock **14**, a high-speed modular exponentiation accelerator for large integers (math coprocessor) **18**, 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 circuitry **26**. The module **10** draws its operating power from the one-wire 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 microcan 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 can be used, or an interface other than a one-wire could be used. The silicon chip can be packaged in credit cards, rings etc.

The module **10** is preferably intended to be used first by a Service Provider who loads the module **10** with data to enable it to perform useful functions, and second by an End User who issues commands to the module **10** to perform operations on behalf of the Service Provider for the benefit of the End User. For this reason, the module **10** 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. **11** and **12**). A transaction group **40** is simply a set of 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 **10**. 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 module **10** 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 module **10**. 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 module **10**. 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 module **10**, 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 the transaction script **40** 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 module **10** 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 **40**, the Service Provider maintains control over what the module **10** 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 MODULE

This section presents a series of practical applications of the module **10**, ranging from the simplest to the most complex. Each of these applications is described in enough detail to make it clear why the module **10** is the central enabling technology for that application.

A. BACKGROUND OF SECURE E-MAIL

In this section we provide an example of how a module **10** could be used to allow anyone to receive his or her own e-mail securely at any location.

1. Standard E-Mail

In a standard e-mail system, a user's computer is connected to a provider of Internet services, and the user's computer provides an e-mail password when polling the provider's computer for new mail. The mail resides on the provider's computer in plain text form, where it can be read by anyone working there. In addition, while traveling from its source, the mail passes through many computers and was also exposed at these locations. If the user receives his mail from his provider over a local area network, anyone else on the same network can capture and read the mail. Finally, with many e-mail systems that do not require the user to enter the password, anyone sitting at the user's computer can retrieve and read his mail, since his computer automatically provides the password when it polls the provider's computer.

It is frequently also possible to copy the password from a configuration file in the user's computer and use it to read his mail from a different computer. As a result of this broad distribution of the e-mail in plain text form and the weakness of password protection, standard e-mail is regarded as very insecure.

To counter this problem, the security system known as P.G.P. (Pretty Good Privacy) was devised. To use P.G.P., a user generates a complete RSA key set containing both a public and private component. He makes his public key widely available by putting it in the signature block of all his e-mail messages and arranging to have it posted in publicly accessible directories of P.G.P. public keys. He stores his private key on his own personal computer, perhaps in a password-protected form. When someone wishes to send private e-mail to this user, he generates a random IDEA encryption key and encrypts the entire message with the IDEA encryption algorithm. He then encrypts the IDEA key itself using the public key provided by the intended recipient. He e-mails both the message encrypted with IDEA and the IDEA key encrypted with the user's public key to the user. No one that sees this transmission can read it except the intended recipient because the message is encrypted with IDEA and the IDEA key is encrypted with the intended recipient's public key. The recipient's computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message. This provides security from those who might try to read the user's mail remotely, but it is less effective when the user's computer is accessible to others because the computer, itself, contains the private key. Even if the private key is password protected, it is often easy to guess the user's password or eavesdrop on him when he enters it, so the user's computer provides little security. In addition, the user can receive secure e-mail only at his own computer because his private key is stored in that computer and is not available elsewhere. Therefore, the weakness of P.G.P. is that it is tied strongly to the user's computer where the private key resides.

2. Module Protected E-Mail

With the exemplary module **10** being used to protect e-mail, a user could have his e-mail forwarded to him wherever he goes without fear that it would be read by others or that his PC would be the weak link that compromises the security of his mail. The module protected e-mail system is similar to the P.G.P. system, except that the private key used for decrypting the IDEA key is stored in a privatized object in a transaction group of the module **10** instead of in a PC. The module protected e-mail system operates as follows:

a. Referring to FIGS. **2**, **11** and **12**, the user creates a transaction group **40**, **S1**, generates an RSA key set S2 . and loads it into three objects **42** of the transaction group **40** (one RSA modulus object, N, and two RSA exponent objects, E and D). He then privatizes the decryption exponent S3, D. Finally, he creates a transaction script **44**, **S4** to take data placed in the input data object, encrypt it with the modulus N and private exponent D and place the result in the output data object. He locks the group **S5** to prevent any additional transaction scripts **44** from being added. He "forgets" the value of D and publishes the values of E and N in public directories and in the signature blocks of his e-mail messages. Since he has forgotten D and since the D exponent object has been privatized, there is no way that anyone will ever find out the value of D.

b. Referring to FIG. **3**, to send secure e-mail to the user, the P.G.P. system is used. When the user receives the secure e-mail **A1**, he transmits the encrypted IDEA key into the input data object of the transaction group **40**, **A2** and then calls the transaction script **44** to decrypt this key **A3** and place the decrypted result in the output data object **A4**. He then reads the decrypted IDEA key from the output data object and uses it to decrypt his mail **A5**. Note that it is now impossible for anyone, including the user, to read any new mail without having physical possession of the module **10**. There is therefore no way that a user's mail can be read without his knowledge, because the module **10** must be physically present on the computer where the mail is read. The user can carry his module **10** wherever he goes and use it to read his forwarded mail anywhere. His home computer is not the weak point in the security system.

Secure e-mail, as described above, is the simplest possible module application, requiring only one RSA key and one transaction script **44**. It is unnecessary even to store the public key E in the module **10**, but it is a good idea to do so because the public key is supposed to be publicly accessible. By storing E in an exponent object and not privatizing that object or the modulus object, N, the user insures that the public key can always be read from the module **10**. There are no transaction scripts **44** involving E because the module **10** will never be required to perform an encryption.

B. DIGITAL NOTARY SERVICE

This section describes a preferred notary service using the module **10**.

1. Background of a Standard Notary Service

A conventional Notary Service Provider receives and examines a document from an End User and then supplies an uncounterfeitable mark on the document signifying that the document was presented to the notary on a certain date, etc. One application of such a notary service could be to record disclosures of new inventions so that the priority of the invention can later be established in court if necessary. In this case, the most important service provided by the notary is to certify that the disclosure existed in the possession of the inventor on a certain date. (The traditional method for establishing priority is the use of a lab notebook in which inventors and witnesses sign and date disclosures of significant inventions.)

2. Electronic Notary Service Using The Module

A company, hereafter referred to as the Service Provider, decides to go into business to supply a notary service (strictly, a priority verification service) for its customers, hereafter referred to as the End Users. The Service Provider chooses to do this by using the module **10** as its "agents" and gives them the authority to authenticate (date and sign) documents on his behalf. The preferred operation of this system is as follows:

a. Referring to FIGS. **4**, **11** and **12**, the Service Provider creates a transaction group **40** for performing electronic notary functions in a "registered lot" of modules **10**, B1.

b. The Service Provider uses a secure computing facility to generate an RSA key set and program the set into every module **10** as a set of three objects **42**, a modulus object and two exponent objects B2. The public part of the key set is made known as widely as possible, and the private part is forgotten completely by the Service Provider. The private exponent object is privatized to prevent it from being read back from the modules **10**.

c. The Service Provider reads the real-time clock **14** from each module **10** and creates a clock offset object that contains the difference between the reading of the real-time clock **14** and some convenient reference time (e.g., 12:00 a.m. Jan. 1, 1970). The true time can then be obtained from any module **10** by adding the value of the clock offset object to the real-time clock B**3**.

d. The Service Provider creates a transaction sequence counter object initialized to zero B**4**.

e. The Service Provider creates a transaction script **44** which appends the contents of the input data object to the true time (sum of real-time clock **14** and the value of the clock offset object) followed by the value of the transaction counter followed by the unique lasered registration number. The transaction script **44** then specifies that all of this data be encrypted with the private key and placed in the output data object. The instructions to perform this operation are stored in the transaction group **40** as a transaction script object B**5**.

f. The Service Provider privatizes any other objects **42** that it does not wish to make directly readable or writable B**6**.

g. The Service Provider locks the transaction group **40**, preventing any additional transaction scripts **44** from being added B**7**.

h. Referring to FIG. **5**, now the Service Provider distributes the modules to paying customers (End Users) to use for notary services. Anytime an End User wishes to have a document certified, the End User performs the Secure Hash Algorithm (Specified in the Secure Hash Standard, FIPS Pub. 180) to reduce the entire document to a 20 byte message digest. The End User then transmits the 20 byte message digest to the input data object C**1** and calls on the transaction script **44** to bind the message digest with the true time, transaction counter, and unique lasered serial number and to sign the resulting packet with the private key C**2**.

i. The End User checks the certificate by decrypting it with the public key and checking the message digest, true time stamp, etc. to make sure they are correct C**3**. The End User then stores this digital certificate along with the original copy of the document in digital form C**4**. The Service Provider will attest to the authenticity of the certificates produced by its modules.

j. After a period of time specified by the Service Provider, the user returns his module **10**, pays a fee, and gets a new module containing a new private key. The old modules can be recycled by erasing the entire transaction group and reprogramming them. The Service Provider maintains an archive of all the public keys it has ever used so that it can testify as needed to the authenticity of old certificates.

C. DIGITAL CASH DISPENSER

This exemplary usage model focuses on the module **10** as a cash reservoir from which payments can be made for goods or services. (To simplify the discussion, the subject of refilling the module **10** with cash is postponed until later). In this case the Service Provider is a bank or other financial institution, the End User is the bank's customer who wishes to use the module **10** to make purchases, and the Merchant is the provider of the purchased goods or services. The roles of the Service Provider, the Merchant, and the End User in these transactions are explained in detail below.

The fundamental concept of the digital cash purse as implemented in the module **10** is that the module **10** initially contains a locked money object containing a given cash value, and the module **10** can generate, on demand, certificates which are essentially signed documents attesting to the fact that the amount of money requested was subtracted from the value of the money object. These signed documents are equivalent to cash, since they attest to the fact that the internal money object was decreased in value by an amount corresponding to the value of the certificate. The merchant can redeem these certificates for cash by returning them to the Service Provider.

When dealing with digital certificates representing cash, "replay" or duplication is a fundamental problem. Since digital data can be copied and retransmitted easily, it differs from ordinary coins or paper money which are difficult to reproduce because of the special technology that is used in their manufacture. For this reason, the receiver of the payment must take special steps to insure that the digital certificate he receives is not a replay of some previously issued certificate. This problem can be solved by having the payee generate a random "SALT", a challenge number, and provide it to the payer.

SALT is a method of preventing replay. A random number is sent and used in a challenge/response mode. The other party is challenged to return the random number as part of their response.

The payer constructs a signed certificate which includes both the money amount and the payee's SALT. When the payee receives this certificate, he decrypts it with the public key, checks the money amount, and then confirms that the SALT is the same as the one he provided. By personalizing the certificate to the payee, the payer proves to the payee that the certificate is not a duplicate or replay and is therefore authentic. This method can be used regardless of whether the module **10** is the payer or the payee.

Another problem that must be addressed is irrepudiability. This means that none of the parties to the transaction should be able to argue that he did not actually participate in the transaction. The transaction record (money certificate) should contain elements to prove that each party to the transaction was a willing participant.

1. Background Conventional Cash Transactions

In a conventional cash transaction, the End User first receives Federal Reserve Notes from a bank and the bank subtracts the equivalent amount of money from the balance in his account. The End User can verify the authenticity of the Federal Reserve Notes by means of the "public key", which includes:

a. Magnetic ink attracted by a magnet.

b. Red and blue threads imbedded in the paper.

c. Microfine printing surrounding the engraved portrait.

d. Embedded stripe printed with USA and denomination of the note.

The "private key" to this system is the details of how the raw materials for printing money are obtained and how the money is actually printed. This information is retained by the government and not revealed.

These notes are carried by the End User to the Merchant, where they are exchanged for goods or services. The Merchant also uses the "public key" of the notes to verify that they are legitimate.

Finally, the Merchant carries the notes to a Bank, where the "public key" is again examined by the teller. If the notes are legitimate, the Merchant's bank account balance is increased by the face value of the notes.

The end result of this transaction is that the End User's bank balance is reduced, the Merchant's bank balance is increased by the same amount, the goods or services are transferred from the Merchant to the End User, and the Federal Reserve Notes are ready to be reused for some other transaction.

2. Exemplary Monetary Transactions Using The Module

Monetary transactions using the module **10** and digital certificates are somewhat more complicated because digital data, unlike Federal Reserve Notes, can be copied and duplicated easily. Nevertheless, the use of "SALTs" and transaction sequence numbers can guarantee the authenticity of digital certificates. (In the following discussion, it is assumed that every party to the transaction has its own RSA key set with a private key that it is able to keep secret.)

a. Referring to FIG. **6**, the Service Provider (bank) prepares the module **10** by creating a transaction group **40** containing a money object representing the monetary value stored in the module **10**. The Service Provider also creates a transaction count object, a modulus object, and an exponent object and stores the provider's private key in the exponent object **D1**. He privatizes the key so that it cannot be read **D2**. Next, he stores a transaction script **44** in the transaction group **40** to perform the monetary transaction and locks the group so that no further objects can be made **D3**, **D4**. (The details of what this transaction script does are described further below.) Finally, he publishes the corresponding public key widely so that anyone can obtain it **D5**.

b. The End User receives the module **10** from the Service Provider, and the End User's bank account is debited by the amount stored in the module **10**. Using a PC or handheld computer, the End User can interrogate the module **10** to verify that the balance is correct.

c. Referring to FIG. **7**, when the End User wishes to purchase some goods or services from a Merchant **E1**, the Merchant reads the unique lasered registration number of the module and places it in a packet along with a random SALT **E2**, **E3**. The merchant then signs this packet with the merchant's own private key **E4** and transmits the resulting encrypted packet along with the amount of the purchase to the input data object of the transaction group **40**, **E5**.

d. The Merchant then invokes the transaction script **44** programmed into the module **10** by the Service Provider. This transaction script **44** subtracts the amount of the purchase from the money object **E6**, appends the value of the transaction counter object to the contents of the input data object **E7**, signs the resulting packet with the private key, and places the result in the output data object **E8**.

e. The Merchant then reads the result from the output data object and decrypts it with the Service Provider's public key **E9**. He then confirms that the amount of the purchase is correct and that the remaining data is identical to the packet he signed in step c., **E10**.

f. Having confirmed that the certificate provided by the module **10** is both authentic and original (not a duplicate), the Merchant delivers the goods or services **E11**. Later the Merchant sends the digital certificate to a bank.

g. The bank decrypts the certificate with the Service Provider's public key **E12**, extracts the amount of the purchase and the transaction count, and decrypts the remaining data with the Merchant's public key to reveal the unique lasered registration number of the module **E14**. The bank then looks up the module **10** by the unique lasered registration number in a database to confirm that the transaction count for this transaction has not been submitted before. When this test is passed, the bank adds the transaction count value to the database, and then increases the Merchant's bank balance by the amount of the purchase **E15**. The fact that portions of the certificate were signed by both the module **10** and the Merchant confirms that the transaction was freely agreed to by both the Merchant and the module **10**.

Note that there are many different ways of combining data combinations of the transaction counter value, the unique lasered registration number, the random SALT provided by payee, and the amount of purchase, encrypted by the module's private key, the Merchant's private key, or both. Many of these combinations can also provide satisfactory guarantees of uniqueness, authenticity, and irrepudiability, and the design of the firmware allows the Service Provider flexibility in writing the transaction script **44** to serve his particular needs.

D. DIGITAL CASH REPLENISHMENT

The discussion of a digital cash purse is section II.C., above, did not address the issue of cash replenishment. The Service Provider can add cash replenishment capability to the module **10**, as discussed in section II.C., simply by adding another modulus object and exponent object containing the Service Provider's public key, a random SALT object, and a transaction script **44** for adding money to the balance. The Service Provider can add money to a module **10** either in person or remotely over a network. The process of adding money is as follows:

1. Referring to FIG. **8**, the Service Provider reads the unique lasered registration number (ID number) of the module **F1**, **F2** and calls on a transaction script **44** to return the value of a random SALT object. The module **10** calculates a new random SALT value from the previous value and the random number generator and returns it to the Service Provider **F3**.

2. The Service Provider places the random SALT returned by the module **10** in a packet along with the amount of money to be added and the unique lasered registration number of the module **10** and then encrypts the resulting packet with the Service Provider's private key **F4**. This encrypted packet is then written back into the input data object of the transaction group **40**.

3. The Service Provider invokes a transaction script **44** which decrypts the contents of the input data object with the Service Provider's public key and then checks the unique lasered registration number and the value of the random SALT against the one that it originally provided. If the SALT matches, the money amount is extracted from the packet and added to the value of the money object in the module **F5**.

Note that the inclusion of the unique lasered registration number is not strictly necessary, but it is included to insure that the Service Provider knows exactly which module is receiving the funds.

E. EXEMPLARY DESCRIPTION OF DIRECT TRANSFER OF FUNDS BETWEEN MODULES

Section II.C.2.g. above reveals a problem that occurs when the Merchant returns the digital certificates to his bank for crediting to his account. The Merchant's bank must either send the certificates back to the Service Provider for redemption, or have access to the Service Provider's records in a database so that it can determine whether the value of the transaction count object is unique. This is inconvenient and requires infrastructure. It also prevents any of the transactions from being anonymous (as they would have been if cash had been used), because the Merchant's bank must log used certificate numbers into a database to prevent them from being reused. These problems can all be eliminated by making use of fund transfers between modules. In addition, the steps required to accomplish a fund transfer between modules are considerably simpler than those described in section II.C.2.

In the discussion which follows, it is assumed that the Merchant also has a module which he uses to collect the funds received from End Users (customers). The module in the possession of the End User will be called the Payer, and the module in the possession of the Merchant will be called the Payee. The steps to accomplish the funds transfer are as follows:

1. Referring to FIGS. **9**, **11** and **12**, using his computer, the Merchant calls on a transaction script **44** in the Payee to provide a random SALT. He reads this SALT from the output object of the transaction group **40**.

2. The Merchant copies the SALT and the amount of the End User's purchase to the input data object of the Payer **G1**, then calls on a transaction script **44** in the Payer to subtract the amount of the purchase from the balance, combine the Payee's SALT in a packet with the amount of the purchase, encrypt the resulting package with the Service Provider's private key, and return it in the output data object **G2**.

3. The Merchant then reads this packet and copies it to the input data object of the Payee, then calls on a transaction script **44** in the Payee to decrypt the packet with the Service Provider's public key **G3** and check the SALT against the one originally generated by the Payee. If they agree, the Payee adds the amount of the purchase to its balance **G4**.

This completes the funds transfer. Note that this transaction effectively transferred the amount of the purchase from the Payer to the Payee, and the steps of the transaction were much simpler than the three-way transaction described in II.C.2. The Merchant can transfer the balance to his bank account by a similar transaction in which the bank provides a SALT to Merchant's module and the Merchant's module prepares a certificate for the balance which it delivers to the bank. Use of a module by the Merchant to collect funds simplifies the transaction, eliminates the need for a database to confirm uniqueness, and preserves the anonymity of the End User that would normally result from a cash transaction.

F. EXEMPLARY TRANSACTIONS WITH A MODULE OVER A NETWORK

The transactions described in section II.C.2., II.D. and II.E. above could also be performed over a network, allowing a physical separation between the Merchant, End User, and modules. However, this could produce a potential problem because one of the communications to the module **10** is unencrypted and therefore subject to falsification. To avoid this problem, both parties must produce a SALT so that the other can demonstrate its ability to encrypt the SALT with the Service Provider's private key and therefore prove authenticity. The operation of this protocol is described as follows as it relates to the transfer of funds between modules (section II.E. above). This method can be employed to allow any of the transactions described above to take place over a network. This clearly enables secure electronic commerce over the Internet.

1. Referring to FIG. **10**, **11** and **12**, the Payer generates a random SALT and transmits it over the network to the Payee **H1**.

2. The Payee appends the amount of the purchase to the Payer's SALT, followed by a SALT randomly generated by the Payee. The Payee then encrypts this packet with the Service Provider's private key and sends it back to the Payer **H2**.

3. The Payer decrypts the packet with the Service Provider's public key **H3**, extracts the Payer SALT, and compares it with the SALT that the Payer provided in step 1. If they agree, the Payer subtracts the amount of the purchaser from its balance **H4** and generates a certificate consisting of the amount of the purchase and the Payee's SALT, which it encrypts with the Service Provider's private key and returns to the Payee **H5**.

4. The Payee decrypts the packet with the Service Provider's public key **H6**, extracts the Payee SALT, and compares it with the SALT that the Payee provided in step 2. If they agree, the Payee adds the amount of the purchase to its balance **H7**.

The exchange of SALTs allows each module to confirm that it is communicating with another module, and that the funds transfer requested is therefore legitimate. The SALT comparison described in step 3 allows the Payer to confirm that the Payee is a legitimate module **10** before the funds are withdrawn, and the comparison described in step 4 allows the Payee to confirm that the Payer is a legitimate module **10** before the funds are deposited. The transactions described above provide the minimum necessary information in the encrypted packets to confirm that the funds are being transferred from one module **10** to another. Other information, such as the unique lasered registration number, could be included (at the cost of anonymity) to provide additional information and greater control over the transaction.

G. AN EXEMPLARY TECHNIQUE FOR SOFTWARE AUTHORIZATION AND USAGE METERING

The module **10** is well-suited for the tasks of enabling specific software features in a comprehensive software system and for metering usage of those features. (This usage model parallels the previously described model for withdrawing money from a module **10**.)

1. Preparation

Referring to FIGS. **11** and **12**, the Service Provider creates a transaction group **40** and stores a configuration object in the group detailing which software within the module **10** the End User is allowed to use. The Service Provider also creates a money object containing the allowed usage credit (which could be in units of time rather than the actual dollar amount), and stores and privatizes a private RSA key pair to use for authentication. A transaction script **44** is stored to receive a SALT and the amount to withdraw from the End User, decrement the balance by the amount withdrawn, and output an RSA signed certificate containing the amount withdrawn, the sale, and the value of the configuration object.

2. Usage

At periodic intervals during the use of the software within the module **10**, the PC program generates a random SALT and an amount to charge for the use of the module **10** and transmits this information to the module **10**. The module **10** decrements the balance and returns the certificate. The PC decrypts the certificate and confirms that the SALT is the same, the amount withdrawn is correct, and the use of the software within the module **10** is authorized by the information stored in the configuration object. If all of these tests are successful, the module **10** executes for a specified period of time or for a given number of operations before asking the module **10** for another certificate.

There are many possible variations on this usage model. For example, the transaction script **44** could also bind up the true time in the certificate so that the application program running on the PC could guarantee that the execution time is accurately measured. (This would require the Service Provider to create a clock offset object during initialization to provide a reference for measuring time.)

H. SIMULATION OF TRANSACTION TOUCH MEMORY™

This usage model describes how the module **10** can be used to simulate the behavior of the simpler Transaction Touch Memory™ (DS 1962) (hereinafter "TTM") or any similar device or substitute that can operate in a nearly equivalent or similar fashion. The principal feature of the TTM is that there is a counter associated with a block of memory in such a way that the counter is incremented automatically whenever the contents of the memory block are changed.

1. Preparation

This simple feature can be programmed into the module **10** by creating a configuration object, a transaction counter object, and a transaction script object which combines the contents of the input object with the value of the transaction counter object and places them in the configuration object, incrementing the counter automatically in the process. All three objects **42** are locked, but none are privatized.

2. Usage

To add or remove money, the End User reads the values of the configuration object and the transaction counter object directly, then decrypts the configuration object and checks the transaction count from the decrypted package against the value of the counter object. The End User also checks the unique lasered registration number from the encrypted packet against the registration number of the module **10**. If these both agree, the balance is considered valid. An amount is added to or subtracted from the balance, the transaction count is incremented, and the packet is re-encrypted and stored in the input data object. The transaction script **44** is then invoked to move the data and the transaction counter value to the configuration object, automatically incrementing the counter value in the process. (The transaction script **44** guarantees that the counter object's value will be incremented anytime data in the configuration object is changed.)

This simple operation can be performed relatively quickly since the module **10** does not have to perform any encryption itself. However, as with the TTM, the End User must now use a secure computing facility to perform the encryption and decryption operations. This usage is therefore less protected than those which depend on the module's encryption capabilities.

I. EXEMPLARY TECHNIQUE FOR POSTAL METERING SERVICE

This usage model describes an application in which the module **10** is used to dispense postage certificates. The digital information which constitutes the certificate is printed on the envelope in the form of a two-dimensional barcode which can be read and authenticated by the Service Provider (U.S.P.S.). A computer program running on an ordinary PC attached to a laser printer in combination with the module **10** can be used to print the postage certificates.

1. Preparation

The Service Provider creates a group containing a money register, a private RSA key (exponent object and modulus object) common to every module, and a transaction script **44**. The script **44** combines the SALT and the amount to be withdrawn (provided by the End User's computer) with the unique lasered registration number of the module **10**, encrypts this packet with the private key, subtracts the amount withdrawn from the balance, and places the encrypted certificate in the output object where it can be read by the PC.

The Service Provider initializes the balance with a specific amount of money, locks the balance and script **44**, privatizes the RSA key objects, and locks the group so that no more scripts can be added. The modules prepared in this way can then be sold over the counter for use with PC-based postage metering programs.

2. Usage

When the first envelope is to be printed, the PC program prepares the first SALT by calculating a one-way hash (e.g., the Secure Hash Standard, FIBS PUB 180) of the date and the unique lasered registration number of the part. This information is passed to the module **10** along with the amount of postage to be withdrawn. The resulting certificate is printed in the two-dimensional barcode along with the hash generation number (one for the first hash), the unique lasered registration number, the plaintext denomination of the stamp, the date, and other information as desired to identify the End User. Subsequent SALTs are generated by performing the one-way hash again on the previous SALT and incrementing the hash generation number.

When the Service Provider receives the envelopes, most of them are taken at face value and the digital barcode is not read. However, a statistical sampling of the barcodes are read and the information provided is decrypted with the public key and verified. Discrepancies are investigated, and fraud is prosecuted under existing law. Verification is possible because the Service Provider can recreate the SALT from the unique lasered registration number, date, and hash generation number, and thereby verify that the transaction is not only current but also linked to a specific module **10**.

Note that there are many possible variations on the method described above, leading to similar results. The most likely fraud would be duplication, in which a user captures the digital information sent to the printer to produce the postage certificate and makes many duplicate copies of the same certificate. This could be detected easily by the Service Provider simply by reading the hash generation number and unique registration number and looking them up in a database to make sure that the user is not duplicating the same certificate. (This check could be performed more often than full certificate verification, which would require RSA decryption.)

J. SUBSCRIPTION INFORMATION SERVICE

This usage model describes an application in which a Service Provider makes available information in encrypted form over the internet to users who have agreed to pay for such information. This application works exactly the same way as the Secure E-mail usage model described in section A above, except that the Service Provider bills the user for the encrypted information that the Service Provider e-mails to him. The billing information is obtained from a registry of pubic RSA keys which allows the Service Provider to identify and bill a user, based on his public key or on the unique lasered serial number of his module **10**.

K. REGISTRY WITH GUARANTEED PRIVATE KEY SECURITY

In order to provide Merchants with an independent confirmation of the identity of an End User, a Service Provider may wish to maintain a registry containing the pubic key of a particular module **10** along with the name, address, and other identifying information of the person to whom the module **10** is issued. For this purpose, it is essential for the Service Provider to make sure that the public key in the registry corresponds to a private key which is known only to the module **10**. In order to guarantee this, the module **10** must be in the possession of the Service Provider at the time the public key is extracted from the module **10** and placed in the registry. After recording this information in the registry, the Service Provider can ship the module **10** to the End User named in the registry.

It is also important for the End User to be able to confirm, when he receives the module **10**, that the private key is not known to the Service Provider or any of the Service Provider's employees. This is important because an ideal registry system should not require that any party trust any other party. The system works to everyone's satisfaction only when each party can be convinced that none of the other parties could possibly know the private key.

One way to accomplish this, the Service Provider sends a command to the module **10** to cause it to generate a complete RSA key set using random numbers, and then to automatically make one of the exponents private, so that there is no way any person can discover the value of the private key. This key set has a special type, different from that of a key set programmed into the can by a Service Provider, so that anyone doing business directly with the module **10** can determine for themselves that the private key is known only to the module **10**.

