2. If the first byte is 0xFF and the next word is between 0 and 0xFFFD, inclusive, then the WORD contains the character count.

3. Finally, if the first byte is 0xFF and the next word is 0xFFFF, then the following DWORD contains the character count.

4. RESERVATION: in the future, STT may support UNICODE CStrings. These are denoted by (BYTE 0xFF), followed by (WORD 0xFFFE), followed by a UNICODE character count -- not a byte count -- as encoded in 1, 2, and 3. above.

4. Low-level Composites

4A. GUID

OSF/DCE Globally Unique ID. GUIDs are also known as UUIDs in the network literature. There is an ISO standard for their format and generation. They must be guaranteed to be unique across space and time. They are a standard part of the Open Software Foundation's (OSF) Distributed Computing Environment (DCE). They are necessary for the correct operation of many network protocols, such as Kerberos. It is very unlikely that an STT developer will be working on a platform that does not support validated GUID-generating software.

The following is a brief synopsis of one GUID-generating algorithm. More details may be found in the citations below.

If your machine contains a network card with a 48-bit IEEE network card hardware address, this globally unique address will be incorporated into the GUID. Otherwise a random pseudo-address is created from machine state information that is extremely likely to have been affected by truly random events, especially human interaction with devices and the file system. See the Note on Randomness in the Introduction for more.

The following excerpts on net hardware addresses are taken from

```
   Project 802: Local and Metropolitan Area Network Standard
   Draft Standard P802.1A/D10 1 April 1990
   Prepared by the IEEE 802.1

--- begin quote ----------------------------------------------

Page 18: "5.  Universal Addresses and Protocol Identifiers

The IEEE makes it possible for organizations to employ unique
individual LAN MAC addresses, group addresses, and protocol
identifiers.  It does so by assigning organizationally unique
identifiers, which are 24 bits in length.  [...] Though the
organizationally unique identifiers are 24 bits in length, their
true address space is 22 bits.  The first bit can be set to 1 or
0 depending on the application.  The second bit for all
assignments is zero.  The remaining 22 bits [...] result in
2**22 (approximately 4 million identifiers).

[...] The multicast bit is the least significant bit of the
first octet, A.

[...] 5.1 Organizationally Unique Identifier
```

```
[...] The organizationally unique identifier is 24 bits in
length and its bit pattern is shown below.  Organizationally
unique identifiers are assigned as 24 bit values with both
values (0,1) being assigned to the first bit and the second bit
being set to 0 indicates that the assignment is universal.
Organizationally unique identifiers with the second bit set to 1
are locally assigned and have no relationship to the
IEEE-assigned values (as described herein).

The organizationally unique identifier is defined to be:

   1st bit                24th bit
     |                       |
     a  b  c  d  e  .......  x  y
     |  |
     |  Always set to zero
     Bit can be set to 0 or 1 depending on application

[...] 5.2 48-Bit Universal LAN Mac Addresses

[...] A 48 bit universal address consists of two parts.  The
first 24 bits correspond to the organizationally unique
identifier as assigned by the IEEE except that the assignee may
set the first bit to 1 for group addresses or set it to 0 for
individual addresses.  The second part, comprising the remaining
24 bits, is administered locally by the assignee.
[...]

octet:
    0          1          2          3          4          5
0011 0101  0111 1011  0001 0010  0000 0000  0000 0000  0000 0001
|
First bit transmitted on the LAN medium. (Also the
Individual/Group Address Bit.) The hexadecimal representation
is: AC-DE-48-00-00-80

The Individual/Group (I/G) Address Bit (1st bit of octet 0) is
used to identify the destination address either as an individual
or as a group address.  If the Individual/Group Address Bit is
0, it indicates that the address field contains an individual
address.  If this bit is 1, the address field contains a group
address that identifies one or more (or all) stations connected
to the LAN.  The all-stations broadcast address is a special,
pre-defined group address of all 1's.

The Universally or Locally Administered Address Bit (2nd bit of
octet 0) is the bit directly following the I/G bit.  This bit
indicates whether the address has been assigned by a local or
universal administrator.  Universally administered addresses
have this bit set to 0.  If this bit is set to 1, the entire
address (i.e.: 48 bits) has been locally administered."

--- end quote ----------------------------------------------
```

Also, see the following

> DEC / HP, Network Computing Architecture Remote Procedure Call Run Time Extensions Specification Version OSF TX1.0.11 Steven Miller July 23, 1992 (Chapter 10 describes UUID allocation)

A GUID has the following wire format:

```
(define-type GUID
  ((DWORD   data1)
   (WORD    data2)
   (WORD    data3)
   (BYTE[8] data4)))
```

4B. XID

Each entity, e.g., cardholder, merchant, bank, in STT has a GUID. In the Microsoft implementation, the lifetime of this GUID is the lifetime of the installation of the STT software. It is possible for the same entity to have many GUIDs: typically one for every time STT software has been installed.

Transaction-initiating messages sent by an entity are stamped with its current GUID preceded by a QWORD containing a non-decreasing serial number. The composite of a GUID and a qwSerial is called an XID, for transaction ID. Responses to the transaction-initiating message contain the XID of the corresponding initiating message.

STT-compliant applications must guarantee that the serial number never decrease for a given GUID, and that the GUID is generated by validated software when STT software is installed on a machine. Implementations must guarantee that the serial number is non-decreasing for each GUID, and, thus, that no two transactions have the same XID.

STT-compliant applications shall guarantee idempotency of the protocol by examining XIDs. For example, a payment server will reject attempts to replay payment requests from merchants. It will detect these attempts by examining the XID of the payment request and XID of the embedded payment instruction, separately signed and encrypted by the cardholder.

An XID has the following wire format:

```
(define-type XID
  ((QWORD SerialNumber)      ;Per-Guid, non-decreasing
   (GUID  InstallationGuid)))
```

4C. CMoney

All amounts in STT are contained in CMoneys, which appear as follows:

```
(define-type CMoney
  ((WORD  CountryCode)  ;ISO 4217 Country Code.
   (QWORD Amount)))     ;fixed-point with four decimals
```

4D. DATE

A QWORD representing the number of 100-nanosecond intervals since midnight UTC at the beginning of 1 Jan 1601.

```
(define-type DATE
  (QWORD))
```

4E. TLV

(Tag, Length, Value) A TLV is a metadata format for generic, self-describing, byte-packed, streamed.

aggregate data objects.

Messages are composed of TLVs to support forward and backward compatibility. Old software will be able to read new messages because it will tags it does not recognize. New software will continue to read old messages since tags are never removed from the TLV tag space documented below.

The full notation for a TLV is

```
(<Tag> <Length> <Value>)
```

where <Tag> is replaced with a member of the Tag Space documented below, <Length> is a byte count for the <Value>, <Value> is replaced with actual notations of the kind shown so far and to follow. This denotes a TLV with the indicated Tag, Length, and Value. There are many cases where the Length equals the sum of the lengths of a set of nested data objects, and the Value equals a concatenation of the nested objects. The shorthand

```
(<Tag> <Value>)
```

denotes this case. Since TLV notations tend to become deeply nested, it is sometimes convenient to give the value field a symbolic name for documentation purposes. The name is written in a comment on the same line as the tag:

```
(<Tag>        ;My Value's name is "Foo"
 <Value>)     ;This is the definition of "Foo"
```

Note this differs from the notation for Atoms and Composites, where a symbolic name is enclosed with the type in parentheses. In all these cases, a description of the Value contents is carried out in embedded Cambtidge Notation.

In some cases, the Value is an undifferentiated byte stream. The notation may be further streamlined in these cases by omitting the Value altogether, resulting in merely

```
(<Tag>)
```

On the wire, all TLVs appear as follows:

```
((DWORD            dwTag)
 (DWORD            dwLength)
 (BYTE[dwLength]  rgbValue))
```

4F. TV

(Tag, Value) A TV is an optimized metadata format similar to TLVs except that the length of a TV is either statically known or can be determined by another method, as with CStrings, and therefore the Length field of a TLV is unecessary.

The notation

```
(<Tag> <Value>)
```

suffices for TVs, with a possible name as a comment.

On the wire, TVs appear as follows:

```
((DWORD             dwTag)
 (BYTE[knownLength] rgbValue))
```

4G. RSAKey

This is the type of RSA Encryption and Signature Keys. STT RSA moduli have the followinglengths:

```
* Root signature key:                     2048 bits (256 bytes)
* All other signature keys:               1024 bits (128 bytes)
* Issuer & Acquirer key-exchange keys:    1024 bits (128 bytes)
* Merchant key-exchange key:               768 bits ( 96 bytes)
* Client key-exchange key:                 512 bits ( 64 bytes)
```

Thus, there are four key formats, distinguished by key size. On the wire, RSA keys appear as follows:

```
((BYTE[4]           "RSA1")
 (DWORD             cbitsMod)   ;bit length of modulus
 (DWORD             publicexp)  ;public exponent
 (BYTE[cbitsMod/8]  modulus))   ;modulus data, little-endian.
```

The complete RSA Key block typess have the following symbolic names (which are used frequently in the rest of this document) and sizes, including the 12 bytes of overhead documented above:

```
* RSA2K:   268 B (cbitsMod = 2048)
* RSA1K:   140 B (cbitsMod = 1024)
* RSA.75K: 108 B (cbitsMod =  768)
* RSA.5K:   76 B (cbitsMod =  512)
```

It is therefore useful to add the following composites to the type system:

```
(define-type RSA-common
  ((BYTE[4]  "RSA1")
   (DWORD    cbitsMod)
   (DWORD    publicExp)))

(define-type RSA2K   (RSA-common (BYTE[256] modulus)))
(define-type RSA1K   (RSA-common (BYTE[128] modulus)))
(define-type RSA.75K (RSA-common (BYTE [96] modulus)))
(define-type RSA.5K  (RSA-common (BYTE [64] modulus)))
```

4H. DESKey

This is the RSA Envelope for DES keys and bank card Account Numbers. DESKeys are used to hide DES keys and account numbers from adversaries. The DES keys are generated randomly and used to encrypt bulk financial data.

There is some similarity to RC4Keys, documented further below. It would be possible to document a common abstraction, but it was deemed less confusing to document DESKeys and RC4Keys separately, despite the common elements.

The first 12 bytes are header data in the clear. Following the header data is a 128-byte, RSA-encrypted DEKB, and then an 8 byte initialization vector. A DEKB is a DESK diffused with Optimal Asymmetric Encryption Padding (OAEP), a method first described by Bellare and Rogaway [2] for diffusing the contents of RSA envelopes to forestall information-theoretic attacks.

All DESKeys are the same length since they are all encrypted with RSA1K keys. All DESKeys are 12+128+8=148 bytes long, with 12 bytes of fixed overhead, 128 bytes of RSA-encrypted DEKB, and 8 bytes containing an initialization vector.

First, we describe DESK, then DEKB, and finally DESKey

DESK

A DESK is a plaintext DES key concatenated with a Bank Card Account Number of at most 32 bytes. Its format is:

```
(define-type DESK                            ;total length = 119
  ((DWORD       8 cbKeyProper)
   (BYTE[8]       rgbKey)                    ;the DES key proper
   (DWORD      32 cbBankCardNumber)          ;actually, up to 32 bytes
   (BYTE[32]      BCN)                       ;bank card number
   (BYTE[71]    0 padding)))
```

Every DESK is 119 bytes long because the RSA modulus for encrypting DES keys in STT is always 128 bytes = 1024 bits and nine bytes are needed for OAEP and overflow protection.

Each byte of rgbKey contains 7 bits of key data + 1 check bit in position 0, as specified in FIPS 81.

The byte length of the bank card number data must be less than or equal to 32. The data format is application-dependent.

DEKB

To diffuse a DESK and, thereby, to create a DEKB:

1. Generate a fresh, 8-byte, random RC4 key -- the OAEP key
2. Generate 119 bytes from RC4 using the OAEP key
3. XOR these bytes into DESK, resulting in DiffusedDESK
4. Hash DiffusedDESK with SHA
5. XOR the OAEP key with the hash, resulting in rgbHx
6. Concatenate rgbHx and a byte of overflow space to DiffusedDESK, resulting in DEKB

The plaintext of a DEKB, then, is the following:

```
(define-type DEKB
  ((BYTE[119]     DiffusedDESK)
   (BYTE[8]       rgbHx)
   (BYTE        0 padding))) ;prevents overflow when
                             ;exponentiating
```

To reverse the process, recovering a DESK from a DEKB, do the following:

1. Hash DiffusedDESK with SHA
2. XOR rgbHx with the hash, resulting in the OAEP key
3. Generate 119 bytes from RC4 using the OAEP key
4. XOR these bytes into DiffusedDESK, resulting in DESK

The DESK, finally, may be used to decrypt other, DES-encrypted data outside the RSA envelope.

Finally, the entire DESKey format can be desribed:

```
(define-type DESKey
  ((BYTE            1 keyBlockType)
   (BYTE            2 keyVersion)
   (WORD          334 reservedWord)
   (DWORD  0x0000CC01 algorithmIdentifier)
   (DWORD  0x00014800 keyExchAlgIdOfRSA)
   (RSA1KE            DEKB)          ;RSA-encrypted DEKB
   (BYTE[8]           InitVector)))  ;DES IV, as in FIPS 81
```

The notation (RSA1KE DEKB) refers to the RSA encryption of a DEKB. That is, a DEKB raised to the power of the public key modulo the RSA modulus found in an instance of RSA1K (all DESKeys are encrypted with RSA1Ks). To recover DEKB, one must know the modulus and the secret, RSA private key. Given DEKB, one must further undo OAEP as described to recover a DESK.

4I. RC4Key

This is the RSA Envelope for protecting RC4 keys. These keys are used in the International version of STT for bulk encryption of receipts, the GSO, authorization responses, and credential responses.

There is some similarity to the RSA Envelope format for DES keys and bank card account numbers, documented above. The first 12 bytes of an RC4Key are header data in the clear. Following the header data is an RSA-encrypted REKB and three bytes of salt. A REKB, in the RC4 context, contains a diffused RC4K, via OAEP, exactly as with DESKeys. An RC4K is an RC4 Plaintext Key Block. REKBs come in three lengths: 128, 96, and 64 bytes, equaling the size of the corresponding RSA modulus. Since nine bytes of the REKB are needed for OAEP and overflow protection, just as with DESKeys, RC4Ks come in the following sizes: 119, 87, and 55. Including the 12 bytes of overhead preceding and the three bytes of salt following the REKB, the total lengths of RC4 Keys are 143, 111, or 79 bytes. The size of an RC4Key is known implicitly, by the context of the allowed RSA key length used for its final encryption. First, types for the three kinds of RC4Ks and REKBs are defined, then the types of the three lengths of RC4Keys are defined.

RC4K

There are three different RC4Ks, corresponding to the three RSA modulus sizes for encrypting RC4 keys.

```
(define-type LengthAndKey
  ((DWORD              5)  ;STT RC4 keys are always 5 bytes long
   (BYTE[5] rgbKeyProper)))

(define-type RC4K1K   (LengthAndKey (BYTE[110] 0 padding)))
(define-type RC4K.75K (LengthAndKey (BYTE[78]  0 padding)))
(define-type RC4K.5K  (LengthAndKey (BYTE[46]  0 padding)))
```

REKB

There are three REKB's corresponding to the three RSA modulus sizes:

```
(define-type OAEPkeyPad
  ((BYTE[8]   rgbHx)                  ;obscured OAEP key
   (BYTE    0 padding)))              ;RSA overflow protection

(define-type REKB1K   ((BYTE[119] DiffusedRC4K) (OAEPkeyPad)))
```

```
(define-type REKB.75K ((BYTE[87]  DiffusedRC4K) (OAEPkeyPad)))
(define-type REKB.5K  ((BYTE[55]  DiffusedRC4K) (OAEPkeyPad)))
```

Each of these REKBs contains an rgbEKey and an OAEPkeyPad. The process for creating a REKB from a RC4K is analogous to the process for creating a DEKB from a DESK. The process is

1. Generate a fresh, 8-byte, random RC4 key -- the OAEP key
2. Generate 119 bytes from RC4 using the OAEP key
3. XOR these bytes into an RC4K, resulting in DiffusedRC4K
4. Hash DiffusedRC4K with SHA
5. XOR the OAEP key with the hash, resulting in rgbHx
6. Concatenate rgbHx and a byte of overflow space to DiffusedRC4K, resulting in a REKB

To reverse the process, recovering a RC4K from a REKB, do the following:

1. Hash DiffusedRC4K with SHA
2. XOR rgbHx with the hash, resulting in the OAEP key
3. Generate 119 bytes from RC4 using the OAEP key
4. XOR these bytes into DiffusedRC4K, resulting in an RC4K

The RC4K, finally, may be used to decrypt other, RC4-encrypted data outside the RSA envelope.

Finally, there are three kinds of RC4Key:

```
(define-type RC4KeyCommon
  ((BYTE              1  keyBlockType)
   (BYTE              2  keyVersion)
   (WORD          16718  reservedWord)
   (DWORD   0x0000D001  algorithmIdentifier)
   (DWORD   0x00014800  keyExchAlgIdOfRSA)))

(define-type RC4Key1K      ;total length = 143
  ((RC4KeyCommon    com)
   (RSA1KE       REKB1K)   ;RSA-encrypted REKB
   (BYTE[3]     rgbSalt))) ;Key salt

(define-type RC4Key.75K    ;total length = 111
  ((RC4KeyCommon    com)
   (RSA.75KE  REKB.75K)    ;RSA-encrypted REKB
   (BYTE[3]    rgbSalt)))  ;Key salt

(define-type RC4Key.5K     ;total length = 79
  ((RC4KeyCommon    com)
   (RSA.5KE     REKB.5K)   ;RSA-encrypted REKB
   (BYTE[3]    rgbSalt)))  ;Key salt
```

The notation (RSA... REKB) refers to the RSA encryption of a REKB. That is, a REKB raised to the power of the public key modulo the RSA modulus found in an RSA1K, RSA.75K, or RSA.5K. To recover REKB, one must know the modulus and the secret, RSA private key. Given REKB, one must further undo OAEP as described.

The final three bytes of any RC4Key are key salt used to complete an 8 byte RC4 key. The salt is in the clear. Its purpose is to foil quick table lookup attacks that may be feasible with a 40-bit key.

5. TLV/TV Tag Space

This section contains symbolic names and numerical values for TLV and TV tags. STT-compliant software should not use values that do not appear in this table. A range of keys is set aside for application-dependent use. No version of STT will ever use these tags.

```
(TLV_NULL                   0x00000000)
(TV_DUALHASH                0x00000021)   // for dual signature
(TV_HASH                    0x00000022)   // hash value
(TV_ROOTSIGNATURE           0x0000003F)   // root signature
(TV_SIGNATURE               0x00000040)   // signature on Cred
(TLV_SIGNED_DATA            0x00000041)   // signed data
(TLV_DATA                   0x00000042)   // binary data
(TLV_ENCRYPTED_DATA         0x00000043)   // encrypted data
(TLV_DUALSIGNED_DATA        0x00000045)   // dual-signed data
(TLV_KEYBLOCK               0x00000046)   // key exchange block
(TLV_AUTHINFO               0x00000047)   // authorization information
(TLV_CARDINFO               0x00000048)   // bank card info
(TLV_CARD_NONCE             0x0000004A)   // for card no.
(TLV_HASHED_DATA            0x0000004B)   // hashed, unsigned data
(TV_VERSION                 0x0000014C)   // version information
(TLV_DATA_FLAG              0x0000004D)   // message format info
(TV_DATA_FLAG               0x00000102)   // message format flag

(TV_CMR_XID                 0x00000103)   // transaction id
(TV_MER_NAME                0x00000104)   // merchant name
(TV_CMR_AMT                 0x00000105)   // amount req. by cardholder
(TLV_SHIP_INFO              0x00000106)   // shipping information
(TV_CHARGE_SLIP             0x00000107)   // charge slip
(TLV_DETAILS                0x00000108)   // details
(TV_CARD_NAME               0x00000109)   // name as on card
(TV_EXP_DATE                0x0000010A)   // card expiration date
(TLV_BILLING_INFO           0x0000010B)   // billing information
(TV_XID                     0x0000010D)   // transaction id
(TV_ISSUER                  0x0000010E)   // issuer name
(TV_RCPT_FLAG               0x0000010F)   // fail flag in receipt
(TV_RCPT_MSG                0x00000110)   // message in receipt
(TLV_HASH_NONCE             0x00000111)   // for gso hashing
(TV_CRDRSP_CODE             0x00000112)   // cred response fail code
(TV_ATHRSP_CODE             0x00000113)   // auth response fail code
(TV_MER_AMT                 0x00000114)   // amount req. by merchant
(TV_RCPT_AMT                0x00000115)   // amount chgd by merchant

// Tags for credentials (all have the 13th bit set)

(TLV_CRDINFO                0x00001001)   // Cred common info
(TV_CRDSERIALNUM            0x00001002)   // Cred serial number
(TV_CRDOWNER                0x00001004)   // Cred owner name
(TV_CRDROOTNAME             0x00001008)   // name of the Cred root
(TV_CRDLEVEL                0x00001011)   // level in trust hierarchy
(TV_CRDVALIDITY             0x00001012)   // dates of validity
(TV_CRDACCTHASH             0x00001014)   // hash of acct # etc
(TLV_CRDKEY                 0x00001018)   // public key value
(TLV_CRDKEYEX               0x00001020)   // extra public key
(TLV_SIGNERCRD              0x00001021)   // Cred of signer
(TV_CARDTYPE                0x00001022)   // card type field
(TLV_MERACCTNUM             0x00001023)   // mer acct # with acquirer
(TV_CREATOR                 0x00001024)   // vendor identifier
(TV_ALTERNATE_NAME          0x00001025)   // alternate name
(TV_KEY_ID                  0x00001026)   // public key id
(TV_KEY_IDEX                0x00001027)   // extra public key id
(TLV_INSTITUTION_ID         0x00001028)   // institution identifier
(TLV_CRD_CARDHOLDERSIG      0x00001802)   // cardholder sig Cred
(TLV_CRD_CARDHOLDEREXCH     0x00001803)   // cardholder key exch Cred
```

```
    (TLV_CRD_MERCHANTSIG      0x00001804)   // merchant sig Cred
    (TLV_CRD_MERCHANTEXCH     0x00001805)   // merchant key exch Cred
    (TLV_CRD_ACQUIRERSIG      0x00001808)   // acquirer sig Cred
    (TLV_CRD_ACQUIREREXCH     0x00001809)   // acquirer key exch Cred
    (TLV_CRD_CAEXCH           0x00001813)   // bindery key exch Cred
    (TLV_CRD_CARDISSSIG       0x00001814)   // issuer sig Cred
    (TLV_CRD_CARDISSEXCH      0x00001815)   // issuer key exch Cred
    (TLV_CRD_BRANDCASIG       0x00001818)   // brand sig Cred
    (TLV_CRD_BRANDCAEXCH      0x00001819)   // brand key exch Cred

// values for card types in TV_CARDTYPE

    (VISA                     0x2)
    (RESERVED                 0x3)
    (RESERVED                 0x4)
    (RESERVED                 0x5)
    (RESERVED                 0x6)

// Tags for credential requests

    (TLV_SIGKEY               0x00002001)   // sig key in Cred req
    (TLV_EXCHKEY              0x00002002)   // key-exch key in Cred req
    (TLV_SIGKEYEX             0x00002004)   // extra sig key in Cred req
    (TLV_EXCHKEYEX            0x00002008)   // extra key exch key

// Tags for message components

    (TLV_GSO                  0x00004001)
    (TLV_PI                   0x00004002)
    (TLV_MERCHANT_REQUEST     0x00004004)
    (TLV_CRD_RESPONSE         0x00004080)
    (TLV_EMERGENCY            0x00004100)

// Tags for message types

    (TLV_CMRCRDREQ            0x00008002)
    (TLV_MERCRDREQ            0x00008003)
    (TLV_CMRCRDRSP            0x00008006)
    (TLV_MERCRDRSP            0x00008007)
    (TLV_PURORD               0x00008009)
    (TLV_ATHREQ               0x0000800A)
    (TLV_ATHRSP               0x0000800B)
    (TLV_RCEIPT               0x0000800C)

// Reserved Range; width = 4096

    (MSAPP_RESERVED_FIRST     0x0000A000)
    (MSAPP_RESERVED_LAST      0x0000AFFF)

// Tag range reserved for VISA

    (TLV_VISA_FIRST           0x00020000)
    (TLV_VISA_LAST            0x0002FFFF)

// User-Defined Tag range -- not used by STT

    (TLV_USER_FIRST           0x00800000)
    (TLV_USER_LAST            0x008FFFFF)

// mask for extended TAGS for the future

    (TLV_EXTENDED             0x80000000)
```

 10/12/95 14:12

6. Credentials

STT messages often contain credentials, also called just creds hereafter. An STT Credential is a binding between a banking account number, such as a cardholder bank card number or a merchant BIN number, and an RSA key-exchange key or RSA signature key. There is an analogy to certificates in other public-key systems. However, credentials are specialized to STT, they do not affirm general identity, and must not be mistaken for certificates.

