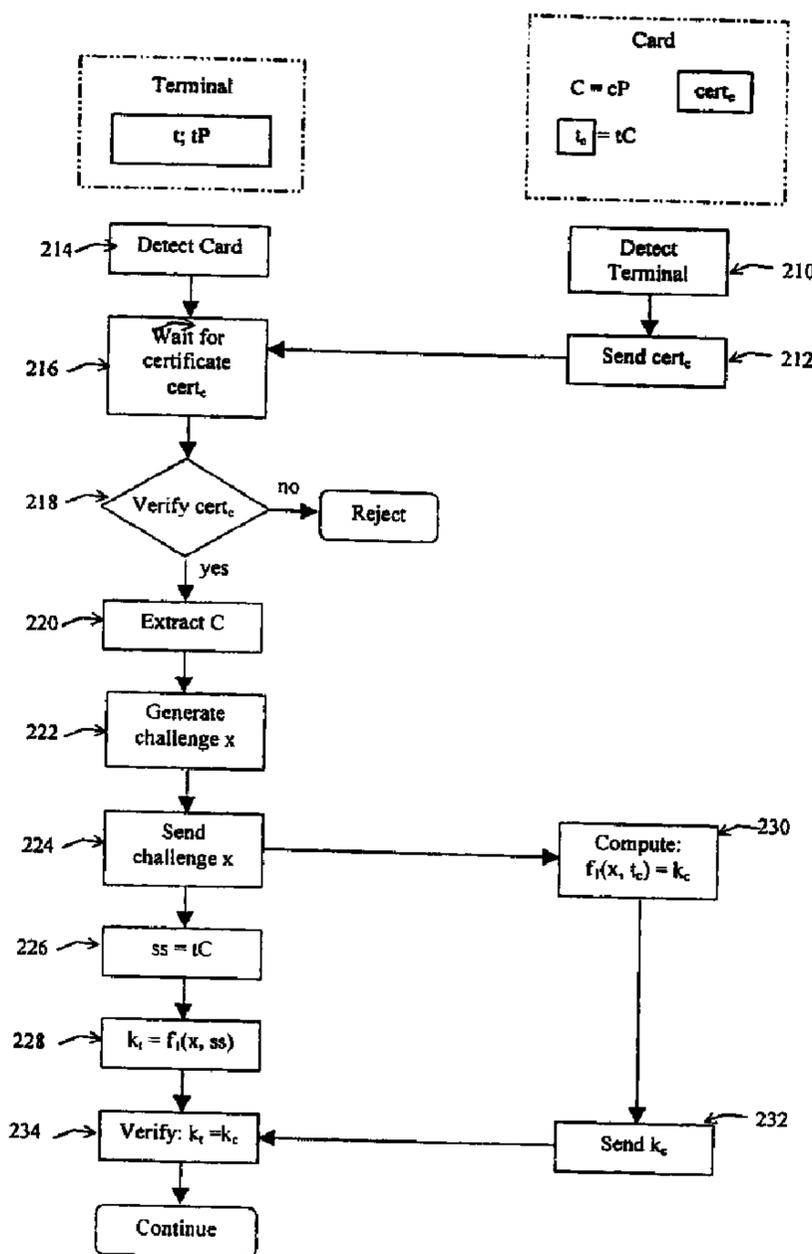




(86) Date de dépôt PCT/PCT Filing Date: 1999/02/01
 (87) Date publication PCT/PCT Publication Date: 1999/08/05
 (45) Date de délivrance/Issue Date: 2009/12/22
 (85) Entrée phase nationale/National Entry: 2000/07/28
 (86) N° demande PCT/PCT Application No.: CA 1999/000053
 (87) N° publication PCT/PCT Publication No.: 1999/039476
 (30) Priorité/Priority: 1998/01/30 (GB9802152.0)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
G07F 7/10 (2006.01)
 (72) Inventeurs/Inventors:
VANSTONE, SCOTT A., CA;
VADEKAR, ASHOK V., CA;
LAMBERT, ROBERT J., CA;
GALLANT, ROBERT P., CA
 (73) Propriétaire/Owner:
CERTICOM CORP., CA
 (74) Agent: BLAKE, CASSELS & GRAYDON LLP

(54) Titre : SYSTEME DE COMMUNICATION AVEC AUTHENTIFICATION UNIDIRECTIONNELLE SECURISEE
 (54) Title: SECURE ONE-WAY AUTHENTICATION COMMUNICATION SYSTEM



(57) Abrégé/Abstract:

A protocol for authenticating at least one of a pair of first and second correspondents C and T in a data communication system, the method comprising the steps of storing a public key in the first correspondent C; computing a shared secret by the second