1. Preparation

The Service Provider creates a password-protected transaction group **40** for the application, and then creates an RSA key set in the group that is generated by the module **10**. (After generating the key set, the modulus and one exponent will be locked automatically, while the second exponent will be privatized automatically by the firmware of the module **10**. The Service Provider then creates a transaction script **44** which will encrypt data from the input object with the private key and place the encrypted result in the output object. The transaction script **44** might optionally append additional information (e.g., the transaction counter) to the data from the input object, in order to satisfy any additional objectives of the application. Other objects **42** and transaction scripts **44** may also be added at the discretion of the Service Provider. The transaction group **40** is locked by the Service Provider when it is complete.

Next, the Service Provider reads the RSA modulus and public exponent from the transaction group **40** and records them in the registry along with the information identifying the End User. Finally, the Service Provider ships the module **10** to the End User, and later conveys to the End User the password that can be used to access the transaction group **40**.

2. Usage

When a Merchant wishes to obtain positive identification of an End User over the Internet or other network, the Merchant generates a unique packet of data and transmits it to the End User, and the End User passes the data into the input object and invokes the transaction script **44** which causes it to be encrypted with the private key generated by the module **10**. The resulting encrypted packet is transmitted back to the Merchant. The Merchant then accesses the data base provided by the Service Provider to obtain the public key belonging to the End User, and attempts to decrypt the encrypted packet using the End User's public key. If the decryption succeeds, the Merchant has proven the physical presence of the End User's module **10** at the remotely networked location. By guaranteeing the presence of the End User's module **10** at the remote site, this identification validates and legitimizes the contents of the data packet and therefore also any financial transactions, represented by the contents of the packet, that may be requested by the End User.

The model described here is one in which the authority to perform financial transactions derives from the registry maintained by the Service Provider. It is therefore essential that this information be accurate and that the private key in the module **10** can be secure from all parties. Because each module **10** has its own unique RSA key set, there is no provision in this model for the module **10** to represent money independently of the registry maintained by the Service Provider. Instead, the registry and the ability of the module **10** to sign with its private key together serve as a definitive means of identifying the End User remotely to any other party.

L. TAXATION OF TRANSACTION VOLUME

This usage applies to a business model in which the Service Provider intends to collect a service charge from the End User that is a percentage of the total amount of money transferred by the module **10**. This model is similar to those described in sections C D, E, and F above, but with the addition of a destructor object that can cause any particular transaction script **44** to expire at a predetermined date and time. This model also requires the use of an additional money object which is programmed (with a suitable transaction script **44**) to accumulate the total value of all the money passed out of the module **10**.

1. Preparation

The Service Provider creates a transaction group **40** containing money objects, etc. as described in sections D and E above. The Service Provider also creates an additional money object to serve as the volume accumulator. The Service Provider also creates transaction scripts **44** for withdrawing or depositing money as in D and E, except that the transaction script for adding money to the module **10** includes a destructor object set to expire at a predetermined time in the future, and the transaction script **44** for withdrawing money includes an instruction to add the amount of the withdrawal to the money object serving as the volume accumulator. The service provider then locks the group and ships the module **10** to the End User.

2. Usage

The End user uses the module **10** for deposits and withdrawals as described in sections D and E above. During the time that the module **10** is used, the cumulative total of all the money spent from the module **10** is accumulated in the money object serving as the volume accumulator. When the time limit expires, the End User can no longer add money to his module **10**, although he can continue to withdraw money if desired until there is none left. The End User then returns the module **10** to the Service Provider to be restored. The Service Provider reads the remaining amount of money and also the amount of money recorded in the volume accumulator. The Service Provider bills the End User a service charge that is a percentage of the amount in the volume accumulator. If the End User is willing to pay this amount to continue his service, the transaction group **40** is destroyed and rebuilt, then the amount of money remaining in the module **10** when the End User returned it is programmed back into the money object of the transaction group **40**. The Service Provider then returns the restored module to the End User, provided that the End User pays the service charge.

The system described above allows a Service Provider to collect periodic fees for service without having to monitor and be involved in every financial transaction performed by the End user. The fee is based on actual usage, as determined by the contents of the volume register.

Exemplary Firmware Definitions for Use With the Module

Object The most primitive data structure accepted by and operated on by the modules firmware. A list of valid objects and their definitions is provided in the next section.

Group A self-contained collection of objects. An object's scope is restricted to the group of which it is a member.

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.

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.

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

Audit Trail A record of transactions occurring after the 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.

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.

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 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 M:

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

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

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

RSA Exponent 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 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.

Transaction Script A transaction script is a series of instructions to be carried out by the module. When invoked the 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 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 transaction counter increments by 1. Once a transaction counter has been locked it is read only and provides an irreversible counter.

Money Register 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.

Clock Offset This object is preferably a 4 byte number which contains the difference between the reading of the module's real-time clock and some convenient time (e.g., 12:00 a.m., Jan. 1, 1970). The true time can then be obtained from the module by adding the value of the clock offset to the real-time clock.

SALT 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 module combines the previous SALT with the 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 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™.

Preferred Module Firmware Command Set

Set Common PIN(01H)

Transmit (to module)

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

Receive data

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

Output length=0

Output Data=0

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)

PIN_TO_CREATE 00000010b (require PIN for group creation).

Initially the 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:

ERR_BAD_COMMON_PIN (Common PIN match failed)

ERR_BAD_PIN_LENGTH (New PIN length>8 bytes)

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:

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

Output data length (Command output length, 2 bytes)

Output data (Command output, length specified above).

Master Erase (02H)

Transmit data

02H, Common PIN

Receive data

CSB=0 if command was successful, ERR_BAD_COMMON_PIN otherwise

Output length=0

Output data=0

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 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 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)

Transmit data

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

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 bit is set in the common PIN option byte and the PIN transmitted does not match the common PIN the module will set the OSC to ERR_BAD_COMMON_PIN.

Possible error return codes for the create group command:

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 module has been locked)

ERR_INSUFFICIENT_RAM (Not enough memory for new group)

Set Group PIN (04H)

Transmit data

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)

ERR_BAD_PIN_LENGTH (New group PIN length>8 bytes)

Create Object (05H)

Transmit data

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

Receive data

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:

If the Create Object command is successful the 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 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)

ERR_MIAC_LOCKED (The 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)

Object types:

RSA modulus 0

RSA exponent 1

Money register 2

Transaction counter 3

Transaction script 4

Clock offset 5

Random SALT 6

Configuration object 7

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 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 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 module has been locked)

ERR_BAD_GROUP_ID (Specified group does not exist)

ERR_BAD_OBJECT_ID (Specified object does not exist)

Privatize Object (07H)

Transmit data

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)

ERR_MIAC_LOCKED (The module has been locked)

ERR_BAD_GROUP_ID (Specified group does not exist)

ERR_BAD_OBJECT_ID (Specified object does not exist)

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 module has been locked)

ERR_BAD_GROUP_ID (Specified group does not exist)

ERR_BAD_OBJECT_ID (Specified object does not exist)

Lock 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 module has not previously been locked, the command will succeed. When the 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 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 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 module command:

ERR_BAD_COMMON_PIN (Supplied common PIN was incorrect)

ERR_MIAC_LOCKED (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 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 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 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 module checks the attribute byte of the specified object. If the object has not been privatized the module will transmit the object data to the host. If the Group PIN was invalid or the object has been privatized the 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)

ERR_BAD_OBJECT_ID (Object did not exist in group)

ERR_OBJECT_PRIVATIZED (Object has been privatized)

Write Object (0DH)

Transmit data .

0DH, 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 module checks the attribute byte of the specified object. If the object has not been locked or privatized the 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 module will delete the specified group. Deleting a group causes the automatic destruction of all objects within the group. If the 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)

ERR_MIAC_LOCKED (Module has been locked)

Get Command Status Info (10H)

Transmit data

10H

Receive data

CSB=0

Output length=6

Output data=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)

Get Module Configuration Info (11H)

Transmit data

11H

Receive data

CSB=0

Output length=4

Output data=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 (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 (S) if successful, 0 otherwise

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

Notes:

If the transmitted Common PIN is valid and the 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 since previous read command

Possible error codes for the read audit trail info command:

ERR_BAD_COMMON_PIN (Common PIN was incorrect)

ERR_MIAC_NOT_LOCKED (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 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 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 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 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 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 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 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 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 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. 11. 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 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 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 module.

ERR_MIAC_LOCKED (87H)

When the 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.

ERR_MIAC_NOT_LOCKED (88H)

If the 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 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 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 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 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 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 module will return an ERR_OBJECT_PRIVATE error code.

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

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

1) who is the module user via a unique registration number.

2) when the transaction took place via a true-time stamping of the transaction.

3) where the transaction took place via a registered module interface site identification.

4) security information via uniquely serialized transactions and digital signitures on message digests.

5) 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 method for adding a monetary equivalent to an electronic module, comprising the steps of:

a. placing the module in communication with an electronic device;

b. indicating an amount requested to said electronic device;

c. communicating a random number from said module to said electronic device;

d. combining said random number and said amount requested thereby creating a first data packet in said electronic device;

e. encrypting said first data packet with a first key thereby creating a signed certificate in said electronic device;

f. communicating said signed certificate from said electronic device to said module;

g. decrypting said signed certificate in said module with a second key thereby creating a decrypted random number and a decrypted amount requested;

h. comparing said random number with said decrypted random number and determining if they match in said module; and

i. adding said decrypted amount requested to a money register in said module.

2. The method of claim 1, further comprising, after step b, the step of communicating a module identification from said module to said electronic device.

3. The method of claim 2, wherein the step d of combining further comprises the step of combining said module indentification with said random number and said amount requested prior thereby creating said first data packet in said electronic device.

4. The method of claim 3, wherein the step of g of decrypting further comprises the step of creating a decrypted module identification.

5. The method of claim 4, wherein the step h of comparing further comprises the step of comparing said module identification and said decrypted module identification and determining if they match.

6. The method of claim 1, wherein said module is portable.

7. The method of claim 1, wherein said first key is a private key and said second key is a public key.

8. The method of claim 1, wherein said module is programmable.

9. Method of metering a monetary equivalent out of a module and into an electronic equipment, comprising the steps of:

a. placing said electronic equipment in communication with said module;

b. reading a module identifier with said electronic equipment;

c. combining a first random number, a number of units to be metered and said module identifier in said electronic equipment thereby creating a first data packet;

d. encrypting said first data packet in said electronic equipment with a first key thereby creating an encrypted first data packet;

e. passing said encrypted first data packet and a requested monetary value from said electronic equipment to said module;

f. subtracting said requested monetary value from a money register in said module; and

g. incrementing a transaction count in said module.

10. The method of claim 9, wherein after step g said method further comprises the steps of:

h. combining said transaction count, said requested monetary value, and said encrypted first data packet in said module and thereby creating a second data packet;

i. encrypting said second data packet with a second key in said module thereby creating an encrypted second data packet; and

j. passing said encrypted second packet to said electronic equipment.

11. The method of claim 10, further comprising the steps of:

k. decrypting said encrypted second data packet with a third key in said electronic equipment thereby creating a decrypted second data packet;

l. determining whether said requested monetary amount sent to said module is the same as in said decrypted second data packet; and

m. determining whether said encrypted first data packet sent to said module is the same as in said decrypted second data packet.

12. The method of claim **10**, further comprising the steps of:

o. sending said encrypted second data packet from said electronic device to a provider;

p. decrypting said encrypted second data packet with a fourth key by said provider; and

q. decrypting said encrypted first data packet with a fifth key by said provider.

13. The method of claim **9**, wherein said encryption step utilizes a predetermined encryption technique.

14. The method of claim **13**, wherein said predetermined encryption technique is an RSA technique.

15. The method of claim **9**, wherein said module is programmable.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. :	5,805,702
DATED :	Sep. 8, 1998
INVENTOR(S) :	Curry et al.

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

Column 25, line 20	Replace "(S)" With --(5)--

Signed and Sealed this

Sixth Day of April, 1999

Attest:

Q. Todd

Q. TODD DICKINSON

Attesting Officer

Acting Commissioner of Patents and Trademarks

BAR CODE LABEL

U.S. PATENT APPLICATION

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT
08/595,014	01/31/96	235	2514

APPLICANT

STEPHEN M. CURRY, DALLAS, TX; DONALD W. LOOMIS, COPPELL, TX;
CHRISTOPHER W. FOX, DALLAS, TX.

CONTINUING DATA*******************
VERIFIED

FOREIGN/PCT APPLICATIONS**********
VERIFIED U.S. ARMY 60/004510 09/29/95

FOREIGN FILING LICENSE GRANTED 05/18/96

STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS	FILING FEE RECEIVED	ATTORNEY DOCKET NO.
TX	8	28	4	$1,134.00	20661/438

ADDRESS

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

TITLE

METHOD, APPARATUS, AND SYSTEM FOR TRANSFERING UNITS OF VALUE

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

Pw

6-8-96

PATENT APPLICATION SERIAL NO. 08/595014

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

330 SD 10-0447 02/21/96 08595014
33042 101 982.00CH 20661438

SE18063 11/08/96 0859501[illegible] 10-0447 180 101 982.00CH

SE18064 11/08/96 08595014 04-0031 180 101 982.00CH

982

PTO-1556
(5/87)

8

MAIL ROOM
JAN
31 64
1996
PAT. & TRADEMARK OFF.

A

08/595014

Patent Application
Docket No. 20661/438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: 1-00 et al

STEPHEN M. CURRY, DONALD W. LOOMIS, and CHRISTOPHER W. FOX

For: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

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

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. IB 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

Jeanne A. Howard
Signature

Dear Sir:

REQUEST FOR FILING A NATIONAL PATENT APPLICATION

Transmitted herewith for filing, please find the following:

_X_ 1. Specification, claims and abstract of the above-referenced patent application having 129 pages.

_X_ 2. _1_ set(s) of drawing(s) (____ formal / _X_ informal).

_X_ 3. Combined Declaration and Power of Attorney (___ signed _X_ 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.

____ 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)__.

	Application No.	Filing Date
(1)	____	____
(2)	____	____
(3)	____	____

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

X 7.A. Priority is claimed under 35 U.S.C. § 119(e) based on Provisional Application Number 60/004,510, filed on September 29, 1995.

____ 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.

					SMALL ENTITY RATE		LARGE ENTITY RATE		
BASIC FEE					$365	OR	$730	=	$730.00
	NUMBER FILED			NUMBER EXTRA					
TOTAL CLAIMS	28	-20	=	8 (at least 0)	x 11	OR	x 22	=	+$176.00
INDEP. CLAIMS	4	-3	=	1 (at least 0)	x 38	OR	x 76	=	+$ 76.00
If any proper multiple dependent claim (ignore improper) is present (Enter $0.00 if this is a reissue 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									=$982.00

____ 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 $982.00 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 Depost Account No. 04-0031, **for which purpose a duplicate copy of this sheet is attached.***

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. 38,166

Date: January 31, 1996

Jenkens & 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.

08/595014

Patent Application
Docket #20661/438

MAIL ROOM
JAN
31 64
1996
PAT. & TRADEMARK OFF.

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. IB885275721 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
Jeanne A. Howard
Signature

METHOD, APPARATUS, AND SYSTEM FOR TRANSFERING UNITS OF VALUE

RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 60/004,510, filed September 29, 1995.

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

Serial No.: unknown, filed January 31, 1996, entitled METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS;

08/595014

Patent Application
Docket #20661/438

OMS
JAN 31 1996
64
PAT. & TRADEMARK OFF.

Serial No.: unknown, filed January 31, 1996, entitled TRANSFER OF VALUABLE INFORMATION BETWEEN A SECURE MODULE AND ANOTHER MODULE.

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates to a method, apparatus and system for transferring money or its equivalent electronically. In particular, in an electronic module based system, the module can be configured to provide at least secure data transfers or to authorize monetary transactions.

Description of Related Art

Presently, credit cards that have a magnetic strip associated with them, are a preferred monetary transaction medium in the market place. A card user can take the card to an automatic cash machine, a local store or a bank and make monetary transactions. In many instances the card is used via a telephone interface to make monetary exchanges. The magnetic strip card is used to help identify the card and user of the card. The card provides a relatively low level of security for the transfer. Regardless, the card enables a card holder to buy products, pay debts and make monetary exchanges between separate bank accounts.

Improvements have been made to the magnetic strip card. There have been cards created with microcircuits instead of magnetic strips. In general the microcircuit, like a magnetic strip, is used to enable a card-reader to perform a transaction.

SUMMARY OF THE INVENTION

The present invention is an apparatus, system and method for communicating encrypted information between a preferably portable module and a service provider's equipment. The invention comprises a module, that has a unique identification, that is capable of creating a random number, for example, a SALT, and passing the random number, along with, for example, a request to exchange money, to a service provider's equipment. The service provider's equipment may in return encrypt the random number with a private or public key (depending on the type of transaction), along with other information and pass the encrypted information back to the module as a signed certificate. The module, upon receiving the signed certificate, will decrypt the certificate with a public or private key (depending on the type of transaction) and compare the decrypted number with the original random number. Furthermore, if the numbers are the same then the transaction that was requested may be deemed secure and thereby proceeds. The module is capable of time stamping and storing in memory information about the transaction for later review.

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:

FIGURE 1 is a block diagram of an embodiment of a module;

FIGURE 2 is an exemplary process for creating a transaction group;

FIGURE 3 is an exemplary technique for receiving an E-mail message;

FIGURE 4 is an exemplary technique for preparing a module for notary functions;

FIGURE 5 is an exemplary technique for using the module as a notary;

FIGURE 6 is an exemplary technique for preparing a module to perform a money transaction;

FIGURE 7 is an exemplary technique for performing a money transaction using a module;

FIGURE 8 is an exemplary technique for performing a money transaction using a module;

FIGURE 9 is an exemplary technique for performing a money transaction using a module;

FIGURE 10 is an exemplary technique for passing data over a network;

FIGURE 11 is an exemplary organization of the software and firmware within a module; and

FIGURE 12 is an exemplary configuration of software and firmware within a module.

DETAILED DESCRIPTION OF A PRESENTLY PREFERRED EXEMPLARY EMBODIMENT

FIGURE 1 depicts a block diagram of an exemplary module 10 that incorporates an exemplary embodiment of the present invention. The module circuitry can be a single integrated circuit. It is understood that the module 10 could also be on multiple integrated or descrete element circuits combined combined together. The module 10 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.

The module 10 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, badge, jewelry, stamp, or practically any object that can be grasped and/or articulated by a user of the object.

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.

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 could 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 module 10. The input/output circuitry 26 preferably comprises at least an output buffer 28 and an input buffer. For communication via a one-wire bus, one-wire interface circuitry 32 can be included with the input/output circuitry 26.

An energy circuit 34 may be necessary to maintain the memory circuitry 20 and/or aid in powering the other circuitry in the module 10. 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 a preferred embodiment of a secure transaction module and a series of sample applications using the module 10 will now be discussed. These examples are intended to illustrate a preferred feature set of the module 10 and to explain the services that the module offers. These applications by no means limit the capabilities of the invention, but instead bring to light a sampling of its capabilities.

I. OVERVIEW OF THE PREFERRED MODULE AND ITS FIRMWARE DESIGN

The module 10 preferably contains a general-purpose, 8051-compatible micro controller 12 or a reasonably similar product, a continuously running real-time clock 14, a high-speed modular exponentiation accelerator for large integers (math coprocessor) 18, 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 circuitry 26. The module 10 draws its operating power from the one-wire 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 microcan 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 can be used, or an interface other than a one-wire could be used. The silicon chip can be packaged in credit cards, rings etc.

The module 10 is preferably intended to be used first by a Service Provider who loads the module 10 with data to enable it to perform useful functions, and second by an End User who issues commands to the module 10 to perform operations on behalf of the Service Provider for the benefit of the End User. For this reason, the module 10 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 FIGURES 11 and 12). A transaction group 40 is simply a set of 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 10. 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
RSA Exponent
Transaction Script
Transaction Counter
Money Register
Destructor

Clock Offset
Random SALT
Configuration Data
Input Data
Output Data

Within each transaction group 40 the module 10 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 module 10. 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 module 10. 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 Transaction Group
- Lock Object
- 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 module 10, 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 the transaction script 40 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 module 10 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 40, the Service Provider maintains control over what the module 10 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 MODULE

This section presents a series of practical applications of the module 10, ranging from the simplest to the most complex. Each of these applications is described in enough detail to make it clear why the module 10 is the central enabling technology for that application.

A. BACKGROUND OF SECURE E-MAIL

In this section we provide an example of how a module 10 could be used to allow anyone to receive his or her own e-mail securely at any location.

1. Standard E-Mail

In a standard e-mail system, a user's computer is connected to a provider of Internet services, and the user's computer provides an e-mail password when polling the provider's computer for new mail. The mail resides on the provider's computer in plain text form, where it can be read by anyone working there. In addition, while traveling from its source, the mail passes through many computers and was also exposed at these locations. If the user receives his mail from his provider over a local area network, anyone else on the same network can capture and read the mail. Finally, with many e-mail systems that do not require the user to enter the password, anyone sitting at the user's computer can retrieve and read his mail, since his computer automatically provides the password when it polls the provider's computer.

It is frequently also possible to copy the password from a configuration file in the user's computer and use it to read his mail from a different computer. As a result of this broad distribution of the e-mail in plain text form and the weakness of password protection, standard e-mail is regarded as very insecure.

To counter this problem, the security system known as P.G.P. (Pretty Good Privacy) was devised. To use P.G.P., a user generates a complete RSA key set containing both a public and private component. He makes his public key widely available by putting it in the signature block of all his e-mail messages and arranging to have it posted in publicly accessible directories of P.G.P. public keys. He stores his private key on his own personal computer, perhaps in a password-protected form. When someone wishes to send private e-mail to this user, he generates a random IDEA encryption key and encrypts the entire message with the IDEA encryption algorithm. He then encrypts the IDEA key itself using the public key provided by the intended recipient. He e-mails both the message encrypted with IDEA and the IDEA key encrypted with the user's public key to the user. No one that sees this transmission can read it except the intended recipient because the message is encrypted with IDEA and the IDEA key is encrypted with the intended recipient's public key. The recipient's computer contains the corresponding private key, and hence can decrypt the IDEA key and use the decrypted IDEA key to decrypt the message. This provides security from those who might try to read the user's mail remotely, but it is less effective when the user's computer is accessible to others because the computer, itself, contains the private key. Even if the private key is password protected, it is often easy to guess the user's password or eavesdrop on him when he enters it, so the user's computer provides little security. In addition, the user can receive secure e-mail only at his own computer because his private key is stored in that computer and is not available elsewhere. Therefore, the weakness of P.G.P. is that it is tied strongly to the user's computer where the private key resides.

2. Module Protected E-Mail

With the exemplary module 10 being used to protect e-mail, a user could have his e-mail forwarded to him wherever he goes without fear that it would be read by others or that his PC would be the weak link that compromises the security of his mail. The module protected e-mail system is similar to the P.G.P. system, except that the private key used for decrypting the IDEA key is stored in a privatized object in a transaction group of the module 10 instead of in a PC. The module protected e-mail system operates as follows:

a. Referring to FIGURES 2, 11 and 12, the user creates a transaction group 40, S1, generates an RSA key set S2 and loads it into three objects 42 of the transaction group 40 (one RSA modulus object, N, and two RSA exponent objects, E and D). He then privatizes the decryption exponent S3, D. Finally, he creates a transaction script 44, S4 to take data placed in the input data object, encrypt it with the modulus N and private exponent D and place the result in the output data object. He locks the group S5 to prevent any additional transaction scripts 44 from being added. He "forgets" the value of D and publishes the values of E and N in public directories and in the signature blocks of his e-mail messages. Since he has forgotten D and since the D exponent object has been privatized, there is no way that anyone will ever find out the value of D.

b. Referring to FIGURE 3, to send secure e-mail to the user, the P.G.P. system is used. When the user receives the secure e-mail A1, he transmits the encrypted IDEA key into the input data object of the transaction group 40, A2 and then calls the transaction script 44 to decrypt this key A3 and place the decrypted result in the output data object A4. He then reads the decrypted IDEA key from the output data object and uses it to decrypt his mail A5. Note that it is now impossible for anyone, including the user, to read any new mail without having physical possession of the module 10. There is therefore no way that a user's mail can be read without his knowledge, because the module 10 must be physically present on the computer where the mail is read. The user can carry his module 10 wherever he goes and use it to read his forwarded mail anywhere. His home computer is not the weak point in the security system.

Secure e-mail, as described above, is the simplest possible module application, requiring only one RSA key and one transaction script 44. It is unnecessary even to store the public key E in the module 10, but it is a good idea to do so because the public key is supposed to be publicly accessible. By storing E in an exponent object and not privatizing that object or the modulus object, N, the user insures that the public key can always be read from the module 10. There are no transaction scripts 44 involving E because the module 10 will never be required to perform an encryption.

B. DIGITAL NOTARY SERVICE

This section describes a preferred notary service using the module 10.

1. Background of a Standard Notary Service

A conventional Notary Service Provider receives and examines a document from an End User and then supplies an uncounterfeitable mark on the document signifying that the document was presented to the notary on a certain date, etc. One application of such a notary service could be to record disclosures of new inventions so that the priority of the invention can later be established in court if necessary. In this case, the most important service provided by the notary is to certify that the disclosure existed in the possession of the inventor on a certain date. (The traditional method for establishing priority is the use of a lab notebook in which inventors and witnesses sign and date disclosures of significant inventions.)

2. Electronic Notary Service Using The Module

A company, hereafter referred to as the Service Provider, decides to go into business to supply a notary service (strictly, a priority verification service) for its customers, hereafter referred to as the End Users. The Service Provider chooses to do this by using the module 10 as its "agents" and gives them the authority to authenticate (date and sign) documents on his behalf. The preferred operation of this system is as follows:

a. Referring to FIGURES 4, 11 and 12, the Service Provider creates a transaction group 40 for performing electronic notary functions in a "registered lot" of modules 10, B1.

b. The Service Provider uses a secure computing facility to generate an RSA key set and program the set into every module 10 as a set of three objects 42, a modulus object and two exponent objects B2. The public part of the key set is made known as widely as possible, and the private part is forgotten completely by the Service Provider. The private exponent object is privatized to prevent it from being read back from the modules 10.

c. The Service Provider reads the real-time clock 14 from each module 10 and creates a clock offset object that contains the difference between the reading of the real-time clock 14 and some convenient reference time (e.g., 12:00 a.m. January 1, 1970). The true time can then be obtained from any module 10 by adding the value of the clock offset object to the real-time clock B3.

d. The Service Provider creates a transaction sequence counter object initialized to zero B4.

e. The Service Provider creates a transaction script 44 which appends the contents of the input data object to the true time (sum of real-time clock 14 and the value of the clock offset object) followed by the value of the transaction counter followed by the unique lasered registration number. The transaction script 44 then specifies that all of this data be encrypted with the private key and placed in the output data object. The instructions to perform this operation are stored in the transaction group 40 as a transaction script object B5.

f. The Service Provider privatizes any other objects 42 that it does not wish to make directly readable or writable B6.

g. The Service Provider locks the transaction group 40, preventing any additional transaction scripts 44 from being added B7.

h. Referring to FIGURE 5, now the Service Provider distributes the modules to paying customers (End Users) to use for notary services. Anytime an End User wishes to have a document certified, the

End User performs the Secure Hash Algorithm (Specified in the Secure Hash Standard, FIPS Pub. 180) to reduce the entire document to a 20 byte message digest. The End User then transmits the 20 byte message digest to the input data object C1 and calls on the transaction script 44 to bind the message digest with the true time, transaction counter, and unique lasered serial number and to sign the resulting packet with the private key C2.

i. The End User checks the certificate by decrypting it with the public key and checking the message digest, true time stamp, etc. to make sure they are correct C3. The End User then stores this digital certificate along with the original copy of the document in digital form C4. The Service Provider will attest to the authenticity of the certificates produced by its modules.

j. After a period of time specified by the Service Provider, the user returns his module 10, pays a fee, and gets a new module containing a new private key. The old modules can be recycled by erasing the entire transaction group and reprogramming them. The Service Provider maintains an archive of all the public keys it has ever used so that it can testify as needed to the authenticity of old certificates.

C. DIGITAL CASH DISPENSER

This exemplary usage model focuses on the module 10 as a cash reservoir from which payments can be made for goods or services. (To simplify the discussion, the subject of refilling the module 10 with cash is postponed until later). In this case the Service Provider is a bank or other financial institution, the End User is the bank's customer who wishes to use the module 10 to make purchases, and the Merchant is the provider of the purchased goods or services. The roles of the Service Provider, the Merchant, and the End User in these transactions are explained in detail below.

