Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2543094 A1 1997/07/31

(21) 2 543 094

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 1997/01/30
(41) Mise à la disp. pub./Open to Public Insp.: 1997/07/31
(62) Demande originale/Original Application: 2 196 356
(30) Priorité/Priority: 1996/01/31 (GB9601924.5)

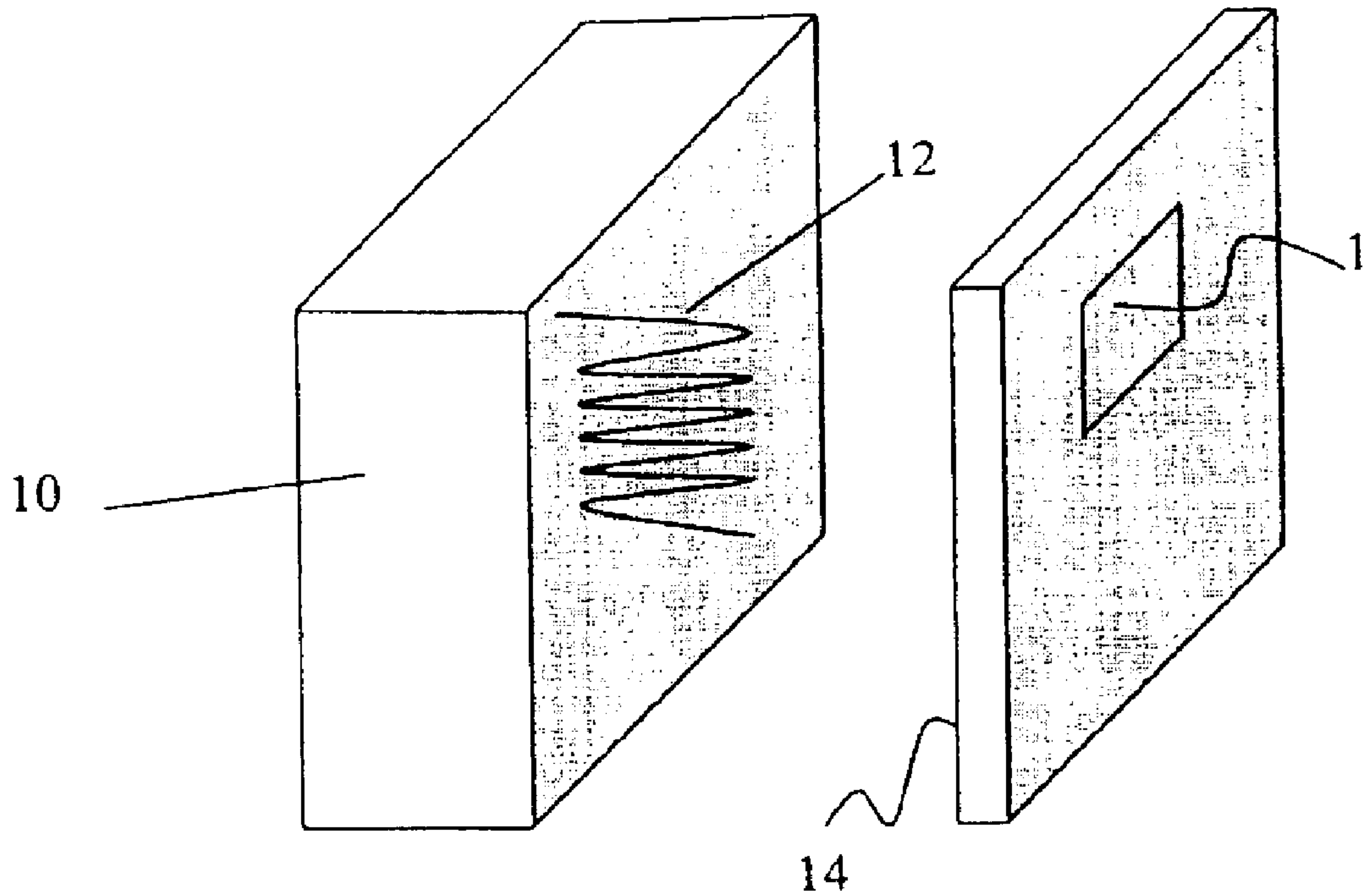
(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01), *G07F 7/10* (2006.01), *G06Q 20/00* (2006.01), *H04L 9/30* (2006.01)