(57) **Abrégé(suite)/Abstract(continued):**

correspondent T incorporating the public key C; storing the shared secret in the first correspondent C; the second correspondent T generating a challenge value χ ; the first correspondent C transmitting to the second correspondent T information including the stored public key C; the second correspondent T computing a test shared secret from the received public key C; the first and second correspondents computing response signals using the challenge value χ and the shared secret in a one-way function f_1 ; and the first correspondent C transmitting the computed response signal to the second correspondent T whereby the second correspondent verifies the first correspondent.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



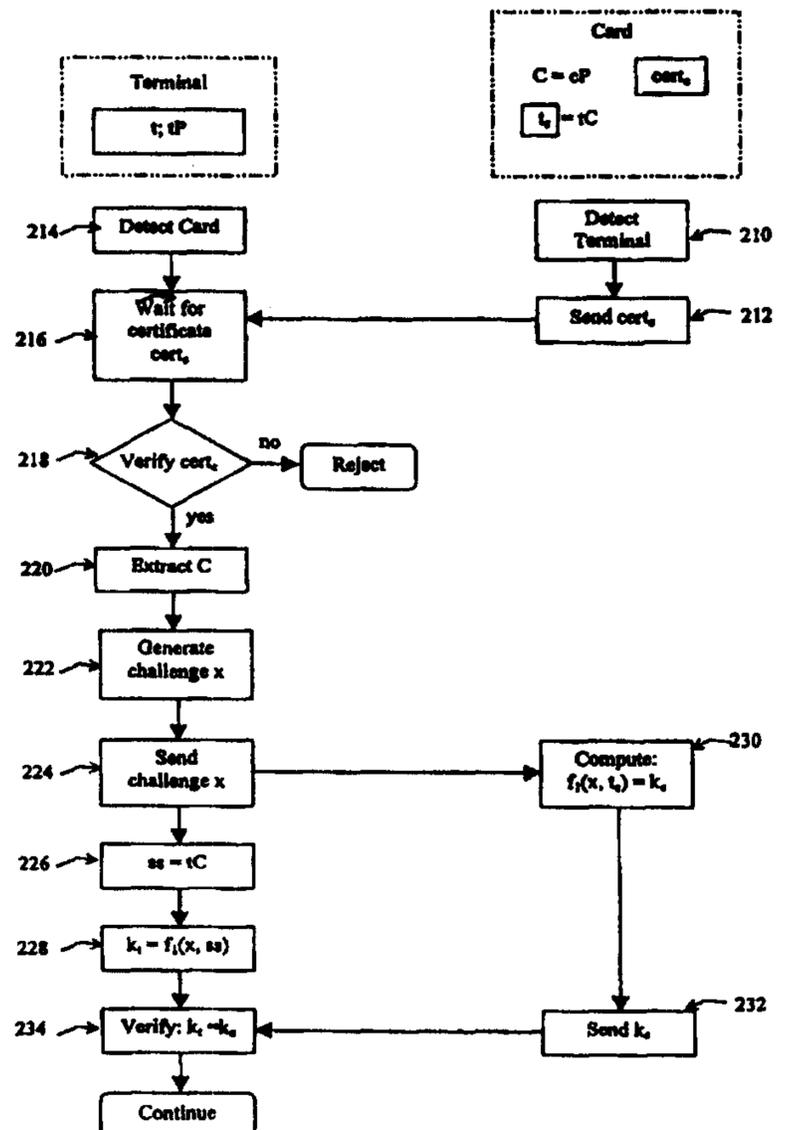
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)-

<p>(51) International Patent Classification ⁶ : H04L 9/32, G07F 7/10</p>	<p>A1</p>	<p>(11) International Publication Number: WO 99/39476 (43) International Publication Date: 5 August 1999 (05.08.99)</p>
<p>(21) International Application Number: PCT/CA99/00053 (22) International Filing Date: 1 February 1999 (01.02.99) (30) Priority Data: 9802152.0 30 January 1998 (30.01.98) GB (71) Applicant (for all designated States except US): CERTICOM CORP. [CA/CA]; Suite 103, 200 Matheson Boulevard West, Mississauga, Ontario L5R 3L7 (CA). (72) Inventors; and (75) Inventors/Applicants (for US only): VANSTONE, Scott, A. [CA/CA]; 539 Sandbrook Court, Waterloo, Ontario N2T 2H4 (CA). VADEKAR, Ashok, V. [CA/CA]; 250 Harris Street, R.R. 4, Rockwood, Ontario N0B 2K0 (CA). LAMBERT, Robert, J. [CA/CA]; 63 Holm Street, Cambridge, Ontario N3C 3N3 (CA). GALLANT, Robert, P. [CA/CA]; 4788 Rosebush Road, Mississauga, Ontario L5M 5N1 (CA). (74) Agents: PILLAY, Kevin et al.; Orange Chari Pillay, Toronto Dominion Bank Tower, Toronto-Dominion Centre, Suite 3600, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).</p>	<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, 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, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</p>	