The fundamental concept of the digital cash purse as implemented in the module 10 is that the module 10 initially contains a locked money object containing a given cash value, and the module 10 can generate, on demand, certificates which are essentially signed documents attesting to the fact that the amount of money requested was subtracted from the value of the money object. These signed documents are equivalent to cash, since they attest to the fact that the internal money object was decreased in value by an amount corresponding to the value of the certificate. The merchant can redeem these certificates for cash by returning them to the Service Provider.

When dealing with digital certificates representing cash, "replay" or duplication is a fundamental problem. Since digital data can be copied and retransmitted easily, it differs from ordinary coins or paper money which are difficult to reproduce because of the special technology that is used in their manufacture. For this reason, the receiver of the payment must take special steps to insure that the digital certificate he receives is not a replay of some previously issued certificate. This problem can be solved by having the payee generate a random "SALT", a challenge number, and provide it to the payer.

SALT is a method of preventing replay. A random number is sent and used in a challenge/response mode. The other party is challenged to return the random number as part of their response.

The payer constructs a signed certificate which includes both the money amount and the payee's SALT.

When the payee receives this certificate, he decrypts it with the public key, checks the money amount, and then confirms that the SALT is the same as the one he provided. By personalizing the certificate to the payee, the payer proves to the payee that the certificate is not a duplicate or replay and is therefore authentic. This method can be used regardless of whether the module 10 is the payer or the payee.

Another problem that must be addressed is irrepudiability. This means that none of the parties to the transaction should be able to argue that he did not actually participate in the transaction. The transaction record (money certificate) should contain elements to prove that each party to the transaction was a willing participant.

1. Background Conventional Cash Transactions

In a conventional cash transaction, the End User first receives Federal Reserve Notes from a bank and the bank subtracts the equivalent amount of money from the balance in his account. The End User can verify the authenticity of the Federal Reserve Notes by means of the "public key", which includes:

a. Magnetic ink attracted by a magnet.

b. Red and blue threads imbedded in the paper.

c. Microfine printing surrounding the engraved portrait.

d. Embedded stripe printed with USA and denomination of the note.

The "private key" to this system is the details of how the raw materials for printing money are obtained and how the money is actually printed. This information is retained by the government and not revealed.

These notes are carried by the End User to the Merchant, where they are exchanged for goods or services. The Merchant also uses the "public key" of the notes to verify that they are legitimate.

Finally, the Merchant carries the notes to a Bank, where the "public key" is again examined by the teller. If the notes are legitimate, the Merchant's bank account balance is increased by the face value of the notes.

The end result of this transaction is that the End User's bank balance is reduced, the Merchant's bank balance is increased by the same amount, the goods or services are transferred from the Merchant to the End User, and the Federal Reserve Notes are ready to be reused for some other transaction.

2. Exemplary Monetary Transactions Using The Module

Monetary transactions using the module 10 and digital certificates are somewhat more complicated because digital data, unlike Federal Reserve Notes, can be copied and duplicated easily. Nevertheless, the use of "SALTs" and transaction sequence numbers can guarantee the authenticity of digital certificates. (In the following discussion, it is assumed that every party to the transaction has its own RSA key set with a private key that it is able to keep secret.)

a. Referring to FIGURE 6, the Service Provider (bank) prepares the module 10 by creating a transaction group 40 containing a money object representing the monetary value stored in the module 10. The Service Provider also creates a transaction count object, a modulus object, and an exponent object and stores the provider's private key in the exponent object D1. He privatizes the key so that it cannot be read D2. Next, he stores a transaction script 44 in the transaction group 40 to perform the monetary transaction and locks the group so that no further objects can be made D3, D4. (The details of what this transaction script does are described further below.) Finally, he publishes the corresponding public key widely so that anyone can obtain it D5.

b. The End User receives the module 10 from the Service Provider, and the End User's bank account is debited by the amount stored in the module 10. Using a PC or handheld computer, the End User can interrogate the module 10 to verify that the balance is correct.

c. Referring to FIGURE 7, when the End User wishes to purchase some goods or services from a Merchant E1, the Merchant reads the unique lasered registration number of the module and places it in a packet along with a random SALT E2, E3. The merchant then signs this packet with the merchant's own private key E4 and transmits the resulting encrypted packet along with the amount of the purchase to the input data object of the transaction group 40, E5.

d. The Merchant then invokes the transaction script 44 programmed into the module 10 by the Service Provider. This transaction script 44 subtracts the amount of the purchase from the money object E6, appends the value of the transaction counter object to the contents of the input data object E7, signs the resulting packet with the private key, and places the result in the output data object E8.

e. The Merchant then reads the result from the output data object and decrypts it with the Service Provider's public key E9. He then confirms that the amount of the purchase is correct and that the remaining data is identical to the packet he signed in step c., E10.

f. Having confirmed that the certificate provided by the module 10 is both authentic and original (not a duplicate), the Merchant delivers the goods or services E11. Later the Merchant sends the digital certificate to a bank.

g. The bank decrypts the certificate with the Service Provider's public key E12, extracts the amount of the purchase and the transaction count, and decrypts the remaining data with the Merchant's public key to reveal the unique lasered registration number of the module E14. The bank then looks up the module 10 by the unique lasered registration number in a database to confirm that the transaction count for this transaction has not been submitted before. When this test is passed, the bank adds the transaction count value to the database, and then increases the Merchant's bank balance by the amount of the purchase E15. The fact that portions of the certificate were signed by both the module 10 and the Merchant confirms that the transaction was freely agreed to by both the Merchant and the module 10.

Note that there are many different ways of combining data combinations of the transaction counter value, the unique lasered registration number, the random SALT provided by payee, and the amount of purchase, encrypted by the module's private key, the Merchant's private key, or both. Many of these combinations can also provide satisfactory guarantees of uniqueness, authenticity, and irrepudiability, and the design of the firmware allows the Service Provider flexibility in writing the transaction script 44 to serve his particular needs.

D. DIGITAL CASH REPLENISHMENT

The discussion of a digital cash purse is section II.C., above, did not address the issue of cash replenishment. The Service Provider can add cash replenishment capability to the module 10, as discussed in section II.C., simply by adding another modulus object and exponent object containing the Service Provider's public key, a random SALT object, and a transaction script 44 for adding money to the balance. The Service Provider can add money to a module 10 either in person or remotely over a network. The process of adding money is as follows:

1. Referring to FIGURE 8, the Service Provider reads the unique lasered registration number (ID number) of the module F1, F2 and calls on a transaction script 44 to return the value of a random SALT object. The module 10 calculates a new random SALT value from the previous value and the random number generator and returns it to the Service Provider F3.

2. The Service Provider places the random SALT returned by the module 10 in a packet along with the amount of money to be added and the unique lasered registration number of the module 10 and then encrypts the resulting packet with the Service Provider's private key F4. This encrypted packet is then written back into the input data object of the transaction group 40.

3. The Service Provider invokes a transaction script 44 which decrypts the contents of the input data object with the Service Provider's public key and then checks the unique lasered registration

number and the value of the random SALT against the one that it originally provided. If the SALT matches, the money amount is extracted from the packet and added to the value of the money object in the module F5.

Note that the inclusion of the unique lasered registration number is not strictly necessary, but it is included to insure that the Service Provider knows exactly which module is receiving the funds.

E. EXEMPLARY DESCRIPTION OF DIRECT TRANSFER OF FUNDS BETWEEN MODULES

Section II.C.2.g. above reveals a problem that occurs when the Merchant returns the digital certificates to his bank for crediting to his account. The Merchant's bank must either send the certificates back to the Service Provider for redemption, or have access to the Service Provider's records in a database so that it can determine whether the value of the transaction count object is unique. This is inconvenient and requires infrastructure. It also prevents any of the transactions from being anonymous (as they would have been if cash had been used), because the Merchant's bank must log used certificate numbers into a database to prevent them from being reused. These problems can all be eliminated by making use of fund transfers between modules. In addition, the steps required to accomplish a fund transfer between modules are considerably simpler than those described in section II.C.2.

In the discussion which follows, it is assumed that the Merchant also has a module which he uses to collect the funds received from End Users (customers). The module in the possession of the End User will be called the Payer, and the module in the possession of the Merchant will be called the Payee. The steps to accomplish the funds transfer are as follows:

1. Referring to FIGURES 9, 11 and 12, using his computer, the Merchant calls on a transaction

script 44 in the Payee to provide a random SALT. He reads this SALT from the output object of the transaction group 40.

2. The Merchant copies the SALT and the amount of the End User's purchase to the input data object of the Payer G1, then calls on a transaction script 44 in the Payer to subtract the amount of the purchase from the balance, combine the Payee's SALT in a packet with the amount of the purchase, encrypt the resulting package with the Service Provider's private key, and return it in the output data object G2.

3. The Merchant then reads this packet and copies it to the input data object of the Payee, then calls on a transaction script 44 in the Payee to decrypt the packet with the Service Provider's public key G3 and check the SALT against the one originally generated by the Payee. If they agree, the Payee adds the amount of the purchase to its balance G4.

This completes the funds transfer. Note that this transaction effectively transferred the amount of the purchase from the Payer to the Payee, and the steps of the transaction were much simpler than the three-way transaction described in II.C.2. The Merchant can transfer the balance to his bank account by a similar transaction in which the bank provides a SALT to Merchant's module and the Merchant's module prepares a certificate for the balance which it delivers to the bank. Use of a module by the Merchant to collect funds simplifies the transaction, eliminates the need for a database to confirm uniqueness, and preserves the anonymity of the End User that would normally result from a cash transaction.

F. EXEMPLARY TRANSACTIONS WITH A MODULE OVER A NETWORK

The transactions described in section II.C.2., II.D. and II.E. above could also be performed over a network, allowing a physical separation between the Merchant, End User, and modules. However, this could produce a potential problem because one of the communications to the module 10 is unencrypted and therefore subject to falsification. To avoid this problem, both parties must produce a SALT so that the other can demonstrate its ability to encrypt the SALT with the Service Provider's private key and therefore prove authenticity. The operation of this protocol is described as follows as it relates to the transfer of funds between modules (section II.E. above). This method can be employed to allow any of the transactions described above to take place over a network. This clearly enables secure electronic commerce over the Internet.

1. Referring to FIGURE 10, 11 and 12, the Payer generates a random SALT and transmits it over the network to the Payee H1.

2. The Payee appends the amount of the purchase to the Payer's SALT, followed by a SALT randomly generated by the Payee. The Payee then encrypts this packet with the Service Provider's private key and sends it back to the Payer H2.

3. The Payer decrypts the packet with the Service Provider's public key H3, extracts the Payer SALT, and compares it with the SALT that the Payer provided in step 1. If they agree, the Payer subtracts the amount of the purchaser from its balance H4 and generates a certificate consisting of the amount of the purchase and the Payee's SALT, which it encrypts with the Service Provider's private key and returns to the Payee H5.

4. The Payee decrypts the packet with the Service Provider's public key H6, extracts the Payee SALT, and compares it with the SALT that the Payee provided in step 2. If they agree, the Payee adds the amount of the purchase to its balance H7.

The exchange of SALTs allows each module to confirm that it is communicating with another module, and that the funds transfer requested is therefore legitimate. The SALT comparison described in step 3 allows the Payer to confirm that the Payee is a legitimate module 10 before the funds are withdrawn, and the comparison described in step 4 allows the Payee to confirm that the Payer is a legitimate module 10 before the funds are deposited. The transactions described above provide the minimum necessary information in the encrypted packets to confirm that the funds are being transferred from one module 10 to another. Other information, such as the unique lasered registration number, could be included (at the cost of anonymity) to provide additional information and greater control over the transaction.

G. AN EXEMPLARY TECHNIQUE FOR SOFTWARE AUTHORIZATION AND USAGE METERING

The module 10 is well-suited for the tasks of enabling specific software features in a comprehensive software system and for metering usage of those features. (This usage model parallels the previously described model for withdrawing money from a module 10.)

1. Preparation

Referring to FIGURES 11 and 12, the Service Provider creates a transaction group 40 and stores a configuration object in the group detailing which software within the module 10 the End User is allowed to use. The Service Provider also creates a money object containing the allowed usage credit (which could be in units of time rather than the actual dollar amount), and stores and privatizes a private RSA key pair to use for authentication. A transaction script 44 is stored to receive a SALT and the amount to withdraw from the End User, decrement the balance by the amount withdrawn, and output an RSA signed certificate containing the amount withdrawn, the sale, and the value of the configuration object.

2. Usage

At periodic intervals during the use of the software within the module 10, the PC program generates a random SALT and an amount to charge for the use of the module 10 and transmits this information to the module 10. The module 10 decrements the balance and returns the certificate. The PC decrypts the certificate and confirms that the SALT is the same, the amount withdrawn is correct, and the use of the software within the module 10 is authorized by the information stored in the configuration object. If all of these tests are successful, the module 10 executes for a specified period of time or for a given number of operations before asking the module 10 for another certificate.

There are many possible variations on this usage model. For example, the transaction script 44 could also bind up the true time in the certificate so that the application program running on the PC could guarantee that the execution time is accurately measured. (This would require the Service Provider to create a clock offset object during initialization to provide a reference for measuring time.)

H. SIMULATION OF TRANSACTION TOUCH MEMORY™

This usage model describes how the module 10 can be used to simulate the behavior of the simpler Transaction Touch Memory™ (DS 1962) (hereinafter "TTM") or any similar device or substitute that can operate in a nearly equivalent or similar fashion. The principal feature of the TTM is that there is a counter associated with a block of memory in such a way that the counter is incremented automatically whenever the contents of the memory block are changed.

1. Preparation

This simple feature can be programmed into the module 10 by creating a configuration object, a transaction counter object, and a transaction script object which combines the contents of the input object with the value of the transaction counter object and places them in the configuration object, incrementing the counter automatically in the process. All three objects 42 are locked, but none are privatized.

2. Usage

To add or remove money, the End User reads the values of the configuration object and the transaction counter object directly, then decrypts the configuration object and checks the transaction count from the decrypted package against the value of the counter object. The End User also checks the unique lasered registration number from the encrypted packet against the registration number of the module 10. If these both agree, the balance is considered valid. An amount is added to or subtracted from the balance, the transaction count is incremented, and the packet is re-encrypted and stored in the input data object. The transaction script 44 is then invoked to move the data and the transaction counter value to the configuration object, automatically incrementing the counter value in the process. (The transaction script 44 guarantees that the counter object's value will be incremented anytime data in the configuration object is changed.)

This simple operation can be performed relatively quickly since the module 10 does not have to perform any encryption itself. However, as with the TTM, the End User must now use a secure computing facility to perform the encryption and decryption operations. This usage is therefore less protected than those which depend on the module's encryption capabilities.

I. EXEMPLARY TECHNIQUE FOR POSTAL METERING SERVICE

This usage model describes an application in which the module 10 is used to dispense postage certificates. The digital information which constitutes the certificate is printed on the envelope in the form of a two-dimensional barcode which can be read and authenticated by the Service Provider (U.S.P.S.). A computer program running on an ordinary PC attached to a laser printer in combination with the module 10 can be used to print the postage certificates.

1. Preparation

The Service Provider creates a group containing a money register, a private RSA key (exponent object and modulus object) common to every module, and a transaction script 44. The script 44 combines the SALT and the amount to be withdrawn (provided by the End User's computer) with the unique lasered registration number of the module 10, encrypts this packet with the private key, subtracts the amount withdrawn from the balance, and places the encrypted certificate in the output object where it can be read by the PC.

The Service Provider initializes the balance with a specific amount of money, locks the balance and script 44, privatizes the RSA key objects, and locks the group so that no more scripts can be added. The modules prepared in this way can then be sold over the counter for use with PC-based postage metering programs.

2. Usage

When the first envelope is to be printed, the PC program prepares the first SALT by calculating a one-way hash (e.g., the Secure Hash Standard, FIBS PUB 180) of the date and the unique lasered registration number of the part. This information is passed to the module 10 along with the amount of postage to be withdrawn. The resulting certificate is printed in the two-dimensional barcode along with the hash generation number (one for the first hash), the unique lasered registration number, the plaintext denomination of the stamp, the date, and other information as desired to identify the End User. Subsequent SALTs are generated by performing the one-way hash again on the previous SALT and incrementing the hash generation number.

When the Service Provider receives the envelopes, most of them are taken at face value and the digital barcode is not read. However, a statistical sampling of the barcodes are read and the information provided is decrypted with the public key and verified. Discrepancies are investigated, and fraud is prosecuted under existing law. Verification is possible because the Service Provider can recreate the SALT from the unique lasered registration number, date, and hash generation number, and thereby verify that the transaction is not only current but also linked to a specific module 10.

Note that there are many possible variations on the method described above, leading to similar results. The most likely fraud would be duplication, in which a user captures the digital information sent to the printer to produce the postage certificate and makes many duplicate copies of the same certificate. This could be detected easily by the Service Provider simply by reading the hash generation number and unique registration number and looking them up in a database to make sure that the user is not duplicating the same certificate. (This check could be performed more often than full certificate verification, which would require RSA decryption.)

J. SUBSCRIPTION INFORMATION SERVICE

This usage model describes an application in which a Service Provider makes available information in encrypted form over the internet to users who have agreed to pay for such information. This application works exactly the same way as the Secure E-mail usage model described in section A above, except that the Service Provider bills the user for the encrypted information that the Service Provider e-mails to him. The billing information is obtained from a registry of pubic RSA keys which allows the Service Provider to identify and bill a user, based on his public key or on the unique lasered serial number of his module 10.

K. REGISTRY WITH GUARANTEED PRIVATE KEY SECURITY

In order to provide Merchants with an independent confirmation of the identity of an End User, a Service Provider may wish to maintain a registry containing the pubic key of a particular module 10 along with the name, address, and other identifying information of the person to whom the module 10 is issued. For this purpose, it is essential for the Service Provider to make sure that the public key in the registry corresponds to a private key which is known only to the module 10. In order to guarantee this, the module 10 must be in the possession of the Service Provider at the time the public key is extracted from the module 10 and placed in the registry. After recording this information in the registry, the Service Provider can ship the module 10 to the End User named in the registry.

It is also important for the End User to be able to confirm, when he receives the module 10, that the private key is not known to the Service Provider or any of the Service Provider's employees. This is important because an ideal registry system should not require that any party trust any other party. The system works to everyone's satisfaction only when each party can be convinced that none of the other parties could possibly know the private key.

One way to accomplish this, the Service Provider sends a command to the module 10 to cause it to generate a complete RSA key set using random numbers, and then to automatically make one of the exponents private, so that there is no way any person can discover the value of the private key. This key set has a special type, different from that of a key set programmed into the can by a Service Provider, so that anyone doing business directly with the module 10 can determine for themselves that the private key is known only to the module 10.

1. Preparation

The Service Provider creates a password-protected transaction group 40 for the application, and then creates an RSA key set in the group that is generated by the module 10. (After generating the key set, the modulus and one exponent will be locked automatically, while the second exponent will be privatized automatically by the firmware of the module 10. The Service Provider then creates a transaction script 44 which will encrypt data from the input object with the private key and place the encrypted result in the output object. The transaction script 44 might optionally append additional information (e.g., the transaction counter) to the data from the input object, in order to satisfy any additional objectives of the application. Other objects 42 and transaction scripts 44 may also be added at the discretion of the Service Provider. The transaction group 40 is locked by the Service Provider when it is complete.

Next, the Service Provider reads the RSA modulus and public exponent from the transaction group 40 and records them in the registry along with the information identifying the End User. Finally, the Service Provider ships the module 10 to the End User, and later conveys to the End User the password that can be used to access the transaction group 40.

2. Usage

When a Merchant wishes to obtain positive identification of an End User over the Internet or other network, the Merchant generates a unique packet of data and transmits it to the End User, and the End User passes the data into the input object and invokes the transaction script 44 which causes it to be encrypted with the private key generated by the module 10. The resulting encrypted packet is transmitted back to the Merchant. The Merchant then accesses the data base provided by the Service Provider to obtain the public key belonging to the End User, and attempts to decrypt the encrypted packet using the End User's public key. If the decryption succeeds, the Merchant has proven the physical presence of the End User's module 10 at the remotely networked location. By guaranteeing the presence of the End User's module 10 at the remote site, this identification validates and legitimizes the contents of the data packet and therefore also any financial transactions, represented by the contents of the packet, that may be requested by the End User.

The model described here is one in which the authority to perform financial transactions derives from the registry maintained by the Service Provider. It is therefore essential that this information be accurate and that the private key in the module 10 can be secure from all parties. Because each module 10 has its own unique RSA key set, there is no provision in this model for the module 10 to represent money independently of the registry maintained by the Service Provider. Instead, the registry and the ability of the module 10 to sign with its private key together serve as a definitive means of identifying the End User remotely to any other party.

L. TAXATION OF TRANSACTION VOLUME

This usage applies to a business model in which the Service Provider intends to collect a service charge from the End User that is a percentage of the total amount of money transferred by the module 10. This model is similar to those described in sections C D, E, and F above, but with the addition of a destructor object that can cause any particular transaction script 44 to expire at a predetermined date and time. This model also requires the use of an additional money object which is programmed (with a suitable transaction script 44) to accumulate the total value of all the money passed out of the module 10.

1. Preparation

The Service Provider creates a transaction group 40 containing money objects, etc., as described in sections D and E above. The Service Provider also creates an additional money object to serve as the volume accumulator. The Service Provider also creates transaction scripts 44 for withdrawing or depositing money as in D and E, except that the transaction script for adding money to the module 10 includes a destructor object set to expire at a predetermined time in the future, and the transaction script 44 for withdrawing money includes an instruction to add the amount of the withdrawal to the money object serving as the volume accumulator. The service provider then locks the group and ships the module 10 to the End User.

2. Usage.

The End user uses the module 10 for deposits and withdrawals as described in sections D and E above. During the time that the module 10 is used, the cumulative total of all the money spent from the module 10 is accumulated in the money object serving as the volume accumulator. When the time limit expires, the End User can no longer add money to his module 10, although he can continue to withdraw money if desired until there is none left. The End User then returns the module 10 to the Service Provider to be restored. The Service Provider reads the remaining amount of money and also the amount of money recorded in the volume accumulator. The Service Provider bills the End User a service charge that is a percentage of the amount in the volume accumulator. If the End User is willing to pay this amount to continue his service, the transaction group 40 is destroyed and rebuilt, then the amount of money remaining in the module 10 when the End User returned it is programmed back into the money object of the transaction group 40. The Service Provider then returns the restored module to the End User, provided that the End User pays the service charge.

The system described above allows a Service Provider to collect periodic fees for service without having to monitor and be involved in every financial transaction performed by the End user. The fee is based on actual usage, as determined by the contents of the volume register.

Exemplary Firmware Definitions for Use With the Module

Object The most primitive data structure accepted by and operated on by the modules firmware. A list of valid objects and their definitions is provided in the next section.

Group A self-contained collection of objects. An object's scope is restricted to the group of which it is a member.

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.

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.

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

Audit Trail A record of transactions occurring after the 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.

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.

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 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 M:

$$\text{Encryption:} \quad C = M^{e} \pmod{N} \tag{1}$$

$$\text{Decryption:} \quad M = C^{d} \pmod{N} \tag{2}$$

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

RSA Exponent 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 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.

Transaction Script A transaction script is a series of instructions to be carried out by the module. When invoked the 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 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 transaction counter increments by 1. Once a transaction counter has been locked it is read only and provides an irreversible counter.

Money Register 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.

Clock Offset This object is preferably a 4 byte number which contains the difference between the reading of the 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 module by adding the value of the clock offset to the real-time clock.

SALT 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 module combines the previous SALT with the 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 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™.

Preferred Module Firmware Command Set

Set Common PIN(01H)

Transmit (to module)

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

Receive data

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

Output length = 0

Output Data = 0

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)

PIN_TO_CREATE 00000010b (require PIN for group creation).

Initially the 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:

ERR_BAD_COMMON_PIN (Common PIN match failed)

ERR_BAD_PIN_LENGTH (New PIN length > 8 bytes)

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:

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

Output data length (Command output length, 2 bytes)

Output data (Command output, length specified above).

Master Erase (02H)

Transmit data

02H, Common PIN

Receive data

CSB = 0 if command was successful, ERR_BAD_COMMON_PIN otherwise

Output length = 0

Output data = 0

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 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 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)

Transmit data

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

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 bit is set in the common PIN option byte and the PIN transmitted does not match the common PIN the module will set the OSC to ERR_BAD_COMMON_PIN.

Possible error return codes for the create group command:

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 module has been locked)

ERR_INSUFFICIENT_RAM (Not enough memory for new group)

Set Group PIN (04H)

Transmit data

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)

ERR_BAD_PIN_LENGTH (New group PIN length > 8 bytes)

Create Object (05H)

Transmit data

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

Receive data

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:

If the Create Object command is successful the 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 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)

ERR_MIAC_LOCKED	(The 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)

Object types:	RSA modulus	0
	RSA exponent	1
	Money register	2
	Transaction counter	3
	Transaction script	4
	Clock offset	5
	Random SALT	6
	Configuration object	7
	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 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 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 module has been locked)

ERR_BAD_GROUP_ID (Specified group does not exist)

ERR_BAD_OBJECT_ID (Specified object does not exist)

Privatize Object (07H)

Transmit data

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. <u>Privatizing an object is an irreversible operation</u>.

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 module has been locked)
ERR_BAD_GROUP_ID	(Specified group does not exist)
ERR_BAD_OBJECT_ID	(Specified object does not exist)

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 module has been locked)

ERR_BAD_GROUP_ID (Specified group does not exist)

ERR_BAD_OBJECT_ID (Specified object does not exist)

Lock 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 module has not previously been locked, the command will succeed. When the 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 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 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 module command:

ERR_BAD_COMMON_PIN (Supplied common PIN was incorrect)

ERR_MIAC_LOCKED (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 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 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 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 module checks the attribute byte of the specified object. If the object has not been privatized the module will transmit the object data to the host. If the Group PIN was invalid or the object has been privatized the 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)
ERR_BAD_OBJECT_ID	(Object did not exist in group)
ERR_OBJECT_PRIVATIZED	(Object has been privatized)

Write Object (0DH)

Transmit data

0DH, 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 module checks the attribute byte of the specified object. If the object has not been locked or privatized the 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 module will delete the specified group. Deleting a group causes the automatic destruction of all objects within the group. If the 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)

ERR_MIAC_LOCKED (Module has been locked)

Get Command Status Info (10H)

Transmit data

10H

Receive data

CSB = 0

Output length = 6

Output data = 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)

Get Module Configuration Info (11H)

Transmit data

11H

Receive data

CSB = 0

Output length = 4

Output data = 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 (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 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 (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 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 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 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 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 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 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 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 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 module's common PIN. Initially the common PIN is set to 0.

ERR_BAD_GROUP_PIN (82H)

Transaction groups may have their own PIN, FIGURE 11. 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 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 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 module.

ERR_MIAC_LOCKED (87H)

When the 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.

ERR_MIAC_NOT_LOCKED (88H)

If the 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 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 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 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 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 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 module will return an ERR_OBJECT_PRIVATE error code.

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

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

1) who is the module user via a unique registration number.

2) when the transaction took place via a true-time stamping of the transaction.

3) where the transaction took place via a registered module interface site identification.

4) security information via uniquely serialized transactions and digital signitures on message digests.

5) 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 method for adding a monetary equivalent to an electronic module, comprising the steps of:

a. placing the module in communication with an electronic device;

b. indicating an amount requested to said electronic device;

c. communicating a random number from said module to said electronic device;

d. combining said random number and said amount requested thereby creating a first data packet ~~paket~~ in said electronic device;

e. encrypting said first data packet with a first key thereby creating a signed certificate in said electronic device;

f. communicating said signed certificate from said electronic device to said module;

g. decrypting said signed certificate in said module with a second key thereby creating a decryted ~~decypted~~ random number and a decrypted amount requested;

h. comparing said random number with said decrypted random number and determining if they match in said module; and

i. adding said decrypted amount requested to a money register in said module.

2. The method of claim 1, further comprising, after step b, the step of communicating a module identification from said module to said electronic device.

3. The method of claim 2, wherein the step d of combining further comprises the step of combining said module indentification with said random number and said amount requested prior thereby creating said first data packet in said electronic device.

4. The method of claim 3, wherein the step of g of decrypting further comprises the step of creating a decrypted module identification.

5. The method of claim 4, wherein the step h of comparing further comprises the step of comparing said module identification and said decrypted module identification and determining if they match.