Authentication policy is out-of-band for STT. In other words, it is completely up to banks and higher authorities in the trust tree to decide whether to issue credentials. When an acquiring bank receives a credential request from a merchant, the bank must satisfy itself that the merchant is in good standing before issuing an STT credential. Options for so doing include visiting the merchant face-to-face, checking credential request fields via telephone, fax, or email, and so on. Similarly, issuers must satisfy themselves that cardholder credential requests are valid. Options include a phone call and "mother's maiden name" questions, a separate paper mailer to an address on file containing the credential on diskette, or simply checking that the card is not reported lost or stolen. Since STT is transport-independent, it is important for applications to ensure that the credential is delivered to the party who requests it. STT addresses this requirement by packaging new credentials in credential response messages encrypted under the key-exchange key of the requestor. However, this alone does not prevent the requestor from being an impostor.

To reduce sizes of messages that do not need both kinds, key-exchange credentials and signature credentials are separate. A signature credential binds a signature key with an account number and places the pair in the trust hierarchy for an explicit time. A key-exchange credential binds a key-exchange key to an account number and allows others to encrypt data to the owner of the account with some assurance that the owner can be trusted with encrypted data. There are several different kinds of credentials. The Common Fields appear in all credentials. Other fields only appear in certain kinds of credentials. A credential is a TLV. Its detailed format follows:

CRD

```
(TLV_CRDTAG*                                    ;see explanation below
  (TLV_DATA                                     ;just a container
    (TV_CRDLEVEL WORD)                          ;see explanation below
    (TV_VERSION  (DWORD 0x00000110))
    (TV_CREATOR
      ((WORD  wReserved) ;vendor # assigned by card brand, MS is 1
       (DWORD dwAbilities)))                    ;reserved for vendor
    (TV_CRDSERIALNUM     BYTE[16])              ;assigned by Cred creator
    (TV_CRDOWNER         Cstring)               ;"subject name"
    (TV_ALTERNATE_NAME   CString)
    (TV_CRDVALIDITY
      ((DATE GoodFrom)
       (DATE GoodThru))))

  CDF                                           ;CredType-dependent Fields
  SignatureSection)                             ;see explanations below
```

In this (somewhat abstracted, and therefore impure) notation, TLV_CRDTAG* refers to one of the following:

```
TLV_CRD_CARDHOLDERSIG  0x00001802  sig Cred for cardholder
TLV_CRD_CARDHOLDEREXCH 0x00001803  key exch Cred for cardholder
TLV_CRD_MERCHANTSIG    0x00001804  sig Cred for merchant
```

```
TLV_CRD_MERCHANTEXCH    0x00001805  key exch Cred for merchant
TLV_CRD_ACQUIRERSIG     0x00001808  sig Cred for acquirer
TLV_CRD_ACQUIREREXCH    0x00001809  key exch Cred for acquirer
TLV_CRD_CAEXCH          0x00001813  key exch Cred for bindery
TLV_CRD_CARDISSSIG      0x00001814  sig Cred for card issuer
TLV_CRD_CARDISSEXCH     0x00001815  key exch Cred for card issuer
TLV_CRD_BRANDCASIG      0x00001818  sig Cred for brand bindery
TLV_CRD_BRANDCAEXCH     0x00001819  key exch Cred for brand bindery
```

The TV_CRDLEVEL is a WORD containing the height of the credential in the trust tree. The height is 0 for leaf credentials, i.e., cardholders and merchants. Issuers and Acquirers have height 1, meaning they can sign the credentials of leaf entities. Brand Credential Authorities have height 2, meaning they can sign level-1 credentials, i.e., Acquirers and Issuers.

There are different Credential Type-Dependent Fields for each type of credential. The following streams are mutually exclusive: any credential may have only one of them.

CDF

For cardholder key-exchange credentials, CDF should be replaced by

```
((TV_CARDTYPE     WORD)         ;VISA is 2, all others are reserved
 (TV_CRDACCTHASH BYTE[20])      ;see explanation below
 (TV_KEY_ID       DWORD)        ;assigned by key generator / owner
 (TLV_CRDKEY   76 RSA.5K))
```

The TV_CRDACCTHASH contains the SHA hash of the concatenated card nonce, card account number, and expiration date string - in this specific order

Cardholder Signature Crds have the following CDF:

```
((TV_CARDTYPE     WORD)         ;VISA is 2, all others are reserved
 (TV_CRDACCTHASH BYTE[20])      ;as with cardholder Key-exchange Creds
 (TV_KEY_ID       DWORD)        ;assigned by key generator / owner
 (TLV_CRDKEY 140 RSA1K))
```

Merchant signature Creds have the following CDF:

```
((TV_CARDTYPE     WORD)
 (TLV_MERACCTNUM)              ;identifies merchant to acquirer
 (TV_KEY_ID       DWORD)       ;assigned by key generator / owner
 (TLV_CRDKEY 140 RSA1K))
```

Acquirer, Issuer, and Brand Bindery creds all share the same CDF formats:

```
((TV_CARDTYPE     DWORD)
 (TLV_INSTITUTION_ID)          ;assigned by cred signer
 (TV_KEY_ID       DWORD)       ;assigned by key generator / owner
 (TV_CRDROOTNAME CString)      ;name of root of trust tree
 (TLV_CRDKEY 140 RSA1K))
```

The root credential authority key-exchange Cred has the following CDF:

```
((TLV_INSTITUTION_ID)
 (TLV_CRDKEY 140 RSA1K))
```

Merchant key-exchange creds contain the following CDF fields:

```
((TV_CARDTYPE       DWORD)
 (TLV_MERACCTNUM)              ;identifies merchant to acquirer
 (TV_KEY_ID         DWORD)     ;assigned by merchant
 (TLV_CRDKEY 108    RSA.75K))
 (TV_KEY_IDEX       DWORD)     ;assigned by acquirer
 (TLV_CRDKEYEX 140  RSA1K))
```

Merchant key-exchange creds include the public key-exchange key of the merchant's acquirer in the TLV_CRDKEYEX. This enables cardholder software to encrypt the PI to the acquirer and the GSO to the merchant. The acquirer normally signs this cred, vouching for both keys.

SignatureSection

Following the Credential Type-Dependent fields, a cred includes the creds, recursively, of its signing authorities and the signatures created by the signers. Software will verify the signature on the cred, then the signature on the signer's cred, and so on, until a signature by a root key is reached. A failure at any level of this recursive check must result in a failure to verify the leaf signature. See the cryptography section for details on PKCS #1 signature format.

```
((TLV_SIGNERCRD)                  ;recursively contains signer creds
 (TV_ROOTSIGNATURE BYTE[256]))  ;PKCS #1 sig
```

or, in the case of creds signed directly by the Root Credential Authority (normally, these are just sub-authority creds)

```
(TV_ROOTSIGNATURE BYTE[256])    ;PKCS #1 sig
```

7. Message Formats

An STT Transaction consists of 2 or, in one case, 4 messages. Every STT message can be assigned unambiguously to its transaction via a globally unique XID. Every STT message has its XID explicitly in a field, but the location of the XID is different in each message type. There are two kinds of messages: upward and downward. Upward messages flow from entities lower in the trust hierarchy to higher entities. Downward messages flow from higher authorities to lower. Downward messages may include piggybacked Emergency messages. Emergency messages support global root key replacement in the (very unlikely) case of root key compromise. A proper implementation of STT will ONLY replace the root key if the Emergency message is signed by the old root and if the user successfully types in the hash of the message from an external, trusted source such as Microsoft's support 800 number or an ad in a prominent newspaper. The signature on the Emergency message prevents denial of service attacks, and the hash check ensures that users get crucial information from a trusted source. All Message content fields are TLV/TVs.

A message may be either signed, dual-signed, or hashed, and finally, it may be encrypted. Any signing or hashing is always done before encryption. Every message component includes a TV_DATA_FLAG, which precedes the message content with a WORD specifying extra processing, as follows:

Bit#	Mask	Data Form
1	0x0002	SIGNED
2	0x0004	ENCRYPTED
4	0x0010	DUALSIGNED
5	0x0020	HASHED

Bits 1 and 2 are mutually exclusive. That is, a message may be either signed, dual-signed, or hashed. All other bit mask positions are reserved for enhancements and future versions of STT.

Details are documented in the following sections. The following types are recognized:

Upward Messages

```
PURORD
MERCRDREQ
CMRCRDREQ
ATHREQ
```

Downward Messages

```
RCEIPT
ATHRSP
MERCRDRSP
CMRCRDRSP
```

Detailed Message Formats

7A. PURORD, or GSO/PI

(Goods & Services Order / Payment Instruction)

Sent by cardholder to Merchant, this is an aggregate message containing a hashed GSO followed by a dual-signed PI. The hashed GSO contains a dual-signed GSO core and an unsigned Details field. The Details field is unsigned because secure signature software, without being excessively generic, cannot guarantee display of all formats that might be of interest to merchants and cardholders. Whereas an adversary could tamper with the unsigned Details field through its veil of RC4 encryption, he would not be able to construct a valid hash through that veil without knowing the complete plaintext of the signed GSO core and the Details field.

Typical software scenarios involve a client shopping application interacting with a compatible merchant server application. A shopping protocol must be defined between these applications. For example, the client application must supply a shipping address in a form that the merchant application can interpret. Shopping protocols are out of the scope of STT, but STT provides the Details field for application designers to put higher-level protocol information.

A dual signature is an RSA encryption of the hash of the concatenation of two hashes. A dual signature must be generated for the combined GSO and PI, and affixed to each. The same dual signature is affixed to the GSO and to the PI. The procedure is as follows:

```
1. Hash the GSO, producing H(GSO)
2. Hash the PI, producing H(PI)
3. Concatenate the two, in that order, producing
   H2 = H(GSO) | H(PI)
4. Hash H2, producing H(H2)
5. Sign H(H2), i.e., RSA-encrypt it with the private signature
   key, producing S(H(H2))
6. Affix the concatenation of H2 | S(H(H2)) to each of the
   GSO and the PI.
```

To check the dual signature, if you are a merchant and you have the supposed GSO plaintext, call it GSO',

```
1.  Hash GSO', producing H(GSO')
2.  Overwrite the first twenty bytes in the H2 received from
    the sender with your own H(GSO'), producing H2'
3.  Hash H2', producing H(H2')
4.  RSA-decrypt the S(H(H2)) received from the message sender,
    recovering H(H2))
5.  Compare, bitwise, H(H2') with H(H2); if they match the
    signature is verified.
```

If you have the ansatz PI' plaintext (you are an acquirer), do the following:

```
1.  Hash PI', producing H(PI')
2.  Overwrite the LAST twenty bytes in the H2 received from
    the sender with your own H(PI'), producing H2''
3.  Hash H2'', producing H(H2'')
4.  RSA-decrypt the S(H(H2)) received from the message sender,
    recovering H(H2))
5.  Compare, bitwise, H(H2'') with H(H2); if they match the
    signature is verified.
```

The dual signature is an optimization: it reduces the number of time-consuming signatures the cardholder must compute. Linking of the GSO and PI is accomplished by their sharing a single XID. The XID functions as a shared nonce in this context.

A successful purchasing transaction comprises four messages: a GSO/PI, an AuthRequest, an AuthResponse, and a Receipt. The XID for the transaction is generated by the cardholder when he or she initiates the transaction with the GSO/PI. As an optimization, the AuthResponse does not require the XID of the GSO/PI since it bears the additional XID generated by the merchant for the nested AuthRequest transaction. The outer transaction may be terminated by the merchant, in which case there will be no nested AuthRequest transaction and the merchant will send a negative receipt to the cardholder.

STT's strongest encryption secures the bank card number in the RSA envelope, which is packaged in the DESKey.

```
(TLV_PURORD
  (TV_VERSION (DWORD 0x00000110))
  (TLV_GSO
    (TV_KEY_ID DWORD)                    ;from Merchant's cred
    (TV_DATA_FLAG (WORD 0x0014))         ;dualhashed and encrypted
    (TLV_KEYBLOCK 111 RC4Key)
    (TLV_ENCRYPTED_DATA                  ;RC4-encrypted data
      ;------- The data below is in plaintext form -------
      (TLV_HASHED_DATA
        (TLV_DATA                        ;"XDataToHash"
          (TLV_HASH_NONCE BYTE[16]);foils known plaintext attack
          (TLV_DUALSIGNED_DATA
            (TLV_DATA
              (TV_CMR_XID          XID);of this GSO/PI
              (TV_MER_NAME      CString)
              (TV_CRDSERIALNUM BYTE[16]);from Mer cred
              (TV_CMR_AMT        CMoney);authorized by Cmr
              (TLV_CRD_CARDHOLDEREXCH)
              (TV_CHARGE_SLIP   CString)) ;end of TLV_DATA
            (TLV_CRD_CARDHOLDERSIG)
            (TV_DUALHASH BYTE[40])       ;2 SHA hashes
            (TV_SIGNATURE BYTE[128]))    ;sig of DUALHASH
          (TLV_DETAILS))                 ;unsigned supporting data
        (TV_HASH BYTE[20]))))            ;hash of "XDataToHash"
  (TLV_PI
    (TV_KEY_ID DWORD)                    ;of acquirer from MerCrd
```

```
    (TV_DATA_FLAG (WORD 0x0014))
    (TLV_KEYBLOCK 148 DESKey)
    (TLV_ENCRYPTED_DATA                  ;DES-encrypted data
      ;------- The data below is in plaintext form -------
      (TLV_DUALSIGNED_DATA
        (TLV_DATA
          (TV_CMR_XID           XID)     ;of this GSO/PT
          (TV_MER_NAME       CString)    ;merchant name
          (TV_CRDSERIALNUM   BYTE[16])   ;from Mer Crd
          (TV_CMR_AMT        CMoney)     ;authorized by Cmr
          (TLV_BILLING_INFO)             ;Application-defined
          (TV_CARD_NAME      CString)    ;Name as on Card
          (TV_EXP_DATE       CString)    ;from card, for hash chk
          (TLV_CARD_NONCE)) ;end of data;for hash check
        (TLV_CRD_CARDHOLDERSIG)
        (TV_DUALHASH BYTE[40])           ;2 SHA hashes
        (TV_SIGNATURE BYTE[128])))))     ;sig of DUALHASH
```

7B. Merchant Credential Request

```
(TLV_MERCRDREQ
  (TV_VERSION    (DWORD 0x00000110))
  (TV_KEY_ID     (DWORD AcquirerKeyId))
  (TV_DATA_FLAG  (WORD  0x0024))
  (TLV_KEYBLOCK 148 DESKey)
  (TLV_ENCRYPTED_DATA                   ;DES-encrypted data
  ;------- The data below is in plaintext form -------
    (TLV_HASHED_DATA
      (TLV_DATA
        (TV_XID)
        (TV_CREATOR
          ((WORD  wReserved)     ;vendor #, MS is 1
           (DWORD dwAbilities)));reserved for vendor
        (TV_ALTERNATE_NAME  CString)
        (TV_CRDOWNER (CString MerchantName))
        (TLV_DATA)                      ;Application-defined
        (TV_KEY_ID requestedKeyId)
        (TLV_SIGKEY RSA1K)
        (TLV_EXCHKEY RSA.75K))          ;end of TLV_DATA
      (TV_HASH (BYTE[20] HashOfData))))
```

7C. Cardholder Credential Request

The bank card number goes in the (TLV_KEYBLOCK DESKey), which is the RSA envelope, as with a PI.

```
(TLV_CMRCRDREQ
  (TV_VERSION     (DWORD 0x00000110))
  (TV_KEY_ID      (DWORD IssuerKeyId))
  (TLV_DATA_FLAG  (WORD  0x0024))
  (TLV_KEYBLOCK 148 DESKey)
  (TLV_ENCRYPTED_DATA                   ;DES-encrypted data
  ;------- The data below is in plaintext form -------
    (TLV_HASHED_DATA
      (TLV_DATA
        (TV_XID)
        (TV_CREATOR
          ((WORD  wReserved)     ;vendor #, MS is 1
           (DWORD dwAbilities)));reserved for vendor
        (TV_ALTERNATE_NAME  CString)
        (TLV_CARDINFO
          (TLV_BILLING_INFO)            ;Application-defined
          (TV_CARD_NAME (CString NameAsOnCard))
```

```
        (TV_EXP_DATE  (CString ExpirationDate))
        (TV_ISSUER    (CString IssuerName)))
      (TV_KEY_ID requestedKeyId)
      (TLV_SIGKEY RSA1K)
      (TLV_EXCHKEY RSA.5K))           ;end of TLV_DATA
    (TV_HASH (BYTE[20] HashOfData)))))
```

7D. Merchant Authorization Request (ATHREQ)

This is an aggregate message tied by XID to a GSO/PI and a Receipt. It contains a signed Authorization Request Prefix from the merchant to the acquirer as well as the forwarded PI encrypted by the cardholder to the acquirer. The PI contains the XID of the original GSO/PI. The purpose of the authorization request prefix is to allow the merchant to tell the acquirer the amount he thinks the cardholder has authorized from the GSO. This prevents cardholders and merchants defrauding each other. Some acquirers allow a small percentage difference in the two amounts to account for fluctuations in freight charges and taxes. The existence or width of this slop is entirely a bank policy issue.

```
(TLV_ATHREQ
  (TV_VERSION (DWORD 0x00000110))
  (TLV_MERCHANT_REQUEST
    (TV_KEY_ID     (DWORD AcquirerKeyId))
    (TV_DATA_FLAG (WORD  0x0006))
    (TLV_KEYBLOCK 148 DESKey)
    (TLV_ENCRYPTED_DATA                ;DES-encrypted data
    ;------- The data below is in plaintext form -------
      (TLV_SIGNED_DATA                 ;auth request prefix
        (TLV_DATA
          (TV_XID) ;generated by merchant for nested transaction
          (TV_MER_AMT (CMoney MerchantRequestedAmount))
          (TLV_CRD_MERCHANTEXCH))
        (TLV_CRD_MERCHANTSIG)
        (TV_SIGNATURE (BYTE[128] MerchantSig)))))
  (TLV_PI))                            ;See PURORD section
```

7E. Merchant Receipt (RCEIPT)

Signed receipt from the merchant to the cardholder. The TV_RCPT_FLAG WORD holds a code that indicates whether the transaction were successful. The following values are defined for the TV_RCPT_FLAG:

```
0 - Approved / Card OK
1 - Declined
2 - No Reply
3 - Call Issuer
4 - Amount Error
5 - Expired Card
6 - Invalid Transaction
7 - System Error
```

```
(TLV_RCEIPT
  (TV_VERSION    (DWORD 0x00000110))
  (TV_KEY_ID     (DWORD CardholderKeyId))
  (TV_DATA_FLAG (WORD  0x0006))
  (TLV_KEYBLOCK 76 RC4Key)
  (TLV_ENCRYPTED_DATA                   ;RC4-encrypted data
  ;------- The data below is in plaintext form -------
    (TLV_SIGNED_DATA
      (TLV_DATA
        (TV_XID       (XID OfOriginalGSO))
```

```
        (TV_RCPT_AMT   (CMoney))
        (TV_RCPT_FLAG (WORD ReceiptFlags))
        (TV_RCPT_MSG   (CString MessageFromMerchant)))
      (TLV_CRD_MERCHANTSIG)
      (TV_SIGNATURE (BYTE[128] MerchantSig)))))
```

7F. Acquirer Authorization Response (ATHRSP)

Signed authorization response from the acquirer to the merchant. This indicates to the merchant whether the cardholder's bank card is good. The XID of the original GSO is omitted, as an optimization, since the XID of the corresponding AuthRequest identifies the message uniquely. The following values are defined for the TV_ATHRSP_CODE:

```
0 - Approved / Card OK
1 - Declined
2 - No Reply
3 - Call Cardholder's issuing bank
4 - Amount Error
5 - Cardholder's card has expired
6 - Invalid Transaction
7 - System Error
```

```
(TLV_ATHRSP
  (TV_VERSION    (DWORD x00000110))
  (TV_KEY_ID     (DWORD MerchantKeyId))
  (TV_DATA_FLAG (WORDv 0x0006))
  (TLV_KEYBLOCK 111 RC4Key)
  (TLV_ENCRYPTED_DATA                  ;RC4-encrypted data
  ;------- The data below is in plaintext form -------
    (TLV_SIGNED_DATA
      (TLV_DATA
        (TV_XID (XID OfOriginalAuthRequest))
        (TV_ATHRSP_CODE WORD)
        (TLV_DATA))                    ;Application-defined
      (TLV_CRD_ACQUIRERSIG)
      (TV_SIGNATURE (BYTE[128] AcquirerSig)))))
```

7G. Merchant Credential Response

The TV_CRDRSP_CODE WORD holds a code indicating whether the credential were issued. If the WORD is non-zero, credentials are not present in the response. The following values are defined for the WORD:

```
0 - Credential issued; no error
1 - Contact credentialing authority (one level up the tree)
2 - Try again or contact credentialing authority
3 - Expired Card (cardholder credential)
4 - System Error; contact credentialing authority
```

```
(TLV_MERCRDRSP
  (TV_VERSION    (DWORD 0x00000110))
  (TV_KEY_ID     (DWORD 0))
  (TV_DATA_FLAG (WORD  0x0004))
  (TLV_KEYBLOCK  111 RC4Key)
  (TLV_ENCRYPTED_DATA                  ;RC4-encrypted data
  ;------- The data below is in plaintext form -------
    (TV_CRDRSP_CODE WORD)
    (TV_XID   (XID OfCorrespondingCrdRequest))
    (TLV_CRD_MERCHANTSIG)
    (TLV_CRD_MERCHANTEXCH)))
```

7H. Cardholder Credential Response

The TV_CRDRSP_CODE WORD holds a code indicating whether the credential were issued. If the WORD is non-zero, credentials are not present in the response. The following values are defined for the WORD:

```
0 - Credential issued; no error
1 - Contact credentialing authority (one level up the tree)
2 - Try again or contact credentialing authority
3 - Expired Card (cardholder credential)
4 - System Error; contact credentialing authority
```

```
(TLV_CMRCRDRSP
  (TV_VERSION    (DWORD 0x00000110))
  (TV_KEY_ID     (DWORD 0))
  (TV_DATA_FLAG  (WORD  0x0004))
  (TLV_KEYBLOCK  79 RC4Key)
  (TLV_ENCRYPTED_DATA                 ;RC4-encrypted data
  ;------- The data below is in plaintext form -------
    (TV_CRDRSP_CODE WORD)
    (TV_XID  (XID OfCorrespondingCrdRequest))
    (TLV_CARD_NONCE (BYTE[16] Nonce))
    (TLV_CRD_CARDHOLDERSIG)
    (TLV_CRD_CARDHOLDEREXCH)))
```

8. Cryptography

8A. Encryption for US/Canada only

This is work in progress. A high-level summary is that US/Canada versions of STT will use triple-DES (3DES) for all encrypted messages and will put Bank Card Account Numbers in the RSA envelope of one of the 3DES keys, just as with the International version.