(54) Title: SECURE ONE-WAY AUTHENTICATION COMMUNICATION SYSTEM

(57) Abstract

A protocol for authenticating at least one of a pair of first and second correspondents C and T in a data communication system, the method comprising the steps of storing a public key in the first correspondent C; computing a shared secret by the second correspondent T incorporating the public key C; storing the shared secret in the first correspondent C; the second correspondent T generating a challenge value χ ; the first correspondent C transmitting to the second correspondent T information including the stored public key C; the second correspondent T computing a test shared secret from the received public key C; the first and second correspondents computing response signals using the challenge value χ and the shared secret in a one-way function f_i ; and the first correspondent C transmitting the computed response signal to the second correspondent T whereby the second correspondent verifies the first correspondent.



SECURE ONE-WAY AUTHENTICATION
COMMUNICATION SYSTEM

5 This invention relates to a protocol for the secure verification of
correspondents in a data communication system and in particular to the verification of
at least one of the correspondents having limited computing power.

BACKGROUND OF THE INVENTION

10 Traditionally, a mechanical turnstile system was used to restrict the entry of
persons into or out of a pre-determined area. In order to gain entry, the user is
required to pay a fee, the fee being in the form of cash, tokens, fee cards or other
payment medium. These mechanical turnstiles however allow entry without being
able to identify the persons entering or leaving. In order to monitor users, an operator
15 is required.

In order to alleviate this problem electronic card entry and exit systems were
devised. In these types of systems, a user is issued with an identification card
beforehand which is then inserted into a card reader and upon positive verification
will allow entry via a locked door or similar barrier thus obviating the need for an
operator. A disadvantage of this system is that for a large number of users, a database
20 has to be maintained listing each of the users, particularly if each user has a unique
identification then the verification system is required to scroll through each of the
records to find a matching identity. Secondly, this system is also inconvenient if there
are a large number of users entering a particular location at a given time such as a
25 public transit way, the insertion and withdrawal of cards from a card reader is apt to
cause bottlenecks at the entrance way.

Transit systems have been devised in which users are provided with a pre-
programmed smart card. In this system, the turnstile or a terminal is able to monitor
the smart card remotely thus the user simply walks past the turnstile without having to
30 physically insert the card in a slot. The card is generally activated by the presence of
a electromagnetic field generated by the terminal, the card then transmits an
appropriate identification back to the terminal which verifies the card identification
and allows entry of the user. These cards generally have limited computing power
and are not able to perform complex computations. It is also desirable to authenticate
35 these cards to prevent duplication or fraudulent entry. Because the cards have limited

WO 99/39476

PCT/CA99/00053

computing power, it is necessary to implement a authentication protocol that minimizes the computation performed by the card and furthermore is able to provide verification of the card by the terminal in a very short period of time, generally less than one second.

5

SUMMARY OF THE INVENTION

This invention seeks to provide a solution to the problem of card verification between a terminal and a card where the card device has limited computing power.

According to one aspect of this invention there is provided a method of authenticating at least one of a pair of correspondents **T** and **C** in an information exchange session, and wherein one of the correspondents **T** includes a secret key t and the other correspondent **C** has a public key C and a shared secret value t_C derived from said public key C and said secret key t the method comprising the steps of:

the first correspondent **C** transmitting to the second correspondent **T** said public key C ;

the second correspondent **T** generating a challenge value χ and transmitting said challenge value χ to said first correspondent **C**;

said second correspondent **T** generating a session shared secret value ss by combining said private key t with said public key C of said first correspondent **C**;

said second correspondent **T** generating a response test value k_t by combining said session shared secret ss with said challenge χ , in a mathematical function f_l ;

said first correspondent **C** generating a response value k_c by combining said shared secret t_C with said challenge value χ in said mathematical function f_l and sending said response value k_c to said second correspondent **T**; and

said second correspondent **T** comparing said response test value k_t to said challenge response value k_c to verify said first correspondent **C**.

A further aspect of this invention provides for said public key C being included in a certificate $Cert_C$, whereby the second correspondent verifies the certificate on **C** and the identity of the first correspondent **C** before generating the challenge χ .

In accordance with a further aspect of this invention the mathematical function f_l is a one way function.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention will now be described by way of example only with reference to the accompanying drawings in which:

Figure 1 is a schematic representation of a communication system; and

5 Figure 2 is a flow chart showing a verification protocol according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description like numerals referred to like elements. Referring
10 to figure 1, a transit control system is shown generally by numeral 10. In the system, a user 12 carries an identification card 14. A terminal including a card reader is provided for remote monitoring of card carrying users 12. The terminal 16
communicates with cards in a given area of proximity via, for example,
electromagnetic means 18. These systems are readily available and will not be
15 discussed further.