6. The method of claim 1, wherein said module is portable.

7. The method of claim 1, wherein said first key is a private key and said second key is a public key.

8. The method of claim 1, wherein said module is programmable.

9. Method of metering a monetary equivalent out of a module and into an electronic equipment, comprising the steps of:

a. placing said electronic equipment in communication with said module;

b. reading a module identifier with said electronic equipment;

c. combining a first random number, a number of units to be metered and said module identifier in said electronic equipment thereby creating a first data packet;

d. encrypting said first data packet in said electronic equipment with a first key thereby creating an encrypted first data packet;

e. passing said encrypted first data packet and a requested monetary value from said electronic equipment to said module;

f. subtracting said requested monetary value from a money register in said module; and

g. incrementing a transaction count in said module.

10. The method of claim 9, wherein after step g said method further comprises the steps of:

h. combining said transaction count, said requested monetary value, and said encrypted first data packet in said module and thereby creating a second data packet;

i. encrypting said second data packet with a second key in said module thereby creating an encrypted second data packet; and

j. passing said encrypted second packet to said electronic equipment.

11. The method of claim 10, further comprising the steps of:

k. decrypting said encrypted second data packet with a third key in said electronic equipment thereby creating a decrypted second data packet;

l. determining whether said requested monetary amount sent to said module is the same as in said decrypted second data packet; and

m. determining whether said encrypted first data packet sent to said module is the same as in said decrypted second data packet.

12. The method of claim 10, further comprising the steps of:

o. sending said encrypted second data packet from said electronic device to a provider;

p. decrypting said encrypted second data packet with a fourth key by said provider; and

q. decrypting said encrypted first data packet with a fifth key by said provider.

13. The method of claim 9, wherein said encryption step utilizes a predetermined encryption technique.

14. The method of claim 13, wherein said predetermined encryption technique is an RSA technique.

15. The method of claim 9, wherein said module is programmable.

16. An apparatus for receiving and transmitting encrypted data comprising:

an input/output interface;

a microprocessor circuit connected to said input/output interface; and

a coprocessor circuit, connected to said microprocessor circuit, for performing encryption and decryption algorithms, said apparatus being adapted to receive an encrypted data packet and being adapted to decrypt said encrypted data packet via a key.

17. The apparatus of claim 16, wherein said key used is for an RSA decryption algorithm.

18. The apparatus of claim 16, wherein said apparatus is a compact portable module.

19. The apparatus of claim 16, wherein said input/output interface is at least a single conductive contact.

20. The apparatus of claim 16, wherein said input/output interface is a one-wire interface.

21. An apparatus for receiving and transmitting encrypted data, comprising:

an input/output interface;

a microprocessor circuit connected to said input/output interface;

a coprocessor circuit, connected to said microprocessor circuit, for performing encryption and decryption algorithms, said apparatus being adapted to encrypt a data packet using a key and to transmit said encrypted data packet out of said input/output interface.

22. The apparatus of claim 21, wherein said data packet contains at least a random number.

23. The apparatus of claim 21, wherein said apparatus is programmable.

24. The apparatus of claim 23, wherein said apparatus is programmable via object oriented software.

25. The apparatus of claim 21, wherein said apparatus is capable of producing random encryption key pairs.

26. The apparatus of claim 21, further comprising memory means for storing a predetermined program, said memory means being connected to said microprocessor.

27. The apparatus of claim 21, further comprising a transaction counter for counting a number of transactions that said apparatus performs, said transaction counter being connected to said microprocessor.

28. The apparatus of claim 21, further comprising a timing circuit for time stamping transactions performed by said apparatus, said timing circuit being connected to said microprocessor.

MAIL ROOM
JAN
31
1996
64
PAT. & TRADEMARK OFF.

ABSTRACT OF THE DISCLOSURE

The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing encrypted information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

PRINT OF DRAWINGS
AS ORIGINALLY FILED

20661-438

1 of 8

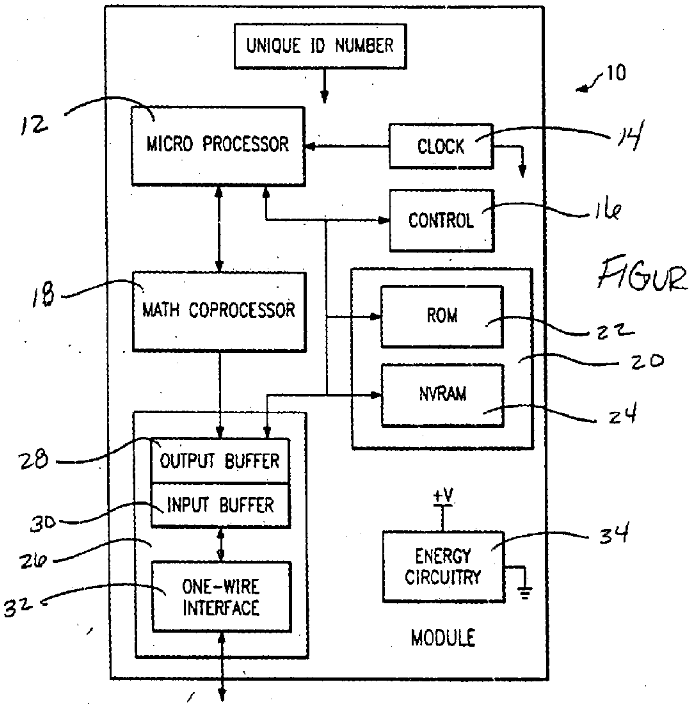
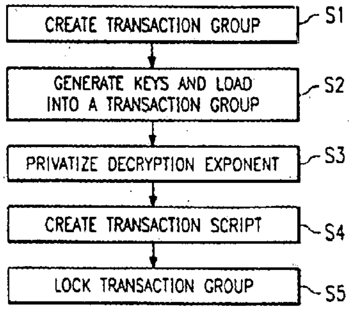


FIGURE 1

FIG. 2


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

PRINT OF DRAWINGS
AS ORIGINAL FILED

438

20661-
2 of 8

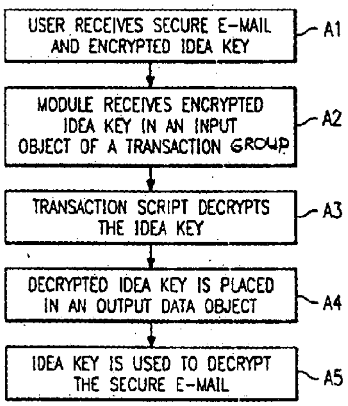

USER RECEIVES SECURE E-MAIL AND ENCRYPTED IDEA KEY
A1
MODULE RECEIVES ENCRYPTED IDEA KEY IN AN INPUT OBJECT OF A TRANSACTION GROUP
A2
TRANSACTION SCRIPT DECRYPTS THE IDEA KEY
A3
DECRYPTED IDEA KEY IS PLACED IN AN OUTPUT DATA OBJECT
A4
IDEA KEY IS USED TO DECRYPT THE SECURE E-MAIL
A5

FIG. 3

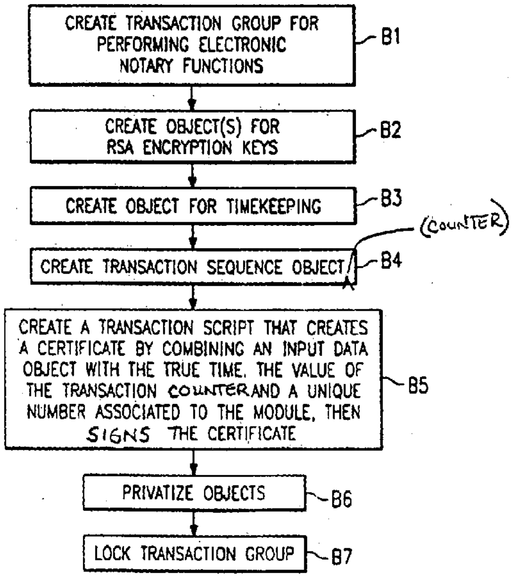

CREATE TRANSACTION GROUP FOR PERFORMING ELECTRONIC NOTARY FUNCTIONS
B1
CREATE OBJECT(S) FOR RSA ENCRYPTION KEYS
B2
CREATE OBJECT FOR TIMEKEEPING
B3
(COUNTER)
CREATE TRANSACTION SEQUENCE OBJECT
B4
CREATE A TRANSACTION SCRIPT THAT CREATES A CERTIFICATE BY COMBINING AN INPUT DATA OBJECT WITH THE TRUE TIME,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

FIG. 4

PRINT OF DRAWINGS
AS ORIGINA FILED

FIG. 5

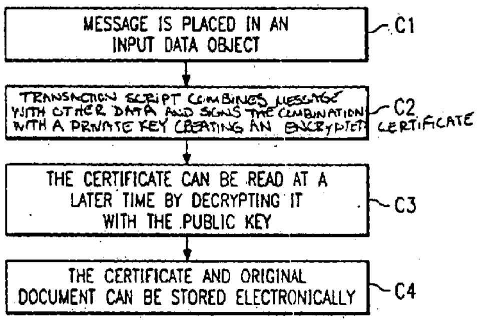
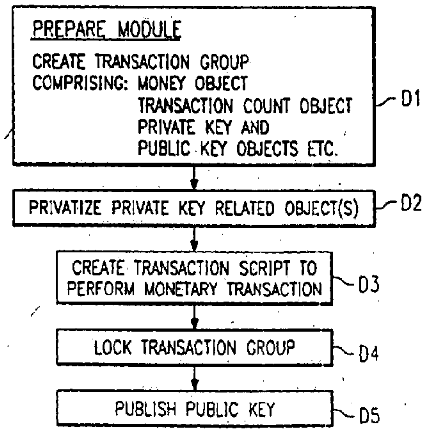

MESSAGE IS PLACED IN AN INPUT DATA OBJECT
C1
TRANSACTION SCRIPT COMBINES MESSAGE WITH OTHER DATA AND SIGNS THE COMBINATION WITH A PRIVATE KEY CREATING AN ENCRYPTED CERTIFICATE
C2
THE CERTIFICATE CAN BE READ AT A LATER TIME BY DECRYPTING IT WITH THE PUBLIC KEY
C3
THE CERTIFICATE AND ORIGINAL DOCUMENT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

FIG. 6



PRINT OF DRAWINGS
AS ORIGINA FILED

438

20661-
4 of 8

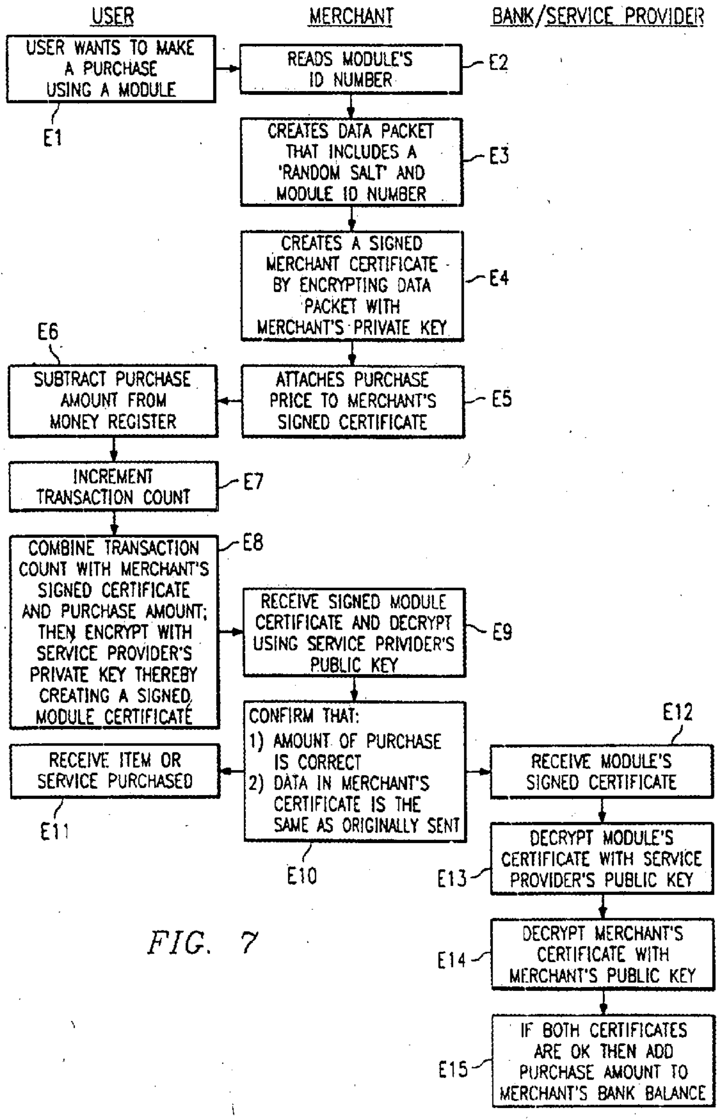

USER
MERCHANT
BANK/SERVICE PROVIDER
USER WANTS TO MAKE A PURCHASE USING A MODULE
E1
READS MODULE'S ID NUMBER
E2
CREATES DATA PACKET THAT INCLUDES A 'RANDOM SALT' AND MODULE ID NUMBER
E3
CREATES A SIGNED MERCHANT CERTIFICATE BY ENCRYPTING DATA PACKET WITH MERCHANT'S PRIVATE KEY
E4
ATTACHES PURCHASE PRICE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

FIG. 7

PRINT OF DRAWINGS
AS ORIGINAL FILED

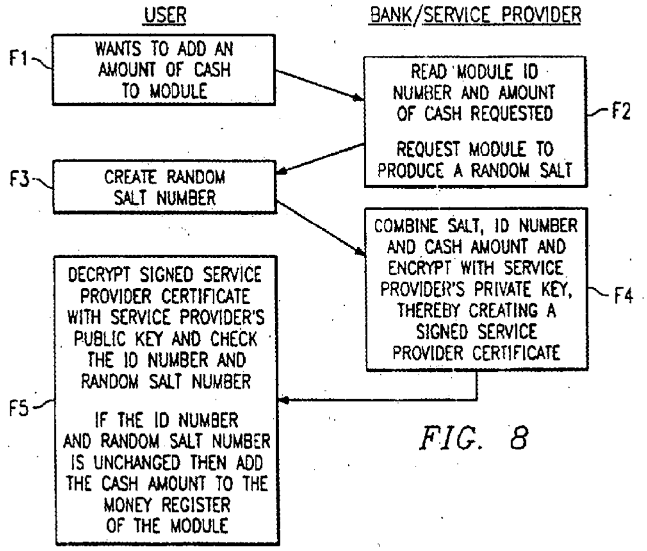

USER
BANK/SERVICE PROVIDER
F1
WANTS TO ADD AN AMOUNT OF CASH TO MODULE
READ MODULE ID NUMBER AND AMOUNT OF CASH REQUESTED
REQUEST MODULE TO PRODUCE A RANDOM SALT
F2
F3
CREATE RANDOM SALT NUMBER
COMBINE SALT, ID NUMBER AND CASH AMOUNT AND ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY, THEREBY CREATING A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

FIG. 8

EXAMPLE OF
TRANSFER FROM USER'S MODULE TO MERCHANT'S MODULE

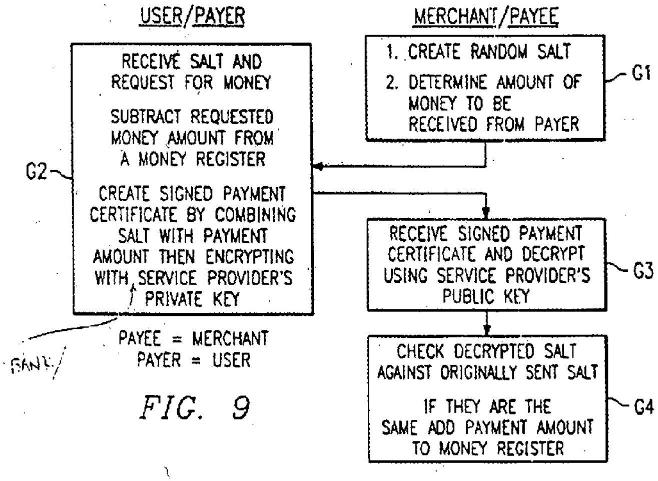

USER/PAYER
MERCHANT/PAYEE
1. CREATE RANDOM SALT
2. DETERMINE AMOUNT OF MONEY TO BE RECEIVED FROM PAYER
G1
RECEIVE SALT AND REQUEST FOR MONEY
SUBTRACT REQUESTED MONEY AMOUNT FROM A MONEY REGISTER
CREATE SIGNED PAYMENT CERTIFICATE BY COMBINING SALT WITH PAYMENT AMOUNT THEN ENCRYPTING WITH SERVICE PROVIDER'S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

FIG. 9

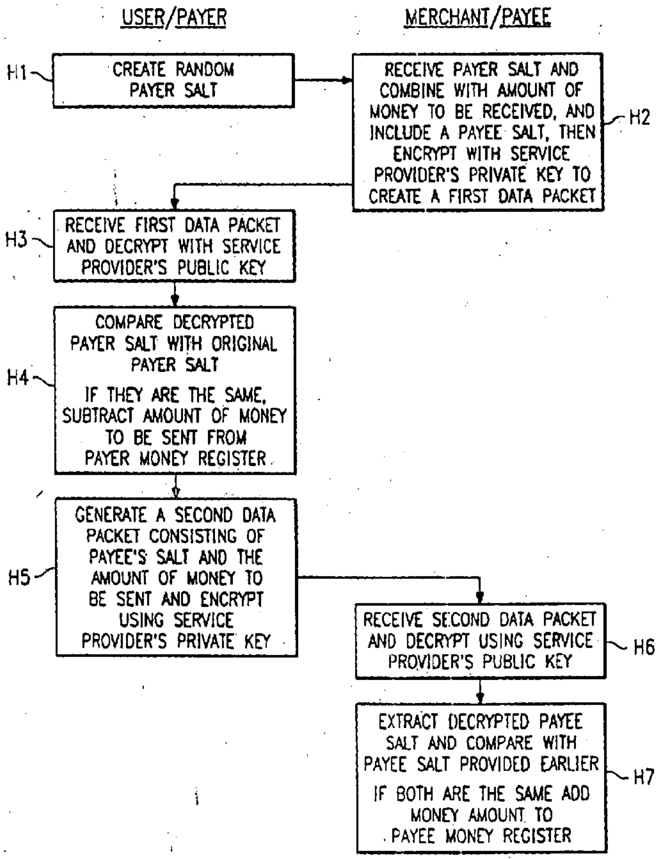
PRINT OF DRAWINGS
AS ORIGINALLY FILED

438

20661-
6 of 8

FIG. 10

TRANSACTION OVER A NETWORK WITH A MODULE


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

PRINT OF DRAWINGS
AS ORIGINAL FILED

09/595014

438
20661-
7 of 8

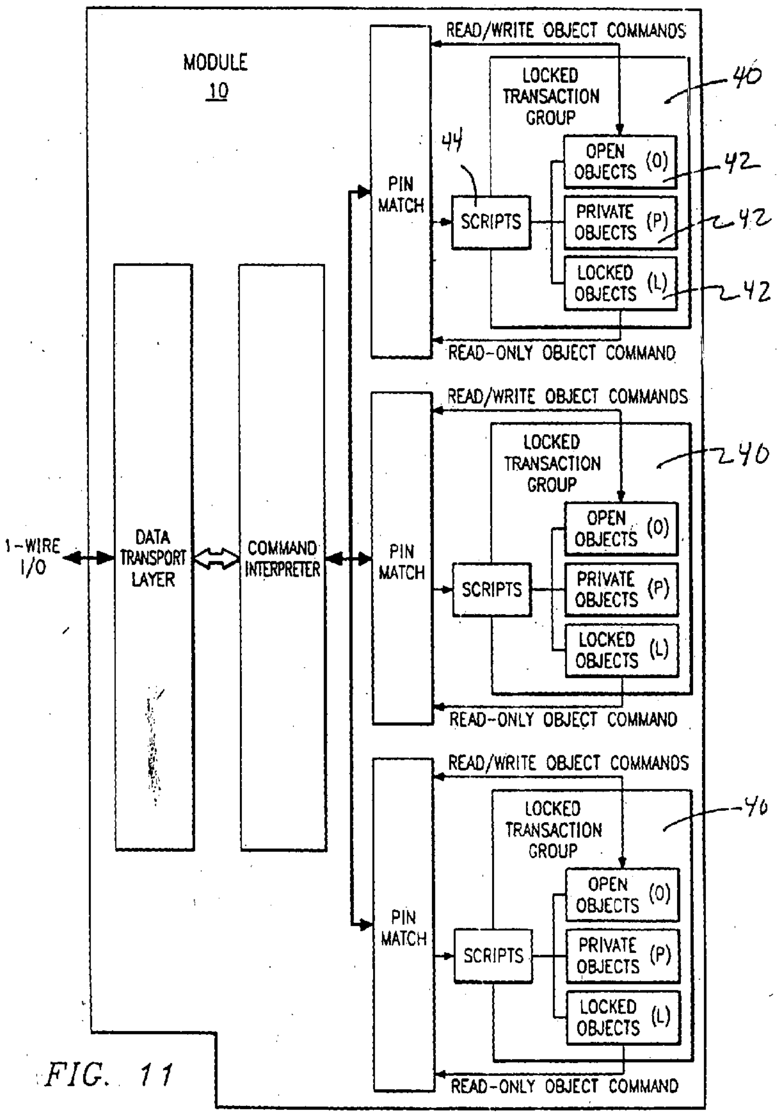


FIG. 11

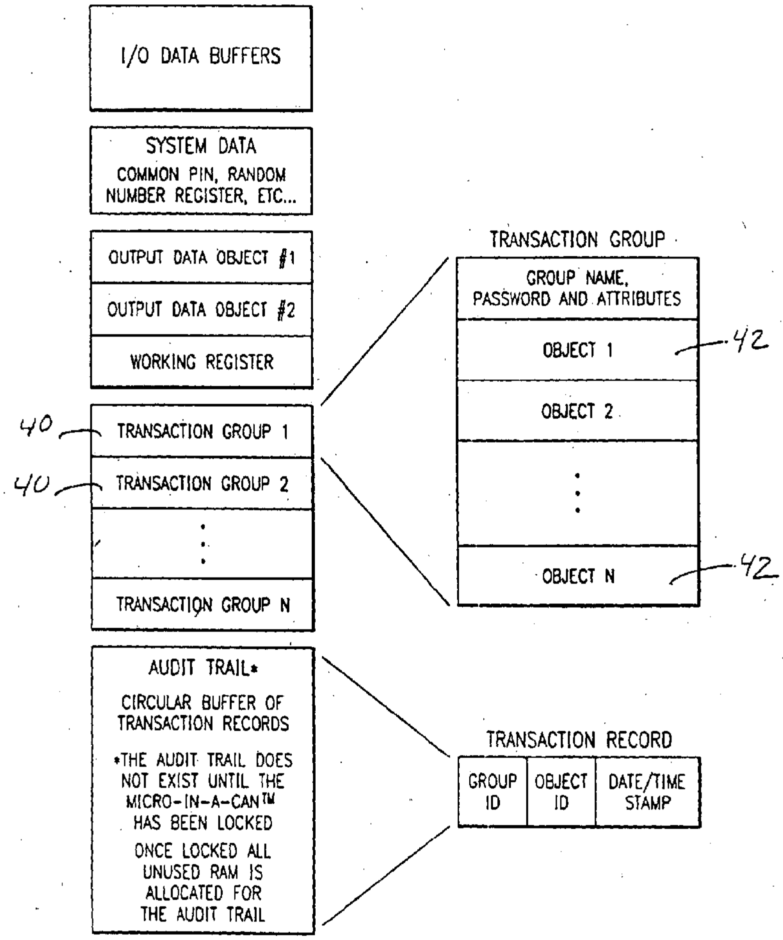
PRINT OF DRAWINGS
AS ORIGINALLY FILED

0°/59501

438

20661--
8 of 8

FIG. 12



08/595014

20661-438

1 of 8

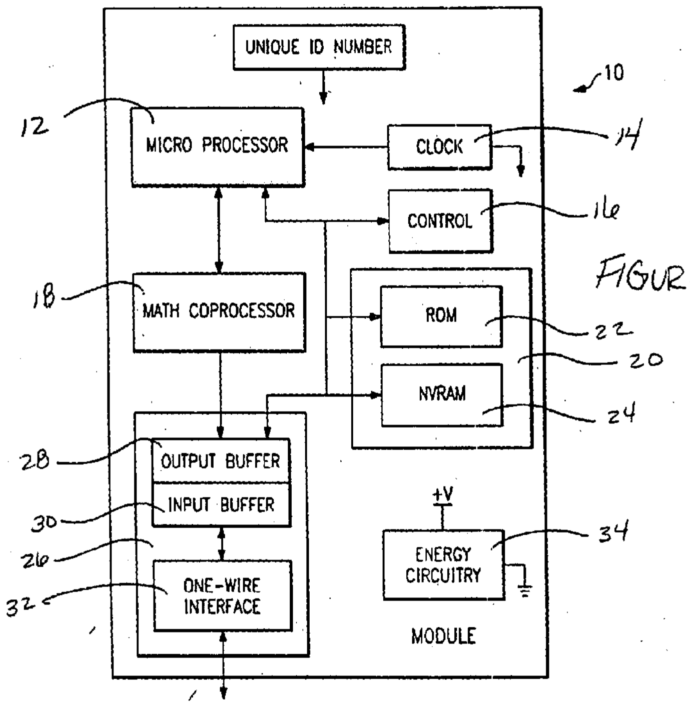
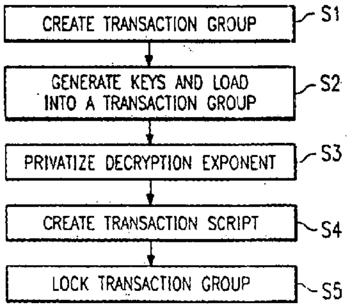


FIGURE 1

FIG. 2



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

FIG. 3

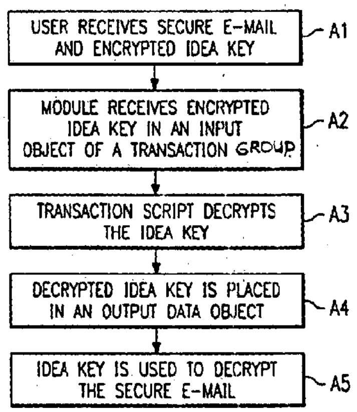

USER RECEIVES SECURE E-MAIL AND ENCRYPTED IDEA KEY
A1
MODULE RECEIVES ENCRYPTED IDEA KEY IN AN INPUT OBJECT OF A TRANSACTION GROUP
A2
TRANSACTION SCRIPT DECRYPTS THE IDEA KEY
A3
DECRYPTED IDEA KEY IS PLACED IN AN OUTPUT DATA OBJECT
A4
IDEA KEY IS USED TO DECRYPT THE SECURE E-MAIL
A5

FIG. 4

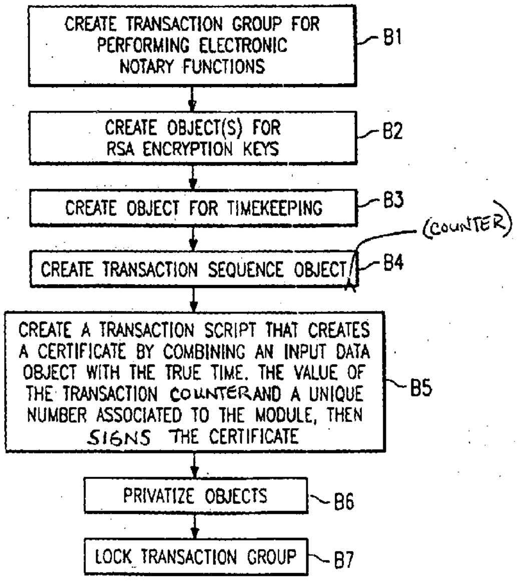

CREATE TRANSACTION GROUP FOR PERFORMING ELECTRONIC NOTARY FUNCTIONS
B1
CREATE OBJECT(S) FOR RSA ENCRYPTION KEYS
B2
CREATE OBJECT FOR TIMEKEEPING
B3
(COUNTER)
CREATE TRANSACTION SEQUENCE OBJECT
B4
CREATE A TRANSACTION SCRIPT THAT CREATES A CERTIFICATE BY COMBINING AN INPUT DATA OBJECT WITH THE TRUE TIME,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