8B. Encryption for the International Version

Two bulk encryption algorithms are used in International STT, RC4 and DES.

1. STT uses RC4 encryption with 8-byte keys, of which 3 bytes are salt, in the clear. See the RC4Key entry under the Low Level Composites section of this document. RC4 is a stream cipher; there are no pad bytes and the encrypted data is the same size as the plaintext data.

2. STT uses the Cipher Block Chaining (CBC) mode of DES, as defined in Federal Information Processing Standard FIPS 81. The key is 8 bytes long, with each byte having a parity bit in position 0. Thus there are 56 bits of random key. STT uses an all-zero byte Initialization Vector (IV). A maximum of 8 bytes of padding is applied to every plaintext message encrypted with DES to pad the message to a length that is a multiple of 8 bytes. Pad bytes have a value of

```
x = 8 - ((length of the plaintext) mod 8)
```

and the number of pad bytes is also x. For example, if the plaintext message was 17 bytes long, then each of the 7 bytes of padding contains the value 0x07. If x is 0, then there are 8 bytes, each containing 0x08. Padding is appended to the end of the plaintext before encryption and is stripped off after decryption.

8C. Signatures

STT uses PKCS #1 Encryption block formatting for RSA signatures. Total length is 128 bytes for the signature (1024-bit modulus), except for signatures by the root key, which are twice as long. The following are the plaintexts:

```
(TV_SIGNATURE
  (BYTE[20]  HashOfData)     ;Hash of the data being signed
  (BYTE      0)              ;parser initializer
  (BYTE[105] 0xff)           ;padding
  (BYTE      0x01)           ;recom. for private key encryptions
  (BYTE      0))             ;overflow protection for RSA

(TV_ROOTSIGNATURE
  (BYTE[20]  HashOfData)     ;Hash of the data being signed
  (BYTE      0)              ;parser initializer
  (BYTE[233] 0xff)           ;padding
  (BYTE      0x01)           ;recom. for private key encryptions
  (BYTE      0))             ;overflow protection for RSA
```

8D. Hashing

All hashes in STT are 20-byte SHA hashes. See Federal Information Processing Standard FIPS 181 for the specification of SHA hashes.

9. Protocols

9A. Entities

```
1.  Cmr   - Cardholder
2.  Mer   - Merchant
3.  Iss   - Issuing Bank, signs Cmr Crds
4.  Acq   - Acquirer Bank, signs Mer Crds, also Payment server
5.  Mer   - Merchant
6.  Brand - Card Brand Binder, signs Iss Crds and Acq Crds
7.  Root  - Signs Brand Crds
```

9B. Messages

1. TLV_PURORD
2. TLV_MERCRDREQ
3. TLV_CMRCRDREQ
4. TLV_ATHREQ
5. TLV_RCEIPT
6. TLV_ATHRSP
7. TLV_MERCRDRSP
8. TLV_CMRCRDRSP

9C. Protocol Quick List

```
1.   Card Registration. Sequentially,
  a)   Cmr sends CMRCRDREQ to Iss
  b)   Iss sends CMRCRDRSP to Cmr

2.   Merchant Registration. Sequentially,
  a)   Mer sends MERCRDREQ to Acq
  b)   Acq sends MERCRDRSP to Mer
```

3. Purchasing, Sequentially,
   a) Cmr sends PURORD to Mer
   b) Either
      (1) Mer sends ATHREQ to Acq
      (2) Acq sends ATHRSP to Mer
      (3) Mer sends RCEIPT to Cmr
   c) or
      (1) Mer sends RCEIPT to Cmr

9D. Protocol Descriptions

Registration

Merchant Registers with Acquirer

Merchants (or their processing agents) must register with their Acquirers, which have been previously registered with their brand bindery, to be able to accept transactions on a particular brand's cards and pass them on their (the Merchant's) Acquirer.

IMPORTANT NOTE

The signer of the Merchant Credential must operate the payment server. This version of STT cannot separate the Credential Server for merchants from the Payment Server operated by the Acquirer. The reason is that the signer of the Merchant's Credential inserts its public key so the cardholder may encrypt PIs to the Acquirer Payment Server. This version of STT does not support export of the public key from the Payment Server. Nor import of a Payment Server public key into a Merchant Credential Server. Such key export and key import would be required to support separation.

Message Types

TLV_MERCRDREQ - the credential request message sent by the merchant to the brand bindery

TLV_MERCRDRSP - the credential request response message sent by the acquirer back to merchant

Cardholder Registers with Card Issuer

Cardholders must register their cards. They do this by registering directly with an issuing bindery. This bindery is operated by their bank, or its agent (which could be the brand itself, for example Visa, MasterCard, American Express)

Message Types

TLV_CMRCRDREQ - the credential request message sent by the cardholder to the bindery that issues the cardholder's card credential

TLV_CMRCRDRSP - the credential request response message sent by the bindery back to the cardholder for the registered card

Purchase and Authorization

This is the only two-step or nested transaction in STT.

Once all parties to a transaction are registered, initial distribution of credentials may occur. Distribution of credentials is NOT defined as part of the STT protocol because it is part of the basic (and variable) business relationships between participants (see Initial Credential Distribution, below).

Given that registration and credential distribution has taken place, a purchase transaction may occur. In STT, this is a three-way communication between a cardholder, a merchant, and an acquirer. The back-end communication between the acquirer and the banking system is neither defined nor affected by STT. It exists today.

The flow begins with a cardholder sending a request to a merchant to purchase goods or services. This includes the "Goods and Services Order" (GSO) and "Payment Instruction" (PI). The GSO is processed locally by the merchant, while the PI is passed on to the acquirer for authorization of the means of payment. STT does not specify the "back end" of the acquirer server, that is, the mechanism by which the acquirer processes the authorization request. Presumably, existing banking systems networks and protocols will be used. The response from the acquirer to the merchant is back in-band for STT, as is the final leg of the transaction, consisting of a receipt from merchant to cardholder.

Message Types

```
TLV_PURORD - the purchase request sent by the cardholder to the
   merchant.  This includes both the GSO and the PI.  See the
   section on encryption for details on encryption and signing.

TLV_ATHREQ - The PI, along with additional merchant information
   is sent from the merchant to the acquirer

TLV_ATHRSP - The result of processing the PI (accomplished
   synchronously, but out of the STT protocol specification) is
   sent from the acquirer to the merchant

TLV_RCEIPT - The receipt (as specified by the merchant) is sent
   back to the cardholder.
```

Settlement

TBD

Not currently defined in the STT Protocol.

Credential Distribution

Credential format is defined by STT, but the means of distribution, i.e., the transport, is not specified. Web-based scenarios are most likely and will be supported directly by Microsoft's implementations.

9E. Message Flows

Registration

Merchant Registration with Acquirer

```
MERCHANT                                 ACQUIRER
   |                                        |
   |          TLV_CRD_ACQUIREREXCH          |
```

```
     |     <----------------------------      |
     |                                        |
     |            TLV_MERCRDREQ               |
     |     ---------------------------->      |
     |                                        |
     |     <----------------------------      |
     |            TLV_MERCRDRSP               |
```

Cardholder Registration with Issuer

```
CARDHOLDER                                  ISSUER
     |                                        |
     |         TLV_CRD_CARDISSEXCH            |
     |     <----------------------------      |
     |                                        |
     |            TLV_CMRCRDREQ               |
     |     ---------------------------->      |
     |                                        |
     |     <----------------------------      |
     |            TLV_CMRCRDRSP               |
```

Purchase

```
CARDHOLDER              MERCHANT              ACQUIRER
   |                       |                      |
   | TLV_CRD_MERCHANTEXCH  |                      |
   | <-------------------  |                      |
   |                       |                      |
   |      TLV_PURORD       |                      |
   | ------------------->  |                      |
   |                       |     TLV_ATHREQ       |
   |                       |  ---------------->   |
   |                       |                      |
   |                       |     TLV_ATHRSP       |
   |                       |  <----------------   |
   |      TLV_RCEIPT       |                      |
   | <-------------------  |                      |
```

10. References

[1] "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" R.L. Rivest, A. Shamir, L. Adelman, MIT Laboratory for Computer Science and Department of Mathematics, S. L. Graham, R. L. Rivest ed. Communications of the ACM, February 1978 (Vol 21, No. 2) pages 120-126.

[2] "Optimal Asymmetric Encryption", M. Bellare and P. Rogaway, Eurocrypt '94.

11. Appendix

ISO 4217 Currency Country Codes

This is not part of STT proper. Interpretation of these fields is an application issue. The following is a non-authoritative sample of popular currencies.

```
36    Australian Dollar; 2; Australia, Christmas Is.,
        Cocos Is., Keeling Is., Heard Is., McDonald Is.,
        Kiribati, Nauru, Norfolk Is., Tuvalu
40    Austrian Schilling; 2; Austria
```

56	Belgian Franc; 0; Belgium
124	Canadian Dollar; 2; Canada
156	Yuan Renminbi; 2; China
280	Deutsche Mark; 2; Germany
300	Drachma; 0; Greece
344	Hong Kong Dollar; 2; Hong Kong
348	Forint; 2; Hungary
360	Rupiah; 2; Indonesia
372	Irish Pound; 2; Ireland
376	Shekel; 2; Israel
380	Italian Lira; 0; Italy, San Marino, Vatican City
392	Yen; 0; Japan
410	Won; 0; Korea, Rep. of Korea, South Korea
442	Luxembourg Franc; 0; Luxembourg
484	Mexican Nuevo Peso; 2; Mexico
528	Netherlands Guilder; 2; Netherlands
620	Portuguese Escudo; 0; Portugal
724	Spanish Peseta; 0; Spain, Andorra
752	Swedish Krona; 2; Sweden
756	Swiss Franc; 2; Switzerland, Liechtenstein
818	Egyptian Pound; 2; Egypt 826; Pound Sterling; 2; United Kingdom
840	U.S. Dollar; 2; United States, US, USA, U.S., U.S.A., Guam, American Samoa, Wake Is., U.S. Misc. Pac. Is., Panama Canal Zone, British Virgin Is., Johnston Is., Marianas Is., Saipan, Midway Is.

MPI Family Report (Family Bibliographic and Legal Status)

In the MPI Family report, all publication stages are collapsed into a single record, based on identical application data. The bibliographic information displayed in the collapsed record is taken from the latest publication.

Report Created Date: 2012-02-21

Name of Report:

Number of Families: 1

Comments:

Table of Contents

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
[illegible]	()	[illegible]	

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

[no drawing available]

Application No: JP 51365296 T

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

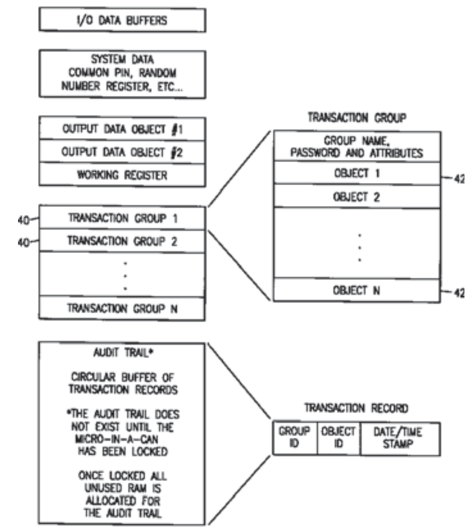
Abstract: (ENG) The present invention relates to an electronic module used for secure transactions. More specifically, the electronic module is capable of passing information back and forth between a service provider's equipment via a secure, encrypted technique so that money and other valuable data 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

(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): 60/004510 19950929 US

IPC (International Class): G07F00708; H04L00932; G06Q02000; G07F00710

ECLA (European Class): H04L00932S; G06Q02000K2C; G07F00708C2; G07F00708C2B; G07F00710D; G07F00710D4E; G07F00710D4E2; 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

US Post Issuance:

--US Litigations: Maxim Integrated Products, Iinc Maxim Integrated Products, Iinc E.D. Texas 4:12cv00006 ; Jack Henry & Associates, Inc. Jack Henry & Associates, Inc. Kansas 2:12cv02018 ; Maxim Integrated Products, Inc. Maxim Integrated Products, Inc. E.D. Texas 4:12cvb00010 ; Maxim Integrated Products, Inc. Maxim Integrated Products, Inc. E.D. Texas 4:12cv00005 ; Maxim Integrated Products, Inc. Maxim Integrated Products, Inc. E.D. Texas 4:12cv00017

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

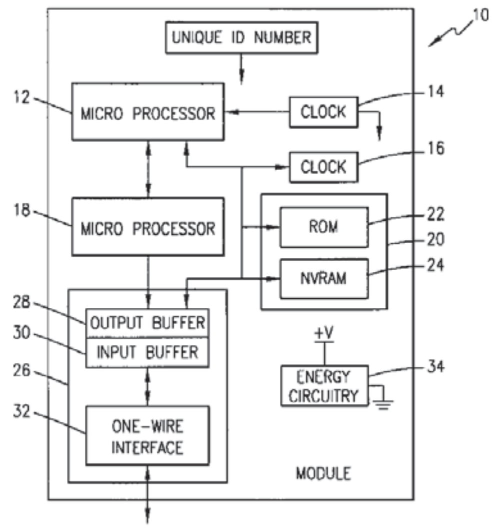
Corres. Addr: NORTHWEBER & BAUGH LLP ATTN: MICHAEL V. NORTH 2479 E. BAYSHORE RD, SUITE 707 PALO ALTO, CA 94303

Brief: MERGER

Legal Status:

Date	+/-	Code	Description
20041208 / 20041228 (overprinted)	()	REAM / FPAY (overprinted)	Year of fee payment: 4;
20080721 / 20041217 (overprinted)	()	AS / SULP (overprinted)	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): 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

Examiner Primary: Gregory, Bernarr E.

US Post Issuance:

--US Certificate of Correction: 20011113 20011204 a Certificate of Correction was issued for this patent
--US Litigations: Jack Henry & Associates, Inc. Jack Henry & Associates, Inc. Kansas 2:12cv02018 ; Maxim Integrated Products, Inc. Maxim Integrated Products, Inc. E.D. Texas 4:12cvb00010 ; Maxim Integrated Products, Inc. Maxim Integrated Products, Inc. E.D. Texas 4:12cv00005 ; Maxim Integrated Products, Inc. Maxim Integrated Products, Inc. E.D. Texas 4:12cv00017

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: NORTHWEBER & 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;
20080312	()	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

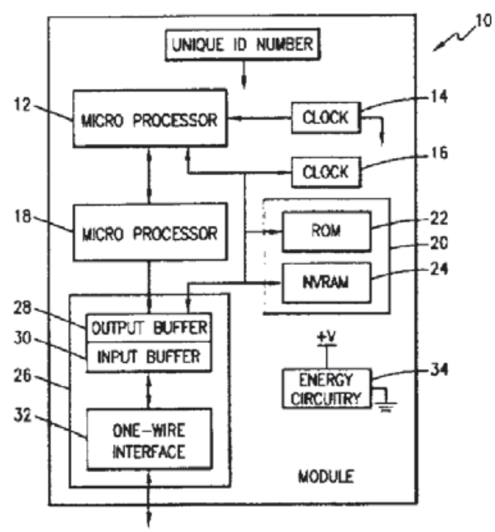
Assignee: DALLAS SEMICONDUCTOR US

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).

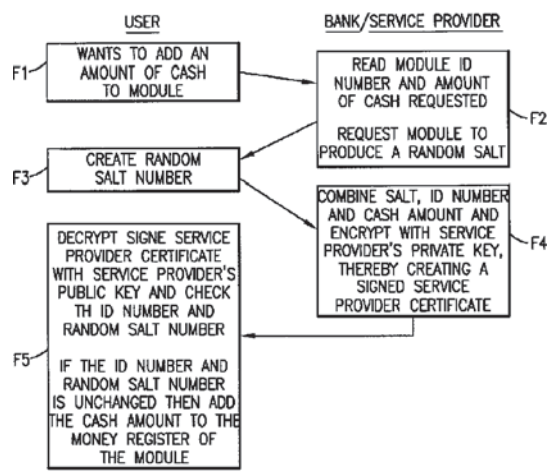
Legal Status:

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
[illegible]	(-)	[illegible]	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



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: White, Carmen 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

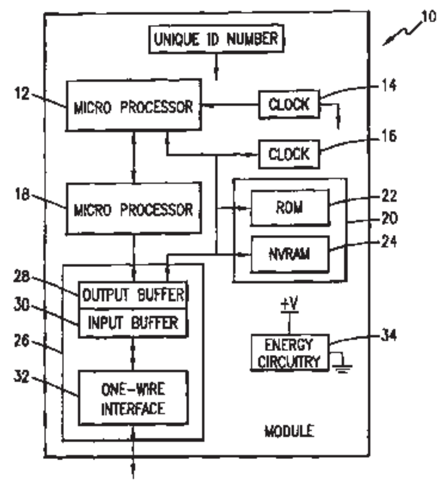
Assignee: DALLAS SEMICONDUCTOR US

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;

USPTO Maintenance Report

Patent Bibliographic Data			02/21/2012 01:38 PM		
Patent Number:	6105013		Application Number:	09041190	
Issue Date:	08/15/2000		Filing Date:	03/10/1998	
Title:	METHOD, APPARATUS, SYSTEM AND FIRMWARE FOR SECURE TRANSACTIONS				
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):	01/31/2012 08/05/2010 08/05/2010 02/12/2008 03/10/2004 03/10/2004 03/04/2004	Payment of Maintenance Fee, 12th Year, Large Entity. Payor Number Assigned. Payer Number De-assigned. Payment of Maintenance Fee, 8th Year, Large Entity. Payment of Maintenance Fee, 4th Year, Large Entity. Surcharge for Late Payment, Large Entity. Maintenance Fee Reminder Mailed. --- End of Maintenance History ---			
Address for fee purposes:	NORTH WEBER & BAUGH LLP 2479 E. BAYSHORE ROAD SUITE 707 PALO ALTO CA 94303				

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 06 602 A 1**

(51) Int. Cl.⁶:
H 04 L 9/32
H 04 M 11/00
H 04 M 3/42
G 07 C 9/00

(21) Aktenzeichen: P 4406 602.3
(22) Anmeldetag: 1. 3. 94
(43) Offenlegungstag: 7. 9. 95

DE 44 06 602 A 1

(71) Anmelder:
Deutsche Bundespost Telekom, 53175 Bonn, DE

(72) Erfinder:
Kowalski, Bernd, Dipl.-Ing., 57072 Siegen, DE; Stolz, Helmut, Dipl.-Ing., 57080 Siegen, DE

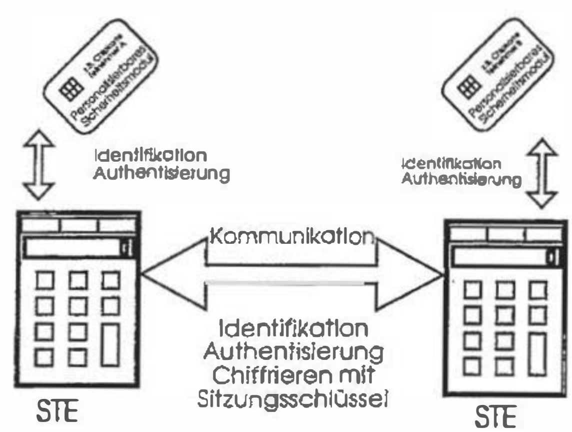
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	41 38 861 A1
US	52 74 699
US	52 39 583
US	52 22 140
US	52 02 921
US	46 79 226
EP	21 401 B1
EP	04 51 695 A2
EP	3 46 180 A1
SU	17 32 362 A1
SU	11 63 744 A1

BELLER,Michael,J.;
et.al.: Privacy and Authenica- tion on a Portable Communications System. In: IEEE Journal on Selected Areas in Communications, Vol.11, No.6, Aug. 1993, S.821-829;
ALLERBECK,Mechthild;
FISCHER,Norbert: Mobile Kom- munikation mit HICOM-Chipkarte. In: telcom report 9, 1986, H.4, S.270-273;
ARNDT,Gerhard;
LUEDER,Reinhard: Bewegungsfreiheit in allen Netzen. In: telcom report 16, 1993, H.2, S.67-69;
GABEL,J.: Die Chipkarte im Funktelefonnetz C. In: ntz Bd.41, 1988, H.10, S.586-589;

(54) Sicherheitssystem zum Identifizieren und Authentisieren von Kommunikationspartnern

(57) Die erfindungsgemäße Lösung betrifft ein Sicherheitssystem, das eine eindeutige Identifizierung und Authentisierung von Kommunikationspartnern ermöglicht und somit die notwendige Sicherheit für den Austausch von vertraulichen Informationen gewährleistet.
Voraussetzung ist, daß alle Kommunikationspartner mit einem individuellen Sicherheitsmodul ausgestattet sind und über sicherheitstechnische Einrichtungen STE verfügen. Der Verbindungsaufbau wird von den STE übernommen. Dabei wird geprüft, ob beim Kommunikationspartner ebenfalls eine aktivierte STE vorhanden ist. Mit dieser STE wird ein Informationsaustausch und ein Authentikations- und Schlüsselaustauschprotokoll vorgenommen. Danach erfolgt eine persönliche Authentizierung und die Betriebsartentscheidung einschließlich evtl. erforderlicher Schlüsselvereinbarung.
Mittels der erfindungsgemäßen Lösung werden sowohl die Sicherheit der Kommunikationspartner als auch die Sicherheit des Kartenterminals in die Prüfung auf Informationssicherheit einbezogen.