In the context of the present data communication system, the card and terminal are designated a pair of first and second correspondents C and T respectively. Depending upon the reading mechanism employed, the card generally is powered when brought in proximity to the magnetic field generated by the terminal 18. The
20 card 14 contains a low power processing unit which is at least capable of performing simple calculations. In a typical data communication session, the card assembles a data string, which when assembled is transmitted to the terminal.

At system set-up, i.e. when a card is issued to a user, an encryption scheme is chosen and appropriate system parameters are defined. In the following example an
25 elliptic curve encryption scheme is used. The details of encryption schemes will not be discussed as they are well known in the art. However, if the elliptic curve encryption system is being utilized, then a public value $C = cP$, is computed where P is a generator point on the elliptic curve. The public value C is signed by a certifying authority (CA) to produce a certificate $Cert_c$, containing the public key C and
30 identification of the card C and stored in the card 14. A shared secret $t_c = tC$ is calculated where t is a secret key known to the terminal T. This shared secret t_c is stored in the card within a secure boundary. Thus after the system set-up phase, the card contains a certificate $Cert_c$ and a shared secret t_c .

Referring now to figure 2, a protocol according to an embodiment of the present invention is shown generally by numeral 200. When the user 12 carrying the card 14 is in proximity to the terminal 18, the card detects the terminal 210 and sends its certificate $Cert_c$ to the terminal T. Similarly when the terminal detects the card 214
 5 it waits for a certificate $Cert_c$ 216. When the terminal receives the certificate, it verifies the certificate using the CA's public key 218. If the certificate is not verified, a rejection signal is generated which may be used to alert or signal an appropriate barrier or event. However if the certificate is verified the terminal extracts the public key C of the card from the certificate 220. The terminal then generates a challenge χ
 10 222, which may be a large integer, or any suitable bit string. This challenge χ is then sent to the card 224. At the same time the terminal computes a shared secret $ss = tC$ and computes a challenge response verification value $k_T = f_l(\chi, ss)$, where f_l is a one-way function such as a secure hash function or one derived from the data encryption standard (DES). The card upon receipt of the challenge χ also computes its challenge
 15 response k_c by applying a one-way function f_l to the challenge value χ and the shared secret t_c to calculate $k_c = f_l(\chi, t_c)$. This challenge response value k_c is then sent back to the terminal 232 where it is verified 234 by the terminal comparing k_t to k_c . If these values are equal then the card is verified.

It may be seen thus that the purpose of the challenge χ is to know that the card
 20 has the shared secret t_c , otherwise the data communication system is open to replay attack, where an observer watches for the k_c and may send it back at a later time. Furthermore it may be seen from the system that the terminal does not have to maintain a record of secret keys for each card authorized in the system. The advantage of this may well be appreciated when for example the card is a public rail
 25 transit card identification and the terminal has to maintain records for each of approximately a few hundred thousand users. Thus the present invention avoids this disadvantage.

In a further embodiment, the card may at step 230 in producing the challenge response compute a value $k_{sig} = f_l(\chi, t_c, m)$ where m is a message to be signed by the
 30 card. The card may then concatenate the challenge response k_{sig} with the message and sends this to the terminal. In this instance, the card is both authenticated and a message generated by the card is signed.

In a still further embodiment, the card may be authenticated as well as send an encrypted message. In this instance, the card calculates its challenge response value $k_{enc} = f_1(\chi, ss)$ and using this value as a key to calculate an encrypted value of a message m using for example a DES or DESX such that $E = E_{K_{enc}}(m)$. In this instance the card is implicitly authenticated with the encrypted message. This may be useful for example when the card sends a P.I.N. back to the terminal.

In a further embodiment, the system rather than utilizing a single value of t , may use many values of t , i.e. t_i thus producing many shared secrets $ss(t_i)$. In this instance, the card will send with its certificate the index i so that the terminal may extract the appropriate t_i to compute its shared secret as shown in step 226 figure 2.

In the above examples, the shared secret $ss = t_C$ was for an elliptic curve implementation. For a finite field implementation, the shared secret may be calculated as $ss = C^T$. Furthermore a more generalized form of the shared secret is a function combining the values of the terminals private key t and the cards public key C using a cryptographic function $f_l(t, C)$.

While the invention has been described in connection with the specific embodiment thereof, and in a specific use various modifications thereof will occur to those skilled in the art without departing from the spirit of the invention as set forth in the appended claims. In general, this invention has application to situations where authenticated access to goods and services are required or where entry is to be controlled.

The terms and expressions which have been employed in this specification are used as terms of description and not of limitations, there is no intention in the use of such terms and expressions to exclude any equivalence of the features shown and described or portions thereof, but it is recognized that various modifications are possible within the scope of the claims to the invention.