(71) Demandeur/Applicant:
CERTICOM CORP., CA

(72) Inventeur/Inventor:
VANSTONE, SCOTT A., CA

(74) Agent: BLAKE, CASSELS & GRAYDON LLP

(54) Titre : PROTOCOLE DE VERIFICATION DE TRANSACTIONS POUR CARTE A PUCE
(54) Title: TRANSACTION VERIFICATION PROTOCOL FOR SMART CARDS



(57) Abrégé/Abstract:
A protocol appropriate for smartcard purchase applications such as those that might be completed between a terminal or ATM and a users personal card is disclosed. The protocol provides a signature scheme which allows the card to authenticate the terminal without unnecessary signature verification which is an computationally intense operation for the smart card. The only signature verification required is that of the terminal identification (as signed by the certifying authority, or CA, which is essential to any such protocol). In the preferred embodiment, the protocol provides the card and terminal from fraudulent attacks from impostor devices, either a card or terminal.

ABSTRACT

A protocol appropriate for smartcard purchase applications such as those that might be completed between a terminal or ATM and a users personal card is disclosed. The protocol provides a signature scheme which allows the card to authenticate the terminal without unnecessary signature verification which is an computationally intense operation for the smart card. The only signature verification required is that of the terminal identification (as signed by the certifying authority, or CA, which is essential to any such protocol). In the preferred embodiment, the protocol provides the card and terminal from fraudulent attacks from impostor devices, either a card or terminal.

TRANSACTION VERIFICATION PROTOCOL FOR SMART CARDS

The present invention relates to methods for verifying the authenticity of partners in an electronic transaction.

It has become widely accepted to conduct transactions such that as financial transactions or exchange of documents electronically. In order to verify the transaction, it is also well-known to "sign" the transaction digitally so that the authenticity of the transaction can be verified. The signature is performed according to a protocol that utilizes the message, i.e. the transaction, and a secret key associated with the party. Any attempt to tamper with the message or to use a key other than that of the signing party will result in an incompatibility between the message and the signature or will fail to identify the party correctly and thereby lead to rejection of the transaction.

The signature must be performed such that the parties' secret key cannot be determined. To avoid the complexity of distributing secret keys, it is convenient to utilize a public key encryption scheme in the generation of the signature. Such capabilities are available where the transaction is conducted between parties having access to relatively large computing resources but it is equally important to facilitate such transactions at an individual level where more limited computing resources are available.

Automated teller machines (ATMs) and credit cards are widely used for personal transactions and as their use expands, so the need to verify such transactions increases. Transaction cards are now available with limited computing capacity, so-called "Smart Cards," but these are not sufficient to implement existing digital signature protocols in a commercially viable manner. As noted above, in order to generate a digital signature, it is necessary to utilize a public key encryption scheme. Most public key schemes are based on the Diffie Helman Public key protocol and a particularly popular implementation is that known as DSS. The DSS scheme utilizes the set of integers Zp where p is a large prime. For adequate security, p must be in the order of 512 bits although the resultant signature may be reduced mod q, where q divides p-1, and may be in the order of 160 bits.

The DSS protocol provides a signature composed of two components r, s. The protocol requires the selection of a secret random integer k from the set of integers (0, 1, 2, . . . q-1), i.e.

$k \in \{0,1,2,\ldots q\text{-}1)$.

The component r is then computed such that

$$r = \{\beta^k \bmod p\} \bmod q$$

where β is a generator of q.