DE 44 06 602 A 1

Beschreibung

Die Erfindung betrifft ein Sicherheitssystem zum Identifizieren und Authentisieren von Kommunikationspartnern der im Oberbegriff des Patentanspruch 1 näher definierten Art, welche die Informationssicherheit mit Sicherheitsmechanismen von hoher Wirksamkeit erreicht. Sie schützt insbesondere gegen die Bedrohungen:

— Verlust der Vertraulichkeit (Schutz vor unbefugter Preisgabe von Informationen)
— Verlust der Integrität (Schutz vor unbefugter Änderung von Informationen)
— Verlust der Anonymität (Schutz vor unbefugter Preisgabe der Identität).

Zusätzlich bietet ein Kommunikationssystem, das mit diesen Einrichtungen ausgestattet ist, die Möglichkeit, daß der Zugriff auf Computersysteme, die in diesem Kommunikationsnetz betrieben werden, gesichert wird.

Bestehende Kommunikationsinfrastrukturen verfügen im allgemeinen nicht über ausreichende Mechanismen, daß Kommunikationspartner sich gegenseitig eindeutig identifizieren und authentisieren können, um anschließend und vertraulich Informationen auszutauschen. Erst durch erhebliche Eingriffe in die benutzten Kommunikationssysteme können die Partner nach vorherigen Verabredungen notwendiger Parameter die Prozesse aktivieren, die z. B. durch kryptographische Verfahren, einen vertrauenswürdigeren Informationsaustausch gestatten und in der Regel noch zusätzliche Maßnahmen notwendig machen. Geeignete kryptographische Verfahren gestatten grundsätzlich eine vertrauliche Kommunikation.

Durch den Einsatz von geeigneten Sicherheitsmodulen (wie z. B. Chipkarten) ist eine Identifikation von Benutzern auf eine höchst vertrauenswürdige Weise möglich.

Geeignete Chipkarten lassen den Zugriff auf interne Funktionen und Daten nur dann zu, wenn sich ein Benutzer gegenüber der Chipkarte durch ein Merkmal oder Geheimnis (persönliche Geheimzahl, Fingerprint, etc.) eindeutig identifiziert. Für die Identifikation des Benutzers gegenüber der Chipkarte muß ein Kartenterminal verwendet werden. Auch die Sicherheit des Kartenterminals muß in die Betrachtung der Informationssicherheit einbezogen werden. Das Kartenterminal hat sich deshalb ebenfalls gegenüber der Chipkarte des Benutzers eindeutig zu identifizieren.

Mit der vorliegenden Erfindung soll ein vom Kommunikationssystem unabhängiges Sicherheitssystem geschaffen werden, das die Identifikation von Benutzern mit einer Chipkarte bei Einsatz eines Chipkartenterminals mit der gegenseitigen Authentikation von Benutzern, dem Parameteraustausch für den Einsatz kryptographischer Verfahren und deren Anwendung für den vertraulichen Informationsaustausch zwischen Kommunikationspartnern verknüpft. Dazu soll kein Eingriff in die bestehenden Kommunikationssysteme notwendig sein.

Diese Aufgabe wird erfindungsgemäß entsprechend dem Kennzeichen des Patentanspruchs 1 gelöst.

Vorteilhafte Weiterbildungen der Erfindung sind in den Kennzeichen der Patentansprüche 2 bis 8 beschrieben.

Unter Verwendung eines individuellen und personalisierbaren Sicherheitsmoduls (z. B. einer Chipkarte) und den Sicherheitsfunktionen von sicherheitstechnischen Einrichtungen (kurz STE) wird der authentische und vertrauliche Informationsaustausch in Kommunikationssystemen, — hierzu zählen sämtliche Daten- und Computernetze im lokalen wie auch im Weitverkehrsbetrieb — für die digitale Übertragung von Daten und Sprache gewährleistet.

Die sicherheitstechnischen Einrichtungen sind gemäß dieser Erfindung in bestehende Kommunikationsinfrastrukturen als aktive Komponenten integrierbar und können zusätzlich einen gesicherten Zugriff auf vorhandene Informationssysteme gewährleisten. Für diese Informationssysteme sollen keine oder nur minimale Erweiterungen oder Konfigurationsänderungen notwendig werden.

Wichtiges technisches Merkmal der STE ist, daß Benutzer sich eindeutig mit Hilfe von personalisierten Sicherheitsmodulen identifizieren und authentisieren müssen. Es ist allerdings auch möglich, daß die Funktionalität eines personalisierten Sicherheitsmoduls in die STE integriert wird.

Nachfolgend wird die Erfindung anhand von Ausführungsbeispielen näher erläutert. In den zugehörigen Zeichnungen zeigen die:

Fig. 1 eine Identifikation und Authentisierung der personalisierbaren Sicherheitsmodule und der sicherheitstechnischen Endeinrichtungen,

Fig. 2 eine Grundstruktur einer systemunabhängigen sicherheitstechnischen Endeinrichtung bzw. Security Base und die

Fig. 3 einen Einsatz von STE und Security Base als systemunabhängige Sicherheitseinrichtungen Voraussetzung für die authentische und vertrauliche Kommunikation ist, daß alle Kommunikationspartner (Teilnehmer) mit einem individuellen Sicherheitsmodul (Chipkarte) ausgestattet sind und über eine STE verfügen.

Will ein Teilnehmer sicher mit einem Partner kommunizieren, so muß er eine gültige Chipkarte in die STE oder einen Kartenleser der STE einführen. Der Teilnehmer muß sich gegenüber der Chipkarte durch Eingabe eines persönlichen Merkmals (z. B. PIN = persönliche Identifikationsnummer) identifizieren. Die Chipkarte authentisiert sich mit einem geeigneten Verfahren gegenüber der STE und die STE authentisiert sich gegenüber der Chipkarte, so daß alle Komponenten ihre Authentizität beweisen können.

Die hierfür zum Einsatz kommende Methode kann ein sogenanntes "challenge-response" Verfahren sein, das mittels eines Chiffrieralgorithmus und eines Geheimnisses (Schlüssel) zwischen den Komponenten eine verschlüsselte Zufallszahl austauschen (Authentisierungsparameter) und dadurch der Gegenseite den Besitz des Geheimnisses beweis, ohne daß dieses selbst preisgegeben werden muß. So kann die Chipkarte eine von der STE erhaltene verschlüsselte Zufallszahl dechiffrieren und an die STE zurückschicken, womit die Chipkarte beweist, daß sie im Besitz eins Geheimnisses ist (korrekter Entschlüsselungsschlüssel) und somit ihre Authentizität beweist. Die Authentikation der STE gegenüber der Chipkarte läuft analog.

Aus Sicherheitsgründen und praktischen Erwägungen soll die STE, die systemunabhängig ist, weil sie gemäß dieser Erfindung als systemunabhängige Komponente in die bestehende Infrastruktur integriert wird, möglichst direkt zwischen der bestehenden Kommunikationseinrichtung und dem Anschluß dieser an das Kommunikationsnetz installiert werden.

Versucht nun die Kommunikationseinrichtung eine

Verbindung zu einem Partner aufzubauen, so wird die STE selbständig aktiv und schaltet sich in den Kommunikationsfluß ein. Zunächst versucht die STE Informationen mit der gegenseitigen STE des Kommunikationspartners auszutauschen.

Gelingt dies nicht, (weil die z. B. gegenseitige STE nicht aktiviert wurde oder nicht vorhanden ist), so läuft die Kommunikation in gewohnter Form ab, wobei die STE eine Warnfunktion aktiviert. Diese Warnung an den Benutzer kann auf einem Display, durch Signallampen, einem Signalton oder ähnlichem ausgeführt werden.

Wird von der STE eine gegenseitige STE erkannt, so wird mit Hilfe eines Authentikations- und Schlüsselaustauschprotokolls ein Verschlüsselungsschlüssel (Sitzungsschlüssel) für ein Chiffrierverfahren zwischen beiden STE ausgehandelt. Das für die Erfindung verwendete Authentikationsprotokoll bietet dabei die sichere gegenseitige Authentikation der Chipkarten der Kommunikationspartner, den verwendeten sicherheitstechnischen Endeinrichtungen (STE) und übernimmt den Schlüsselaustausch. Dazu werden sogenannte "public-key" Verfahren eingesetzt.

Diese Verfahren zeichnen sich dadurch aus, daß für die Verschlüsselung ein anderer Schlüssel als für die Entschlüsselung verwendet wird. Daher kann einer der beiden Schlüssel für eine Verifikation veröffentlicht werden. Die Authentizität der verwendeten öffentlichen Schlüssel wird durch die Prüfung einer elektronischen Unterschrift eines Zertifikates, das den Teilnehmerschlüssel inklusive der Teilnehmeridentität und Zusatzinformationen enthält, gewährleistet. Dieses Zertifikat wird von einer vertrauenswürdigen dritten Instanz herausgegeben, die auch als Ausgabestelle der verwendeten Sicherheitsmodule wirken kann.

Die Identität des Kommunikationspartners, basierend auf dem in die STE eingeführten Sicherheitsmodul, wird der jeweiligen Gegenseite angezeigt, so daß nur mit dem Einverständnis des STE-Benutzers eine Kommunikation mit dem Partner möglich wird. Dazu verfügt die Erfindung über eine Eingabefunktion, die entweder über das angeschlossene Kommunikationsendgerät oder direkt an der STE betätigt werden kann.

Nach dem vertrauenswürdigen Schlüsselaustausch werden die Informationen zwischen den Kommunikationspartnern von STE zu STE mit dem Sitzungsschlüssel chiffriert übertragen.

Die Kommunikationspartner, die mit Chipkarte und STE ausgestattet sind, können somit ein geschlossenes Netz innerhalb einer offenen Kommunikationsinfrastruktur bilden.

Die Erfindung kann optimal zusätzlich gemäß der Ansprüche die Möglichkeit bieten, daß durch eine oder mehrere entsprechend erweiterte STE, sogenannte Security Basis (SB), Authentifikationsinformationen und Capabilities an die Kommunikationssysteme (beliebige Endeinrichtungen in bestehenden Netzen), nach der Authentikation übertragen werden. Mit Hilfe dieser Benutzerkennungen und Capabilities kann ein Kommunikationssystem die Zugriffsrechte auch von diesen verwalteten Objekten regeln. Diese Leistung wird dadurch erbracht, daß die in der SB definierten Benutzerbzw. Teilnehmerkennungen und Capabilities gespeichert und nach dem Ablauf der oben beschriebenen Authentikationsprozedur an das Endgerät übertragen werden.

Die Erfindung sieht vor, daß ein bestehendes Kommunikationssystem mit einem Modul (Security-Dämon) ausgestattet werden kann, das die Capabilities korrekt entgegen nimmt und einer Systemverwaltung zur Weiterverarbeitung übergibt.

Eine SB kann zentrale Sicherheitsmanagementaufgaben in einem Kommunikationsnetz übernehmen, indem sie für alle Teilnehmer Capabilities verwaltet.

STE und SB verfügen über Administrationsschnittstellen, die einem autorisierten Systemverwalter Zugang für Konfigurationsmöglichkeiten gestattet. Über eine derartige Schnittstelle können auch Zertifikate für Benutzer einschließlich öffentlicher Schlüssel geladen werden. STE und SB sind Kommunikationssysteme, deren Kommunikationsfähigkeit an die jeweiligen Systemschnittstellen angepaßt werden kann. So können speziell konfigurierte STE/SB in einem z. B. lokalen Netzwerk betrieben werden, wenn die STE/SB für das verwendete Kommunikationsprotokoll mit entsprechender Schnittstelle ausgerüstet wurde. Die Authentikations- und Chiffrierverfahren als zentrale Sicherheitsmechanismen werden unabhängig von der Systemkonfiguration immer mit gleicher Sicherheit bereitgestellt.

Die Sicherheitsfunktionen der STE und SB können auch angeboten werden, wenn nicht ein Sicherheitsmodul von einem Benutzer verwendet wird, sondern ein integraler Bestandteil einer speziellen STE bzw. SB ist. Die STE und SB wirken dann in einem benutzerlosen automatischen Betrieb. Dieser Betriebsmodus wird einer Gegenstelle während der Verbindungsaufbauphase signalisiert, so daß die Gegenstelle entscheiden kann, ob sie den Verbindungswunsch ablehnt oder annimmt. Auch ist der ausschließlich automatische Betrieb zwischen Kommunikationssystemen möglich.

Jede STE und SB ist eindeutig von einer dritten Instanz personalisierbar, so daß sie durch das Authentikationsprotokoll von einer Gegenstelle eindeutig identifiziert und authentisiert werden kann.

STE und SB enthalten eine Protokollierungskomponente, mit der es für den berechtigten Benutzer möglich ist, Ereignisse, wie z. B. berechtigte und unberechtigte oder abgelehnte Verbindungsaufbauten, Konfigurationsänderungen, abgebrochene Übertragungen usw., nachträglich zu kontrollieren.

Patentansprüche

1. Sicherheitssystem zum Identifizieren und Authentisieren von Kommunikationspartnern für Verbindungen über Kommunikationsnetze mit digitaler Übertragung, dadurch **gekennzeichnet**, daß mindestens allen sicherheitsbedürftigen Kommunikationspartnern, unabhängig vom verwendeten Informationssystem, jeweils an der Schnittstelle zwischen der zu sichernden Kommunikationseinrichtung und dem Kommunikationsnetz, je eine dem Netz angepaßte Sicherheitstechnische Einrichtung (nachfolgend STE) mit Eigenschaften einer Endeinrichtung beziehungsweise eine zur Sicherheitsbasis (nachfolgend SB) erweiterte STE, ein individueller Sicherheitsmodul und ein persönliches Merkmal zugeordnet werden, daß der Verbindungsaufbau von der STE bzw. SB übernommen wird und mit einer Prüfung verbunden ist, ob beim gerufenen Kommunikationspartner ebenfalls eine aktivierte STE bzw. SB erreicht wird und mit dieser ein Informationsaustausch und ein Authentikations- und Schlüsselaustauschprotokoll vorgenommen werden kann bzw. ob ein Warnsignal zu aktivieren ist, daß erst danach eine persönliche Authentisierung und die Betriebsartenentscheidung ein-

schließlich evtl. erforderlicher Schlüsselvereinbarung durchgeführt wird.

2. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE bzw. SB für eine automatische Kommunikation mit einem Sicherheits-Management Center (nachfolgend SMC) vorgesehen sind.

3. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, daß die STE bzw. SB mit Rechtedateien versehen sind, die Einträge und evtl. Leistungsmerkmale enthalten, wer in welchen Betriebsarten und evtl. mit welchen Partnern kommunizieren kann.

4. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE bzw. SB über eine Protokollierungskomponente verfügen, die relevante Ereignisse aufzeichnet und kontrollfähig gestaltet.

5. Sicherheitssystem nach Anspruch 1 bis 4, dadurch gekennzeichnet daß die Rechtedateien und Protokollierungskomponenten teils lokal und teils vom SMC und teils von beiden Seiten beeinflußbar sind und daß Ereignisse an das SMC gemeldet werden.

6. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE/SB bzw. SMC für ein dezentrales bzw. zentrales Sicherheits- und Schlüsselmanagement mit gespeicherten Zertifikaten und Schlüsseln vorgesehen sind.

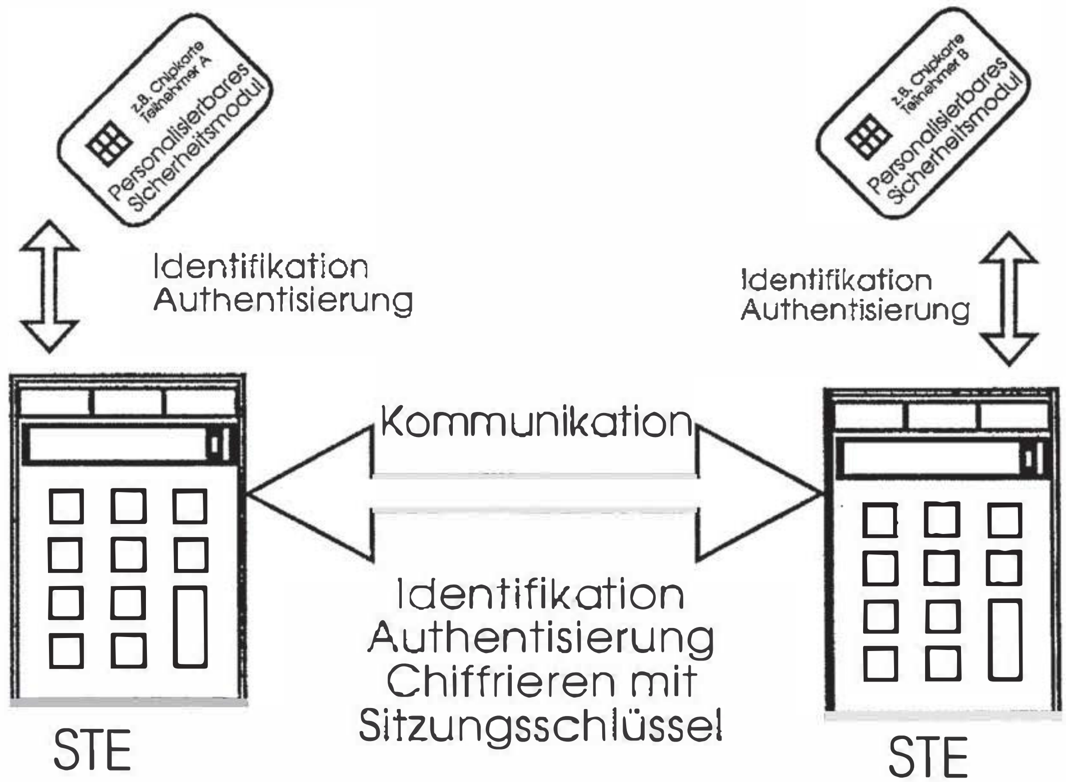
7. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE und SB eine digitale Unterschrift, eine Verifizierung von elektronischen Unterschriften und eine Ver- und Entschlüsselung als integrierten Dienst bereitstellen.

8. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet daß die STE/SB und SMC mit optischen bzw. akustischen Signalisierungsmitteln versehensind.