Claims:

1. A method of authenticating at least one of a pair of first and second correspondents C and T in a data communication system, said method comprising the steps of:

- storing a public key in said first correspondent C;
- computing a shared secret by said second correspondent T incorporating said public key;
- storing said shared secret in said first correspondent C;
- said second correspondent T generating a challenge value χ and transmitting said challenge value χ to said first correspondent C;
- said first correspondent C transmitting to the second correspondent T information including said stored public key;
- said second correspondent T computing a test shared secret from said received public key;
- said first and second correspondents computing response signals using said challenge value χ and said shared secret in a one-way function f_1 ; and
- said first correspondent C transmitting said computed response signal to said second correspondent T whereby said second correspondent T may verify said first correspondent C.

2. A method as defined in claim 1, including said first correspondent C transmitting a signed message m with said response signal.

3. A method as defined in claim 2, including signing said message m with said one way function f_1 .

4. A method as defined in claim 3, said signed message m being included with said computed response signal and concatenated with said message m for transmission.

5. A method as defined in claim 1, including said first correspondent C encrypting a message m in accordance with a symmetric key scheme, wherein a symmetric key is derived from said computed response signal and said method comprises transmitting said encrypted message m to said second correspondent T.

6. A method as defined in claim 5, said scheme being an RSA type signature scheme.
7. A method as defined in claim 1, said shared secret being computed by said second correspondent T by utilizing its secret key and the public key.
8. A method as defined in claim 1, said second correspondent T having a plurality of private keys t_i corresponding to respective first correspondents; said method comprising receiving from said first correspondent C an identification index i and using said corresponding private key t_i and the public key to compute a shared secret ss_i .
9. A method as defined in claim 1, utilizing a public key scheme being an elliptic curve scheme.
10. A method as defined in claim 1, utilizing a public key scheme being an RSA type scheme.
11. A method of authenticating at least one of a pair of correspondents T and C in an information exchange session, and wherein one of the correspondents T includes a secret key t and the other correspondent C has a public key and a shared secret value t_c derived from said public key C and said secret key t , the method comprising the steps of:

the first correspondent C transmitting to the second correspondent T information including said public key;

the second correspondent T generating a challenge value χ and transmitting said challenge value χ to said first correspondent C;

said second correspondent T generating a session shared secret ss by combining said secret key t with said public key of said first correspondent C;

said second correspondent T generating a response signal k_t by combining said session shared secret ss with said challenge value χ , in a mathematical function f_1 ;

said first correspondent C generating a response value k_c by combining said shared secret t_c with said challenge value χ in said mathematical function f_1 and sending said response value k_c to said second correspondent T; and

said second correspondent T comparing said response signal k_t to said response value k_c to verify said first correspondent C.

12. An article of manufacture comprising:

a computer usable medium having computer readable program code embodied therein for authenticating at least one of a pair of correspondents T and C in an information exchange session, and wherein one of the correspondents T includes a secret key t and the other correspondent C has a public key and a shared secret value t_c derived from said public key and said secret key t , the computer readable program code in said article of manufacture comprising;

computer readable program code configured to cause a computer to generate a challenge value χ and transmit said challenge value χ to said first correspondent C in response to received public information from said first correspondent C;

computer readable program code configured to cause a computer to generate a session shared secret ss by combining said secret key t with said public key of said first correspondent C;

computer readable program code configured to cause a computer to generate a test response signal k_t by combining said session shared secret ss with said challenge value χ , in a mathematical function f_1 ;

computer readable program code configured to cause a computer to compare said response test signal k_t to a received response value k_c from said first correspondent C to verify said first correspondent C.

13. A system for authenticating at least one of a pair of first and second correspondents C and T in a data communication system, said system being configured for:

storing a public key in said first correspondent C;

computing a shared secret by said second correspondent T incorporating said public key;

storing said shared secret in said first correspondent C;

having said second correspondent T generate a challenge value χ and transmit said challenge value χ to said first correspondent C;

having said first correspondent C transmit to the second correspondent T information including said stored public key;

having said second correspondent T compute a test shared secret from said received public key;

having said first and second correspondents compute response signals using said challenge value χ and said shared secret in a one-way function f_1 ; and

having said first correspondent C transmit said computed response signal to said second correspondent T whereby said second correspondent T may verify said first correspondent C.

14. A system as defined in claim 13, configured for having said first correspondent C transmit a signed message m with said response signal.

15. A system as defined in claim 14, configured for signing said message m with said one way function f_1 .

16. A system as defined in claim 15, said signed message m being included with said computed response signal and concatenated with said message m for transmission.

17. A system as defined in claim 13, configured for having said first correspondent C encrypt a message m in accordance with a symmetric key scheme, wherein a symmetric key is derived from said computed response signal and said system configured for transmitting said encrypted message m to said second correspondent T.

18. A system as defined in claim 17, said scheme being an RSA type signature scheme.

19. A system as defined in claim 13, configured for having said shared secret be computed by said second correspondent T by utilizing its secret key and the public key.