FIG. 5

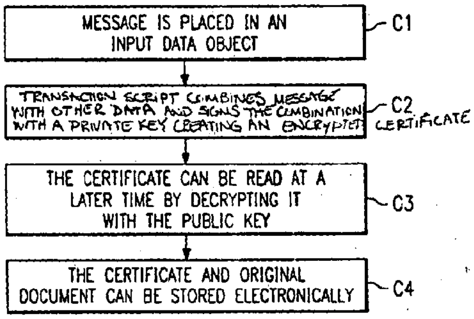
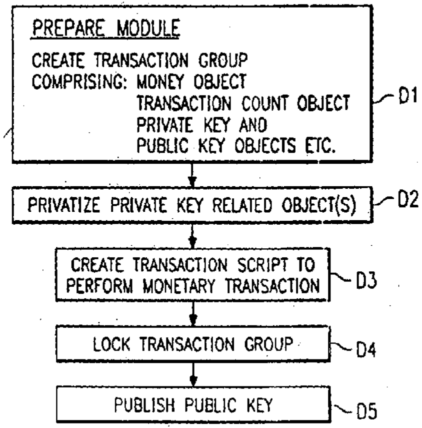

MESSAGE IS PLACED IN AN INPUT DATA OBJECT
C1
TRANSACTION SCRIPT COMBINES MESSAGE WITH OTHER DATA AND SIGNS THE COMBINATION WITH A PRIVATE KEY CREATING AN ENCRYPTED CERTIFICATE
C2
THE CERTIFICATE CAN BE READ AT A LATER TIME BY DECRYPTING IT WITH THE PUBLIC KEY
C3
THE CERTIFICATE AND ORIGINAL DOCUMENT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

FIG. 6


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

08/595014

438

20661-
4 of 8

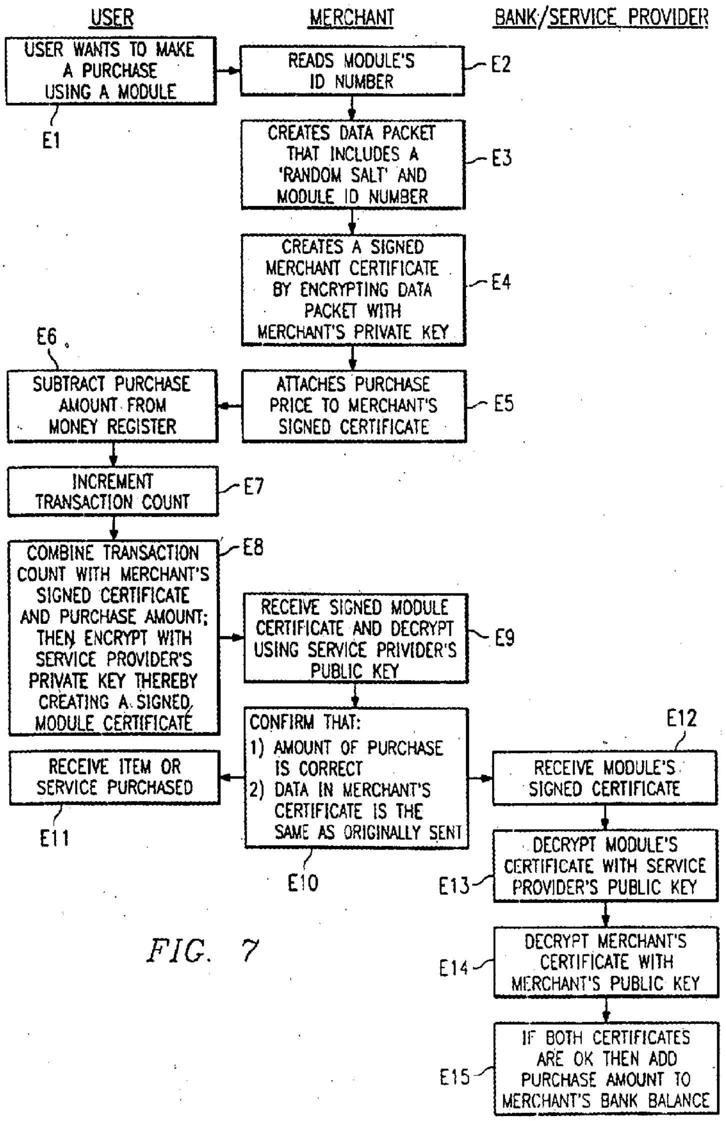
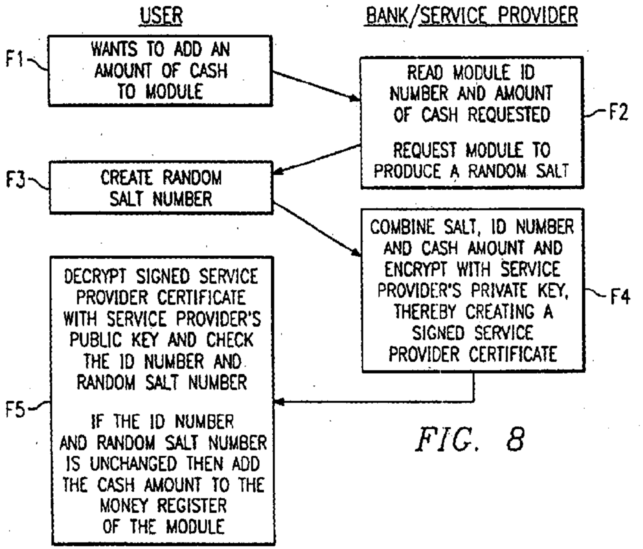

USER
MERCHANT
BANK/SERVICE PROVIDER
USER WANTS TO MAKE A PURCHASE USING A MODULE
E1
READS MODULE'S ID NUMBER
E2
CREATES DATA PACKET THAT INCLUDES A 'RANDOM SALT' AND MODULE ID NUMBER
E3
CREATES A SIGNED MERCHANT CERTIFICATE BY ENCRYPTING DATA PACKET WITH MERCHANT'S PRIVATE KEY
E4
E6
SUBTRACT PURCHASE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

FIG. 7

08/595014

438

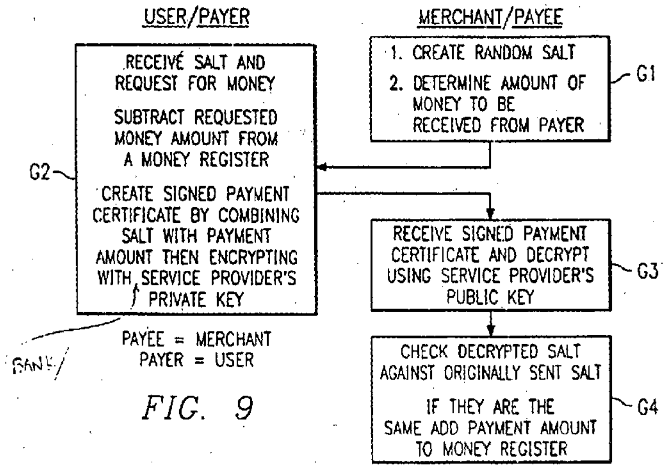
20661-
5 of 8



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

FIG. 8

EXAMPLE OF
TRANSFER FROM USER'S MODULE TO MERCHANT'S MODULE



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

PAYEE = MERCHANT
PAYER = USER

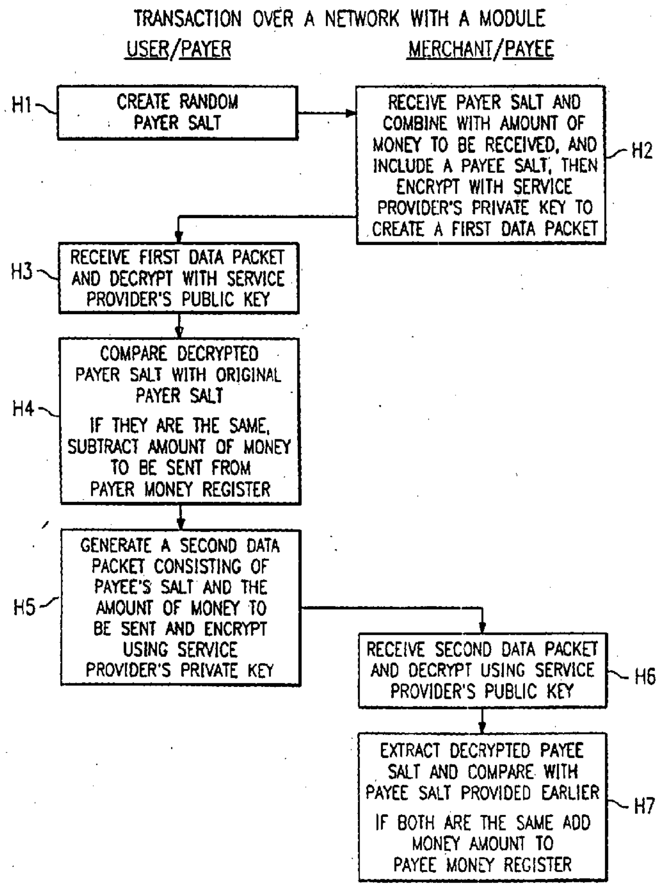
FIG. 9

08/595014

438

20661-
6 of 8

FIG. 10


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

08/595014

438
20661-
7 of 8

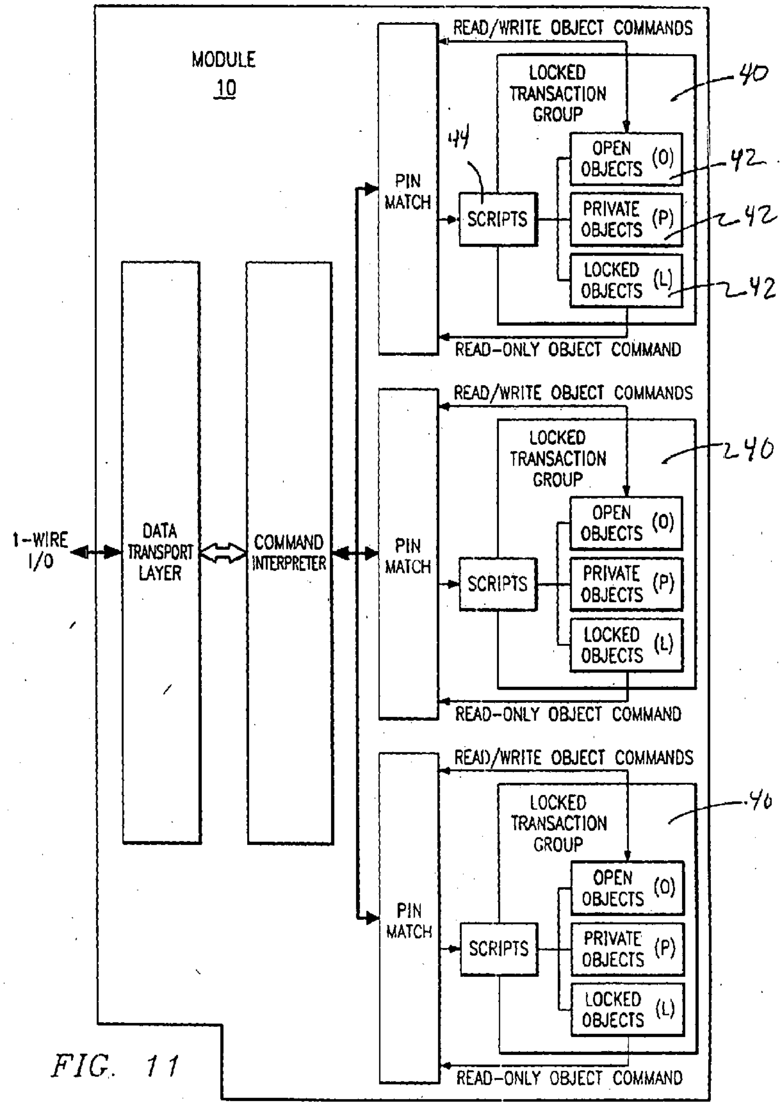
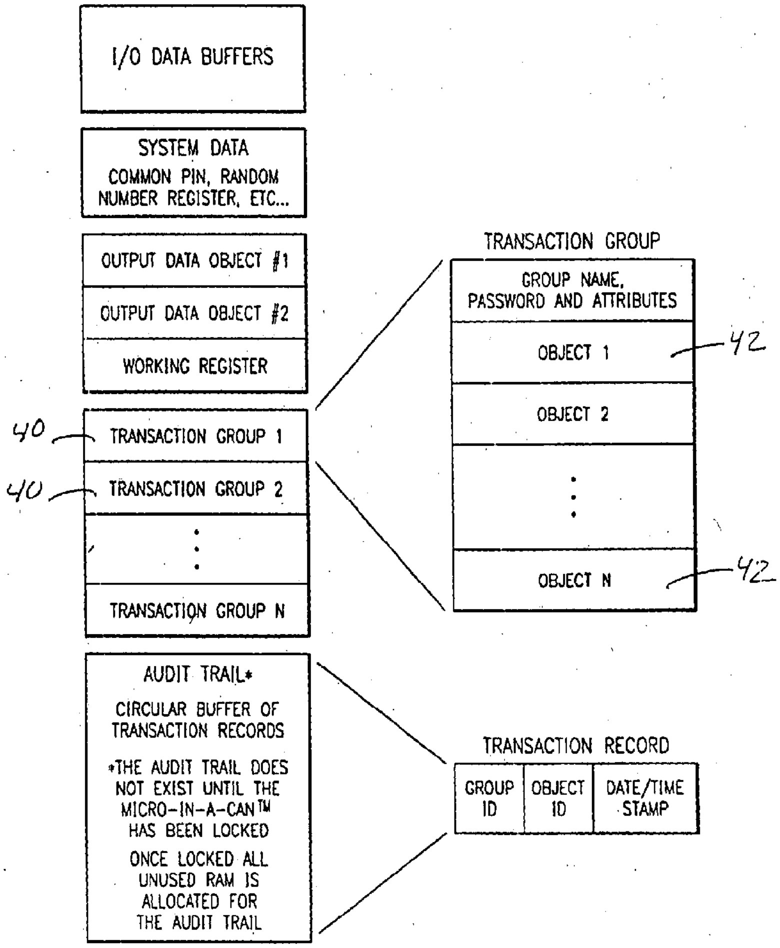


FIG. 11

438
20661-
8 of 8

FIG. 12



MAIL ROOM
JAN
31
1996
64
PAT. & TRADEMARK OFF.

PATENT APPLICATION
DOCKET NO.: 20661/438

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 **CHRISTOPHER W. FOX**, 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: **METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE**, the specification of which: (mark only one)

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

PRIOR FOREIGN PATENTS

			Date first laid-	Date		
		Month/Day/Year	open or	patented or	Priority Claimed	
Number	Country	Filed	Published	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)
____	____	____
____	____	____

_X_ I hereby claim the benefit under 35 U.S.C. § 119(e) of U.S. Provisional Application Serial No. 06/004,510, filed September 29, 1995.

I hereby appoint:

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

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:

PATENT APPLICATION
DOCKET NO.: 20661/438

Steven R. Greenfield
Jenkens & 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 **Residence** (city, state, country)		USA **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 **Residence** (city, state, country)		USA **Citizenship**
	316 Dakota Lane Coppell, TX 75019 **Post Office Address** (include zip code)		

3	CHRISTOPHER W. FOX **Full Name**	**Inventor's Signature**	**Date**
	3847 Timberglen, #4222 Dallas, TX 75287 **Residence** (city, state, country)		USA **Citizenship**
	3847 Timberglen, #4222 Dallas, TX 75287 **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)

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
08/595,014	01/31/96	CURRY S	20661/438

0282/0318

JENKENS & GILCHRIST
1445 ROSS AVENUE
SUITE 3200
DALLAS TX 75202

DATE MAILED: 0000
03/18/96

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 $ 152.00.

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 $ 22.00 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

Transaction History Date 1996-04-18
Date information retrieved from USPTO Patent
Application Information Retrieval (PAIR)
system records at www.uspto.gov

#3 300

MAIL ROOM
53 APR 18 1996
PAT. & TRADEMARK

PATENT APPLICATION
DOCKET NO.: 20661-00438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	§		
Stephen M. Curry et al.	§		
	§		
Serial No.: 08/595,014	§	Group No.:	Not Yet Assigned
	§		
Filed: January 31, 1996	§	Examiner:	Not Yet Assigned

For: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

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

CERTIFICATE OF MAILING

I hereby certify that this paper or fee is being deposited postage paid with the U.S. Postal Service as first class mail on the date indicated below and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231
on 4-15-96

Carol Marstaller
Signature

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;
4) Assignment; 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.

[illegible] 04/23/96 08595014
[illegible] 102 2.00CH
[illegible] 105 130.00CH

IPDAL:77910.1 20661-00438

PATENT APPLICATION
DOCKET NO.: 20661-00438

_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	28	-	28 (at least 20)	=	0 (at least 0)	x11	=	OR	x22	=	$____
INDEP. CLAIMS	4	-	4 (at least 3)	=	0 (at least 0)	x39	=	OR	x78	=	$ 0
FIRST PRESENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a reissue appln)						+125	=	OR	+250	=	$____

	FEE FOR CLAIM AMENDMENTS			$____
____	IDS ATTACHED REQUIRES OFFICIAL FEE - ADD $210 (RULE 1.97(c)) OR $130 (RULE 1.97(d) PETITION)			$____
X	Assignment Recordation Fee ($40)			$ 40
____	IF TERMINAL DISCLAIMER attached add Rule 20(d) Official Fee	$55 (Small Entity)	$110 (Large Entity)	$____
X	Insufficient Filing Fees			$ 22
X	File NOTICE TO FILE MISSING PARTS OF APPLICATIONS (PTO-1532) ($130 - Large Entity)			$ 130

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

	Small Entity	Large Entity
One Month	____ $ 55	___ $110
Two Months	____ $190	___ $380
Three Months	____ $450	___ $900
Four Months	____ $700	___ $1400

ADDITIONAL FEE FOR EXTENDED RESPONSE $____

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

TOTAL FEES $192.00

____ 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 $192.00 to cover the TOTAL FEE. This sheet is attached in duplicate.

CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed 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: April 15, 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.

BEST COPY

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
08/595,014	01/31/96	CURRY	I	S	20661/438

0232/0318

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

DATE MAILED: 03/18/96

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 $ 15 .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 $ - 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.

COPY TO BE RETURNED WITH RESPONSE

#3

MAIL ROOM
53 APR 18 1996
PAT. & TRADEMARK OFF.

PATENT APPLICATION
DOCKET NO.: 20661/438

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 CHRISTOPHER W. FOX**, 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: **METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE**, the specification of which: (mark only one)

_X_ (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 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)

X I hereby claim the benefit under 35 U.S.C. § 119(e) of U.S. Provisional Application Serial No. 06/004,510, filed September 29, 1995.

I hereby appoint:

13

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

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:

PATENT APPLICATION
DOCKET NO.: 20661/438

Steven R. Greenfield
Jenkens & 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)

1-00

1	STEPHEN M. CURRY **Full Name**	Stephen M. Curry **Inventor's Signature**	April 12, 1996 **Date**
	6646 Clearhaven Circle Dallas, TX 75248 **Residence** (city, state, country)		USA **Citizenship**
	6646 Clearhaven Circle Dallas, TX 75248 **Post Office Address** (include zip code)		

2-00

2	DONALD W. LOOMIS **Full Name**	Donald W. Loomis **Inventor's Signature**	April 12, 1996 **Date**
	316 Dakota Lane Coppell, TX 75019 **Residence** (city, state, country)		USA **Citizenship**
	316 Dakota Lane Coppell, TX 75019 **Post Office Address** (include zip code)		

over →

PATENT APPLICATION
DOCKET NO.: 20661/438

3-00

3	CHRISTOPHER W FOX **Full Name**	**Inventor's Signature**	4/12/96 **Date**
	3847 Timberglen, #4222 Dallas, TX 75287 **Residence** (city, state, country)		USA **Citizenship**
	3847 Timberglen, #4222 Dallas, TX 75287 **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)

Application Assignment Record

According to the application transmittal letter, an assignment recording ownership was filed with this application; however, a copy of this record was not located in the original file history record obtained from the United States Patent and Trademark Office. Upon your request, we will attempt to obtain the assignment documents from the Assignment Recordation Branch of of the United States Patent and Trademark Office or from a related application case (if applicable). Please note that additional charges will apply for this service.

This page is not part of the official USPTO record. It has been determined that content identified on this document is missing from the original file history record.

MAIL ROOM
APR
23
1996
PAT. & TRADEMARK OFF.

0150 fc | Refund

PATENT APPLICATION
DOCKET NO.: 20661-00438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

COMPLETED

In re patent application of: Stephen M. Curry et al.	§	
Serial No.: 08/595,014	§	Group No.: Not Yet Assigned
Filed: January 31, 1996	§	Examiner: Not Yet Assigned

For: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

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

CERTIFICATE OF MAILING

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

Date 4-19-96

Carol Marstaller
Signature

PETITION FOR REFUND UNDER 37 C.F.R. §1.26

Dear Sir:

Attached hereto is a true and correct copy of the Monthly Statement of Deposit Account #10-0447 (Exhibit "A") for new application and additional claim fees, and Patent Application Transmittal Letter (Exhibit "B) for the above-referenced patent application submitted with this Request for Refund. The fee in the amount of $982.00 was incorrectly debited from Deposit Account #10-0447. It should have been debited from Deposit Account No. 04-0031 as requested in the transmittal letter (Exhibit "B"). Accordingly, Applicant hereby requests, (1) pursuant to 37 C.F.R. §1.26, for a refund of $982.00 to Deposit Account #10-0447. Applicant further requests,

IPDAL:78282.1 20661-00438

(2) for $982.00 to be correctly debited from Deposit Account #04-0031 as the fee for new application and additional claim fees for the above indicated application for patent.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

By:

Roger L. Maxwell
Registration No. 31,855

Dated: APR 19, 1996

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

(Send this document in duplicate)

JENKENS & GILCHRIST P.C.
ATTN: SANDRA BUKOVIK
1445 ROSS AVENUE
SUITE 3200
DALLAS TEXAS 75202-2711

MONTHLY STATEMENT OF DEPOSIT ACCOUNT

ACCOUNT NO. 10-0447
DATE 02/29/96
CURRENT BAL= $7159.00

DT-POSTED	CON-NO	DESCRIPTION	F-C	$ CHARGES	$ CREDITS	CLT/MT #	
02/01/96	33101	08471606	105	130.00		27946-85 (PI)	AMS/SRM
02/02/96	12080		701		1519.00-		
02/02/96	12080		701		1583.00-		
02/06/96	18017	PCT/US95/11729	801		36.00-	27790-580	TCR/SRM/SOG
02/06/96	28081	08309902	217	450.00		15101-5	J. SICKLER (HOUSTON)
02/06/96	27016	08337685	115	110.00		27798-9	SRM/JKG
02/06/96	14005	08346834	561	30.00		27740-31 (FI)	RLM/SRG/TWM
02/09/96	28024	08259290	103	22.00		20661-135 (FI)	RLM/SRG
02/09/96	28024	08259290	102	228.00		20661-135 (FI)	RLM/SRG
02/12/96	32021	08587558	101	20.00		27771-161 (FI)	TLC/SRM
02/12/96	18118	08379666	122		65.00-	27793-32	SRM/JEB
02/12/96	25103	08221925	126	220.00		27946-47	AMS/GTW/SDD
02/21/96	33042	08595014	101	982.00		20661-438	RLM/SRG
02/22/96	25188	08594185	101	750.00		20661-495	RLM/SRG/CAH
02/27/96	09116		701		4569.00-		

YOU HAVE MORE SCREENS OUTPUT.DEPRESS THE CRDA KEYS & SEND FOR NEX
-BL: $2329.00 TOT-CH: $2942.00 TOT-CR: $7772.00-C-BL:

EXHIBIT A

EXHIBIT B

Patent Application
Docket No. 20661/438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

STEPHEN M. CURRY, DONALD W. LOOMIS, and CHRISTOPHER W. FOX

For: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

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

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. IB 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

Jeanne A. Howard
Signature

Dear Sir:

REQUEST FOR FILING A NATIONAL PATENT APPLICATION

Transmitted herewith for filing, please find the following:

_X_ 1. Specification, claims and abstract of the above-referenced patent application having 129 pages.

_X_ 2. _1_ set(s) of drawing(s) (___ formal / _X_ informal).

_X_ 3. Combined Declaration and Power of Attorney (___ signed _X_ 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.

____ 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)__.

	Application No.	Filing Date
(1)	____	____
(2)	____	____
(3)	____	____

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

_X_ 7.A. Priority is claimed under 35 U.S.C. § 119(e) based on Provisional Application Number 60/004,510, filed on September 29, 1995.

____ 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.

					SMALL ENTITY RATE		LARGE ENTITY RATE		
BASIC FEE					$365	OR	$730	=	$730.00
	NUMBER FILED			NUMBER EXTRA					
TOTAL CLAIMS	28	-20	=	8 (at least 0)	x 11	OR	x 22	=	+$176.00
INDEP. CLAIMS	4	- 3	=	1 (at least 0)	x 38	OR	x 76	=	+$ 76.00
If any proper multiple dependent claim (ignore improper) is present (Enter $0.00 if this is a reissue 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									=$982.00

____ 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 $982.00 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 Depost Account No. 04-0031, **for which purpose a duplicate copy of this sheet is attached.***

Patent Application
Docket No. 20661/438

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

Date: January 31, 1996

Jenkens & 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.

Receipt
#4

MAIL ROOM
JUN 10 1996
PAT. & TRADEMARK OFF.

Patent Application
Attorney Docket No. 20661-00438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
JUL 24 1996
GROUP 2500

RECEIVED
JUL 26 1996
GROUP 2200

In re Application of

STEPHEN M. CURRY et al.

Serial No.	08/595,014	Examiner:	Not Yet Known
Filed:	January 31, 1996	Group No.:	2514
For:	METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE		

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

Dear Sir:

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 June 6, 1996

Carol Marstaller
Signature

PETITION TO CORRECT FILING RECEIPT

Dear Sir:

Applicants hereby request for the Filing Receipt to be correct to 1) correct a misspelling in the title of the application; and 2) correct the priority statement. The correction appears to be needed due to typographical errors at the United States Patent Office.. No charge is required for this petition.

Regarding the Title

Please correct the title of the invention so that "transferring" is spelled correctly and should read -- METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE --.

Regarding the Priority of the Application

The filing receipt incorrectly indicates that there is a "FOREIGN/PCT APPLICATION-U.S. ARMY".

Please correct the filing receipt to indicate that priority is claimed under 35 U.S.C. § 119(e) based on provisional application No. 60/004,510 filed 09/29/1995.

A copy of the incorrect FILING RECEIPT is enclosed as Exhibit A.

Applicants request an amended Filing Receipt be created and forwarded to Applicants' attorneys at the earliest possible date.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

Date: June 6, 1996

Steven R. Greenfield
Reg. No. 38,166

Jenkens & Gilchrist, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202
Tel: (214) 855-4789
Fax: (214) 855-4300

PTO-103X
(Rev. 8-95)

36 MAIL ROOM JUN 10 1996 TRADEMARK OFF.

FILING RECEIPT

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

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTORNEY DOCKET NO.	DRWGS	TOT CL	IND CL
08/595,014	01/31/96	2514	$1,134.00	20661/438	8	28	4

RECEIVED
JUL 24 1996
GROUP 2500

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

INTELLECTUAL PROPERTY
MAY 31 1996
JENKENS & GILCHRIST

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Application Processing Division's Customer Correction Branch within 10 days of receipt. Please provide a copy of the Filing Receipt with the changes noted thereon.**

Applicant(s)

STEPHEN M. CURRY, DALLAS, TX; DONALD W. LOOMIS, COPPELL, TX; CHRISTOPHER W. FOX, DALLAS, TX.

FOREIGN/PCT APPLICATIONS-U.S. ARMY 60/004510 09/29/95

FOREIGN FILING LICENSE GRANTED 05/18/96

TITLE

METHOD, APPARATUS, AND SYSTEM FOR TRANSFERING UNITS OF VALUE

PRELIMINARY CLASS: 235

* DOCKETED

Int: JN DT: 5/31

Due:

Action ______ Due Date: ______

Reg. Corrected Filing Receipt 6/10/96

Status-Office Action? 7/31/96

Complete: Filing Receipt 5/31/96

EXHIBIT A

(see reverse)

#5/Status 2202
Letter
11/21/96

MAIL ROOM
OCT 29 1996
62
PAT. & TRADEMARK OFF.