Hierzu 3 Seite(n) Zeichnungen

– Leerseite –

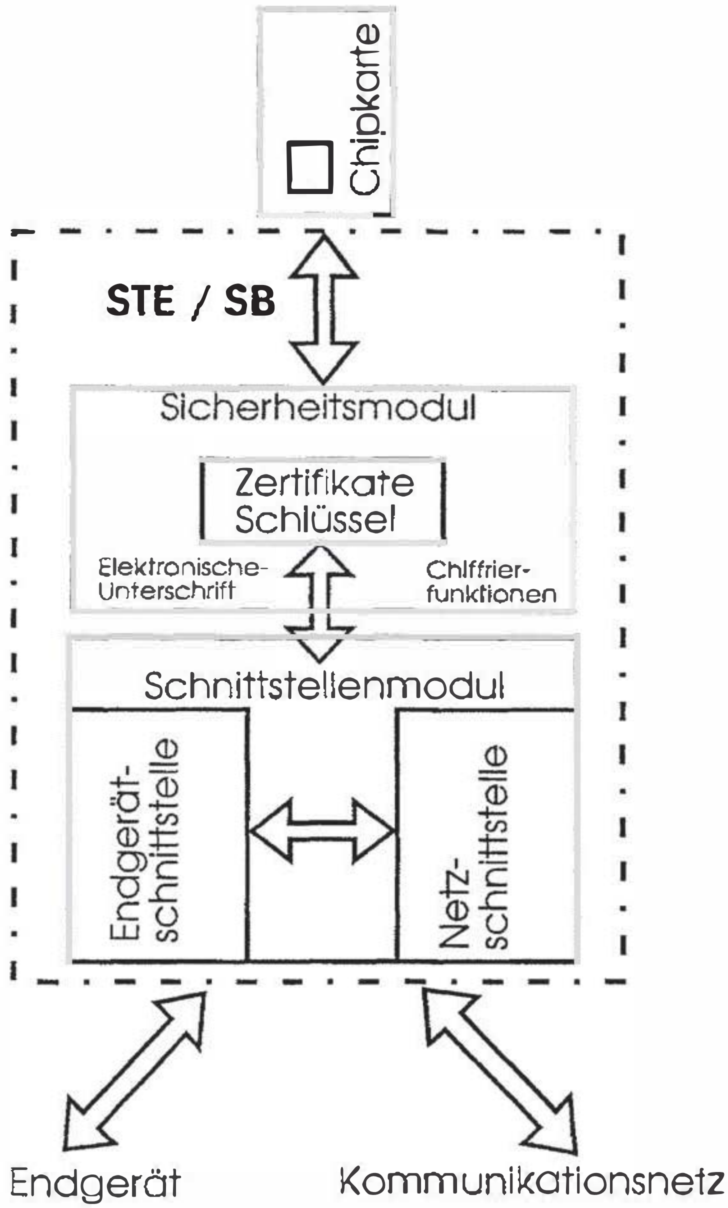
Nummer: DE 44 06 602 A1
Int. Cl.⁶: H 04 L 9/32
Offenlegungstag: 7. September 1995



Figur 1

508 036/84

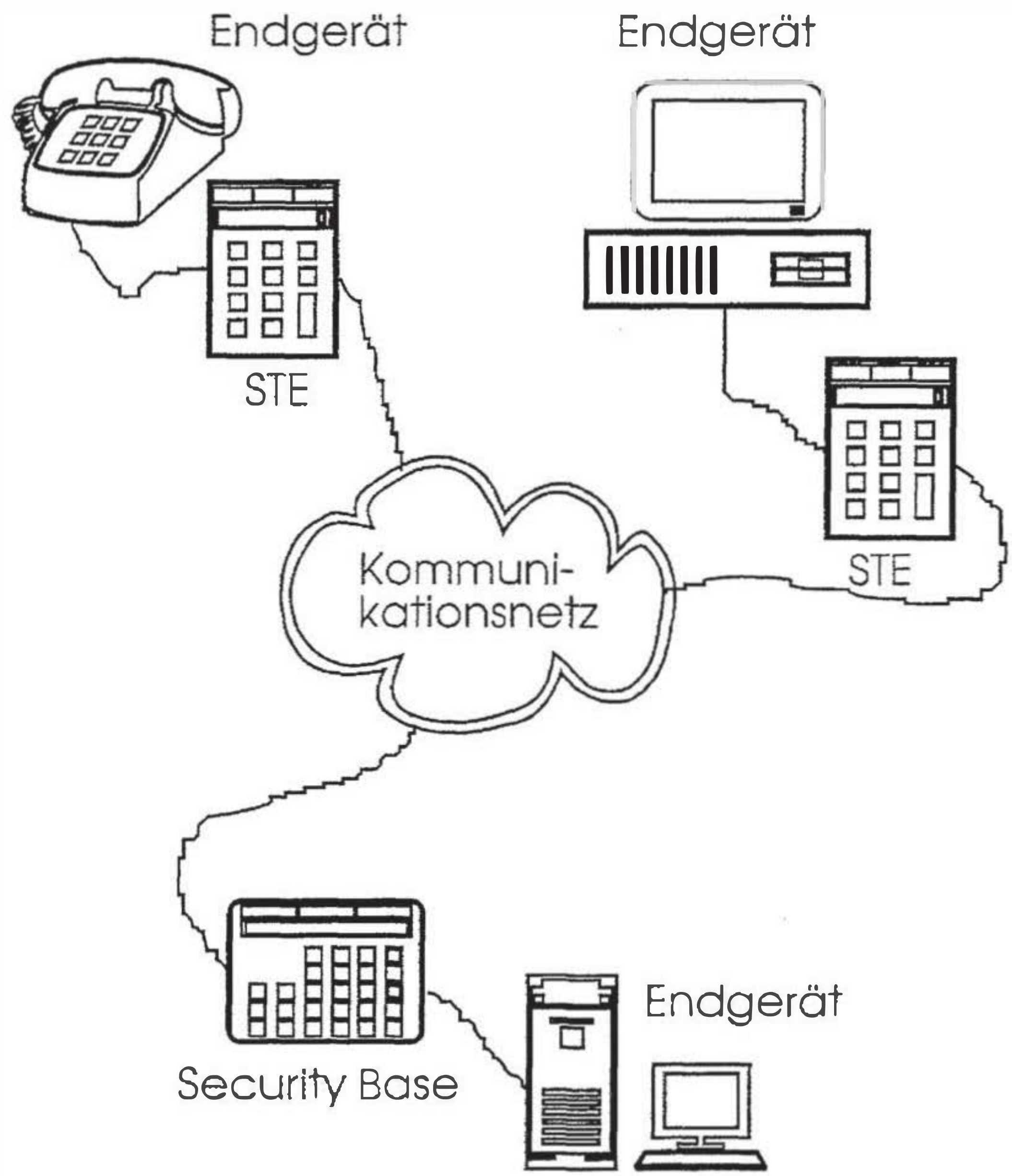
Nummer: DE 44 06 602 A1
Int. Cl.^{6}: H 04 L 9/32
Offenlegungstag: 7. September 1995



Figur 2

508 036/84

Nummer: DE 44 06 602 A1
Int. Cl.6: H 04 L 9/32
Offenlegungstag: 7. September 1995



Figur 3

508 036/84

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 172 670 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 85305293.4

(22) Date of filing: 25.07.85

(51) Int. Cl.4: G07F 7/00

(30) Priority: 27.07.84 US 635258

(43) Date of publication of application:
26.02.86 Bulletin 86/09

(84) Designated Contracting States:
AT BE CH DE FR GB IT LI LU NL SE

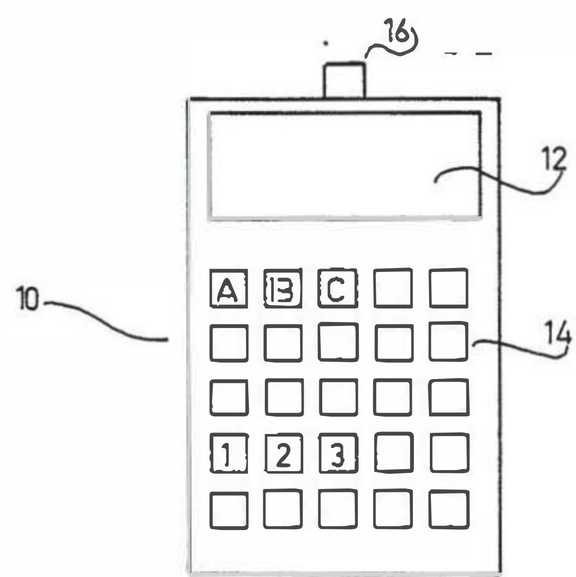
(71) Applicant: Technion Research & Development Foundation
Senate House Technion City
Haifa 32000(IL)

(72) Inventor: Even, Shimon
13 Vitkin St.
34756 Haifa(IL)
Inventor: Goldreich, Oded
42 Pinkas St.
Tel Aviv(IL)
Inventor: Yacobi, Yacov
Moshav Atzmon
Doar-Na Galil Maaravi (20138)(IL)

(74) Representative: Billington, Lawrence Emlyn et al
HASELTINE LAKE & CO Hazlitt House 28 Southampton Buildings Chancery Lane
London WC2A 1AT(GB)

(54) An apparatus for effecting and recording monetary transactions.

(57) Apparatus for effecting and recording monetary transactions including apparatus for registering the present value of money therein, apparatus for selectably adjusting the registered value to indicate a payment and receipt transaction, and identity verification apparatus including asymmetric cryptographic apparatus coupled to the apparatus for adjusting for activation thereof. The apparatus as a whole is provided as an electronic wallet (10) comprising a display (12), a keyboard (14) and a connecting jack (16).



EP 0 172 670 A2

Rank Xerox

AN APPARATUS FOR EFFECTING AND RECORDING MONETARY TRANSACTIONS

The present invention relates to an apparatus for effecting and recording monetary transactions.

Conventional wallets in which one carries cash money have long been known. One can open the wallet and extract an amount which does not exceed the present value therein, in order to make a payment, or one can receive payment from another party and deposit the received amount in the wallet, to increase the value therein accordingly.

Many methods exist for removing the inconvenience and risks of carrying cash in one's wallet. These include personal checks, traveler's checks, vouchers and credit cards, just to name a few. In addition, in order to eliminate the need for proximity during the transaction, methods have been developed for making payments from afar, such as using the mail system, telegraphing money orders and electronic fund transfer systems.

These systems suffer from a number of disadvantages. There is no easy way to verify that a payment received is not forged or that it is backed by proper credit (particularly in the case of checks and credit cards). Payments received cannot easily increase the current value or fund which is available for making payments. Electronic fund transfer systems are not suitable, in their present form, for use by an individual making an everyday payment.

There exist a number of so-called French Smart Cards distributed by a number of French companies which enable one to make payments but not to receive them. They are similar to ordinary automatic credit cards or banking cards, such as BANKOMAT in Europe, but the identification procedure seems to be more reliable since it may involve some cryptographic computations and not merely reading a magnetic tape. The details of their operation have not been published.

Davies' Signature Token described by D.W. Davies in "Use of the 'Signature Token' to Create a Negotiable Document", presented in Crypto 83, Santa Barbara, CA, U.S.A., August 1983 claims to enable the prevention of forgeries, but is unable to register the balance of the value available.

U.S. Patent 4,320,387 to Powell discloses apparatus for providing secured communication of information comprising individual units including display of information to be communicated, electronic circuit means providing automatic security of transmission between relatively remote units that are intended to be included in a specific transfer of information, electronic information storage means for recording of communicated information, and radiant energy signal transmitting devices for effecting coupling of any two selected apparatus units that are to participate in the information transfer. Time-base controlled signal encoding is utilized to effect generation of the communication to the two selected units and to provide security of transmission. This electronic circuitry includes a time-control base which is functional to change its control function in the same amount of time as that which would be required to complete one transaction in the recording phase of operation.

In operation, a coded signal corresponding to the information to be transferred is transmitted by one apparatus and received by the second. The receiving apparatus utilizes the same time-control base encoding to encode the data it expects to receive (i.e., as manually input by the owner). It then compares the received encoded data with the encoded expected data. If identical, the transaction proceeds. Since the encoder signal changes over time, certain fraudulent transactions are prevented since the received encoded data will not accord with the encoded expected data.

This apparatus suffers from a number of disadvantages. First, it is possible to bypass a portion of the identification system of each apparatus unit thereby lowering the security of the system. Second, and more importantly, knowledge of the time-control base function gained from any one apparatus unit permits one to engage in many fraudulent transactions, threatening the entire monetary system with collapse. Third, coded identification for all the other units are included in the memory of each unit, requiring a large memory capacity.

A preferred embodiment of the present invention may provide an electronic wallet which permits both payment and receipt of money, which includes an automatic identification system which prevents forgeries and which cannot be bypassed.

According to one aspect of the present invention there is provided an apparatus for effecting and recording monetary transactions comprising: means for registering the present value of money therein, means for selectably adjusting the registered value to selectably indicate payment and receipt, responsive to a manual control input; and identity verification means coupled to the means for adjusting for activation thereof.

According to a preferred embodiment of the invention, the means for selectably adjusting includes means for determining whether the transaction is permitted, and means for effecting transfer of value coupled to the means for registering present value.

Further according to a preferred embodiment, the means for identity verification includes cryptographic means which may include secret key encoder means arranged to encode data transmitted by the apparatus, and known key decoder means arranged to decode encoded data received by the apparatus.

Further in accordance with a preferred embodiment, the apparatus further includes cryptographic owner identification means.

Additionally in accordance with a preferred embodiment, the apparatus further comprises means for destroying the registered information which is activated by unauthorized physical entry.

There is further provided means for institutional validation of the apparatus.

According to another aspect of the present invention there is provided apparatus for effecting and recording monetary transactions including: means for registering the present monetary value of the apparatus; means operative in response to a first manual control input for identifying a permitted user; means operative in response to a second manual control input for registering the monetary value of a transaction; means for transmitting an encoded output signal corresponding to identification of the apparatus; means for receiving an encoded input signal corresponding to identification of an apparatus with which the transaction is to be effected; means for decoding and verifying the encoded received signal; means for transmitting an output signal corresponding to the monetary value of the transaction to the apparatus with which the transaction is to be effected; means for receiving an input signal corresponding to the monetary value of the transaction from the apparatus with which the transaction is to be effected; means for determining whether the transaction is permitted; means for transmitting an encoded output signal corresponding to the monetary value and direction of the transfer in the transaction to the apparatus with which the transaction is to be effected; means for receiving an encoded input signal corresponding to the monetary value and direction of the transfer in the transaction from the apparatus with which the transaction is to be effected; means for decoding and verifying the received signal; and means for adjusting the registered present value in accordance with the transfer effected by the transaction.

An apparatus of the present invention will be further understood and appreciated from the following detailed description taken in conjunction with the drawings in which:

Fig. 1 is an illustration of an electronic wallet constructed and operative in accordance with an embodiment of the present invention; and

Fig. 2 is a block diagram illustration of the electronic circuitry employed in the electronic wallet of Figure 1.

With reference to Fig. 1 there is shown an electronic wallet generally designated 10 constructed and operative in accordance with an embodiment of the present invention. The wallet may have the general appearance of a small pocket calculator, and comprises a display 12 of any conventional design, a keyboard 14 and a connecting jack or other coupling device 16.

Referring now to Fig. 2 there is shown in block diagram form the electronic circuitry employed in the electronic wallet of Figure 1. The circuitry includes a CPU 20 such as a microprocessor, including input/output interface and a ROM, for example model 8041A of Intel Corp., USA, a RAM 22, such as a 64K RAM, model number 2164 and associated controller 24, such as model 8203, both of Intel Corp., and an E^2PROM 26, such as an E^2PROM, 2K x 8, model 2817 of Intel Corp., all coupled by bus 28. The wallet is powered as by batteries (not shown). RAM 22 serves to register the present value of the wallet along with the various transactions in which it has participated, as will be explained in detail hereinbelow. Microprocessor 20 is operative to adjust the present value registered in E^2PROM 26 at any given time in accordance with a pre-programmed protocol.

A keyboard 30, which may comprise any conventional keyboard, preferably an alphanumerical keyboard, is coupled to microprocessor 20 for input of transaction data and personal identification codes. A display 34, which may comprise any conventional means for providing a visual display, is also coupled to microprocessor 20 for providing a visible output indication of the transaction data. There is also provided connecting means 38, such as a connecting jack or any other conventional means for coupling two electronic wallets for information transfer therebetween.

The electronic wallet also contains a real time clock 40, such as a Time of Day (T.O.D.) Clock, number WD2412, manufactured by Western Digital Corp., USA, which acts to record the time at which each transaction of the wallet occurs (30 bits are sufficient to represent time with resolution of seconds over a period of 30 years). The provision of a real time clock permits transactions between any wallets having compatible hardware and compatible transaction protocol while preventing such fraudulent transactions as improper repetition of a transfer.

In addition, the wallet preferably contains a list of cancelled wallets to prevent receipt of payments from wallets which have been found to be fraudulent or were reported stolen or lost. Such a list could be supplied to the wallet during validation. By issuing new series of identification numbers to the wallets periodically, this list can be kept short.

Preferably the wallet includes an audit trail, a list of all transactions of the wallet since the last validation, including all proofs of payments made to the wallet and receipts of all payments made by the wallet. The audit trail is retained in the RAM of the wallet until the next validation, at which time, the audit trail is transferred to the memory of the institution where validation occurs, and erased from the wallet. In addition to providing a record of transactions of the wallet, the audit trail also allows computation of the balance of a user who has lost his wallet, by tracing his credits and debits in the audit trails of the wallets with which the transactions occurred.

The wallet is also provided with user identification apparatus, which may comprise any conventional cryptographic system, to prevent unauthorized access to the wallet or tampering therewith. Thus, the owner of a wallet will have, for example, a password which is entered via the keyboard to the wallet to identify him at the start of a transaction.

The wallet also comprises, at any given time, an unforgeable "present value". For purposes of this application, unforgeable is defined as cryptographically signed in such a way as to force one to crack the cipher in order to forge a message. The value of the wallet is registered in the memory of the wallet and any increase or decrease due to receipt or payment of money is carried out and registered in accordance with a certain protocol, the new value being registered as the current present value. A conventional cryptosystem, such as the Data Encryption Standard, "DES Modes of Operation", FIPS PUB 81, Federal Information Processing Standards Publication, Dec. 2, 1980, may be utilized for encoding and decoding of information transferred from one wallet to the other.

In order to provide unforgeable present values and receipts, an asymmetric or public key encoding system is preferably employed for identity verification throughout the transaction. This means that a secret key, hard wired into the apparatus and known to no-one, is used to encode the data to be transferred to the other apparatus which is a party to the transaction. Similarly, data received from the other apparatus will be received encoded by the secret key of the other apparatus. A public key, or known decoder means, is provided to each apparatus to permit it to decode the data received by it before proceeding with the next step of the transaction. Thus, while any apparatus is capable of decoding the data received by it, only the legitimate wallet can encode data it transmits with its own secret key. This means that forgery is possible only by cracking the cipher using the public key.

A particularly suitable public key cryptosystem has been proposed by Rivest, Shamir and Adelman in "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Comm. ACM, Vol. 21, February 1978, pp. 120-126, to be utilized for internal encoding of data to be transferred between wallets. Alternatively, any other public-key signature cryptographic system will suffice, such as that described by Rabin, M.O. in "Digitalized Signatures and Public-Key Functions as Intractable as Factorization", MIT/LCS/TR-212, January 1979.

The various keys and passwords utilized by the owner for user identification, by the wallet for decoding and by the validating institution, will be found in the memory of the wallet. It will be appreciated that the preferred user identification and identity verification means are also suitable for identification from afar, such as through a telephone line or other means of communication.

It is a particular feature of the present embodiment that only the public keys of the banks or validating institutions and the public key of the owner signed by the bank need be retained in the memory of the wallet to permit transactions with all other wallets. Thus, a much smaller memory is required than in existing devices.

The particular advantage of using a public key cryptosystem is that, even if someone should manage to break the cipher in one wallet to forge transactions therein, he will be unable to subvert the entire banking system. Furthermore, if the wallet is forged, it will be detectable by means of the audit trails discussed above.

Preferably the wallet also includes means for destroying the information stored therein which is activated in the event that an attempt is made to penetrate the wallet physically or through some signals other than the legitimate signals used in the user identification means or in the protocols. For example, the wallet may be constructed in such a manner that opening it will short circuit the batteries, or destroy the microprocessor, or that x-rays or other attempts to read the encoded information will serve to destroy the coding. This serves to further prevent compromise of the whole monetary system by unauthorized entry into a wallet.

The wallet is validated through a renewal protocol with an authorized institution, such as a bank. The complementary device owned by the institution would read the audit trail of the wallet since its latest validation, erasing it from the wallet, insert the new value and supply additional information which may be useful. A flow chart of a suitable renewal protocol is given in the following chart.

RENEWAL PROTOCOL

Wallet   Authority

(Identification) ------------->

<----------------(Identification)

(Audit trail) ---------------->

<--------------(signed new keys)

<---------(list of invalid wallets)

where (DATA)----> indicates the transfer of data in the direction indicated by the arrow.

Transfers of money are effected by means of a transaction protocol. Operation of the wallet, in general terms, is as follows. For example, suppose i and j have agreed on a payment of v dollars by i to j. Each must first identify himself to his wallet by entering his password on the keyboard. Each enters the value v into his wallet and indicates whether it should be paid or received. Thus, a transaction may take place only if both parties agree to it.

The wallets are now coupled to one another via connecting means which may be a connecting jack or a telephone modem or any other means of coupling the wallets for transmitting and receiving of information from one another. The transfer of value from i's wallet to j's is carried out through a proper transaction protocol. It will be appreciated that such a transfer is only permitted if i's wallet has the necessary value, i.e., if the value of the paying wallet is greater than or equal to the sum to be paid. The result of the transaction is that the value in i's wallet has been reduced by v while the value in j's wallet has increased by v, the sum of the values of the wallets not being changed by the transaction.

An unforgeable receipt, or cryptographically signed proof of having paid the amount of the transaction, is provided to i's wallet in the form of data encoded by j's secret code, and registered therein. At the same time, an unforgeable proof of receipt of payment is registered in j's wallet in the form of data encoded by i's secret code. These proofs of payment and receipts are added to the wallet's audit trail.

A flow chart of an example of a suitable transaction protocol including a public key cryptosystem is as follows.

TRANSACTION PROTOCOL

```
        Wallet of i                                  Wallet of j

-->(i Password; Pay vi)                     -->(j Password; Receive vj)

Is Vi < vi?

If yes, (EM)--------------->

If no, Dx(ei,i)------------>

                                                  (ei,i):= Ex(Dx(ei,i))

                             <-----------(vj, t, Dx(ej,j)

Is vi = vj and is t reasonable?

If no,  (EM)--------------->

If yes,  (ej,j):= Ex(Dx(ej,j))

                             <------------Dj (-vj,t,i)

Di (vi,t,j)---------------->

(v",t",i"):=Ej(Dj(vj,t,j))                  (v',t',j'):=Ei(Di(vi,t,j))

If (v",t",i") = (vj,t,i),                    If (v',t',j') = (vi,t,j),

    then Vi:= Vi - vi                          then Vj:= Vj + vj
```

where: Vy = present value of wallet of y; vy = value in transaction involving wallet y; t = real time; (DATA)---> = transfer of data in the direction of the arrow; and (EM)---> = transmission of an Error Message, terminating the protocol.

Operation of the transaction protocol is as follows, with reference to the transaction protocol flow chart and with further reference to the transfer of the value v from i to j. Assuming a public-key cryptosystem is used, the public-key of user i is a pair of operators (Ei, Di) each of which is operative to cancel the operation of the other, i.e., for every word W, Ei(Di(W)) = W. Operators Ei and Di serve to encode and decode data being transmitted to and from wallet i. In order to operate Ei, one must use the public-key ei, and in order to operate Di, one must use the secret-key di. The knowledge of ei does not help to determine di. Even the owner of a wallet does not know the secret-key, di, stored therein.

The present contents of user j's wallet include ex (the public key of the bank or other renewing institution) and dj (j's secret key), as well as Dx(ej,j) (j's public key certified by the bank and indicating that this is a valid wallet). t represents real time as measured by the real time clock.

After i and j identify themselves to their wallets by inserting their respective passwords, and have inserted the value of the present transaction, the wallets are coupled to one another to establish communication, i.e, direct coupling or via a telephone. It will be appreciated that coupling of the wallets may alternatively be effected before user identification.

The value of the desired transaction vi is compared with the current present value Vi of i's wallet to determine whether the transaction is permitted. If vi is greater than Vi, an error message is sent, thereby terminating the protocol.

If vi is less than or equal to Vi, then i's public key certified by the bank, namely i's public key and identity (ei,i) encoded by operation thereon of the bank's public key (operator Dx) is transmitted to j's wallet. In j's wallet, this data is decoded by the operation of the public key of the bank (Ex).

Upon receipt of this data, the value j punched into his wallet as being the amount of the transaction (vj), the real time (t), and j's public key certified by the bank, namely j's public key and identity (ej,j) encoded by operation thereon of the bank's secret key (operator Dx) are all transmitted to i's wallet. In i's wallet, j's public key is decoded by the operation of the public key of the bank (Ex).