20. A system as defined in claim 13, configured for having said second correspondent T utilize a plurality of private keys t_i corresponding to respective first correspondents; said system also configured for having said second correspondent T receive from said first correspondent C an identification index i and use said corresponding private key t_i and the public key to compute a shared secret ss_i .

21. A system as defined in claim 13, utilizing a public key scheme being an elliptic curve scheme.

22. A system as defined in claim 13, utilizing a public key scheme being an RSA type scheme.

23. A system for authenticating at least one of a pair of correspondents T and C in an information exchange session, and wherein one of the correspondents T includes a secret key t and the other correspondent C has a public key and a shared secret value t_c derived from said public key C and said secret key t , the system configured for:

having the first correspondent C transmit to the second correspondent T information including said public key;

having the second correspondent T generate a challenge value χ and transmit said challenge value χ to said first correspondent C;

having said second correspondent T generate a session shared secret ss by combining said secret key t with said public key of said first correspondent C;

having said second correspondent T generate a response signal k_t by combining said session shared secret ss with said challenge value χ , in a mathematical function f_1 ;

having said first correspondent C generate a response value k_c by combining said shared secret t_c with said challenge value χ in said mathematical function f_1 and send said response value k_c to said second correspondent T; and

having said second correspondent T compare said response signal k_t to said response value k_c to verify said first correspondent C.

24. A method of authenticating at least one of a pair of first and second correspondents C and T in a data communication system, said method comprising the steps of:

storing a public key in said first correspondent C;

computing a shared secret with said second correspondent T which incorporates said public key;

storing said shared secret in said first correspondent C;

said first correspondent C receiving a challenge value χ generated by said second correspondent T;

said first correspondent C transmitting to the second correspondent T information including said stored public key to enable said second correspondent T to compute a test shared secret from said public key;

said first correspondent C computing a response signal using said challenge value χ and said shared secret in a one-way function f_1 ; and

said first correspondent C transmitting said computed response signal to said second correspondent T whereby said second correspondent T may verify said first correspondent C.

25. A method as defined in claim 24, including said first correspondent C transmitting a signed message m with said response signal.

26. A method as defined in claim 25, including signing said message m with said one way function f_1 .

27. A method as defined in claim 26, said signed message m being included with said computed response signal and concatenated with said message m for transmission.

28. A method as defined in claim 24, including said first correspondent C encrypting a message m in accordance with a symmetric key scheme, wherein a symmetric key is derived from said computed response signal and said method comprises transmitting said encrypted message m to said second correspondent T.

29. A method as defined in claim 28, said scheme being an RSA type signature scheme.

30. A method as defined in claim 24, said shared secret being computed by said second correspondent T by utilizing its secret key and the public key.

31. A method as defined in claim 24, said second correspondent T having a plurality of private keys t_i corresponding to respective first correspondents; said method comprising said first correspondent C sending to said second correspondent T, an identification index i to enable said second correspondent T to use said corresponding private key t_i and the public key to compute a shared secret ss_i .

32. A method as defined in claim 24, utilizing a public key scheme being an elliptic curve scheme.

33. A method as defined in claim 24, utilizing a public key scheme being an RSA type scheme.

34. A system for authenticating at least one of a pair of first and second correspondents C and T in a data communication system, said system comprising a computing device at said first correspondent C and being configured for performing the method according to any one of claims 24 to 33.

35. A computer readable medium comprising computer executable instructions for causing a computing device to perform the method according to any one of claims 24 to 33.

36. A method for authenticating at least one of a pair of correspondents T and C in an information exchange session, and wherein one of the correspondents T includes a secret key t and the other correspondent C has a public key and a shared secret value t_c derived from said public key and said secret key t , the method comprising;

generating a challenge value χ and transmitting said challenge value χ to said first correspondent C in response to receiving public information from said first correspondent C;

generating a session shared secret ss by combining said secret key t with said public key of said first correspondent C;

generating a test response signal k_t by combining said session shared secret ss with said challenge value χ , in a mathematical function f_1 ; and

comparing said response test signal k_t to a received response value k_c from said first correspondent C to verify said first correspondent C.

37. A method as defined in claim 36, including receiving from said first correspondent C a signed message m with said response signal.

38. A method as defined in claim 37, wherein said message m is signed with said one way function f_1 .

39. A method as defined in claim 38, said signed message m being included with said computed response signal and concatenated with said message m for transmission.

40. A method as defined in claim 36, wherein said first correspondent C has encrypted a message m in accordance with a symmetric key scheme, wherein a symmetric key is derived from said

computed response signal and said method comprises receiving said encrypted message m by said second correspondent T.

41. A method as defined in claim 40, said scheme being an RSA type signature scheme.

42. A method as defined in claim 36, said shared secret being computed by said second correspondent T by utilizing its secret key and the public key.