The component s is computed as

$$s = [k^{-1} (h(m))+ar] \bmod q$$

where m is the message to be transmitted,

h(m) is a hash of the message, and

a is the private key of the user.

The signature associated with the message is then s,r which may be used to verify the origin of the message from the public key of the user.

The value of β^k is computationally difficult for the DSS implementation as the exponentiation requires multiple multiplications mod p. This is beyond the capabilities of a "Smart Card" in a commercially acceptable time. Although the computation could be completed on the associated ATM, this would require the disclosure of the session key k and therefore render the private key, a, vulnerable.

An alternative encryption scheme that provides enhanced security at relatively small modulus is that utilizing elliptic curves in the finite field 2^m. A value of m in the order of 155 provides security comparable to a 512 bit modulus for RSA and therefore offers significant benefits in implementation. Diffie Helman Public Key encryption utilizes the properties of discrete logs so that even if a generator β and the exponentiation β^k are known, the value of k cannot be determined.

A similar property exists with elliptic curves where the addition of two points on a curve produces a third point on the curve. Similarly, multiplying a point by an integer k produces a point on the curve.

However, knowing the point and the origin does not reveal the value of the integer 'n' which may then be used as a session key for encryption. The value kP, where P is an initial known point, is therefore equivalent to the exponentiation β^k.

Elliptic Curve Crytposystems (ECC) offer advantages over other public key cryptosystems when bandwidth efficiency, reduced computation, and minimized code space are application goals.

The preferred embodiment of the present invention discloses a protocol optimized for an ECC implementation for use with a "Smart Card" having limited computing capacity. The protocol has been found to provide superior performance relative to other Smart Card protocols and is achievable with an ECC implementation.

The protocol disclosed is appropriate for Smart Card purchase applications such as those that might be completed between a terminal or ATM and a users personal card. The protocol provides a signature scheme which allows the card to authenticate the terminal without unnecessary signature verification which is a computationally intense operation for the Smart Card. The only signature verification required is that of the terminal identification (as signed by the certifying authority, or CA, which is essential to any such protocol). In the preferred embodiment, the protocol protects the card and terminal from fraudulent attacks from impostor devices, either a card or terminal.

In accordance with the invention there is provided a method of verifying a pair of participants in an electronic transaction to permit exchange of information therebetween, each of the participants includes a memory and having a respective private key t, a and public key Y_t, Y_c stored therein, the public keys derived from a generator α and respective ones of the private keys t, a, the method comprising the steps of:

(a) a first of the participants generating a unique transaction identification information PID upon initiation of the electronic transaction;

(b) the first participant forwarding to a second participant the transaction identification information PID and a first certificate C1, the first certificate being signed by a certification authority according to a predetermined algorithm and including an identification information TIU ID unique to the first participant and the public key Y_t of the first participant;

(c) the second participant verifying the first certificate C1, according to the predetermined algorithm, upon receipt thereof and extracting the identification information TIU ID and the public key Y, therefrom;

(d) the second participant, upon verification of the first certificate C1, generating a first random integer R2;

(e) the second participant generating a first and second signature components r1, s1 utilizing the public key Y_t of the first participant and the private key a of the second participant, respectively according to a predetermined protocol;

(f) the second participant forwarding a message to the first participant, including the signature components r1, s1 and a second certificate C2 signed by the certification authority according to a predetermined algorithm and including an identification information CID unique to the second participant and the public key Yc of the second participant;

(g) the first participant verifying the second certificate C2 and extracting the identification information CID and public key Y_c and verifying the authenticity of the second participant by extracting the transaction identification information PID from the received message and comparing the received transaction identification information PID to the transmitted value;

(h) the first participant extracting the first random integer R2 from the received message and transmitting the first random integer R2 to the second participant to acknowledge verification of the second participant; and

(i) the second participant verifying the authenticity of the first participant by comparing the received first random integer R2 to the generated first random integer R2 and transmitting a second random integer R3 to the first participant to acknowledge verification of the first participant, thereby permitting exchange of information between the participants.