Wallet i now compares vi and vj to verify that the value of the transaction is equal. It also compares t received from wallet j with the real time at which it transmitted its identifying transmission to be sure that no more than a predetermined limited amount of time has passed since initiation of the transaction. If either vi ≠ vj or there is a mismatch of real time t (e.g., t≠tj + const), an error message is sent, terminating the protocol.

If vi = vj and t is reasonable, transfer of the value of the transaction is effected. J sends a receipt to i which includes the value paid by i (-vj), the real time, and the identity of i, all encoded by Dj (j's secret code known only to his wallet). Since Dj is secret even to j, this receipt is unforgeable unless the cipher is broken. Similarly, i sends a receipt to j which includes the value received by j (vi), the real time, and the identity of j, all encoded by Di (i's secret code known only to his wallet). Since Di is secret even to i, this receipt is unforgeable unless the cipher is broken. t prevents illegal duplication of the transaction.

In order to insure that the receipts correspond to the expected values and time of the transaction, each of wallets i and j decode the receipt using the public code of the other (Ei and Ej) and compare the decoded data with the axpected values of v, t and i. If they are identical, the new present value of wallet i, Vi, which equals former Vi - vi, is registered in the memory of wallet i, and the new present value of wallet j, Vj, which equals former Vj + vj, is registered in the memory of wallet j. To avoid cutting communication before the last transmission, i.e., when only one receipt has been sent, secret exchange methods can be used, such as those set forth in Blum, M., "How to Exchange Secret Keys", Proceedings of the 15th Annual ACM Symposium on Theory of Computing, and Even, S. Goldreich, O. and Lempel, A. "A Randomized Protocol for Signing Contracts", Proceedings of Crypto 82, July 1983, between the last two communications.

It will be appreciated that, while each wallet preferably has its own self-contained power source, the value of the wallet is stored in a non-volatile memory, so that if the battery is inoperative, a transaction may not take place, but the owner of the wallet will not lose his money.

The wallets are protected against loss of money in case of loss of the wallet or misuse by someone other than the owner, since one must know the password in order to operate the wallet. They are protected against fraudulent transactions, as by eavesdropping on telephone lines and attempting to duplicate the transaction, by real time t, which must be reasonable in order for the apparatus to carry out the transaction. Similarly, they are protected against forging a transaction over the telephone lines since a signed or encoded receipt is required to conclude the transaction. And they are protected against the coupling of two legitimate wallets via improper hardware.

It will be appreciated by those skilled in the art that the invention is not limited to what has been shown and described hereinabove merely by way of example. Rather, the scope of the invention is limited solely by the claims which follow.

Claims

1. Apparatus for effecting and recording monetary transactions comprising: means for registering the present value of money therein; means for selectably adjusting the registered value to selectably indicate payment and receipt, responsive to a manual control input; and identity verification means coupled to the means for adjusting for activation thereof.

2. Apparatus according to claim 1 and wherein said means for selectably adjusting comprises: means for determining whether the transaction is permitted; and means for effecting transfer of value coupled to the means for registering present value.

3. Apparatus according to claim 2 and wherein said means for effecting transfer comprises secret key encoder means arranged to encode data to be transmitted by the apparatus, and known key decoder means arranged to decode encoded data received by the apparatus.

4. Apparatus according to any preceding claim and further comprising cryptographic owner identification means.

5. Apparatus according to claim 2, or claim 3 or 4 when appended thereto and wherein said means for determining includes means for comparing the value of the transaction with the registered present value.

6. Apparatus according to claim 2, or claim 3, 4 or 5 when appended thereto, and whererin said means for determining includes means for determining whether the real time of the transaction falls within a predetermined range.

7. Apparatus according to any preceding claim and wherein said identity verification means comprises a public key cryptosystem.

8. Apparatus according to any preceding claim and further comprising means for destroying the registered information activated by physical tampering with the apparatus.

9. Apparatus according to any preceding claim and further comprising means for institutional validation of the apparatus.

10. Apparatus for effecting and recording monetary transactions comprising: means for registering the present monetary value of the apparatus; means operative in response to a first manual control input for identifying a permitted user; means operative in response to a second manual control input for registering the monetary value of a transaction; means for transmitting an encoded output signal corresponding to identification of the apparatus; means for receiving an encoded input signal corresponding to identification of an apparatus with which the transaction is to be effected; means for decoding and verifying the encoded received signal; means for transmitting an output signal corresponding to the monetary value of the transaction to the apparatus with which the transaction is to be effected; means for receiving an input signal corresponding to the monetary value of the transaction from the apparatus with which the transaction is to be effected; means for determining whether the transaction is permitted; means for transmitting an encoded output signal corresponding to the monetary value and direction of the transfer in the transaction to the apparatus with which the transaction is to be effected; means for receiving an encoded input signal corresponding to the monetary value and direction of the transfer in the transaction from the apparatus with which the transaction is to be effected; means for decoding and verifying the received signal; and means for adjusting the registered present value in accordance with the transfer effected by the transaction.

11. Apparatus according to claim 10 and wherein each of said means for transmitting comprises secret encoder means for encoding said output signals.

12. Apparatus according to claim 10 or 11 and wherein

each of said means for receiving comprises known decoder means for decoding said input signals.

13. Apparatus according to claim 10, 11 or 12, and wherein said means for determining includes means for comparing the value of the transaction with the registered present value.

14. Apparatus according to claim 10, 11, 12 or 13, and wherein said means for determining includes a real time clock and means coupled to said real time clock and to said means for receiving for determining whether the real time of the transaction falls within a predetermined range.

15. Apparatus according to any one of claim 1 to 9, wherein said identity verification means includes cryptographic means.

16. Apparatus according to claim 15, wherein said cryptographic means is an asymmetric cryptographic means.

17. Apparatus according to any preceding claim, which has the general size, shape and portability of a pocket calculator.

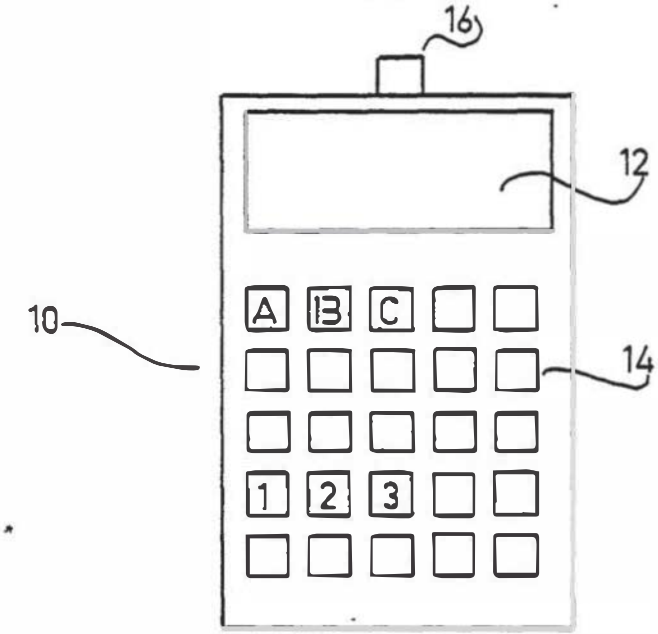

16
12
10
A
B
C
14
1
2
3

FIG 1

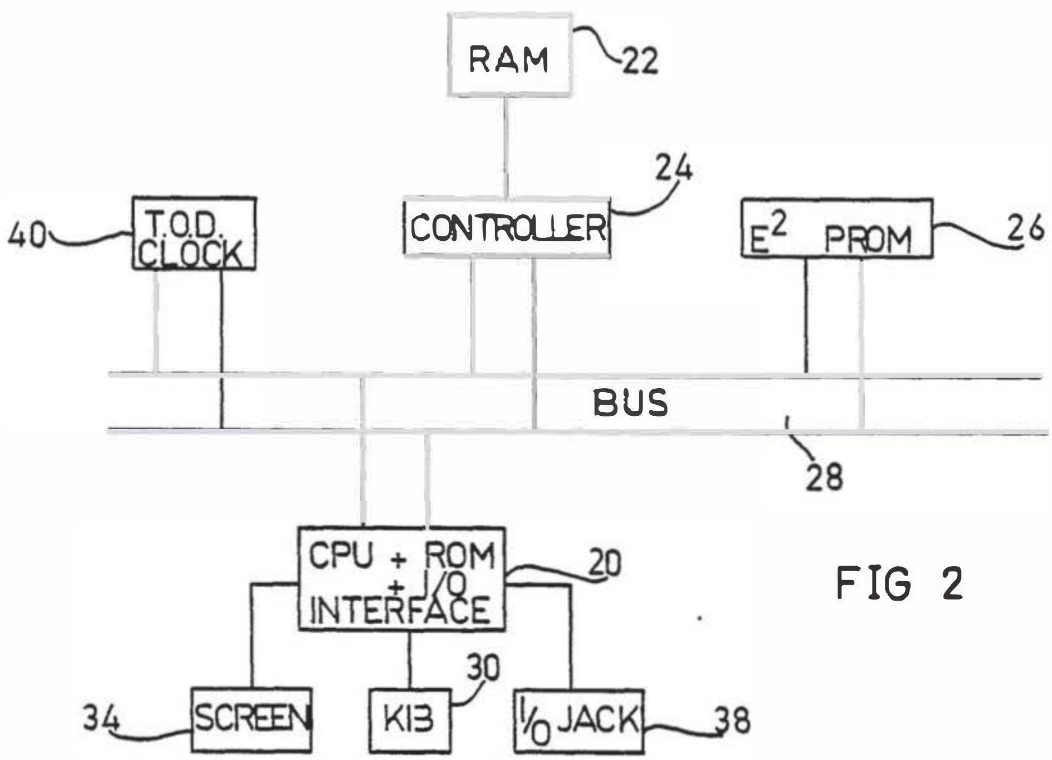

RAM
22
24
40
T.O.D.
CLOCK
CONTROLLER
E^2 PROM
26
BUS
28
CPU + ROM
+ I/O
INTERFACE
20
30
34
SCREEN
KB
I/O JACK
38

FIG 2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 172 670 A3

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number: 85305293.4

(51) Int. Cl.⁴: G07F 7/00

(22) Date of filing: 25.07.85

(30) Priority: 27.07.84 US 635258

(43) Date of publication of application: 26.02.86 Bulletin 86/09

(84) Designated Contracting States: AT BE CH DE FR GB IT LI LU NL SE

(88) Date of deferred publication of the search report: 21.01.87 Bulletin 87/04

(71) Applicant: Technion Research & Development Foundation
Senate House Technion City
Haifa 32000(IL)

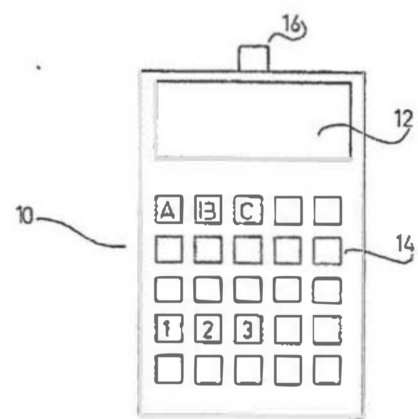
(72) Inventor: Even, Shimon
13 Vitkin St.
34756 Haifa(IL)
Inventor: Goldreich, Oded
42 Pinkas St.
Tel Aviv(IL)
Inventor: Yacobi, Yacov
Moshav Atzmon
Doar-Na Galil Maaravi (20138)(IL)

(74) Representative: Billington, Lawrence Emlyn et al
HASELTINE LAKE & CO Hazlitt House 28
Southampton Buildings Chancery Lane
London WC2A 1AT(GB)

(54) An apparatus for effecting and recording monetary transactions.

(57) Apparatus for effecting and recording monetary transactions including apparatus for registering the present value of money therein, apparatus for selectably adjusting the registered value to indicate a payment and receipt transaction, and identity verification apparatus including asymmetric cryptographic apparatus coupled to the apparatus for adjusting for activation thereof. The apparatus as a whole is provided as an electronic wallet (10) comprising a display (12), a keyboard (14) and a connecting jack (16).

Fig. 1



EP 0 172 670 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application number

EP 85 30 5293

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl 4)
X	ADVANCES IN CRYPTOLOGY, PROCEEDINGS OF CRYPTO '83, 22nd-24th August 1983, pages 383-386, Plenum Press, New York, US; S. EVEN et al.: "Electronic wallet" * Whole document *	1-17	G 07 F 7/10

Y	WO-A-8 102 070 (BENTON) * Page 2, line 6 - page 6, line 27; claims 1-17; figures 1,2; abstract *	1-17	

Y	GB-A-2 102 606 (NATIONAL RESEARCH DEVELOPMENT CORP.) * Claims 1-11; page 1, line 1 - page 2, line 32 *	1-17	
	---		TECHNICAL FIELDS SEARCHED (Int. Cl 4)
A	WO-A-8 303 694 (BENTON) * Page 2, line 33 - page 5, line 13; page 12, line 7 - page 13, line 15; claims 1,4; figures 1,4,5 *	1-17	G 07 F

A	GB-A-2 066 540 (THOMAS)		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	20-10-1986	GUIVOL,O.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
& : member of the same patent family, corresponding document

EPO Form 1503 03.82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 186 981
A2

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: 85308823.5

(22) Date of filing: 04.12.85

(51) Int. Cl.[4]: G07F 7/10

(30) Priority: 12.12.84 GB 8431381

(43) Date of publication of application:
09.07.86 Bulletin 86/28

(84) Designated Contracting States:
DE FR GB IT

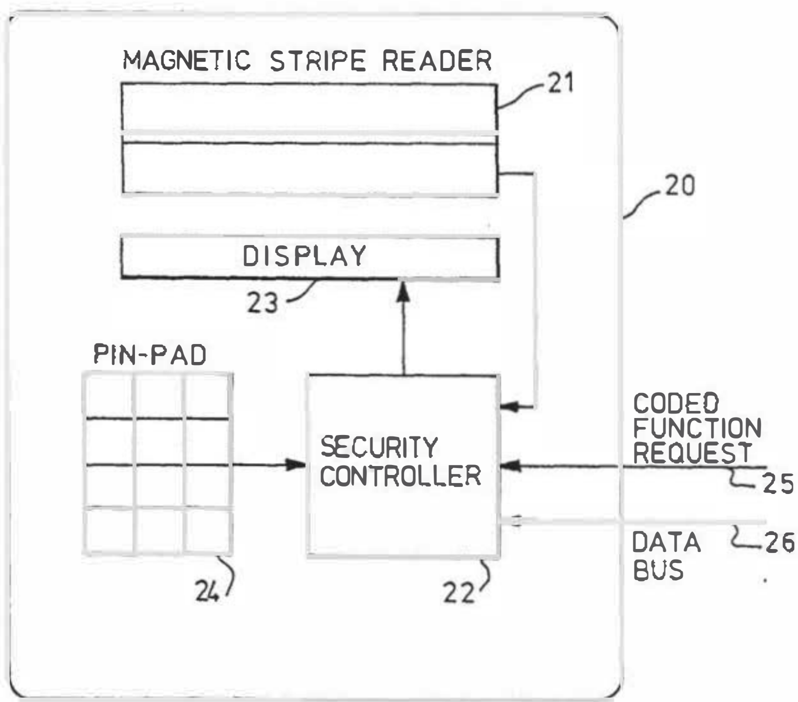
(71) Applicant: International Business Machines Corporation
Old Orchard Road
Armonk, N.Y. 10504(US)

(72) Inventor: Smith, Peter Rigby
1 Carpenters
Alresford Hampshire(GB)

(74) Representative: Appleton, John Edward
IBM United Kingdom Patent Operations Hursley Park
Winchester, Hants, SO21 2JN(GB)

(54) **Security module for an electronic funds transfer system.**

(57) A security module for use in an electronic funds transfer terminal is contained in a tamper-resistant housing. The module has a PIN pad and is designed to encrypt secret data, such as users personal identity numbers (PINs), so that other terminal processes cannot gain access to it. The encryption functions are carried out in a security controller which includes its own microprocessor and encryption/decryption unit.



EP 0 186 981 A2

SECURITY MODULE FOR AN ELECTRONIC FUNDS TRANSFER SYSTEM

The present invention relates to a security module for an electronic funds transfer system (EFT), and particularly to such a module that is to be used at a point of sale terminal in an EFT network designed to connect a plurality of disparate retailer's terminals through a switched telecommunications network to a plurality of funds holder's data processing centres.

In an EFT system in which many retailers having separate and different contractual relationships with card issuing funds holders and controllers it is necessary for the point of sale terminal to be able to respond uniquely to the different cards that it receives, and reads, from the card holding users. It is also necessary for the card holders to have confidence in the retailer's terminals and not be concerned that the retailer is trapping secret information, such as personal identification numbers (PINs), for later fraudulent use.

One system that has been proposed to deal with these problems is described in our UK Patent Applications Nos. 83/24916 and 83/24917. This system relies on the use of the so-called smart card in which the security operations, encryption and decryption of PINs etc., are computed in the card holder's personal portable microprocessor mounted in the card. This use of personal portable microprocessors is obviously a very flexible and secure system, but compared with the cost of magnetic stripe cards and considering the numbers involved the cost of the smart card is proving to be a hurdle to its widespread acceptance.

It is an object of the present invention to provide a technical solution to the problems of terminal flexibility and security confidence for use in an EFT/POS system in which the users have issued cards containing information held on a magnetic stripe and who also have a secret personal identity number, which may, or may not, also be stored on the magnetic stripe.

In broad terms, the present invention provides a technical solution to the problems posed above by including with each retail terminal a tamper-resistent security module. The security module can be physically included in the terminal housing or attached by a short cable through suitable input/output ports. Each module includes a microprocessor that is controlled to perform different message formatting routines depending upon the type and origin of a magnetic stripe card input through a magnetic stripe reader. The module also has incorporated within its structure a PIN pad for a user to enter security information such as a PIN.

According to the invention there is provided a security module, for authenticating messages having a plurality of different formats and cryptographic authenticators, contained in a tamper-proof housing and including two data input devices, a display unit, at least one input/ output port for connecting the module to an external processor and a security controller, characterised in that the security controller includes: at least one read only memory which stores a state table and a module master encryption key; a control logic unit including a microprocessor and a control store which stores a plurality of different control function routines invoked by different entries in the state table; means to generate different encryption keys dependant upon a particular control function and a derivative of the module master key; and means to perform encryption and decryption operations on messages transmitted to and from the module using keys transmitted to the module encrypted under one of a number of derivatives of the module master key, whereby data input to the module at the first of the two data input devices is used to determine the control function routine that the module is to perform and the encryption key used to encode data input at the second data input device.

According to a second aspect of the invention there is also provided a method of using a security module in an electronic funds transfer system terminal to secure secret data from other terminal processes, and in which the security module has a data input device for receiving secret data comprising the steps of: storing in the module a set of master keys each encrypted under a respective function key; transmitting to the security module from a terminal process a function request and a function key; decoding the appropriate master key using the function key; and encoding the secret data using the decoded master key in the security module and transmitting the encoded data to the terminal processes.

In order that the invention may be fully understood a preferred embodiment thereof will now be described with reference to the accompanying drawings in which:

Figure 1 is a schematic diagram of a portion of an EFT/POS network.

Figure 2 is a schematic diagram showing the major components of a security module.

Figure 3 illustrates the connection between the security module, a POS terminal and a remote application processor.

Figure 4 shows how the security module is shared between two applications.

Figures 5, 6, and 7 illustrate the construction and methods of operating the security module.

Figures 8, 9, 10 and 11 are flow charts illustrating the operation of the security module.

Referring now more particularly to the drawings, in order to provide an understanding of the background of the invention there is initially a general discussion on the design of EFT networks.

There are many possible designs and ways of defining the equipment at the point-of-sale in EFTPOS. Most of the designs can be characterised by the fact that the EFTPOS "terminal" is a complete system, that is, it is a complete add-on to the POS equipment, for the purpose of EFTPOS.

Viewed from the Access Controller (AC) the "terminal" is seen as a system with which the AC has a communications session. In Open System Interface (OSI) terms, the AC and terminal are two systems with one or two networks (Telecommunication local network and the In-Store network).

Figure 1 shows a retailers connection to an EFT network. An instore network 10 has several EFT/POS terminals connected to it. Each unit comprises a retailers point of sale terminal 11 and an associated electronic funds transfer terminal 12. The in-store net 10 is provided to link the terminals 11 and 12 and the combined POS equipment to the local network 14 through a network termination point 13. The local telecommunication network 14 has a connection to an access controller (AC) 15.

The network termination point 13 is the retailers connection point to the local network 13, the "phone jack". The combination of 11 and 12 provide the full facilities necessary to perform EFTPOS transactions.

The EFTPOS "Terminal" in the main will be a distinctive secure unit with a magnetic stripe reader, pin-pad, display, security processor and transaction processor. The terminal is responsible for the whole of the transaction, it includes the terminal application control function which performs EFTPOS in conjunction with the AC. It is also necessary for the terminal to support individually managed keys for any card issuer who wants them.

Previously the terminal has been considered to be responsible for the EFTPOS transaction in combination with other retailer equipment such as cashier display for total value input and most, importantly, for communication to the telecommunication network and transaction record printing.

The terminal described below appears similar, but has actually changed significantly. In this view, the EFTPOS "terminal" as seen from the EFTPOS network is an application running in the retailers equipment making use of a security controller in a secure PIN pad (SPP) or security module.

The security module is available to this application to provide an authentication service, its function is to provide a service which allows the card issuer to be satisfied that the correct procedures have been adhered to.

The basic component parts of the security module are shown in Figure 2. The module 20 includes a magnetic stripe reader 21 connected to a security controller 22. A liquid crystal display is also connected to the controller. Typically the display will have two lines of eighteen characters. A pin-pad 24 is connected to the controller and coded function requests are received on a line 25 from an application process running in the main terminal processor. A data bus 26 connects the security controller to the application process which can also have a direct connection to the display.

It may optionally contain a distributed portion of the retailer equipment application running in a processor with memory.

The security controller 22 is the only standard component and must be supplied by an authorised source. It must be connected to the pin-pad 24 and magnetic stripe reader 21 in a manner which satisfies the security requirements of EFTPOS, and the security module must be built to conform to the security and physical standards of EFTPOS.

Within the retailers equipment (optionally within the security module) the terminal system includes a processor (or distributed application on more than one processor). The application supports the management of cryptographic keys and their storage as defined by EFTPOS.