43. A method as defined in claim 36, said second correspondent T having a plurality of private keys t_i corresponding to respective first correspondents; said method comprising receiving from said first correspondent C an identification index i and using said corresponding private key t_i and the public key to compute a shared secret ss_j .

44. A method as defined in claim 36, utilizing a public key scheme being an elliptic curve scheme.

45. A method as defined in claim 36, utilizing a public key scheme being an RSA type scheme.

46. A system for authenticating at least one of a pair of first and second correspondents C and T in a data communication system, said system comprising a computing device at said second correspondent T and being configured for performing the method according to any one of claims 36 to 45.

47. A computer readable medium comprising computer executable instructions for causing a computing device to perform the method according to any one of claims 36 to 45

48. A system for authenticating at least one of a pair of correspondents T and C in an information exchange session, and wherein one of the correspondents T includes a secret key t and the other correspondent C has a public key and a shared secret value t_c derived from said public key C and said secret key t , the system being configured for:

having the first correspondent C transmit to the second correspondent T information including said public key;

having the second correspondent T generate a challenge value χ and transmit said challenge value χ to said first correspondent C;

having said second correspondent T generate a session shared secret ss by combining said secret key t with said public key of said first correspondent C;

having said second correspondent T generate a response signal k_t by combining said session shared secret ss with said challenge value χ , in a mathematical function f_1 ;

having said first correspondent C generate a response value k_c by combining said shared secret t_c with said challenge value χ in said mathematical function f_1 and send said response value k_c to said second correspondent T; and

having said second correspondent T compare said response signal k_t to said response value k_c to verify said first correspondent C.

49. A method of authenticating at least one of a pair of correspondents T and C in an information exchange session, and wherein one of the correspondents T includes a secret key t and the other correspondent C has a public key and a shared secret value t_c derived from said public key C and said secret key t, the method comprising the steps of:

said second correspondent T receiving information including said public key from the first correspondent C;

the second correspondent T generating a challenge value χ and transmitting said challenge value χ to said first correspondent C;

said second correspondent T generating a session shared secret ss by combining said secret key t with said public key of said first correspondent C;

said second correspondent T generating a response signal k_t by combining said session shared secret ss with said challenge value χ , in a mathematical function f_1 ;

said second correspondent receiving from said first correspondent C, a response value k_c generated by combining said shared secret t_c with said challenge value χ in said mathematical function f_1 ; and

said second correspondent T comparing said response signal k_t to said response value k_c to verify said first correspondent C.

50. A system for authenticating at least one of a pair of first and second correspondents C and T in a data communication system, said system comprising a computing device at said second correspondent T and being configured for performing the method according to claim 49.

51. A computer readable medium comprising computer executable instructions for causing a computing device to perform the method according to claim 49.