PATENT
Attorney Docket No. 20661-00438

RECEIVED
NOV 13 1996
GROUP 2200

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

STEPHEN M. CURRY et al.

Serial No.	08/595,014	Examiner:	UNKNOWN
Filed:	January 31, 1996	Group No.:	UNKNOWN
For:	METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE		

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

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner For Patents, Washington, D.C. 20231 on 10-24-96

Carol Marsteller
Signature

Dear Sir:

STATUS INQUIRY

1. More than 6 months have passed since the filing of this Patent Application regarding the above-referenced patent application and we have not received an Office Action.

2. Kindly advise the undersigned of the present status of this application, by checking the appropriate box on the next page. A stamped return-addressed envelope is provided.

Respectfully submitted,

Steven R. Greenfield
Reg. No. 38,166

Dated: Oct 24, 1996

Jenkens & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
214/855-4789

IPDAL:99734.1 20661-00438

MAIL ROOM
62
OCT
29
1996
PAT. & TRADEMARK OFF.

PATENT
Attorney Docket No. 20661-00438

STATUS INQUIRY REPLY

RECEIVED
NOV 1 3 1996
GROUP 2200

APPLICATION TITLE: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

INVENTOR: STEPHEN M. CURRY et al.

Docket: 20661-00438

Filed: January 31, 1996

APPLICATION SERIAL NO. 08/595,014 IS CURRENTLY

ASSIGNED TO GROUP UNKNOWN AND AWAITS:

□ ACTION BY THE EXAMINER (name: ______)

□ APPLICANT'S RESPONSE TO THE OFFICE ACTION MAILED ______

IPDAL:99734.1 20661-00438

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.
08/595,014	01/31/96	CURRY	S	20661/438

22M2/1126

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

EXAMINER	
GREGORY, B	
ART UNIT	PAPER NUMBER
2202	#6

DATE MAILED: 11/26/96

Please find below a communication from the EXAMINER in charge of this application.

Commissioner of Patents

PTOL-90 (Rev. 6/84)

1 - PATENT APPLICATION FILE COPY

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

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/595,014	01/31/96	CURRY	20661/438

22M2/1126

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

EXAMINER	
GREGORY, B	
ART UNIT	PAPER NUMBER
2202	

DATE MAILED: 11/26/96

This is a communication from the EXAMINER in charge of your application
Commissioner of Patents and Trademarks

In response to the Status Inquiry that was received on October 29, 1996, it appears that 08/595,014 will not receive a First Office Action until sometime in the Spring of 1997.

Bernard E. Gregory

BERNARD E. GREGORY
PRIMARY EXAMINER
GROUP 2200

TEL,1(703) 306-4153
FAX! (703) 306-4195

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.
08/595,014	01/31/96	CURRY	S 206617438

22M2/0721

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

EXAMINER	
WHITE, C	
ART UNIT	**PAPER NUMBER**
2202	7

DATE MAILED: 07/21/97

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 1 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) 1-28 is/are pending in the application.

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

☐ Claim(s) ______ is/are allowed.

☐ Claim(s) ______ is/are rejected.

☐ Claim(s) ______ is/are objected to.

☒ Claims 1-28 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 --

PTOL-326 (Rev. 10/96)

★ U.S. GPO: 1996-409-290/40029

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 method for adding a monetary equivalent to electronic equipment, classified in class 380, subclass 24.

   II. Claims 16-28, drawn to a method for receiving and transmitting encrypted data, classified in class 380, subclass 24.

2. Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention II has separate utility such as a method for receiving and transmitting encrypted data that performs the same functions independent of adding a monetary equivalent to electronic equipment. See MPEP § 806.05(d).

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. A telephone call was made to Stephen Greenfield on May 7, 1997, to request an oral election to the above restriction requirement, but did not result in an election being made.

5. Applicant is advised that the response to this requirement to be complete must include an election of the invention to be examined even though the requirement be traversed (37 CFR 1.143).

6. 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).

Conclusion

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.

Carmen White

Thomas H. Tarcza

THOMAS H. TARCZA
SUPERVISORY PATENT EXAMINER
GROUP 2200

OIPE
SEP - 8 1997
JCS
PATENT & TRADEMARK OFFICE

GP 2202 $

PATENT APPLICATION
DOCKET NO.: 20661/438

8

Req. Ext. of Time Grtd 1 mo. Cofer 9-24-97

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: STEVEN R. CURRY ET AL.	§	Examiner: WHITE, C.
Serial No.: 08/595,014	§	Art Unit: 2202
Filed: JANUARY 31, 1996	§	

Title: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

To Assistant Commissioner for Patents
Washington DC 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. EM492664013US
Date of Deposit: 9/8/97
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: CAROL MARSTALLER
Carol Marstaller
Signature

TRANSMITTAL LETTER

Dear Sir:

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

Transmitted herewith in the above-identified application are:

1) Transmittal letter (in duplicate);

2) Election in response to restriction requirement made in the Official Action mailed on July 21, 1997; and

RECEIVED
SEP 23 1997
GROUP 2[illegible]

PATENT APPLICATION
DOCKET NO.: 20661/438

3) Acknowledgment postcard.

____ No additional fee is required.

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

	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST # PREVIOUSLY PAID FOR		PRESENT EXTRA	SMALL ENTITY RATE			LARGE ENTITY RATE		
TOTAL CLAIMS	28	-	20 (at least 20)	=	0 (at least 0)	x11	=	OR	x22	=	$ 0
INDEP. CLAIMS	4	-	8 (at least 3)	=	____ (at least 0)	x39	=	OR	x78	=	$ 0
FIRST PRESENTATION OF PROPER MULTIPLE DEPENDENT CLAIMS (leave blank if this is a reissue appln)						+120	=	OR	+240	=	$____

FEE FOR CLAIM AMENDMENTS $ 0

____ IDS ATTACHED REQUIRES OFFICIAL FEE - ADD $220 (RULE 1.97(c)) OR $130 (RULE 1.97(d) PETITION) $ 0

____ Assignment Recordation Fee ($40) $____

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

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

	Small Entity	Large Entity
One Month	____ $ 55	_X_ $110
Two Months	____ $185	____ $380
Three Months	____ $435	____ $900
Four Months	____ $680	____ $1400

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.

TOTAL FEES $ 110.00

____ 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 $110.00 to cover the TOTAL FEE. This sheet is attached in duplicate.

CHARGE STATEMENT: The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and may be required under 37 CFR 1.16-1.18 (missing or insufficiencies only) now or hereafter relative to this application and for the resulting Official Document under 37 CFR 1.20, OR credit any overpayment to **Dallas Semiconductor Corporation Deposit Account No. 04-0031**, for which purpose a duplicate copy of this sheet is attached[1].

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: Sept 8, 1997

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

[1] 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.

9A

OIPE
SEP - 8 1997
JC69
PATENT & TRADEMARK OFFICE

Patent Application
Docket No. 20661-00438

Cofer
9-24-97

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:

STEPHEN M. CURRY ET AL. §
§
Examiner: WHITE, C.
Serial No.: 08/595,014 §
§
Group Art Unit: 2202
Filed: JANUARY 31, 1996 §
§

For: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

RECEIVED
SEP 25 1997
GROUP 2200

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. EM492664013US
Date of Deposit: September 8, 1997
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: CAROL MARSTALLER
Carol P. Marstaller
Signature

Dear Sir:

RESPONSE TO RESTRICTION REQUIREMENT

Responsive to the Official Action mailed on July 21, 1997, reconsideration and allowance of the present application are respectfully requested and believed to be appropriate in view of the following remarks:

In the Claims:

Please cancel claims 16-28 without prejudice.

Regarding Section 121 Restriction Requirement

Applicants respectfully request to select Group I, claims 1-15 for examination.

Applicants have canceled the remaining claims 16-28.

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

In view of the above, it is believed that Applicants have been fully responsive to the Restriction Requirement and 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: Sept 8, 1997

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

O I P E
70110
SEP 12 1997
PATENT & TRADEMARK OFFICE

~~8~~ 2

Patent Application
Attorney Docket No. 20661-00438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
NOV 17 1997
GROUP 2500

In re Application of

STEPHEN M. CURRY et al.

Serial No.	08/595,014	Examiner:	Not Yet Known
Filed:	January 31, 1996	Group No.:	2514
For:	METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE		

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

Dear Sir:

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 June 6, 1996

Carol Marsteller
Signature

RECEIVED
NOV 19 1997
GROUP 2200

PETITION TO CORRECT FILING RECEIPT

Dear Sir:

Applicants hereby request for the Filing Receipt to be correct to 1) correct a misspelling in the title of the application; and 2) correct the priority statement. The correction appears to be needed due to typographical errors at the United States Patent Office. No charge is required for this petition.

Regarding the Title

Please correct the title of the invention so that "transferring" is spelled correctly and should read -- METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE --.

Regarding the Priority of the Application

The filing receipt incorrectly indicates that there is a "FOREIGN/PCT APPLICATION-U.S. ARMY".

Please correct the filing receipt to indicate that priority is claimed under 35 U.S.C. § 119(e) based on provisional application No. 60/004,510 filed 09/29/1995.

A copy of the incorrect FILING RECEIPT is enclosed as Exhibit A.

Applicants request an amended Filing Receipt be created and forwarded to Applicants' attorneys at the earliest possible date.

Respectfully submitted,

JENKENS & GILCHRIST, P.C.

Date: June 6, 1996

Steven R. Greenfield
Reg. No. 38,166

Jenkens & Gilchrist, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202
Tel: (214) 855-4789
Fax: (214) 855-4300

PTO-103X
(Rev. 8-95)

FILING RECEIPT

O.I.P.E.
70110
SEP 12 1997
PATENT & TRADEMARK

UNITED STATE. ARTMENT OF COMMERCE
Patent and Trade..ark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTORNEY DOCKET NO.	DRWGS	TOT CL	IND CL
08/595,014	01/31/96	2514	$1,134.00	20661/438	8	28	4

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

RECEIVED
NOV 17 1997
GROUP 2500

INTELLECTUAL PROPERTY
MAY 31 1996
JENKENS & GILCHRIST

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Application Processing Division's Customer Correction Branch within 10 days of receipt. Please provide a copy of the Filing Receipt with the changes noted thereon.

Applicant(s)

STEPHEN M. CURRY, DALLAS, TX; DONALD W. LOOMIS, COPPELL, TX; CHRISTOPHER W. FOX, DALLAS, TX.

FOREIGN/PCT APPLICATIONS-U.S. ARMY 60/004510 09/29/95

FOREIGN FILING LICENSE GRANTED 05/18/96

TITLE

METHOD, APPARATUS, AND SYSTEM FOR TRANSFERING UNITS OF VALUE

PRELIMINARY CLASS: 235

*DOCKETED
Int: JW DT: 5/31
Due:
Action ______ Due Date: ______
Req. Corrected Filing Receipt 6/10/96
Status-Office Action? 7/31/96
Complete: Filing Receipt 5/31/96

EXHIBIT A

(see reverse)

Receipt
Cust Clk

O I P E
70110
SEP 12 1997
PATENT & TRADEMARK OFFICE

RECEIVED
[illegible] 19 [illegible]
GROUP 2200

PATENT
Attorney Docket No. 20661-00438

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

STEPHEN M. CURRY et al.

Serial No.	08/595,014	Examiner:	WHITE, C.
Filed:	January 31, 1996	Group No.:	2202
For:	METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE		

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

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

on 9-8-97

Carol Naistaller
Signature

Dear Sir:

STATUS INQUIRY

1. More than 14 months have passed since the filing of a Petition to Correct Filing Receipt regarding the above-referenced patent application and we have not received a corrected filing receipt.

2. Kindly advise the undersigned of the present status of this application, by checking the appropriate box on the next page. A stamped return-addressed envelope is provided.

Respectfully submitted,

Steven R. Greenfield

Steven R. Greenfield
Reg. No. 38,166

Dated: Sept 8, 1997

Jenkens & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
214/855-4789

PATENT
Attorney Docket No. 20661-00438

STATUS INQUIRY REPLY

APPLICATION TITLE: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

INVENTOR: STEPHEN M. CURRY et al.

Docket: 20661-00438

Filed: January 31, 1996

APPLICATION SERIAL NO. 08/595,014 IS CURRENTLY

ASSIGNED TO GROUP 2202 AND AWAITS:

☒ ACTION BY PTO REGARDING CORRECTED FILING RECEIPT ____________

□ ACTION BY THE EXAMINER (name: ________________________________)

□ APPLICANT'S RESPONSE TO THE OFFICE ACTION MAILED __________

IPDAL:116405.1 20661-00438

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 2134 DALLAS, TX

POSTAGE WILL BE PAID BY ADDRESSEE

Jenkens & Gilchrist
A PROFESSIONAL CORPORATION
1445 ROSS AVE STE 3200
DALLAS TX 75202-9809

ATT: Steve Greenfield
C/M 20661-429

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.
08/595,014	01/31/96	CURRY	S 20661/438

EXAMINER
WHYTE, C

22M2/1002

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

ART UNIT	PAPER NUMBER
2202	10/B

DATE MAILED:
10/02/97

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

NOTICE OF ALLOWABILITY

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to papers filed on September 8, 1997.

☒ The allowed claim(s) is/are 1-15.

☐ The drawings filed on ______________________ are acceptable.

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

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

☐ received.

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

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

*Certified copies not received: ______________________.

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

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

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

☒ Applicant MUST submit NEW FORMAL DRAWINGS

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

☐ including changes required by the Notice of Draftperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. _____.

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

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

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

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

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

Attachment(s)

☒ Notice of References Cited, PTO-892

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

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

☐ Notice of Informal Patent Application, PTO-152

☐ Interview Summary, PTO-413

☒ Examiner's Amendment/Comment

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

☒ Examiner's Statement of Reasons for Allowance

★ U.S. GPO: 1996-404-496/40507

Serial Number: 08/595,014

Art Unit: 2202

DETAILED ACTION

Drawings

1. The application having been allowed, formal drawings are required in response to this Office action.

EXAMINER'S AMENDMENT

2. 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 CFR 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 Greenfield on September 30, 1997.

3. The application has been amended as follows:

In claim 1, line 10, "paket" has been changed to --packet --.

In claim 1, line 18, "decypted" has been changed to --decrypted --.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance:

Neither Herring, White or Davis discloses communicating a random number from the module to the electronic device, combining the random number and the amount requested thereby creating a first data packet in the electronic device, creating a signed certificate in the electronic device and combining a first random number, number of units to be metered and a module identifier. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. 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

September 30, 1997

THOMAS H. TARCZA
SUPERVISORY PATENT EXAMINER
GROUP 2200

TO SEPAI TTOM E.
O TOP AND BO. RBON

FORM PTO-892 (REV. 2-92)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

NOTICE OF REFERENCES CITED	SERIAL NO. 08/595,014	GROUP ART UNIT 2202	ATTACHMENT TO PAPER NUMBER
	APPLICANT(S) Steven M. Curry et al		

U.S. PATENT DOCUMENTS

*		DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
X	A	4630201	12/16/86	White	364	408	
X	B	5077792	12/31/91	Herring	380	24	
X	C	5577121	11/19/96	Davis et al	380	24	6/9/94
	D						
	E						
	F						
	G						
	H						
	I						
	J						
	K						

FOREIGN PATENT DOCUMENTS

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

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

R	
S	
T	
U	

EXAMINER Carmen D. White	DATE 9/30/97

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

File History Content Report

The following content is missing from the original file history record obtained from the United States Patent and Trademark Office. No additional information is available.

Document Date - 1997-10-02

Document Title - Notice of Formal Drawings Required

This page is not part of the official USPTO record. It has been determined that content identified on this document is missing from the original file history record.

BEST COPY

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

22M2/1002

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

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
08/595,014	01/31/96	015	WHITE, C	2202	10/02/97

First Named Applicant CURRY, STEPHEN M.

TITLE OF INVENTION METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 20661/438	380-024.000	S70	UTILITY	NO	$1320.00	01/02/98

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)

Jenkens & Gilchrist
A PROFESSIONAL CORPORATION

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

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

AUSTIN, TEXAS
(512) 499-3800
HOUSTON, TEXAS
(713) 951-3300
SAN ANTONIO, TEXAS
(210) 308-3100
WASHINGTON, D.C.
(202) 326-1500

RECEIVED
Publishing Division
JAN 06 1998
04

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

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

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

on DECEMBER 31, 1997

Carol Marstaller
Signature

Re:	Applicant(s):	Stephen M. Curry et al
	Serial No.:	08/595,014
	Filed:	January 31, 1996
	Batch No.	S70
	NOA Mailed:	October 2, 1997
	For:	Method, Apparatus, and System for Transferring Units of Value
	Docket No.:	20661-438

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 Draftsman
3. 8 Sheets of Formal Drawings

Please address all communications related to this to:

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

In the event there is an under or over payment, please debit or credit our Deposit Account #10-0447. This letter is being filed in duplicate to facilitate processing.

Respectfully submitted,

Steven R. Greenfield

Steven R. Greenfield
Registration No. 38,166

Date DECEMBER 31, 1997

Jenkens & Gilchrist
A PROFESSIONAL CORPORATION

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

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

AUSTIN, TEXAS
(512) 499-3800

HOUSTON, TEXAS
(713) 951-3300

SAN ANTONIO, TEXAS
(210) 308-3100

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

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

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

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

on DECEMBER 31, 1997 ....

Carol Marstaller
Signature

Re:	Applicant(s):	Stephen M. Curry et al
	Serial No.:	08/595,014
	Filed:	January 31, 1996
	Batch No.	S70
	NOA Mailed:	October 2, 1997
	For:	Method, Apparatus, and System for Transferring Units of Value
	Docket No.:	20661-438

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 Draftsman
3. 8 Sheets of Formal Drawings

Please address all communications related to this to:

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

In the event there is an under or over payment, please debit or credit our Deposit Account #10-0447. This letter is being filed in duplicate to facilitate processing.

Respectfully submitted,

Date DECEMBER 31, 1997

Steven R. Greenfield
Registration No. 38,166

IPDAL:147427.1 20661-00438

NW

PART B—ISSUE FEE TRANSMITTAL

Complete and mail this form, together with app.. ıle fees, to: **Box ISSUE FEE**
Assistant Commissioner for Patents
Washington, D.C. 20231

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

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

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

22M2 RECEIVED
Publishing Division
JAN 06 1998
04

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.

CAROL MARSTALLER (Depositor's name)

Carol Marstaller (Signature)

12-31-97 (Date)

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
08/595,014	01/31/96	015	WHITE, C	2202	10/02/97

First Named Applicant CURRY, STEPHEN M.

TITLE OF INVENTION METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 20661/438	380-024.000	S70	UTILITY	NO	$1320.00	01/02/98

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

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47) attached.

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 JENKENS + GILCHRIST
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 appropiate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a subsitiute for filing an assignment.

(A) NAME OF ASSIGNEE DALLAS SEMICONDUCTOR CORPORATION

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

Please check the appropriate assignee category indicated below (will not be printed on the patent)
□ individual ☒ corporation or other private group entity □ government

4a. The following fees are enclosed (make check payable to Commissioner of Patents and Trademarks):
☐ Issue Fee
☐ Advance Order - # of Copies ________

4b. The following fees or deficiency in these fees should be charged to:
DEPOSIT ACCOUNT NUMBER 04-0031
(ENCLOSE AN EXTRA COPY OF THIS FORM)
☒ Issue Fee
☒ Advance Order - # of Copies 10

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

(Authorized Signature) (Date) Dec 29, 1997

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.

01/28/1998 CASHBY 00000020 DAH:040031 08595014
01 FC:142 1320.00 CH
02 FC:561 30.00 CH

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

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

TRANSMIT THIS FORM WITH FEE

PTOL-85B (REV.10-96) Approved for use through 06/30/99. OMB 0651-0033

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

0 380/2, E

DOCKET NO.: 20661-438 4100 PATENT APPLICATION

Issue Batch No.: S70
Date of Notice
of Allowance : October 2, 1997
Serial No. : 08/595,014

RECEIVED
Publishing Division
JAN 06 1998
04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

Serial No.: 08/595,014 Group No.: 2202

Filed: January 31, 1996 Examiner: White, C.

For: **Method, Apparatus, and System for Transferring Units of Value**

BOX ISSUE FEE
Commissioner of Patents
and Trademarks
Washington, D.C. 20231

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

on DECEMBER 31, 1997

Signature

ATTN: Official Draftsman

Sir:

TRANSMITTAL LETTER TO OFFICIAL DRAFTSMAN

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

The enclosed drawings each bear the Issue Batch No., the date of the Notice of Allowance and Serial No. of the application on their reverse side. Please charge any comparison fees to our Deposit Account No. 10-0447.

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

Date: DECEMBER 31, 1997

Steven R. Greenfield
Registration No. 38,166

Jenkens & Gilchrist, P.C.
A Professional Corporation
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
214/855-4789

APPROVED O.G. FIG.
BY CLASS SUBCLASS
DRAFTSMAN

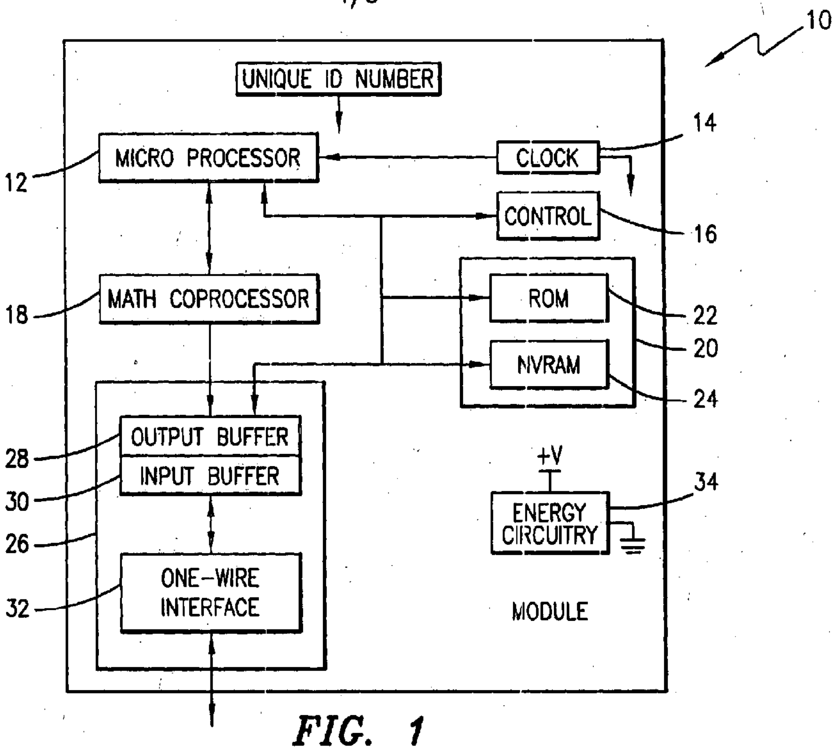


FIG. 1

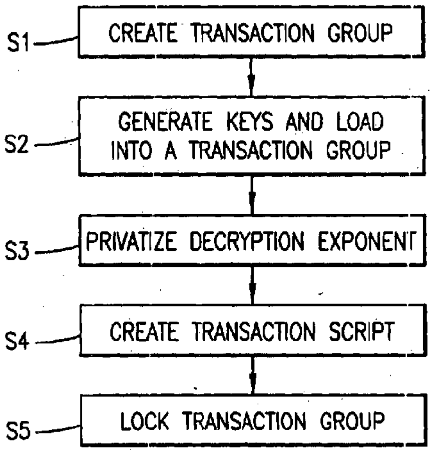

S1
CREATE TRANSACTION GROUP
S2
GENERATE KEYS AND LOAD INTO A TRANSACTION GROUP
S3
PRIVATIZE DECRYPTION EXPONENT
S4
CREATE TRANSACTION SCRIPT
S5
LOCK TRANSACTION GROUP

FIG. 2

APPROVED | O.G. FIG.
BY | CLASS | SUBCLASS
DRAFTSMAN

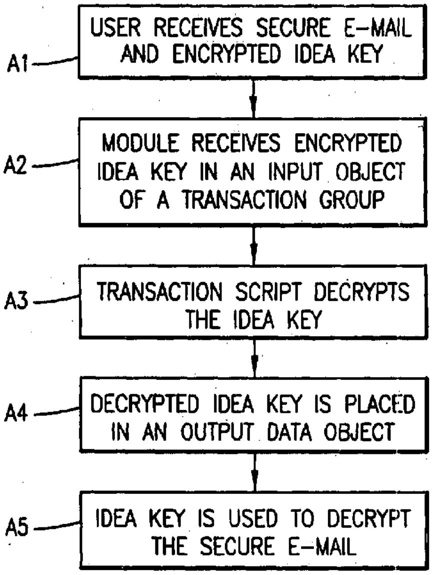

A1
USER RECEIVES SECURE E-MAIL AND ENCRYPTED IDEA KEY
A2
MODULE RECEIVES ENCRYPTED IDEA KEY IN AN INPUT OBJECT OF A TRANSACTION GROUP
A3
TRANSACTION SCRIPT DECRYPTS THE IDEA KEY
A4
DECRYPTED IDEA KEY IS PLACED IN AN OUTPUT DATA OBJECT
A5
IDEA KEY IS USED TO DECRYPT THE SECURE E-MAIL

FIG. 3

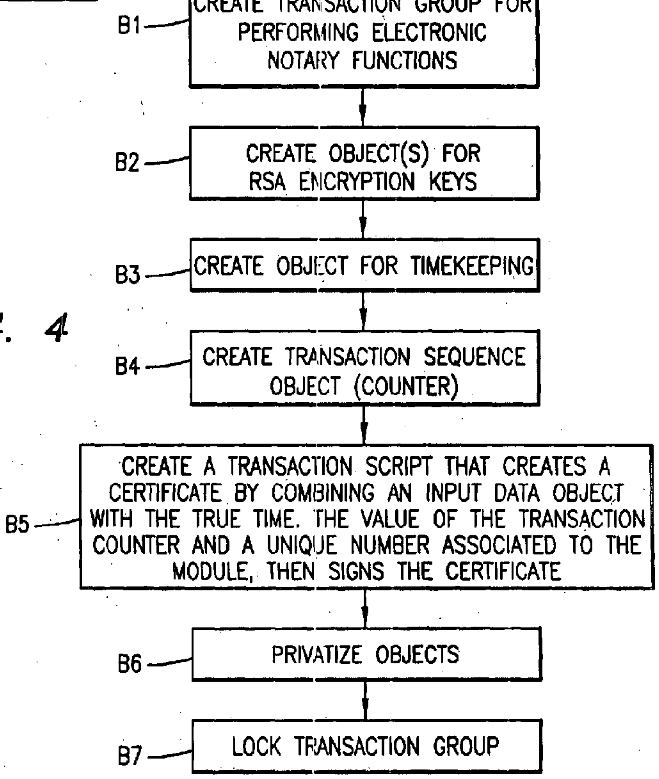

B1
CREATE TRANSACTION GROUP FOR PERFORMING ELECTRONIC NOTARY FUNCTIONS
B2
CREATE OBJECT(S) FOR RSA ENCRYPTION KEYS
B3
CREATE OBJECT FOR TIMEKEEPING
B4
CREATE TRANSACTION SEQUENCE OBJECT (COUNTER)
B5
CREATE A TRANSACTION SCRIPT THAT CREATES A CERTIFICATE BY COMBINING AN INPUT DATA OBJECT WITH THE TRUE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

FIG. 4

APPROVED BY DRAFTSMAN | O.G. FIG. CLASS SUBCLASS

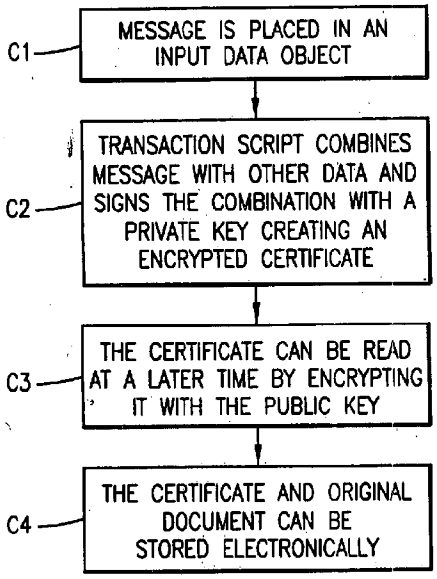

C1
MESSAGE IS PLACED IN AN INPUT DATA OBJECT
C2
TRANSACTION SCRIPT COMBINES MESSAGE WITH OTHER DATA AND SIGNS THE COMBINATION WITH A PRIVATE KEY CREATING AN ENCRYPTED CERTIFICATE
C3
THE CERTIFICATE CAN BE READ AT A LATER TIME BY ENCRYPTING IT WITH THE PUBLIC KEY
C4
THE CERTIFICATE AND ORIGINAL DOCUMENT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