The security controller 22 is a special purpose cryptographic unit. It contains two values - an identification number (SCID) and a master key (SCMK).

The SCID is recorded in the security controller during the manufacture process, the SCMK is installed subsequent to manufacture but prior to first installation onto the network by a secure means specified by EFTPOS. A security controller is regarded as authentic if it produces cryptograms which prove that it contains a valid (SCID, SCMK) pair. The application processor (or processors) will hold keys encrypted under variants of SCMK. The security controller provides a set of functions which will not disclose SCMK. SCMK is held in a secure manner and will be destroyed as a result of any action that might allow SCMK to be discovered.

The identification SCID is not secret, in fact, it may be stamped or written onto the security module to aid the inventory and maintenance processes.

The application may be allowed direct control of the display 23 and the security controller communicates with the application process, via an internal bus. This communication may be extended to a distant processor, or part of the application may be distributed to a processor within the security module, communicating between parts of the systam by any suitable means.

A set of functions communicated over the SC buses are:

0 - Reset

1 - Read MSR

The SC waits for a card to be read, strips out non-transmitted card data (NCD), stores it in a register and sends the transmitted card data (TCD) as a response.

Possible responses:

1 - Card read + TCD

2 - Mis-read

2 - Provide authorisation token

3 - Start message authentication check (MAC) calculation (key provided under variant of SCMK)

4 - MAC input data

5 - Finish MAC calculation - return MAC

6 - Given encrypted CIRN token + key

7- Check PIN

Input authentication token + key

Result indication + confirmation token

Result = 1 PIN ok, + token

2 PIN failure

The security controller will refuse to perform this function more

than three times, after this it will require a reset.

8 - Give next key

Input key under variant of SCMK

Output new key under variant of SCMK

The security module contains a record of the function number of the most recent use. It will respond correctly only if the current function request is the next in an allowable sequence.

Failure to conform to the correct sequence will render the security module inactive, a state which can only be changed by a 0 - Reset function.

Since the security controller has access to important transaction data, and it generates MAC's, there is a wide range of possibilities for the algorithm for generating next key in function at step 8.

The security scheme may call for the security controller to maintain a synchronised time reference value. If this is the case, then there will need to be a further function to set the time reference and a further key TRK in the security controller to authenticate any value set into a time register (TR). The security controller could return the TR on function 0 (reset), or yet a further function call.

The security module is used by the application in a manner similar to the use of a set of support subroutines. If the application uses the correct sequence of calls (functions) providing the correct data and keys (encrypted under SCMK variants) then the result will be tokens and MAC's which will collectively allow the card issuer host to authenticate the security module, the card and card holder. If incorrectly used, the authentication will fail, and the security module cannot be mis-used in a manner which will subvert the system without access to considerable amounts of other data and collusion of several parties in different locations.

This removes the following responsibilities, which are normally considered to be functions of an EFTPOS terminal, from the security module:

Transaction management.

The security module provides services to allow a remote host to be satisfied that a procedure has been followed. This is achieved because of the existence of tokens (MAC's and cryptograms) which can only be produced by a valid security module, together with secret information, which has been used in a correct manner.

Recovery responsibility

The previously assigned recovery responsibility of the EFTPOS terminal can now be assigned to retailers equipment and applications code.

Key management

The security module need only have one key (or possibly a small number as indicated by a need for downloaded information such as synchronised time references). This (or these) keys will be installed by a fixed key loading procedure. In EFTPOS this could be a central facility.

Alternative uses of the security module

The security module finds other uses in networks that require cryptographic transmission of information and further examples are now given as they would apply to an EFTPOS network.

First the use of the security module as an authentication device shared by several applications and secondly the extension of the security module by the addition of a 'state variable' which allows its use in alternative and exclusive cryptographic schemes.

1) Use by Multiple Applications

The partitioning of function is illustrated in Figure 3 which shows the security module 20 connected over lines 25 and 26 to interface A of a terminal 27 which contains local application processes and at least a set of cryptographic keys 28. The terminal is connected through interface B to a processor of remote application processes 29 through a network route indicated as 30.

Interface B is precisely the network appearance of an EFTPOS terminal. Interface A is used to communicate the data which requests the security module to perform its available functions and to return the results to the application.

Since the function of the security module is to provide data and tokens which allow a remote application to validate the procedures employed at the local site, it follows that one security module can be used by any number of local applications, and in turn any number of remote applications for the similar purposes.

The security module represents a serially re-usable resource. It can only be used successfully for a complete legal sequence by one application at any time.

The keys used by the application process will be held at the local processor encrypted under variants of SCMK, the security module's security controller's master key.

Figure 4 shows the security module being made available to two local applications A and B. The security module 20 is connected to a terminal 27 which is running two applications A and B. Three remote processors are shown 31,32 and 33 connected through the switch 30. The security module 20 is used to authenticate procedures and data for the remote hosts 31, 32 and 33 using a combination of applications A and B.

Note : The keys held at the remote hosts will be encrypted under the appropriate host master keys.

2) Use of Alternative Cryptographic Schemes

The security module as described above is defined as enforcing a single procedure. In particular, it withholds data read from the card (or other means) which will be retained as secret from the local application and any other components between the security module and the remote host. Primarily for use in personal key (KP) cryptography where KP must be constructed using that secret.

To extend this scheme, it is necessary to allow the security module to handle several procedures, ie, several sequences of function calls. As an example consider the use of the SC in a second scheme which requires that the entire track 2 of the card be transmitted (encrypted).

To achieve this extension, the security module must contain a 'state variable'. This represents the history of the sequence of functions performed since the last reset operation. The sequences now contain points at which the possible next function is one of a set of functions rather than one function, a branch point.

The state of the terminal takes a value depending upon the function requested at any branch point. Thus, the next allowable function is decided by a combination of the last function requested and the value of the state variable. The state variable is updated to represent the new state once the function is requested. As before, any deviation from the prescribed sequence will result in a security module becoming inactive, ie, the previous description has a single state.

To demonstrate this, consider the list of functions described above.

Following a function 1, the application may decide that the card must be handled without personal key cryptographics. It wishes to read all of track 2. Thus, a new function - say 100, may follow function 1.

100 - Read all card data. Input KEY encrypted under variant variant of SCMK. Return all of card data (including NCD) encrypted under KEY.

The state variable will take a different value if function 100 follows function 1, than it would if function 2 follows function 1. If the function following 1 is 100 then the security controller will prohibit the use of functions 2, 3, 4, etc. This allows alternative exclusive schemes to be implemented.

In particular, subject to secure design of the functions and states, it allows any schemes to be implemented, including conflicting schemes such as those which require track 2 of a card to be partially secret together with those that require the whole of track 2 to be made available.

Master Key Variants.

The use of SCMK variants must be selected, based on the requested function and state variable to enforce partitioned use of security controller functions in the security module in alternative schemes. Thus, each scheme must use selected key variants.

The number of the variant to be used can be selected from a table based on the current state and the requested function. The key used in the operation can be formed by deciphering the selected variant number using SCMK. This means that keys in the application will be held in the following form :-

E (D (SCMK, variant no.), KEY)

Using the notation E (key, data) means data enciphered under key and D (key,ciphertext) means the result of deciphering ciphertext using key.

This approach would allow schemes for separation of function by intended destination. Such a scheme is shown in Figs 6 and 7. The security controller ID and destination data extracted from the card magnetic stripe track 2 are used to provide a separation of keys.

The security can be enhanced if the key variant is produced by a one-way function in place of the simple decipher operation.

The variant number key is loaded at the same time as the state tablle (ie. at manufacture or installation of keys).

This scheme can be further enhanced by selecting further information from a further table to generate the destination information prior to producing the master-key variant as above. This latter table can be down-loaded to the security controller periodically (eg. at start of day). As with other possible down-loaded information the table load operation requires authentication using additional keys.

Security Module

The internal components of the security module will now be describe with reference to Figures 5, 6 and 7. The security controller 22 (Figure 2) is shown in more detail in Figure 5 and comprises a state table 51, which in a preferred embodiment is implemented in a read only memory (ROM) chip, the address is formed by concatenating outputs from three registers. The registers are shown separately as State 52, Last Function 53 and Function 54, but in practice are parts of a random access store (RAS).

The state register 52 holds a value which represents the current state of the security controller. The contents of the state register 52 are also available to be tested by the control unit 56. One value of the state register contents, for example zero, is designated to indicate that the unit is inactive following an invalid function request sequence. The control unit only permits a RESET function request when the inactive state is detected. The value in the last function register 53 represents the function performed on the previous cycle of operations of the security module. The value in the function register 54 represents the current function to be performed. The function register 54 receives its input from the application process on line 25 (Figure 2) and has a direct connection to the last function register 53. The state register 52 receives its input directly from the state table 51.

The output of the state table is split into two fields, one field is entered into the state register and the other is used as the address of a master key table 55. The master key table provides one of a set of master key values to a user key decipher unit 57. The value depends upon the function currently being performed and the values entered into the state table from the three registers. The master key tablle could be part of the state table ROM but it is preferred that the values are generated as functions of a single key. Embodiments implementing the preferred system are described below with reference to Figs 6 and 7.

The operation cycles for each function performed by the security controller are controlled by a control logic unit 56. The control unit interprets the function request and provides the appropriate timing and control signals to route data signals between the other components. The unit comprises a microprocessor and a ROM containing the control routines necessary to provide the required gating and control signals. Each routine is associated with a particular function and will result in a different encoding and decoding operation in the controller.

The user key decipher unit 57 deciphers the user key received from the data bus 26 through a buffer store 60 under the control of unit 56. The decipher key is obtained from the master key table 55. The user key decipher unit implements the decipher function of the Data Encryption Standard (DES).

A working register 58 is loaded with a key produced by the user key decipher unit 57. The working register 58 may also be loaded from the data bus 26 under the control of unit 56 whenever a function routine requires the generation of composite keys, for example a key constructed from card input data, other user data and a variation of the master key. The value loaded into the working register represents a key in the clear and is not transmitted out of the security controller. In order to ensure that the clear key exists for the minimum necessary time, at the end of each cycle the working register is loaded with a string of zeros.

An encryption unit 59 performs the primitive encryption operations needed for the operation of the requested function. This unit implements the DES. The keys for the encryption are received from the working register 58. Output from the encryption unit 59 is fed to a buffer store 60 which temporarily holds all data and intermediate results during the processing required by the requested function.

In operation the security controller reads a value representing a function request into the function register 54. Each function is performed by executing a cycle of operations. The cycle consists of standard initial and final sequences of operations with a main sequence selected on the basis of the requested function. The initial and final sequences are illustrated in the flow-charts of Figures 8 and

9. The reset function is illustrated in Figure 10. The sequence for the function for reading the data input at the magnetic stripe readed is illustrated in Figure 11, this is given as an example of other function sequences that the control unit follows.

In the following description of the operation of the security controller the state register contents will indicate a value of zero when an invalid function sequence is requested, this indicates an inactive state of the module.

The steps of the initial sequence (Figure 8) are:

Step 1 (81): Determine whether the function request = 0, if so them go to the Reset routine (Figure 10), if not then proceed to next step.

Step 2 (82): Determine whether the value in the state register 52 = 0, if so then go to step 3 (83), if not then proceed to step 4 (84).

Step 3 (83): Provide an output failure indication to the terminal processes and to the display unit. Finish the routine.

Step 4 (84): Strobe the function register.

Step5 (85): Strobe the state register.

Step 6 (86): Determine whether the value in the state register 52 = 0, if so then go to step 3 (83), if not then proceed to select the sequence indicated by the value in the state register.

The steps of the final sequence (Figure 9) are as follows;

Step 1 (87): Strobe the last function register to preserve the value of the current function request.

Step 2 (88): Set the working register to all zero contents, to erase the clear version of the encryption key used for the current function. End the function.

The reset function consists of one step (89) and that is to strobe the function register, and then go to the final sequence.

The steps for Function 1 (Read the magnetic stripe reader) are shown in Figure 11 and are as follows:

Step 1 (90): Wait for a card to be read.

Step 2 (91): Read the card, if the read data is satisfactory then go to step 4, if not then go to step 3.

Step 3 (92): Provide an output failure indication to the terminal processes and to the display unit. Finish the routine.

Step 4 (93): Determine the card data to be transmitted (TCD). For example the TCD may be defined as those digits from card track 2 between start sentinel and field separator.

Step 5 (94): Generate an output indication that the previous step has been carried out successfully and transmit it to the terminal processes.

Step 6 (95): Output the TCD to the terminal on data bus 26, then go to the final sequence routine (Figure 9).

This sequence will have a series of sub-routines at step 4 each providing a different set of TCD and chosen on the card issuers identity read at step 2.

Other function routines follow the same general pattern of the sequences described above.

Claims

1. A security module, for authenticating messages having a plurality of different formats and cryptographic authenticators, contained in a tamper-resistant housing and including two data input devices, a display unit, at least one input/output port for connecting the module to an external processor and a security controller, characterised in that the security controller includes:

at least one read only memory which stores a state table and a module master encryption key;

a control logic unit including a microprocessor and a control store which stores a plurality of different control function routines invoked by different entries in the state table;

means to generate different encryption keys dependent upon a particular control function and a derivative of the module master key; and

means to perform encryption and decryption operations on messages transmitted to and from the module using keys transmitted to the module encrypted under one of a number of derivatives of the module master key; whereby data input to the module at the first of the two data input devices is used to determine the control function routine that the module is to perform and the encryption key used to encode data input at the second data input device.

2. A security module as claimed in claim 1 further characterised in the the security controller includes at least three registers:a function register, a last function register and a state register and that the state table is addressed by using a combination of the current entries in the three registers.

3. A security module as claimed in claim 1 or claim 2 further characterised in that the security controller includes a buffer store and data input from the two data input devices are stored in the buffer store before being encoded and in which the first data input device is a magnetic stripe reader and the second data input device is a PIN pad.

4. A security module as claimed in any one of claims 1, 2 or 3 including means to detect when an invalid sequence of functions has been requested for the module to perform and to invoke an abort routine when an invalid sequence is detected.

5. A method of using a security module in an electronic funds transfer system terminal to secure secret data from other terminal processes,and in which the security module has a data input device for receiving secret data comprising the steps of:

storing in the module a set of master keys each encrypted under a respective function key;

transmitting to the security module from a terminal process a function request and a function key;

decoding the appropriate master key using the function key; and

encoding the secret data using the decoded master key in the security module and transmitting the encoded data to the terminal processes.

6. A method as claimed in claim 5 in which a single master key is stored in the security module and derivative master keys are generated from the master key using predetermined function request data received from the terminal processes.

7. A method as claimed in claim 5 or claim 6 in which the terminal has at least a second data input device for receiving data from a user and the operable terminal process is dependant data input at the second data input device.

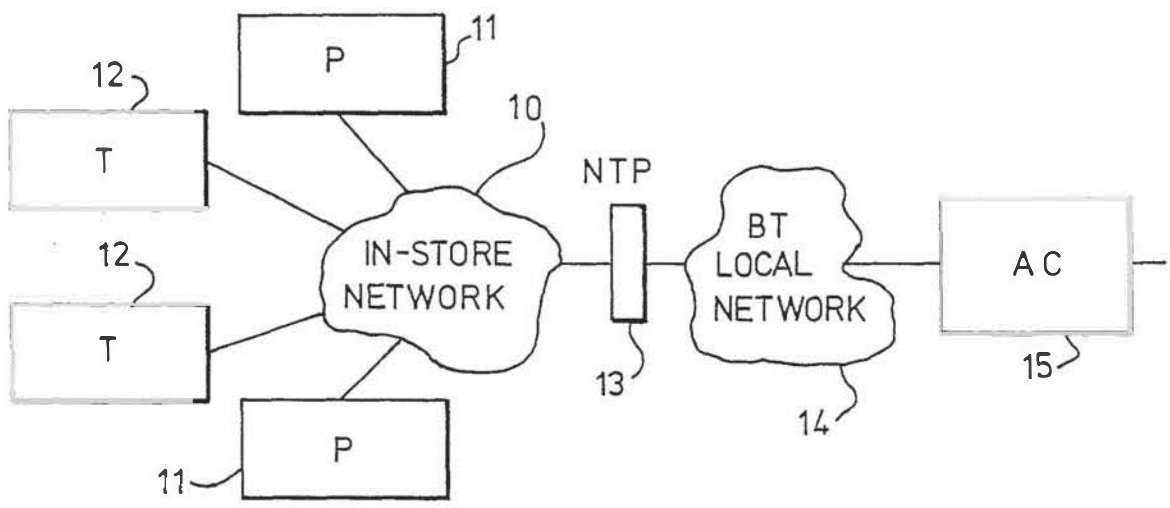

P
11
12
T
10
NTP
BT
LOCAL
NETWORK
IN-STORE
NETWORK
AC
12
T
13
15
14
P
11

FIG. 1

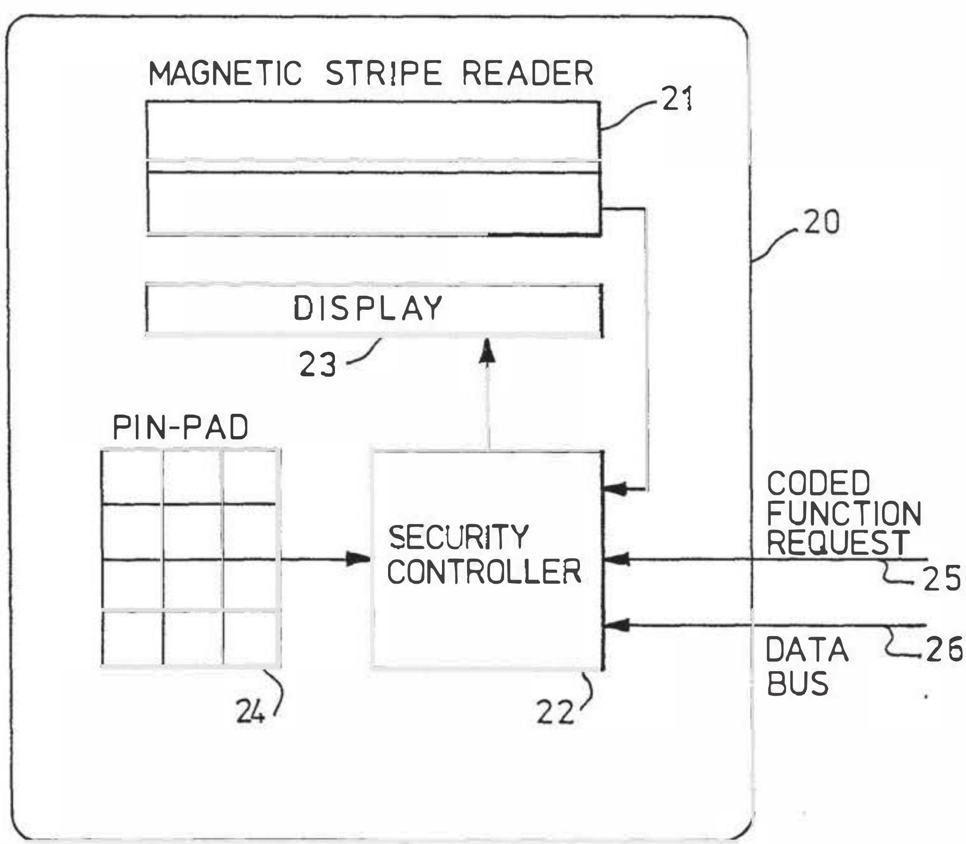

MAGNETIC STRIPE READER
21
20
DISPLAY
23
PIN-PAD
CODED
FUNCTION
REQUEST
SECURITY
CONTROLLER
25
DATA
BUS
26
24
22

FIG. 2

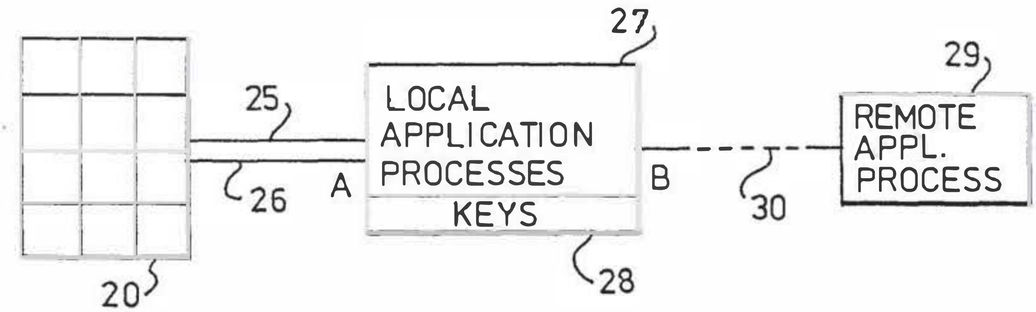

27
29
LOCAL
APPLICATION
PROCESSES
KEYS
REMOTE
APPL.
PROCESS
25
26
A
B
30
20
28

FIG. 3

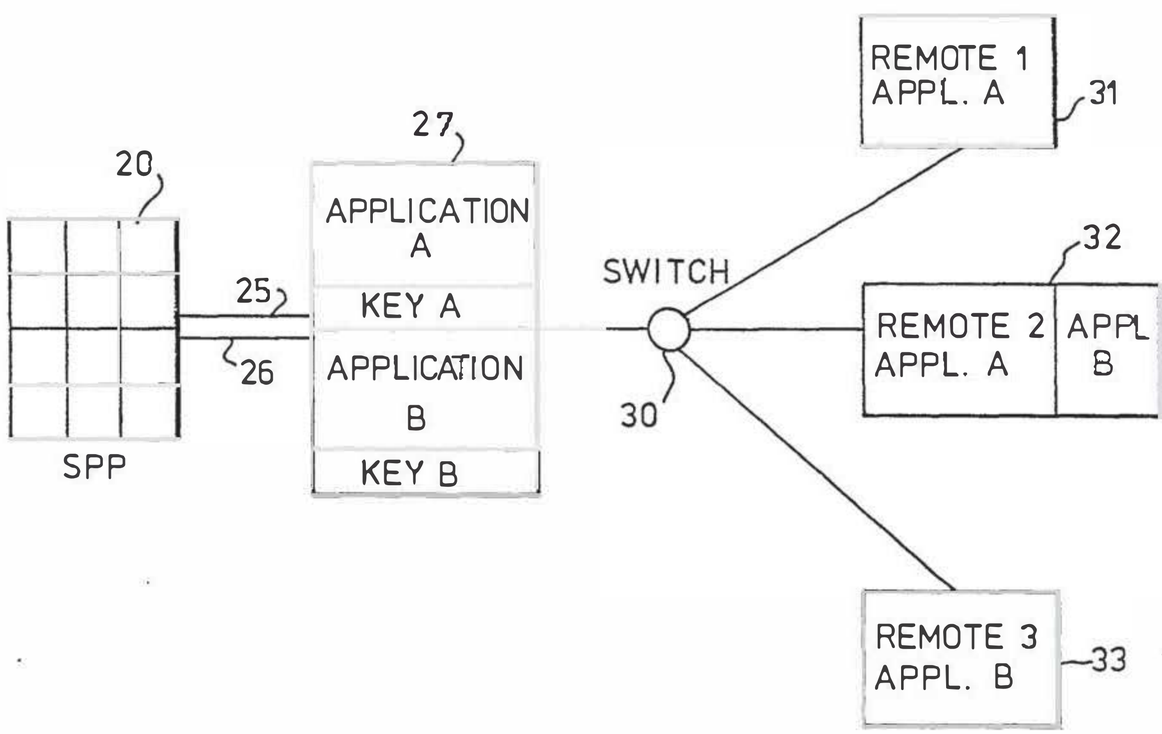

REMOTE 1
APPL. A
31
27
20
APPLICATION
A
KEY A
APPLICATION
B
KEY B
25
26
SPP
SWITCH
30
32
REMOTE 2
APPL. A
APPL
B
REMOTE 3
APPL. B
33