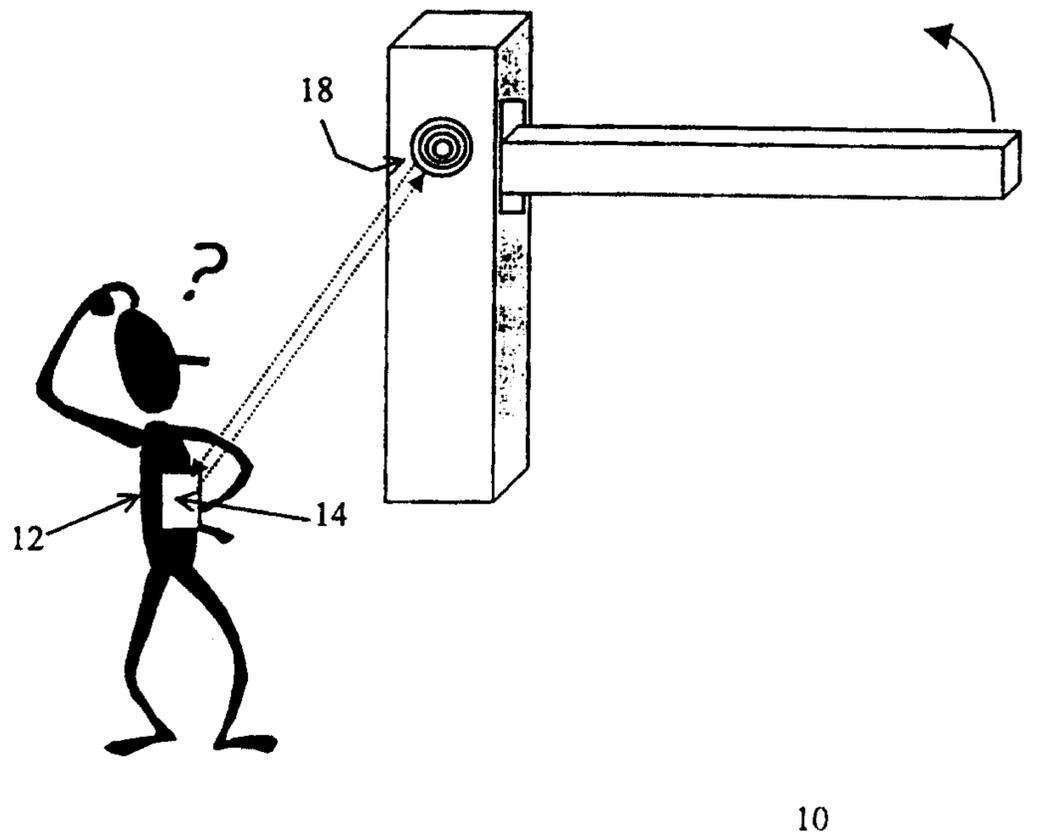


FIG. 1

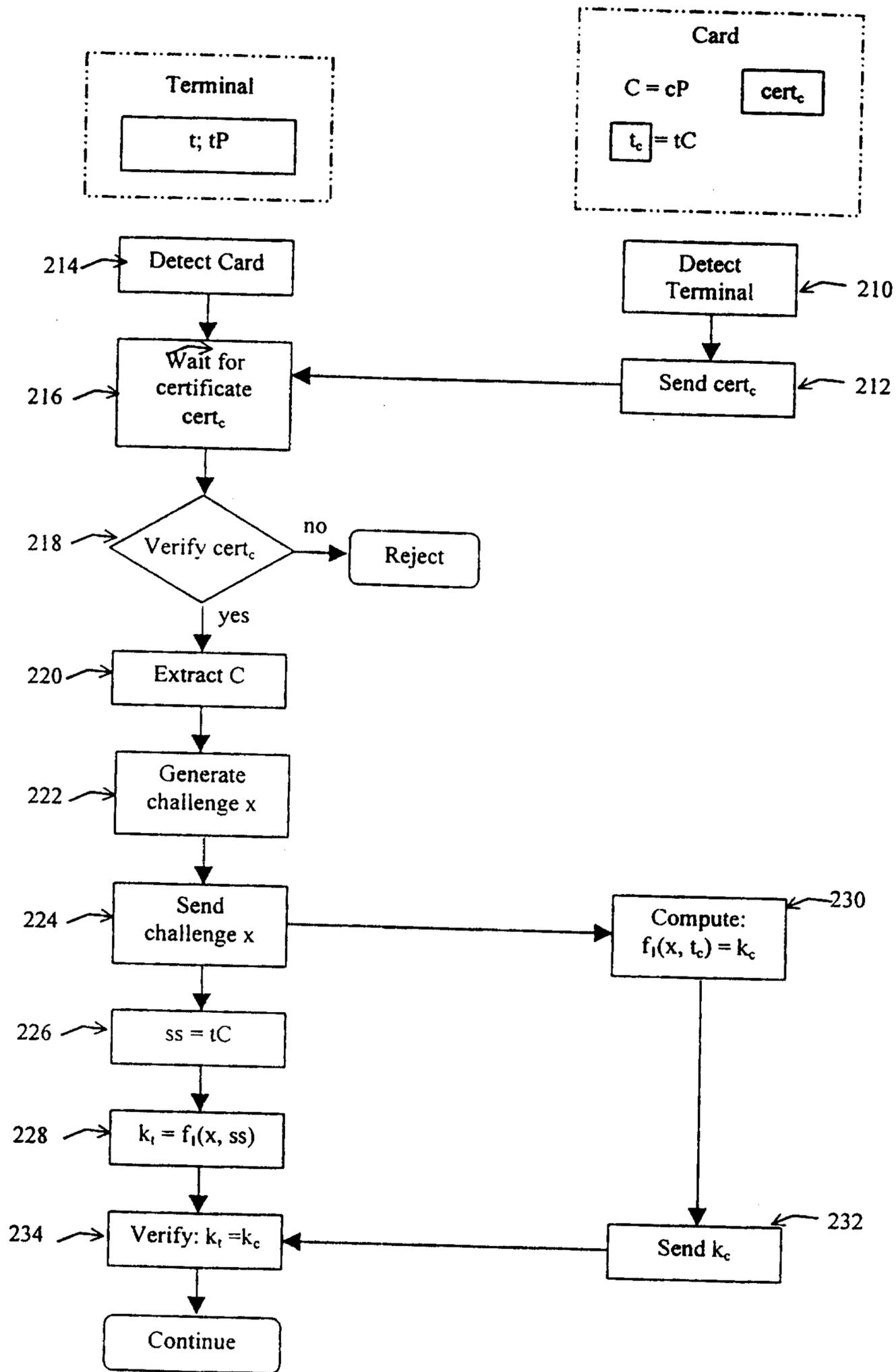


FIG. 2