An embodiment of the invention will now be described by way of example only with reference to the accompanying drawings, in which:

Figure 1 is a diagrammatic representation of a scanning terminal and personal transaction card; and

Figure 2 is a chart that schematically illustrates the protocol.

Referring therefore to figure 1, a scanner terminal 10 has an inductive coupling 12 to cooperate with a card 14. When a card 14 is passed through the inductive coupling 12 a transaction is recorded within a memory 16 on the card 14. Typically the transaction will debit the card with a set amount, e.g. an admission price, and the terminal 10 is credited a corresponding amount. The terminal is connected through a network to a central computer located at a financial institution that maintains records of transactions in a conventional manner.

To avoid fraudulent transactions being recorded at either the card or terminal the protocol shown in figure 2 is utilized.

Upon the scanner sensing the card through coupling 12, a unique purchase I.D. (PID) is generated by the terminal 10. The terminal 10 has a private key, t, stored in a secure location and a corresponding public key Y^t equal to α^1. The terminal 10 generates a message, M1, consisting of the purchase I.D. PID and the transaction amount, TA. It also appends to the message M1 a certificate signed by the certifying authority CA that includes terminal identification information TIU ID and the public key Y_t. The message M1 is received by the card 14.

Card 14 has a private key a stored securely in memory 16 and a public key Y_c equal to α^a. (α is the generator point for the curve). The card verifies the terminals certificate as signed by the certifying authority CA according to a normal elliptic curve scheme. Having verified the certificate, the card generates a pair of random numbers R2 and R3 and signs the unique purchase I.D. PID using the terminals public key according to an established protocol.

To effect signing, the card generates a random integer k and computes a session parameter α^k. It also computes Y_t^k and generates signature components r1 and s1.

The component r1 is provided by M2, Y_t^k mod L where:

M2 is the message TA//TIU ID//R2//PID, and

$L = 2^1-1$ and 1 is an integer greater or equal to the number of bits in M2. (// signifies concatenation).

The component s1 is provided by h.a+k mod q where:

q is the order of the curve and

h is a hash h(M2//α^k //R3).

The card now sends signature components r1, s1 the hash h and a certificate issued by the certifying authority CA containing its ID and public key to the terminal 10.

The terminal verifies the cards credentials as signed by the CA. Given the hash h and s1 it can calculate the value α^{kt} and thereby recover the message M2 from r1 using the cards public key. As the message M2 includes the PID, the terminal is able to verify the authenticity of the card 10.

The recovered message includes R2 which is then returned to the card 10 to prove that the terminal is extracting R2 in real time, i.e. during the transit of the card through the coupling 12, using its private key. This also prevents a reply attack by the terminal 10.

The receipt of R2 also serves to acknowledge provision of the service. Upon receipt, the card checks R2 to ensure the message was recovered using the terminals private key. This confirms that the card was talking to the terminal rather than a fraudulent device which would not have the private key, t, available.

If the card confirms the receipt of R2, it transmits the random R3 to the terminal 10 to complete the transaction. R3 is required for card signature verification by the bank and so R3 is retained by the terminal 10 for central processing purposes. R3 is not released by the card until it has received R2 which confirms that the terminal 10 is performing computations in real time.

The terminal 10 is required to submit to the financial institution the stored values of R2, R3, TA, PID, TIU ID, s1 and α^k in addition to the credentials of both card and terminal 10. With this information the bank card is able to reproduce hash, h, i.e. $h(M2//\alpha^k//R3)$ by using the cards public key Y_c to prove that the transaction was authentic.

It will be noted that the last two passes are essentially trivial and do not require computation. Accordingly the computation required by the card is minimal, being restricted to one verification and one signature that involves two exponentiations, with the balance avoiding computationally intense operations.

As indicated in figure 2, and ECC implementation is the field 2^{155} using an anomalous curve of this protocol would result in less bandwidth (1533 bits) and reduced computation for the Smart Card (31,000 clock cycles). The computational savings over previous protocols are possible due to features of the elliptic curve signature scheme used by the Smart Card.