FIG. 5

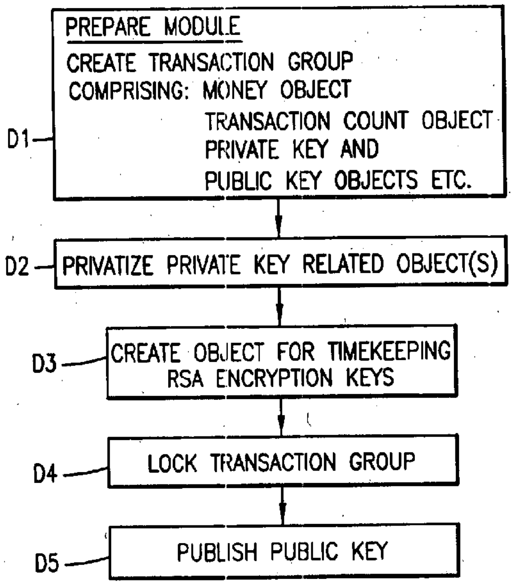


FIG. 6

APPROVED BY DRAFTSMAN | O.G. FIG. | CLASS | SUBCLASS

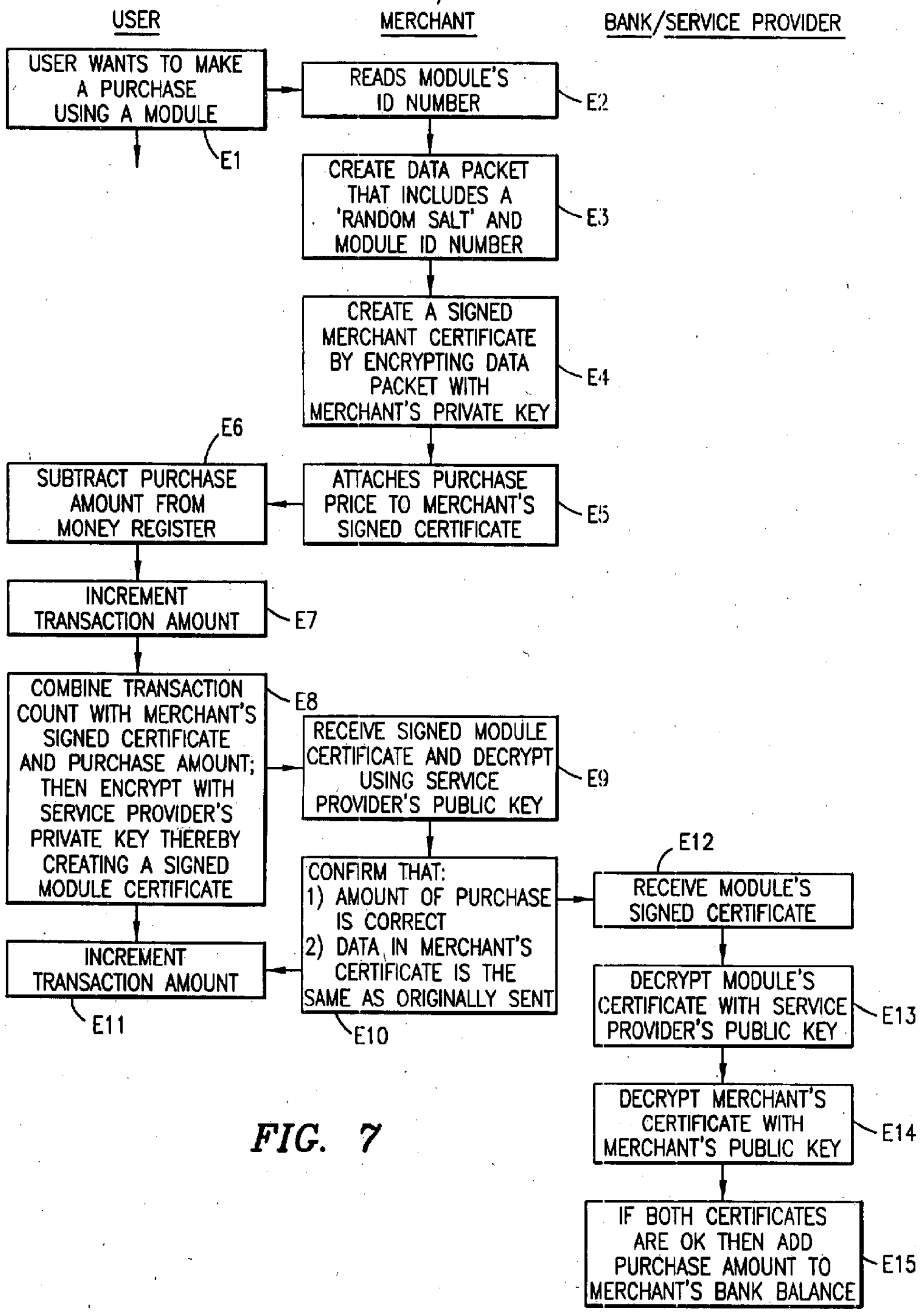

USER
MERCHANT
BANK/SERVICE PROVIDER
USER WANTS TO MAKE A PURCHASE USING A MODULE
E1
READS MODULE'S ID NUMBER
E2
CREATE DATA PACKET THAT INCLUDES A 'RANDOM SALT' AND MODULE ID NUMBER
E3
CREATE A SIGNED MERCHANT CERTIFICATE BY ENCRYPTING DATA PACKET WITH MERCHANT'S PRIVATE KEY
E4
E6
SUBTRACT PURCHASE AMOUNT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

FIG. 7

APPROVED BY DRAFTSMAN | O.G. FIG. | CLASS | SUBCLASS

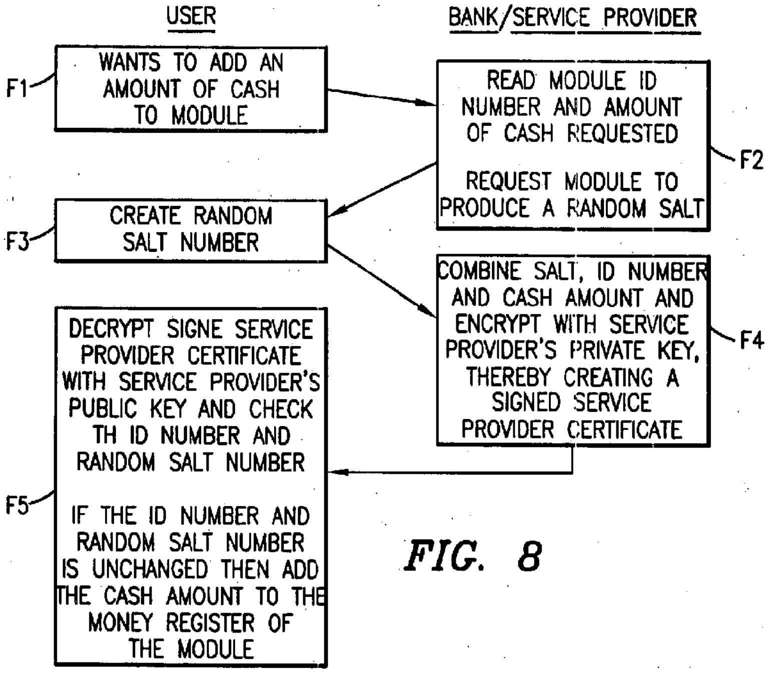

USER
BANK/SERVICE PROVIDER
F1
WANTS TO ADD AN AMOUNT OF CASH TO MODULE
READ MODULE ID NUMBER AND AMOUNT OF CASH REQUESTED
REQUEST MODULE TO PRODUCE A RANDOM SALT
F2
F3
CREATE RANDOM SALT NUMBER
COMBINE SALT, ID NUMBER AND CASH AMOUNT AND ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY, THEREBY CREATING A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

FIG. 8

EXAMPLE OF
TRANSFER FROM USER'S MODULE TO MERCHANT'S MODULE

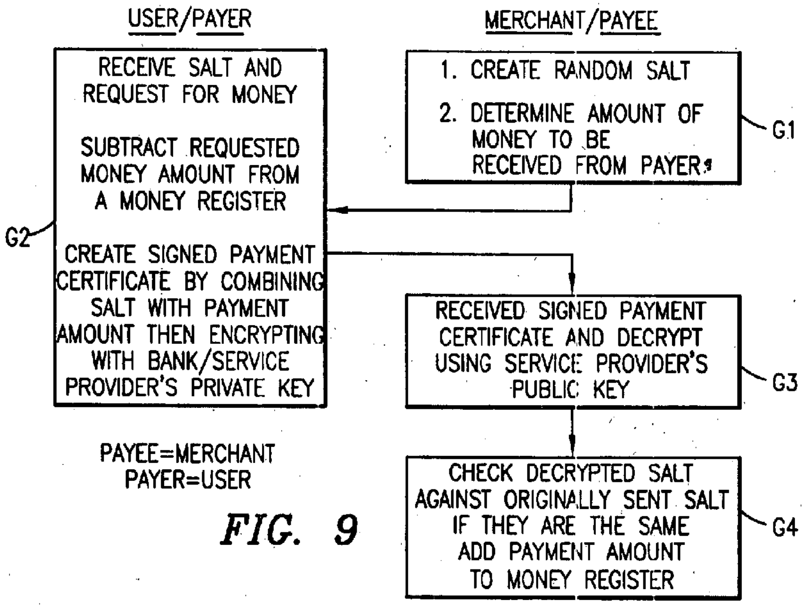

USER/PAYER
MERCHANT/PAYEE
1. CREATE RANDOM SALT
2. DETERMINE AMOUNT OF MONEY TO BE RECEIVED FROM PAYER
G1
RECEIVE SALT AND REQUEST FOR MONEY
SUBTRACT REQUESTED MONEY AMOUNT FROM A MONEY REGISTER
CREATE SIGNED PAYMENT CERTIFICATE BY COMBINING SALT WITH PAYMENT AMOUNT THEN ENCRYPTING WITH BANK/SERVICE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

FIG. 9

APPROVED BY DRAFTSMAN | O.G. FIG. | CLASS | SUBCLASS

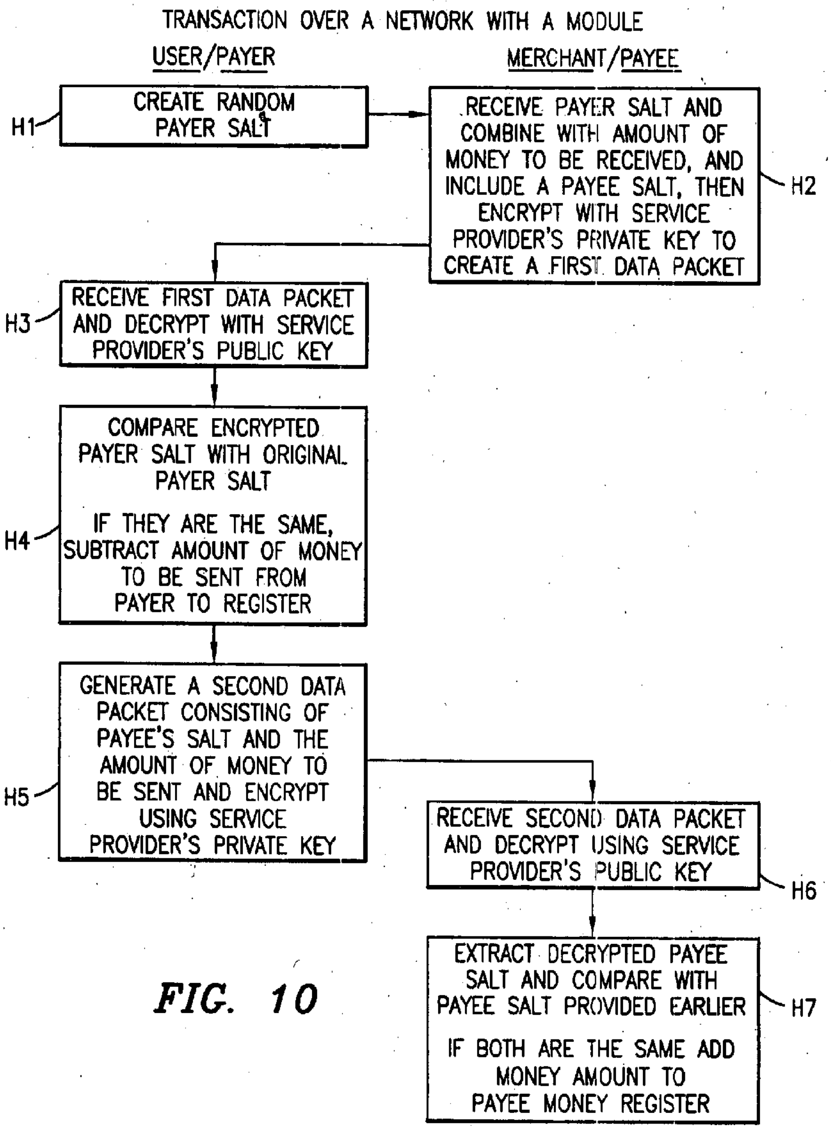

TRANSACTION OVER A NETWORK WITH A MODULE
USER/PAYER
MERCHANT/PAYEE
CREATE RANDOM PAYER SALT
H1
RECEIVE PAYER SALT AND COMBINE WITH AMOUNT OF MONEY TO BE RECEIVED, AND INCLUDE A PAYEE SALT, THEN ENCRYPT WITH SERVICE PROVIDER'S PRIVATE KEY TO CREATE A FIRST DATA PACKET
H2
RECEIVE FIRST DATA PACKET AND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

FIG. 10

APPROVED BY DRAFTSMAN | O.G. FIG. | CLASS | SUBCLASS

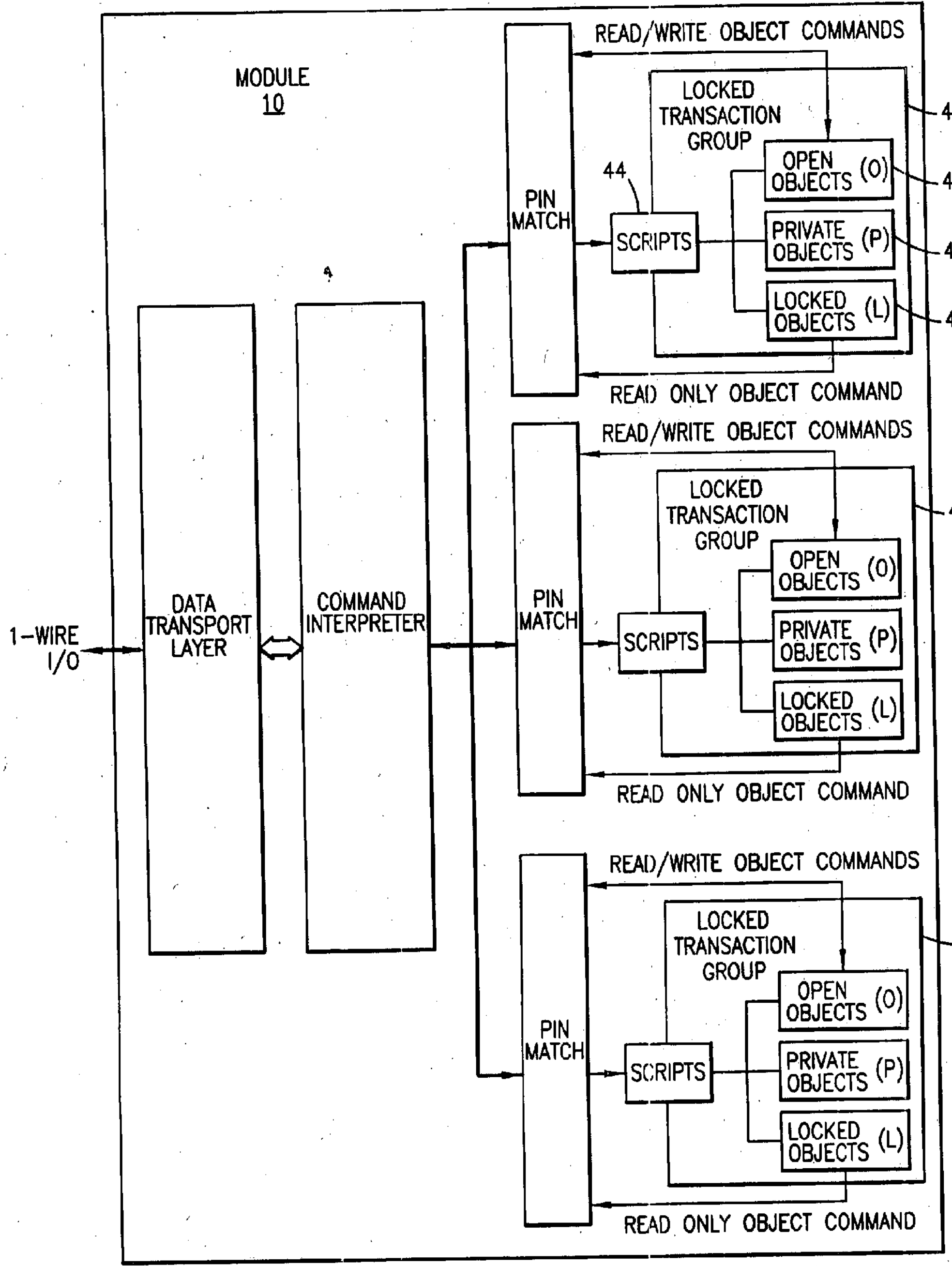


FIG. 11

APPROVED BY DRAFTSMAN | O.G. FIG. | CLASS | SUBCLASS

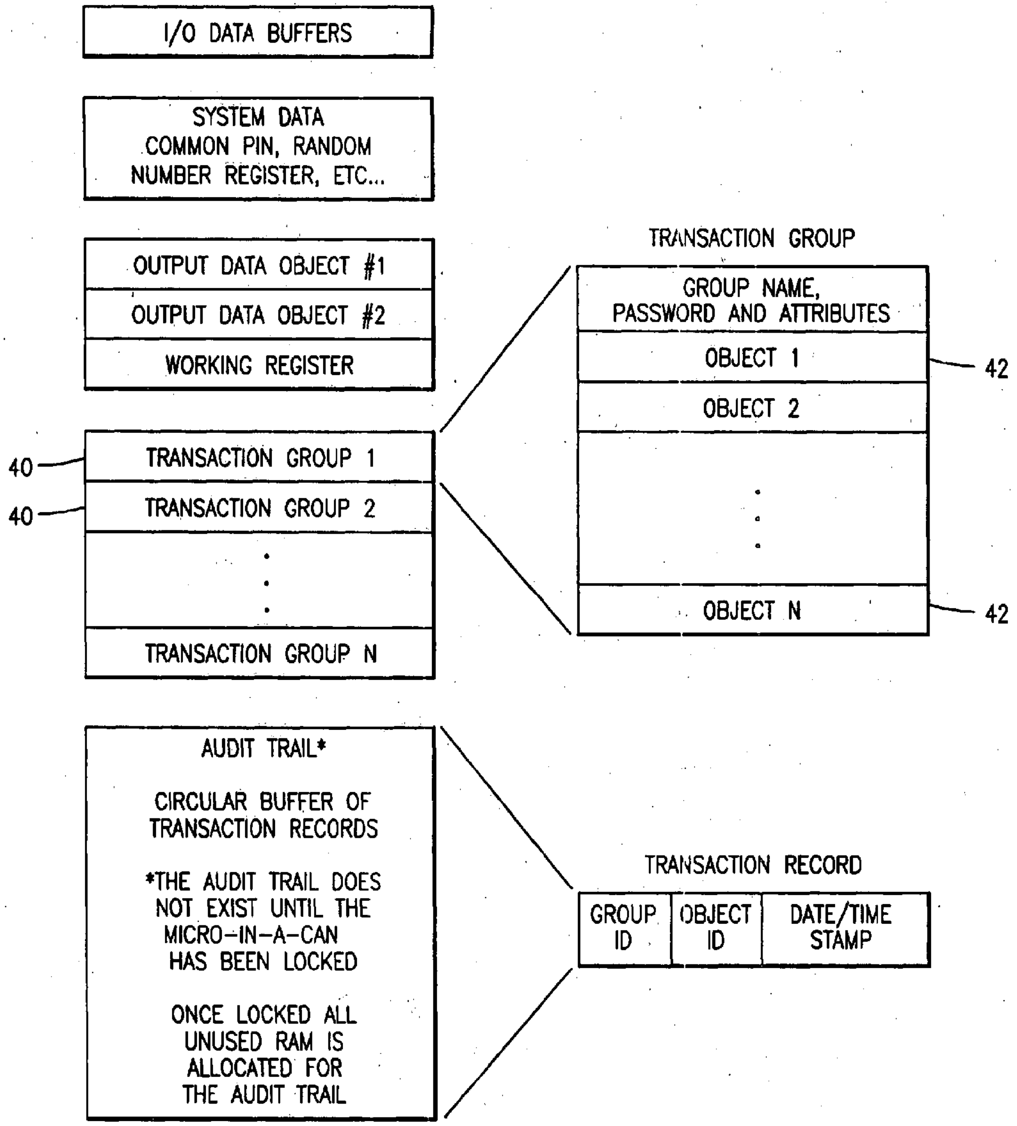
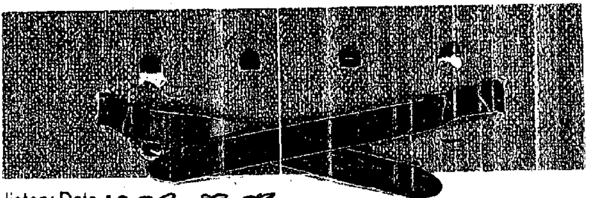


FIG. 12

Serial No. 08/595,014
Filed: January 31, 1996
Batch No. S70
Notice of Allowance Date: October 2, 1997

RECEIVED
Publications Division
JAN 06 1998
04



Transaction History Date 1998-09-08

Date information retrieved from USPTO Patent
Application Information Retrieval (PAIR)
system records at www.uspto.gov

PTO UTILITY GRANT

Paper Number 13

The United States of America

The Commissioner of Patents and Trademarks

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this

United States Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America for the term set forth below, subject to the payment of maintenance fees as provided by law.

If this application was filed prior to June 8, 1995, the term of this patent is the longer of seventeen years from the date of grant of this patent or twenty years from the earliest effective U.S. filing date of the application, subject to any statutory extension.

If this application was filed on or after June 8, 1995, the term of this patent is twenty years from the U.S. filing date, subject to an statutory extension. If the application contains a specific reference to an earlier filed application or applications under 35 U.S.C. 120, 121 or 365(c), the term of the patent is twenty years from the date on which the earliest application was filed, subject to any statutory extension.

Bruce Lehman

Commissioner of Patents and Trademarks

Sandra L Morton

Attest

Form PTO-1584 (Rev. 2/97)

(RIGHT INSIDE)

OIPE JC57
JAN 08 1999
PATENT & TRADEMARK OFFICE

Jenkens & Gilchrist
A PROFESSIONAL CORPORATION

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

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

C OF C
U9
#14

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 Greenfield
(214) 855-4789

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

CERTIFICATE
JAN 19 1999
OF CORRECTION

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 1/5/99
Signature Carol A. Marstaller
Printed Name CAROL MARSTALLER

Re: Patent No.: 5,805,702
Issued: Sep. 8, 1998
Title: METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE
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:

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

In the event there is an under- or over-payment, please debit or credit our Deposit Account #10-0447. This letter is being filed in duplicate to facilitate processing.

Very truly yours,

Steven R. Greenfield
Reg. No. 38,166

SRG/stm
encs.

OIPE JC57
JAN 0 8 1999
PATENT & TRADEMARK OFFICE

Jenkens & Gilchrist

A PROFESSIONAL CORPORATION

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

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

AUSTIN, TEXAS
(512) 499-3800

HOUSTON, TEXAS
(713) 951-3300

SAN ANTONIO, TEXAS
(210) 308-3100

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

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

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 1/5/99

Signature Carol Marstaller

Printed Name CAROL MARSTALLER

Re:	Patent No.:	5,805,702
	Issued:	Sep. 8, 1998
	Title:	METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE
	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:

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

In the event there is an under- or over-payment, please debit or credit our Deposit Account #10-0447. This letter is being filed in duplicate to facilitate processing.

Very truly yours,

Steven R. Greenfield
Reg. No. 38,166

SRG/stm
encs.

OIPE
JC57
JAN 08 1999
PATENT & TRADEMARK OFFICE

PATENT
Docket No. 27951-136USPT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Number:	5,805,702
Issued:	Sep. 8, 1998
Name of Patentee:	Curry et al.
Title of Invention:	METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE

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 1/5/99
Signature Carol Marstaller
Printed Name CAROL MARSTALLER

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

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

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

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

Patent	Application File
Column 25, line 20	Application, page 99, line 14

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:

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

Assignee: Dallas Semiconductor Corporation

Steven R. Greenfield
Assignee's Attorney
Reg. No. 38,166

/ X / Assignment recorded on
Reel/Frame 8095/0854 *et seq.*

/__/ Recordal of assignment attached

Staple
Here
Only !

PRINTER'S TRIM LINE

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	:	5,805,702
DATED	:	Sep. 8, 1998
INVENTOR(S)	:	Curry et al.

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

Column 25, line 20	Replace "(S)" With --(5)--

MAILING ADDRESS OF SENDER:

Steven Greenfield
1445 Ross Avenue
Suite 3200
Dallas, Texas 75202-2799

PATENT NO. 5,805,702

No. of add'l copies
@ 50¢ per page
1 of 1

20661-438

FORM PTO 1050 (Rev. 2-93)

BEST COPY

PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 1995

Application or Docket Number
595014

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE	FEE		RATE	FEE
BASIC FEE				375.00	OR		750.00
TOTAL CLAIMS	28 minus 20 =	* 8	x$11=		OR	x$22=	176
INDEPENDENT CLAIMS	4 minus 3 =	* 1	x39=		OR	x78=	78
MULTIPLE DEPENDENT CLAIM PRESENT			+125=		OR	+250=	
			TOTAL		OR	TOTAL	1004

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

CLAIMS AS AMENDED - PART II

A

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
	Total	* 15	Minus	** 28	= —	x$11=		OR	x$22=	
	Independent	* 2	Minus	*** 4	= —	x39=		OR	x78=	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+125=		OR	+250=	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
	Total	*	Minus	**	=	x$11=		OR	x$22=	
	Independent	*	Minus	***	=	x39=		OR	x78=	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+125=		OR	+250=	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT C		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
	Total	*	Minus	**	=	x$11=		OR	x$22=	
	Independent	*	Minus	***	=	x39=		OR	x78=	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM					+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.

FORM PTO-875
(Rev. 10/95)

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Form PTO 1130
(REV 2/94)

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

PACE DATA ENTRY CODING SHEET

1ST EXAMINER Tekalo	DATE 3/14/96
2ND EXAMINER 540	DATE 5/2/96

APPLICATION NUMBER	TYPE APPL	FILING DATE MONTH	DAY	YEAR	SPECIAL HANDLING	GROUP ART UNIT	CLASS	SHEETS OF DRAWING
08/595014	1	Ø1	31	96	Ø	2514	235	Ø8

TOTAL CLAIMS	INDEPENDENT CLAIMS	SMALL ENTITY?	FILING FEE	FOREIGN LICENSE	ATTORNEY DOCKET NUMBER
28	Ø4	Ø	1134	Y	20661/438

CONTINUITY DATA

CONT CODE	STATUS CODE	PARENT APPLICATION SERIAL NUMBER	PCT APPLICATION SERIAL NUMBER	PARENT PATENT NUMBER	PARENT FILING DATE MONTH	DAY	YEAR
			PCT/ /				
			PCT/ /				
			PCT/ /				
			PCT/ /				
			PCT/ /				

PCT/FOREIGN APPLICATION DATA

FOREIGN PRIORITY CLAIMED	COUNTRY CODE	PCT/FOREIGN APPLICATION SERIAL NUMBER	FOREIGN FILING DATE MONTH	DAY	YEAR
Y	USA	60/004510	Ø9	29	95

☆ U.S. GPO: 1995-401-429

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: 2011-11-09

Name of Report:

Number of Families: 1

Comments:

Table of Contents

1. **US5805702A** 19980908 DALLAS SEMICONDUCTOR US
Method, apparatus, and system for transferring units of value 12

Family1

18 records in the family, collapsed to 15 records.