FIG. 4

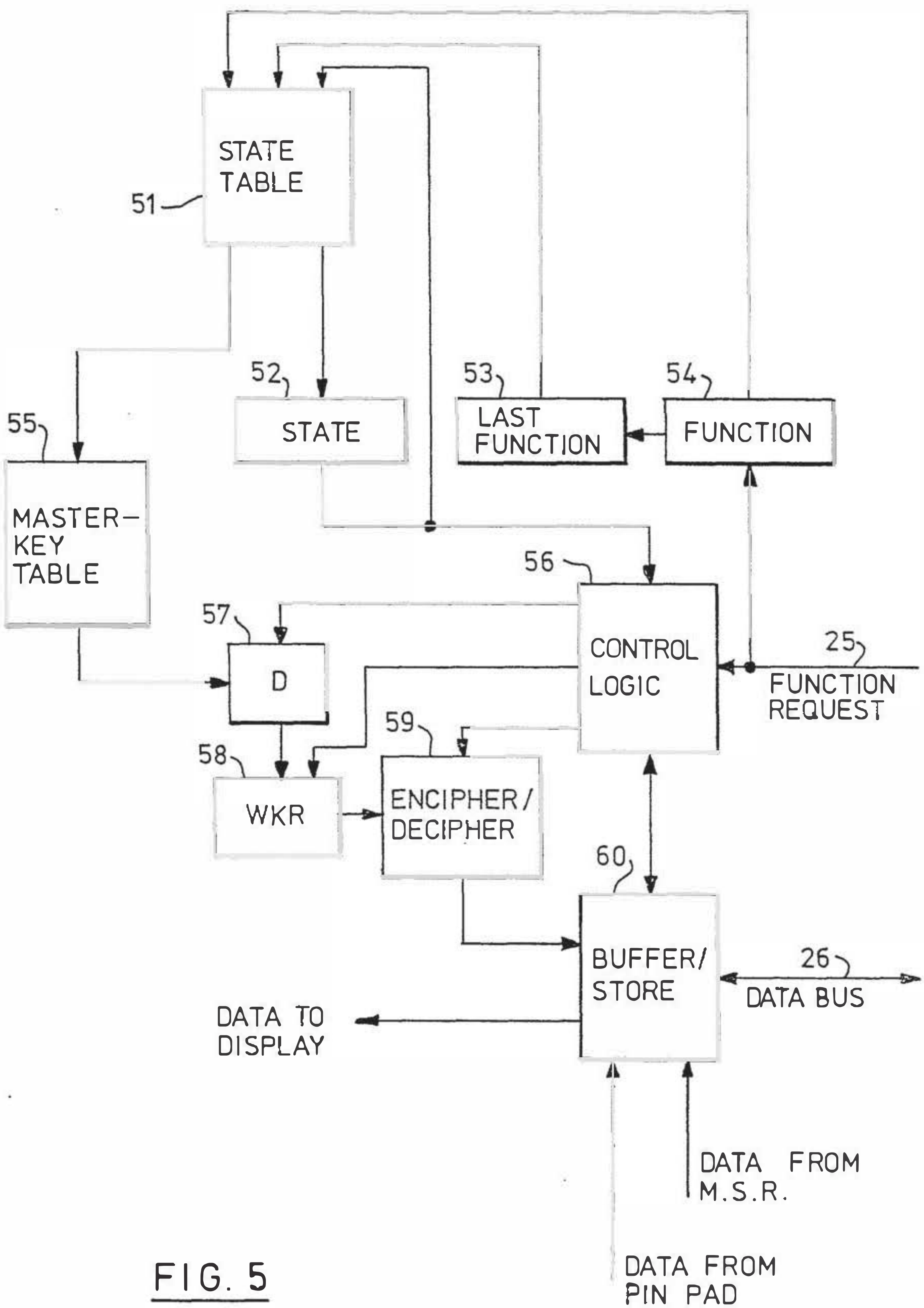

STATE TABLE
51
52
STATE
53
LAST FUNCTION
54
FUNCTION
55
MASTER-KEY TABLE
56
CONTROL LOGIC
57
D
25
FUNCTION REQUEST
58
WKR
59
ENCIPHER/ DECIPHER
60
BUFFER/ STORE
26
DATA BUS
DATA TO DISPLAY
DATA FROM M.S.R.
DATA FROM PIN PAD

FIG. 5

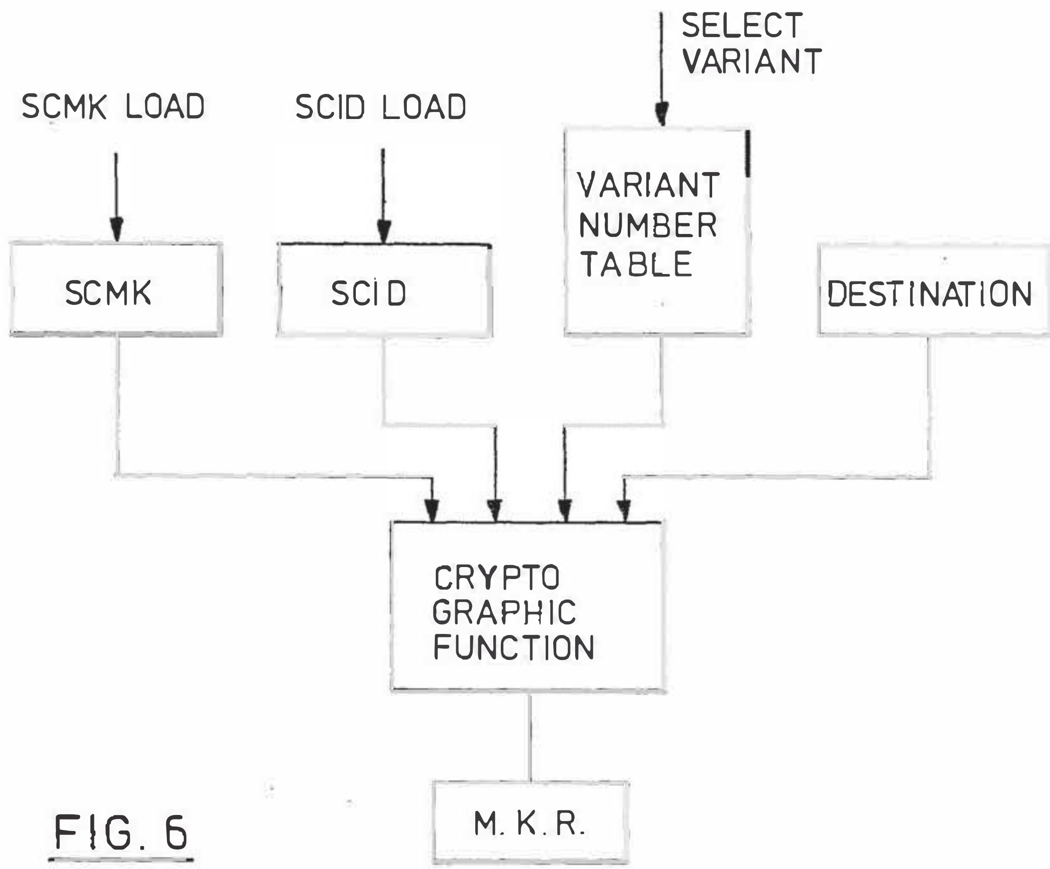

SELECT
VARIANT
SCMK LOAD
SCID LOAD
VARIANT
NUMBER
TABLE
SCMK
SCID
DESTINATION
CRYPTO
GRAPHIC
FUNCTION
M. K. R.

FIG. 6

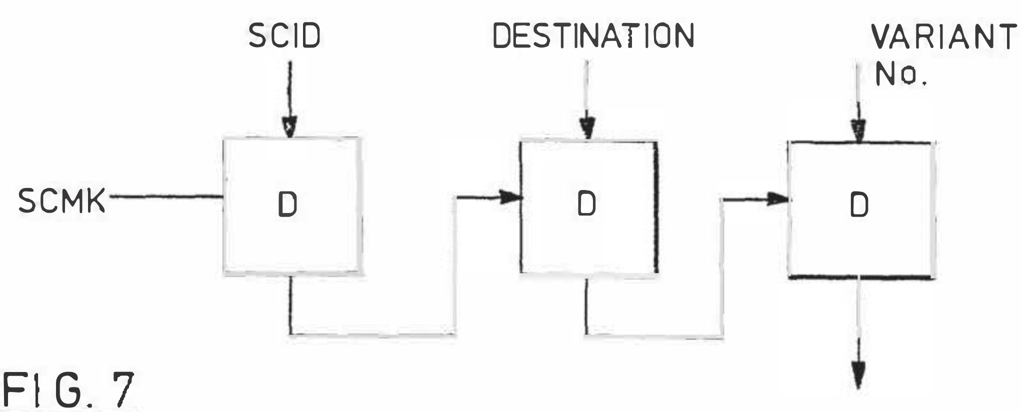

SCID
DESTINATION
VARIANT
No.
SCMK
D
D
D

FIG. 7

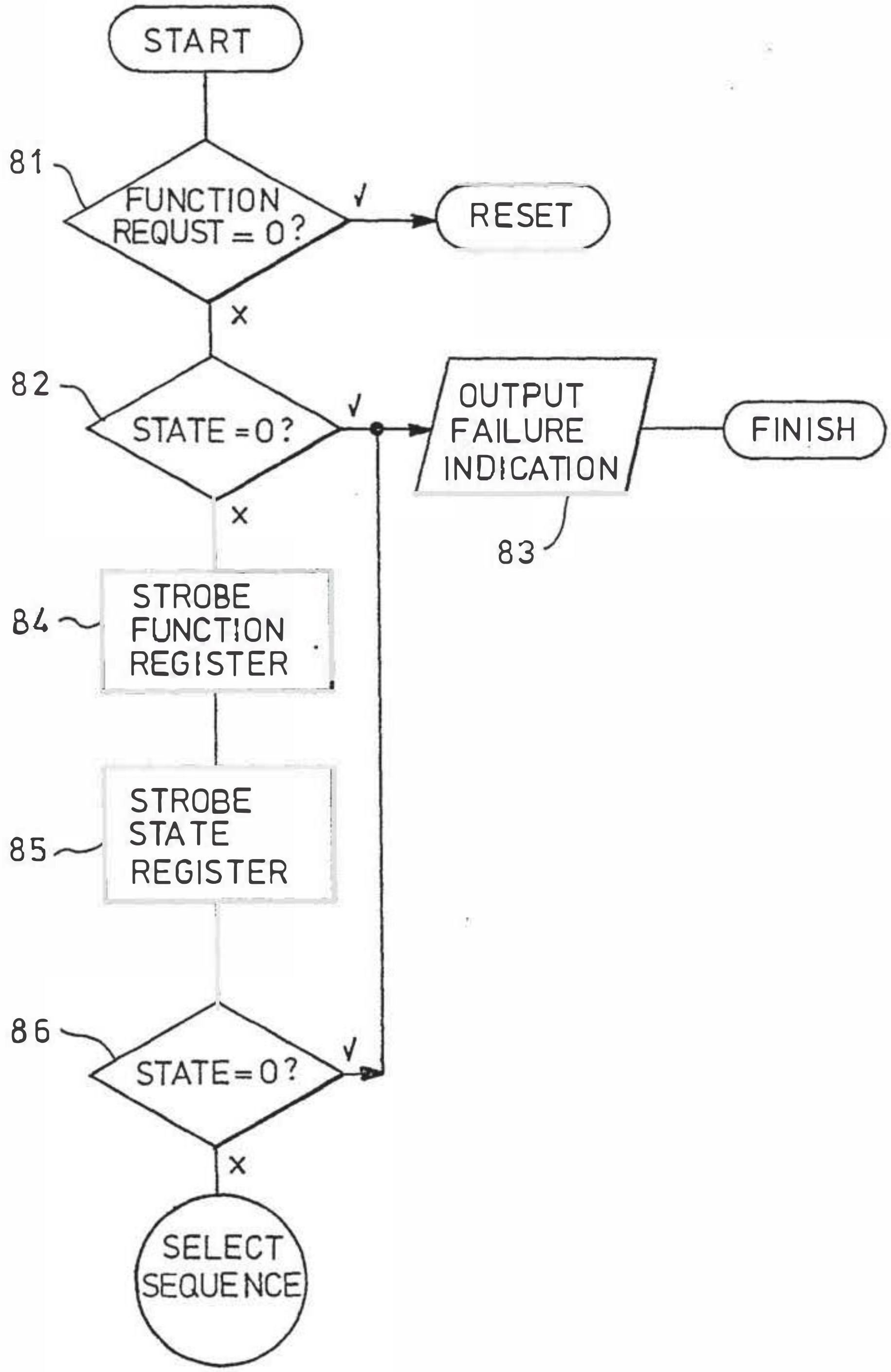

START
81
FUNCTION
REQUST = 0?
√
RESET
X
82
STATE = 0?
√
OUTPUT
FAILURE
INDICATION
FINISH
83
X
84
STROBE
FUNCTION
REGISTER
STROBE
STATE
REGISTER
85
86
STATE = 0?
√
X
SELECT
SEQUENCE

FIG. 8

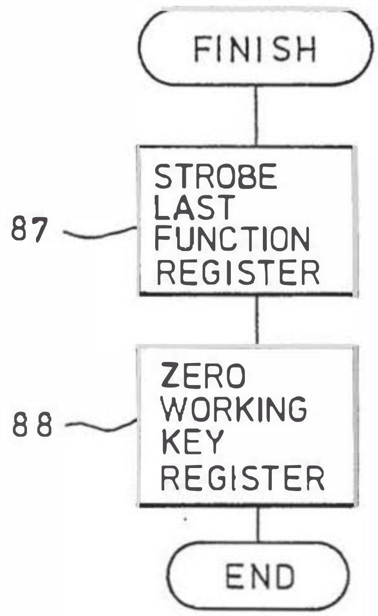

FINISH
STROBE LAST FUNCTION REGISTER
87
ZERO WORKING KEY REGISTER
88
END

FIG. 9

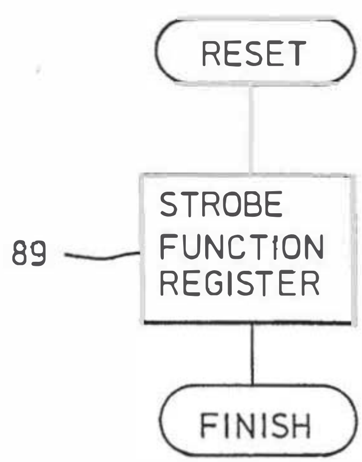

RESET
STROBE FUNCTION REGISTER
89
FINISH

FIG. 10

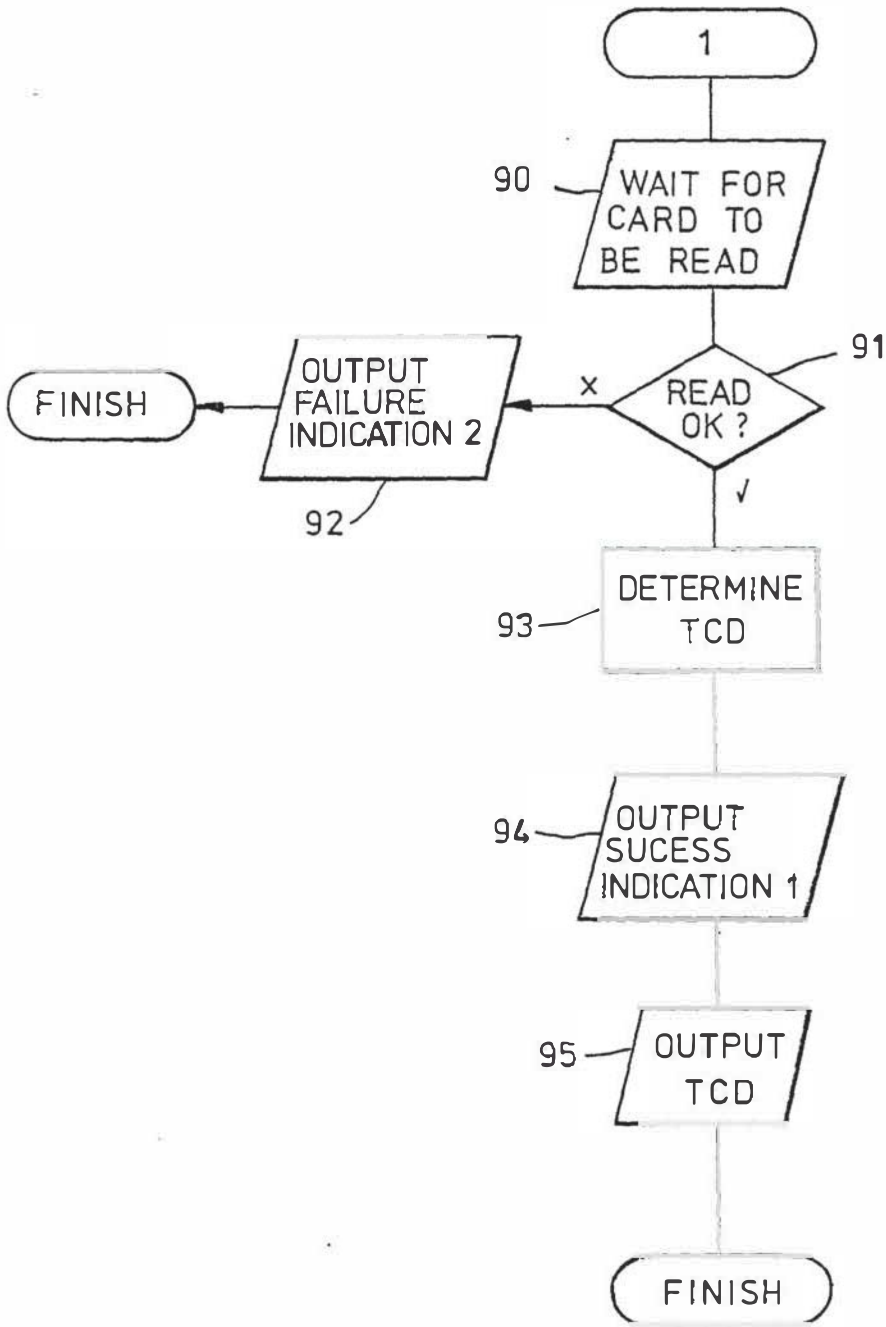

1
90
WAIT FOR CARD TO BE READ
91
READ OK ?
x
√
OUTPUT FAILURE INDICATION 2
FINISH
92
93
DETERMINE TCD
94
OUTPUT SUCESS INDICATION 1
95
OUTPUT TCD
FINISH

FIG. 11

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 186 981 A3**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: 85308823.5

(51) Int. Cl.4: G07F 7/10

(22) Date of filing: 04.12.85

(22) Priority: 12.12.84 GB 8431381

(43) Date of publication of application: 09.07.86 Bulletin 86/28

(84) Designated Contracting States: DE FR GB IT

(88) Date of deferred publication of the search report: 02.11.88 Bulletin 88/44

(71) Applicant: International Business Machines Corporation
Old Orchard Road
Armonk, N.Y. 10504(US)

(72) Inventor: Smith, Peter Rigby
1 Carpenters
Alresford Hampshire(GB)

(74) Representative: Appleton, John Edward
IBM United Kingdom Limited Intellectual Property Department Hursley Park
Winchester Hampshire SO21 2JN(GB)

(54) **Security module for an electronic funds transfer system.**

(57) A security module for use in an electronic funds transfer terminal is contained in a tamper-resistant housing. The module has a PIN pad and is designed to encrypt secret data, such as users personal identity numbers (PINs), so that other terminal processes cannot gain access to it. The encryption functions are carried out in a security controller which includes its own microprocessor and encryption/decryption unit.

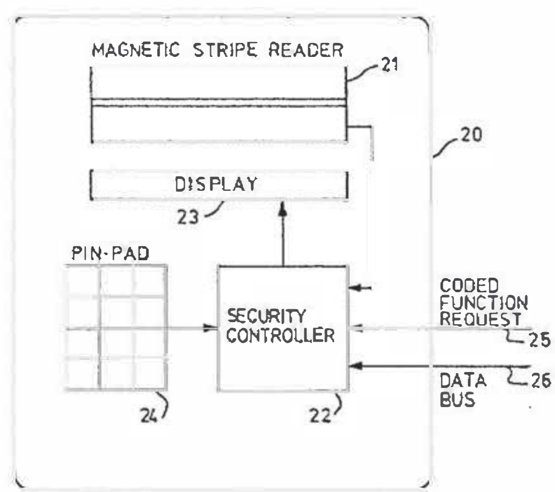


FIG.2

EP 0 186 981 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application number

EP 85308823.5

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int Cl 4)
A	US - A - 4 408 203 (CAMPBELL) * Totality * --	1,3,5,6	G 07 F 7/10
A	EP - A2 - 0 063 794 (SIEMENS AKTIENGESELLSCHAFT) * Totality * --	1,3	
A	EP - A2 - 0 117 907 (GABE) * Totality * --	1	
A	EP - A1 - 0 008 033 (BEST) * Totality * ----	1	
			TECHNICAL FIELDS SEARCHED (Int Cl 4)
			G 07 F 7/00

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
VIENNA	08-08-1988	BEHMER

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document
T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
& : member of the same patent family, corresponding document

EPO Form 1503 03 82