The particular benefits and attributes may be summarized as:

1. The purchase identifier PID is unique and is required to prevent terminal replay to the bank. If the purchase identifier is not unique, a random number R1 will also be required to provide the equivalent of the PID.
2. The random bit string R2 is required to prevent replay to the card.
3. A has function (h) such as the SHA1 is required to prevent modification of the message (m) and the terminal's identification (TIU ID).
4. There appears to be no advantage to having the transaction amount signed by the terminal, resulting in one less signature verification for the card. The reason for this is that the message signed by the card contains a random number R2 which can only be recovered by the terminal.
5. Using this scheme, the message m may only be recovered by the terminal (note the terminal's public key is used in step III therefore requiring the terminal's private key to verify and recover contents). By demonstrating to the card that the random string (R2) was obtained from the message, the terminal can be authenticated to the card.

1. A method of performing a transaction in a communication system between a first and a second participant wherein said second participant permits a service to be provided to said first participant in exchange for a payment, said method comprising the steps of:

a) upon initiation of said transaction by said first participant, said second participant sending a first message to said first participant, said first message including information pertaining to said second participant;

b) said first participant verifying said information pertaining to said second participant to obtain assurance that said service will be provided upon assuring said payment;

c) said first participant sending a second message to said second participant, said second message including information pertaining to said first participant;

d) said second participant verifying said information pertaining to said first participant to obtain assurance that payment will be secured upon provision of said service; and

e) upon verification of said information pertaining to said first participant, said second participant obtaining a digital signature for said first participant on said transaction using said second message, whereby said second participant may obtain said payment from a third participant using said digital signature.

2. A method according to claim 1 wherein said first participant is a holder of a card which performs cryptographic operations.

3. A method according to claim 2 wherein said second participant is a terminal.

4. A method according to claim 3 wherein said third participant is a financial institution.

5. A method according to claim 1 wherein said information pertaining to said second participant included in said first message includes details and credentials of said second participant; and said first participant verifies said details and said credentials in step b).

6. A method according to claim 1 wherein said information pertaining to said first participant included in said second message includes details and credentials of said first participant; and said second participant verifies said details and credentials in step d).

7. A method according to claim 1 wherein said second message includes a challenge and step e) further comprises:

i) said second participant generating a response to said challenge;

ii) said second participant sending a third message including said response to said first participant;

iii) said first participant verifying said response; and

iv) said first participant sending a fourth message to said second participant such that said digital signature is provided by said second message and said fourth message.

8. A method according to claim 7 further comprising:

i) said second participant verifying information in said fourth message;

ii) said second participant completing said transaction by providing said service; and

iii) said second participant sending said third participant a subset of said first, second, third and fourth messages to obtain said payment.

9. A method according to claim 8 further comprising:

i) said third participant verifying said subset;

ii) said third participant providing said payment to said second participant.