AU702508B2 19990225

[no drawing available]

(ENG) Method, apparatus, system and firmware for secure transactions

Assignee: DALLAS SEMICONDUCTOR

Inventor(s): CURRY STEPHEN M ; LOOMIS DONALD W ; FOX CHRISTOPHER W

Application No: AU 7374596 A

Filing Date: 19960926

Issue/Publication Date: 19990225

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y; US 9615471 19960926 W W N;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Legal Status:

Date	+/-	Code	Description
20020502	(-)	MK14	PATENT CEASED SECTION 143(A) (ANNUAL FEES NOT PAID) OR EXPIRED

AU7374596A 19970417

(ENG) Method, apparatus, system and firmware for secure transactions

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR

Inventor(s): CURRY STEPHEN M ; LOOMIS DONALD W ; FOX CHRISTOPHER W

Application No: AU 7374596 D

Filing Date: 19960926

Issue/Publication Date: 19970417

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y; US 9615471 19960926 W W N;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Legal Status:

Date	+/-	Code	Description
20020502	(-)	MK14	PATENT CEASED SECTION 143(A) (ANNUAL FEES NOT PAID) OR EXPIRED

CA2232791A1 19970403

(ENG) METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): FOX CHRISTOPHER W US ; LOOMIS DONALD W US ; CURRY STEPHEN M US

Application No: CA 2232791 A

Filing Date: 19960926

Issue/Publication Date: 19970403

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Publication Language: ENG

Legal Status:

Date	+/-	Code	Description
20030403	(+)	AFNE	NATIONAL PHASE ENTRY Effective date: 19980323;
20030403	(+)	AFNE	NATIONAL PHASE ENTRY Effective date: 19980323;
20030403	(-)	FZDE	DEAD Effective date: 20020926;
20030403	(-)	FZDE	DEAD Effective date: 20020926;

CN1198233A 19981104

(ENG) Method, apparatus, system and firmware for secure transactions

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: CN 96197307 A

Filing Date: 19960926

Issue/Publication Date: 19981104

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Legal Status:

Date	+/-	Code	Description
19980400	()	C00	

EP1020821A3 20000802
EP1020821A2 20000719

(ENG) Method, apparatus, system and firmware for secure transactions

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: EP 00109707 A

Filing Date: 19960926

Issue/Publication Date: 20000802

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: EP 96935993 19960926 A 3 Y; US 451095 19950929 P Y; US 59498396 19960131 A Y;

Related Application(s): 96935993.4 0862769 19970403

IPC (International Class): G07F00710

Designated Countries:

Publication Language: ENG

Filing Language: ENG

Agent(s): BROOKES & MARTIN 00100141 High Holborn House 52/54 High Holborn London, WC1V 6SE GB

Date of Deferred Publication of Search Report:
--20000802

Legal Status:

Date	+/-	Code	Description
20000719	( )	AC	DIVISIONAL APPLICATION (ART. 76) OF: Corresponding patent document: 862769; Country code of corresponding patent document: EP;
20000719	(+)	AK	DESIGNATED CONTRACTING STATES: Kind code of corresponding patent document: A2; List of designated states: AT BE CH DE DK ES FI FR GB GR IE IT LI NL PT SE;
20000802	(+)	AK	DESIGNATED CONTRACTING STATES: Kind code of corresponding patent document: A3; List of designated states: AT BE CH DE DK ES FI FR GB GR IE IT LI NL PT SE;
20000802	( )	RIC1	CLASSIFICATION (CORRECTION) : 7G 07F 7/10 A, 7H 04L 9/08 B;
20010307	(+)	17P	REQUEST FOR EXAMINATION FILED Effective date: 20010105;
20010418	(+)	AKX	PAYMENT OF DESIGNATION FEES : AT BE CH DE DK ES FI FR GB GR IE IT LI NL PT SE;
20021009	(-)	18D	DEEMED TO BE WITHDRAWN Effective date: 20020403;

EP0862769A2 19980909

(ENG) METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: EP 96935993 A

Filing Date: 19960926

Issue/Publication Date: 19980909

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y; US 9615471 19960926 W W N;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Designated Countries:

Publication Language: ENG

Filing Language: ENG

Agent(s): Sanders, Peter Colin Christopher 00035571 Brookes Batchellor 1 Boyne Park Tunbridge Wells Kent TN4 8EL GB

Date of Deferred Publication of Search Report:
--19970515

Legal Status:

Date	+/-	Code	Description
19980909	(+)	17P	REQUEST FOR EXAMINATION FILED Effective date: 19980427;
19980909	(+)	AK	DESIGNATED CONTRACTING STATES: Kind code of corresponding patent document: A2; List of designated states: AT BE CH DE DK ES FI FR GB GR IE IT LI NL PT SE;
20000301	(+)	17Q	FIRST EXAMINATION REPORT Effective date: 20000113;
20021009	(-)	18D	DEEMED TO BE WITHDRAWN Effective date: 20020403;

IL123851A 20010111
IL123851D0 19981030

(ENG) METHOD, APPARATUS, SYSTEMS AND FIRMWARE FOR SECURE TRANSACTIONS

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR US

Application No: IL 12385196 A

Filing Date: 19960926

Issue/Publication Date: 20010111

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y; US 9615471 19960926 W W N;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Legal Status:

Date	+/-	Code	Description
20010520	(+)	FF	PATENTS GRANTED
20010724	(+)	KB	PATENTS RENEWED
20030212	(+)	KB	PATENTS RENEWED
20070724	(-)	MM9K	PATENT NOT IN FORCE DUE TO NON-PAYMENT OF RENEWAL FEES

JPH11513509A 19991116

NotAvailable

Application No: JP 51365296 T

[no drawing available]

Filing Date: 19960926

Issue/Publication Date: 19991116

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 9615471 19960926 W W N; US 451095 19950929 P Y; US 59498396 19960131 A Y;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Legal Status: There is no Legal Status information available for this patent

MX9802375A 19981129

(ENG) METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS.

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W ; FOX CHRISTOPHER W

Application No: MX 9802375 A

Filing Date: 19980326

Issue/Publication Date: 19981129

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Publication Language: SPA

Legal Status: There is no Legal Status information available for this patent

---

TR9800565T1 19980622

(TUR) Guevenli parasal islemleri gerçeklestirmeye mahsus yoentem, cihaz, sistem ve bellenim.

[no drawing available]

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: TR 9800565 T

Filing Date: 19960926

Issue/Publication Date: 19980622

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

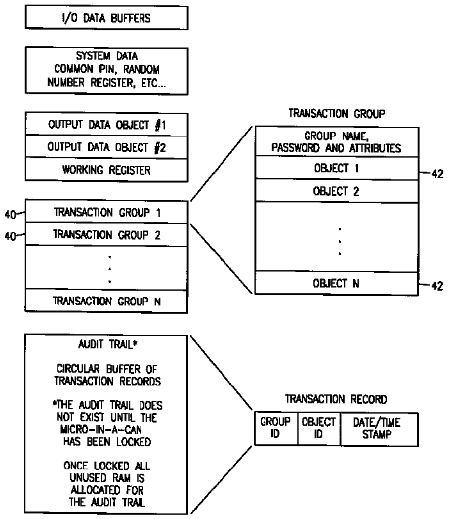
Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Legal Status: There is no Legal Status information available for this patent

---

US6237095B1 20010522


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

(ENG) Apparatus for transfer of secure information between a data carrying module and an electronic device

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: US 354198 A

Filing Date: 19980106

Issue/Publication Date: 20010522

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing encrypted information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 354198 19980106 A N; US 59501496 19960131 A 3 Y; US 451095 19950929 P Y;

Related Application(s): 45/1095 19950929 US

IPC (International Class): G07F00708; H04L00932; G06Q02000; G07F00710

ECLA (European Class): G06Q02000K2C; G07F00708C2; G07F00708C2B; G07F00710D4E; G07F00710D4E2; G07F00710D4T; G07F00710E; H04L00932T

US Class: 713178

Publication Language: ENG

Filing Language: ENG

Agent(s): Jenkens & Gilchrist, A Professional Corporation

Examiner Primary: Swann, Tod R.

Examiner Assistant: Smithers, Matthew

Assignments Reported to USPTO:

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
20041208	()	RFEAM	Year of fee payment: 4;
20080721	()	SISLP	New owner name: MAXIM INTEGRATED PRODUCTS, INC.,

			CALIFORNIA; : MERGER;ASSIGNOR:DALLAS SEMICONDUCTOR CORPORATION;REEL/FRAME:021253/0637; Effective date: 20080610;
20081120	()	FPAY	Year of fee payment: 8;

US6105013A 20000815

(ENG) Method, apparatus, system and firmware for secure transactions

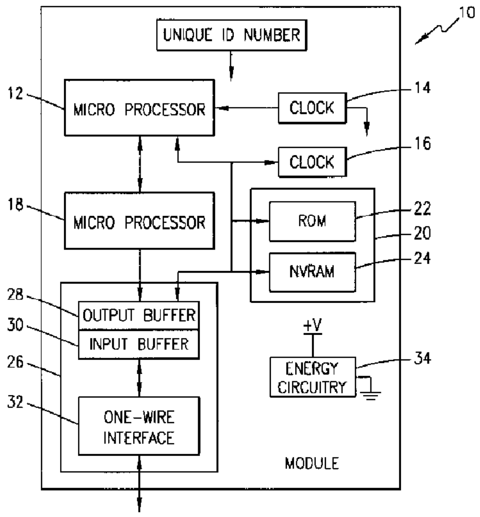
Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: US 4119098 A

Filing Date: 19980310

Issue/Publication Date: 20000815



Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 4119098 19980310 A N; US 59498396 19960131 A 1 Y; US 451095 19950929 P Y;

Related Application(s): 08/594983 19960131 5748740 US GRANTED

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

ECLA (European Class): G07F00708C2; G07F00708C2B; G07F00710D4E2; G07F00710D4T; G07F00710E

US Class: 705065; 235379; 380030; 705075; 713156; 713173; 713174

Publication Language: ENG

Filing Language: ENG

Agent(s): Jenkens & Gilchrist

Examiner Primary: Gregory, Bernarr E.

US Post Issuance:
--US Certificate of Correction: 20011113

Assignments Reported to USPTO:
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

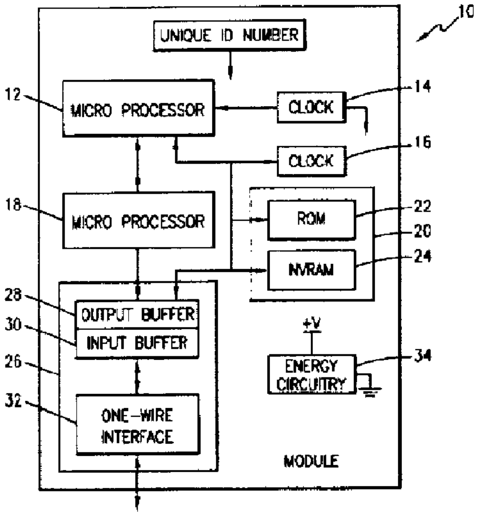
Corres. Addr: NORTH WEBER & BAUGH LLP ATTN: MICHAEL V. NORTH 2479 E. BAYSHORE RD, SUITE 707 PALO ALTO, CA 94303
Brief: MERGER

Legal Status:

Date	+/-	Code	Description
20011113	( )	CC	CERTIFICATE OF CORRECTION
20040304	()	FPAY	Year of fee payment: 4;
20080310	()	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;

US5748740A 19980505

(ENG) Method, apparatus, system and firmware for secure transactions



Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: US 59498396 A

Filing Date: 19960131

Issue/Publication Date: 19980505

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 59498396 19960131 A Y; US 451095 19950929 P Y;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

ECLA (European Class): H04L00932T; G07F00708C2; G07F00708C2B; G07F00710D; G07F00710D4E2; G07F00710E

US Class: 705065; 235379; 380030; 705075; 713156; 713173; 713174

Publication Language: ENG

Filing Language: ENG

Agent(s): Jenkens & Gilchrist, P

Examiner Primary: Gregory, Bernarr E.

US Post Issuance:

--US Expiration Date: 20020505 20020702 DUE TO FAILURE TO PAY MAINTENANCE FEES
--US Certificate of Correction: 19990216

Assignments Reported to USPTO:

Reel/Frame: 07959/0932 **Date Signed:** 19960412 **Date Recorded:** 19960429
Assignee: DALLAS SEMICONDUCTOR CORPORATION 4401 S. BELTWOOD PARKWAY DALLAS TEXAS 75244

Assignor: CURRY, STEPHEN M.; LOOMIS, DONALD W.; FOX, CHRISTOPHER W.

Corres. Addr: JENKENS &GILCHRIST, P.C. STEVEN R. GREENFIELD 1445 ROSS AVENUE, SUITE 3200 DALLAS, TX 75202-2799
Brief: ASSIGNMENT OF ASSIGNORS INTEREST(SEE DOCUMENT FOR DETAILS).

Reel/Frame: 24666/0786 **Date Signed:** 20080609 **Date Recorded:** 20100712
Assignee: MAXIM INTEGRATED PRODUCTS, INC. 120 SAN GABRIEL DRIVE SUNNYVALE CALIFORNIA 94086

Assignor: DALLAS SEMICONDUCTOR CORPORATION

Corres. Addr: NORTHWEBER & BAUGH LLP 2479 E. BAYSHORE RD. SUITE 707 PALO ALTO, CA 94303
Brief: MERGER (SEE DOCUMENT FOR DETAILS).

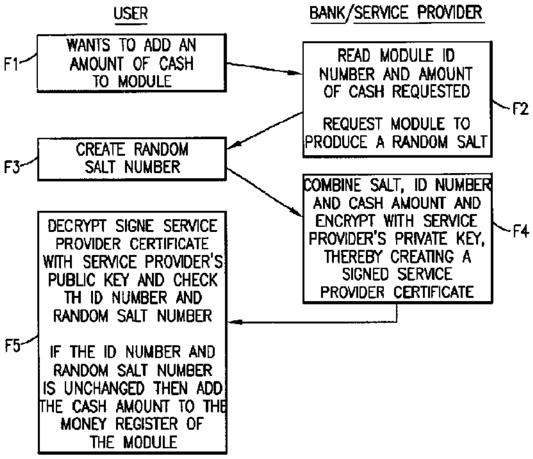
Legal Status:

Date	**+/-**	**Code**	**Description**
19960429	()	AS	New owner name: DALLAS SEMICONDUCTOR CORPORATION, TEXAS; : ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNORS:CURRY, STEPHEN M.;LOOMIS, DONALD W.;FOX, CHRISTOPHER W.;REEL/FRAME:007959/0932; Effective date: 19960412;
19960429	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: DALLAS SEMICONDUCTOR CORPORATION 4401 S. BELTWOOD; Effective date: 19960412;
19960429	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: CURRY, STEPHEN M.; Effective date: 19960412;
19960429	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: LOOMIS, DONALD W.; Effective date: 19960412;
19960429	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: FOX, CHRISTOPHER W.; Effective date: 19960412;
19960429	()	AS02	New owner name: DALLAS SEMICONDUCTOR CORPORATION 4401 S. BELTWOOD; Effective date: 19960412;
19960429	()	AS02	New owner name: CURRY, STEPHEN M.; Effective date: 19960412;
19960429	()	AS02	New owner name: LOOMIS, DONALD W.; Effective date: 19960412;
19960429	()	AS02	New owner name: FOX, CHRISTOPHER W.; Effective date: 19960412;
19990216	( )	CC	CERTIFICATE OF CORRECTION
20021506	(-))	RKEPS	EXPIRED DUE TO FAILURE TO PAY MAINTENANCE FEE Effective date: 20020505;
20100712	()	AS	New owner name: MAXIM INTEGRATED PRODUCTS, INC.,CALIFORNIA; : MERGER;ASSIGNOR:DALLAS

			SEMICONDUCTOR CORPORATION;REEL/FRAME:24666/786; Effective date: 20080609;
20100712	()	AS	New owner name: MAXIM INTEGRATED PRODUCTS, INC., CALIFORNIA; : MERGER;ASSIGNOR:DALLAS SEMICONDUCTOR CORPORATION;REEL/FRAME:024666/0786; Effective date: 20080609;

US5805702A 19980908

(ENG) Method, apparatus, and system for transferring units of value


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

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M US ; LOOMIS DONALD W US ; FOX CHRISTOPHER W US

Application No: US 59501496 A

Filing Date: 19960131

Issue/Publication Date: 19980908

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing encrypted information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 59501496 19960131 A Y; US 451095 19950929 P Y;

IPC (International Class): G07F00708; H04L00932; G06Q02000; G07F00710

ECLA (European Class): G06Q02000K2C; G07F00708C2; G07F00708C2B; G07F00710D4E; G07F00710D4E2; G07F00710D4T; G07F00710E; H04L00932T

US Class: 705066

Publication Language: ENG

Filing Language: ENG

Agent(s): Jenkens & Gilchrist

Examiner Primary: Tarcza, Thomas H.

Examiner Assistant: Whitc, Carmcn D.

US Post Issuance:
--US Certificate of Correction: 19990406

Assignments Reported to USPTO:
Reel/Frame: 08095/0854 **Date Signed:** 19960412 **Date Recorded:** 19960418
Assignee: DALLAS SEMICONDUCTOR CORPORATION 4401 S. BELTWOOD PARKWAY DALLAS TEXAS 75244

Assignor: CURRY, STEPHEN M.; LOOMIS, DONALD W.; FOX, CHRISTOPHER W.

Corres. Addr: JENKENS & GILCHRIST, P.C. STEVEN R. GREENFIELD 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

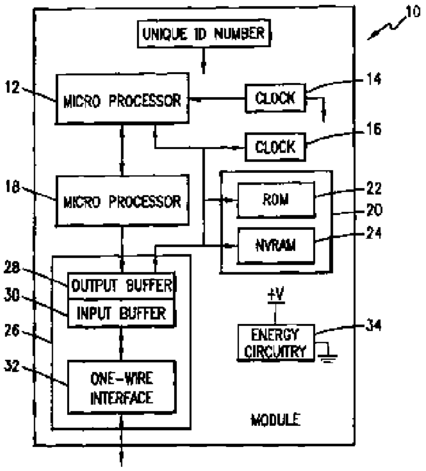
Assignor: DALLAS SEMICONDUCTOR CORPORATION

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
19960418	()	AS	New owner name: DALLAS SEMICONDUCTOR CORPORATION, TEXAS; : ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNORS:CURRY, STEPHEN M.;LOOMIS, DONALD W.;FOX, CHRISTOPHER W.;REEL/FRAME:008095/0854; Effective date: 19960412;
19960418	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: DALLAS SEMICONDUCTOR CORPORATION 4401 S. BELTWOOD; Effective date: 19960412;
19960418	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: CURRY, STEPHEN M.; Effective date: 19960412;
19960418	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: LOOMIS, DONALD W.; Effective date: 19960412;
19960418	( )	AS02	ASSIGNMENT OF ASSIGNOR'S INTEREST New owner name: FOX, CHRISTOPHER W.; Effective date: 19960412;
19960418	()	AS02	New owner name: DALLAS SEMICONDUCTOR CORPORATION 4401 S. BELTWOOD; Effective date: 19960412;
19960418	()	AS02	New owner name: CURRY, STEPHEN M.; Effective date: 19960412;
19960418	()	AS02	New owner name: LOOMIS, DONALD W.; Effective date: 19960412;
19960418	()	AS02	New owner name: FOX, CHRISTOPHER W.; Effective date: 19960412;
19990406	( )	CC	CERTIFICATE OF CORRECTION
20080717	()	AS	New owner name: MAXIM INTEGRATED PRODUCTS, INC., CALIFORNIA; : MERGER;ASSIGNOR:DALLAS SEMICONDUCTOR CORPORATION;REEL/FRAME:021253/0637; Effective date: 20080610;

WO9712344A3 19970515
WO9712344A2 19970403



(ENG) METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS

Assignee: DALLAS SEMICONDUCTOR US

Inventor(s): CURRY STEPHEN M ; LOOMIS DONALD W ;
FOX CHRISTOPHER W

Application No: US 9615471 W

Filing Date: 19960926

Issue/Publication Date: 19970515

Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data can be securely passed electronically. The module is capable of being programmed, keeping track of real time, recording transactions for later review, and creating encryption key pairs.

Priority Data: US 451095 19950929 P Y; US 59498396 19960131 A Y;

IPC (International Class): G09C00100; G06Q02000; G06Q05000; G06Q01000; G06Q04000; G07F00708; G07F00710

Designated Countries:

----Designated States: (national) AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN AM AZ BY KG KZ MD RU TJ TM

----Regional Treaties: (ARIPO) AP KE LS MW SD SZ UG

----EPO Extension States: (EPO) EP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

----Elected States (PCT): (OAPI) OA BF BJ CF CG CI

Publication Language: ENG

Filing Language: ENG

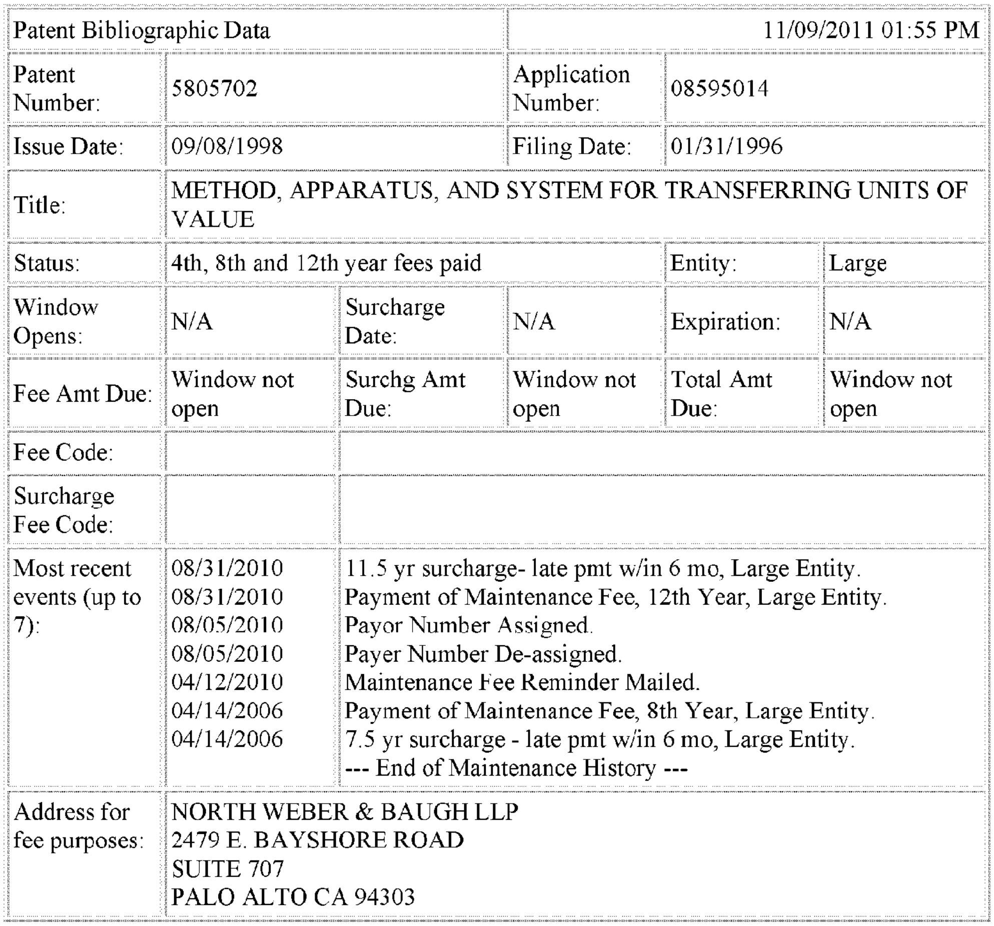
Agent(s): MAXWELL, Roger, L. Jenkens & Gilchrist, P.C., Suite 3200, 1445 Ross Avenue, Dallas, TX 75202 US

Legal Status:

Date	+/-	Code	Description
19970403	(+)	AK	DESIGNATED STATES Kind code of corresponding patent document: A2; List of designated states: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN AM AZ BY KG KZ MD RU TJ TM;
19970403	(+)	AL	DESIGNATED COUNTRIES FOR REGIONAL PATENTS Kind code of corresponding patent document: A2; List of designated states: KE LS MW SD SZ UG AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI;
19970515	(+)	AK	DESIGNATED STATES Kind code of corresponding patent

			document: A3; List of designated states: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN AM AZ BY KG KZ MD RU TJ TM;
19970515	(+)	AL	DESIGNATED COUNTRIES FOR REGIONAL PATENTS Kind code of corresponding patent document: A3; List of designated states: KE LS MW SD SZ UG AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI;
19970723	( )	121	EP: THE EPO HAS BEEN INFORMED BY WIPO THAT EP WAS DESIGNATED IN THIS APPLICATION
19971218	( )	DFPE	REQUEST FOR PRELIMINARY EXAMINATION FILED PRIOR TO EXPIRATION OF 19TH MONTH FROM PRIORITY DATE (PCT APPLICATION FILED BEFORE 20040101)
19980323	( )	ENP	ENTRY INTO THE NATIONAL PHASE IN: Corresponding country code for PRS Code (EP REG): CA; Corresponding patent document: 2232791; Kind code of corresponding patent document: A;
19980330	( )	ENP	ENTRY INTO THE NATIONAL PHASE IN: Corresponding country code for PRS Code (EP REG): JP; Corresponding patent document: 1997 513652; Kind code of corresponding patent document: A;
19980330	(+)	WWE	WIPO INFORMATION: ENTRY INTO NATIONAL PHASE Corresponding patent document: 1019980702358; Country code of corresponding patent document: KR;
19980427	(+)	WWE	WIPO INFORMATION: ENTRY INTO NATIONAL PHASE Corresponding patent document: 1996935993; Country code of corresponding patent document: EP;
19980730	( )	REG	REFERENCE TO NATIONAL CODE Corresponding country code for PRS Code (EP REG): DE; Corresponding EP Code 1 for PRS Code (EP REG): 8642;
19980909	(+)	WWP	WIPO INFORMATION: PUBLISHED IN NATIONAL OFFICE Corresponding patent document: 1996935993; Country code of corresponding patent document: EP;
19990726	(+)	WWP	WIPO INFORMATION: PUBLISHED IN NATIONAL OFFICE Corresponding patent document: 1019980702358; Country code of corresponding patent document: KR;
20020313	(-)	WWW	WIPO INFORMATION: WITHDRAWN IN NATIONAL OFFICE Corresponding patent document: 1019980702358; Country code of corresponding patent document: KR;
20020403	(-)	WWW	WIPO INFORMATION: WITHDRAWN IN NATIONAL OFFICE Corresponding patent document: 1996935993; Country code of corresponding patent document: EP;

Maintenance Report



Patent Bibliographic Data			11/09/2011 01:55 PM		
Patent Number:	5805702		Application Number:	08595014	
Issue Date:	09/08/1998		Filing Date:	01/31/1996	
Title:	METHOD, APPARATUS, AND SYSTEM FOR TRANSFERRING UNITS OF VALUE				
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):	08/31/2010 08/31/2010 08/05/2010 08/05/2010 04/12/2010 04/14/2006 04/14/2006	11.5 yr surcharge- late pmt w/in 6 mo, Large Entity. Payment of Maintenance Fee, 12th Year, Large Entity. Payor Number Assigned. Payer Number De-assigned. Maintenance Fee Reminder Mailed. Payment of Maintenance Fee, 8th Year, Large Entity. 7.5 yr surcharge - late pmt w/in 6 mo, Large Entity. --- End of Maintenance History ---			
Address for fee purposes:	NORTH WEBER & BAUGH LLP 2479 E. BAYSHORE ROAD SUITE 707 PALO ALTO CA 94303				