10. A method according to claim 5 wherein said credentials include a public key certificate.

11. A method according to claim 7 wherein said challenge is a nonce.

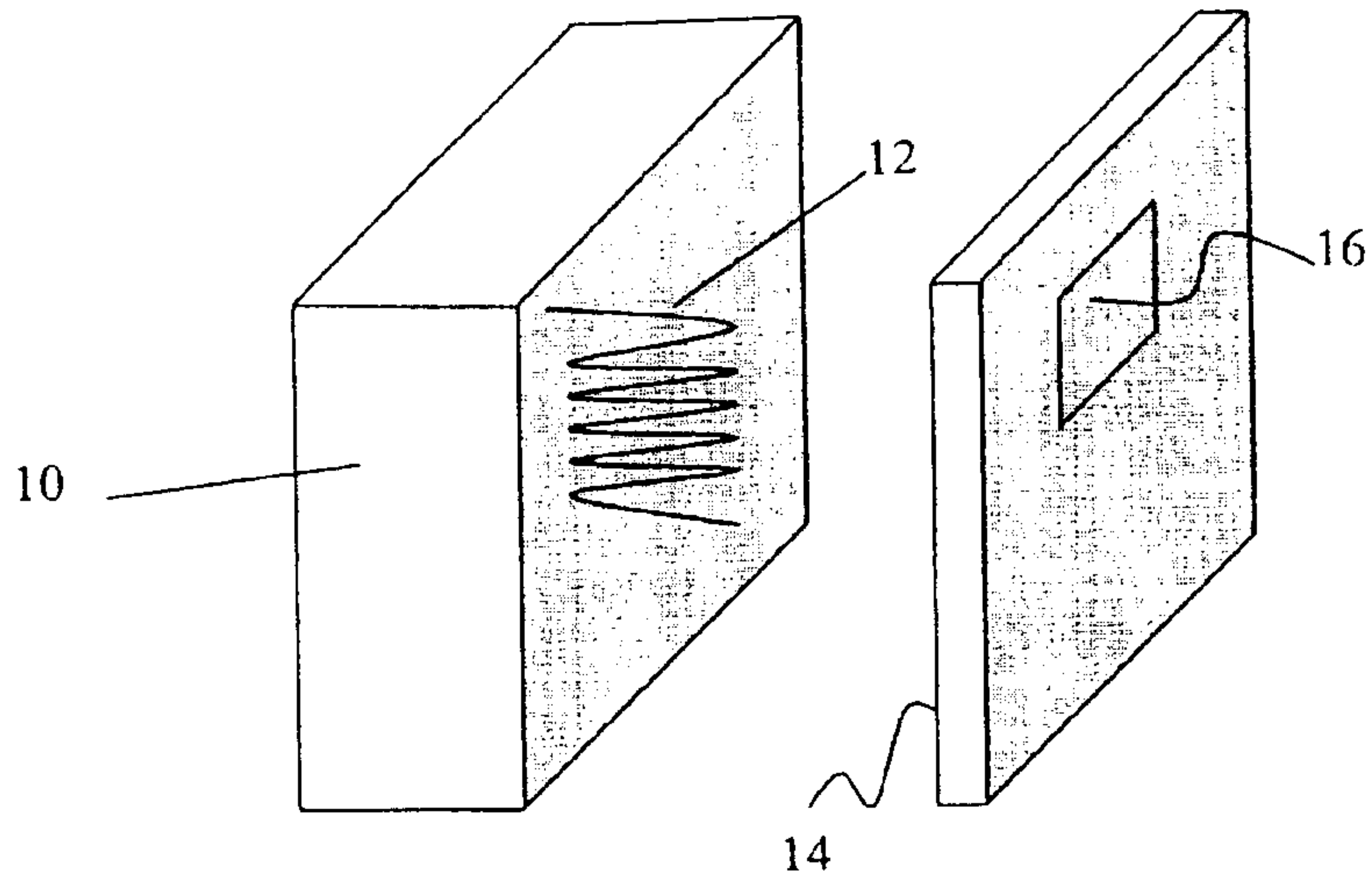
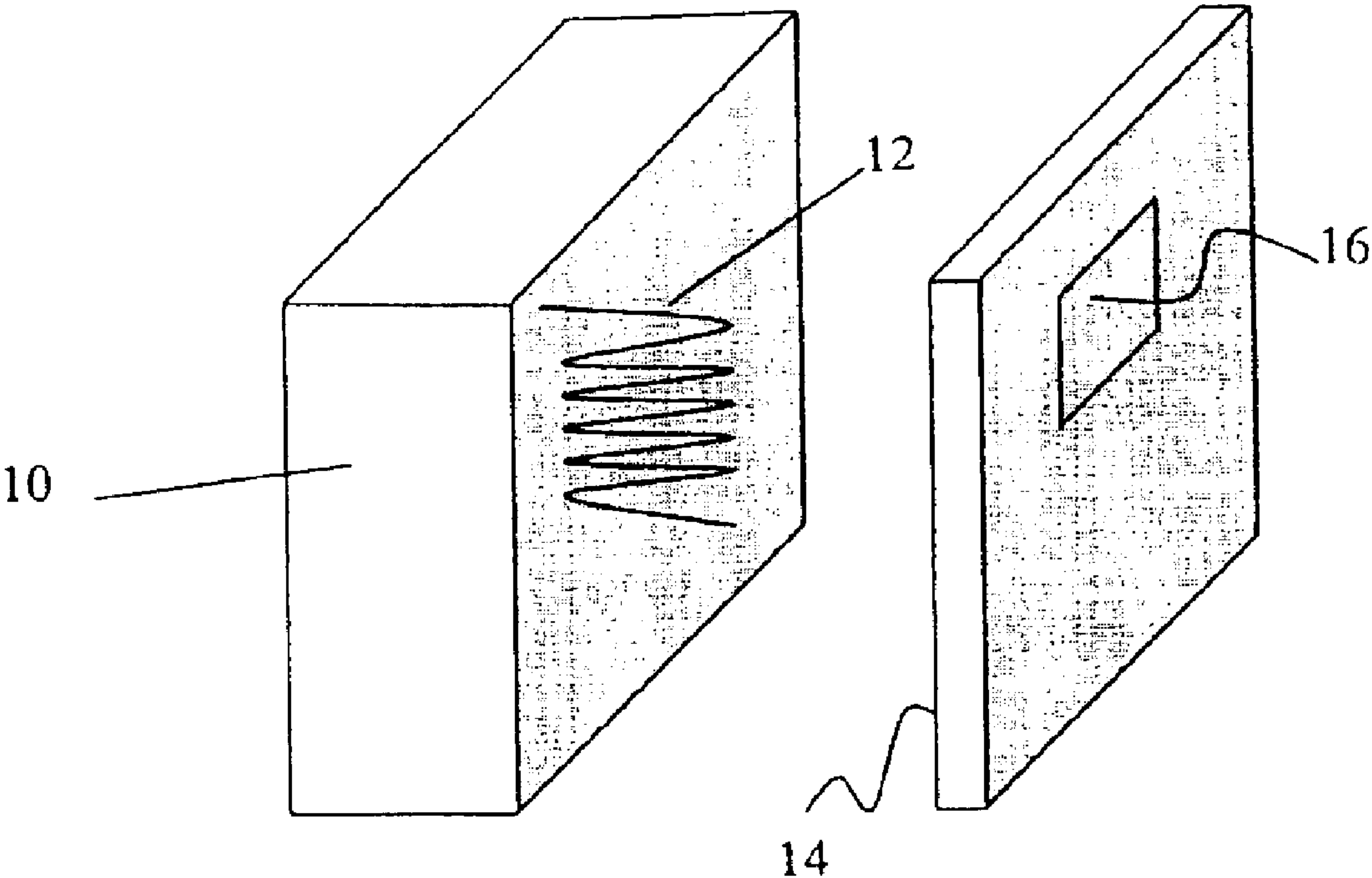


Figure 1

Smartcard Action	Transmission	Terminal Action
		Generate unique purchase ID and create transaction message
	← Purchase ID, TA 220 bits [TIU ID, Y_T] CA 355 bits	
Verify Certificate signed by CA 15,500 clock cycles Generate Random Number (R2) and sign transaction number using terminal's public key 15,500 clock cycles		
Send signed transaction data, hash and certificate signed by CA	→ [r1,s1] card 375 bits Hash 128 bits [Smartcard ID, Smartcard Public Key] CA 355 bits	
	←	Verify Certificate signed by CA Given the hash h and s1, deduce α^{kT} session key Recover message from r1
	R2 100 bits	Send R2 contained in message to card to prove identity and to acknowledge the provision of service
Check R2 to complete transaction		
Total computation time = 31,000 clock cycles	Total bits transmitted = 1533	

Figure 2


12
16
10
14