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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 July 2004 (08.07.2004)

PCT

(10) International Publication Number
WO 2004/057547 A1

(51) International Patent Classification[7]: G07F 7/10, 19/00, H04L 9/32

(21) International Application Number: PCT/SE2003/001980

(22) International Filing Date: 17 December 2003 (17.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0203877-6 23 December 2002 (23.12.2002) SE

(71) Applicant *(for all designated States except US)*: **TELIA AB (PUBL)** [SE/SE]; Mårbackagatan 11, S-123 86 Farsta (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ERIKSSON, Jonas** [SE/SE]; John Ericssongatan 16, S-652 22 Karlstad (SE). **KÅWE, Rolf** [SE/SE]; Lingonstigen 7, S-654 68 Karlstad (SE).

(74) Agent: **SVENSSON, Peder**; TeliaSonera Sverige AB, Patent, Vitsandsgatan 9, S-123 86 Farsta (SE).

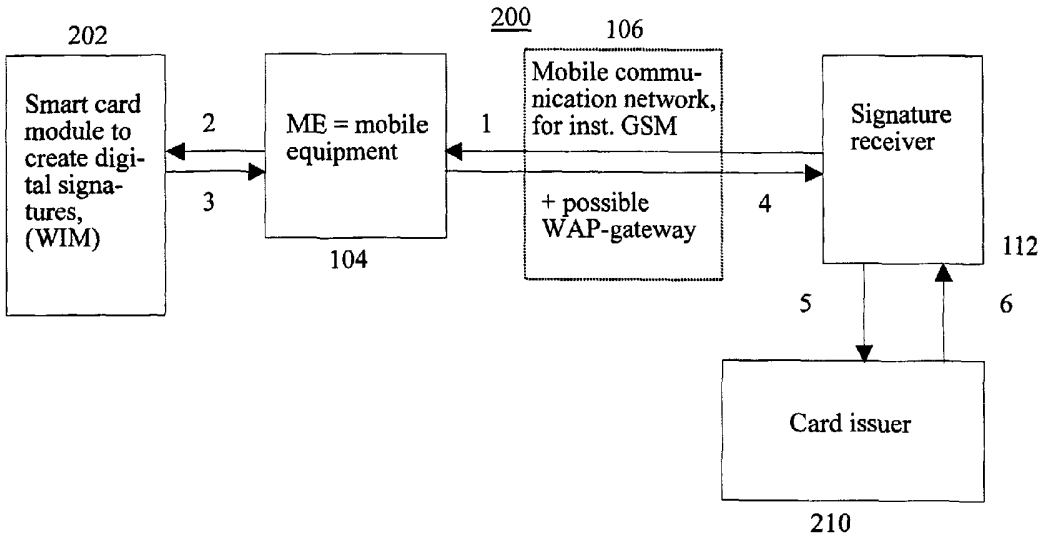
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR TRANSMISSION OF DATA



(57) Abstract: A verification system (200) and a method to, at a wireless telecommunication and data communication network (100), make earnings possible for a card issuer (118). The verification system is based on open, standardized interfaces. When a digital signature has been created on a smart card (102) in a mobile unit (104), the digital signature is encrypted with/by a key which belongs to the card issuer before the signature leaves the smart card. The encrypted signature is transmitted/transferred to the signature receiver (112) in the same way as if it had not been encrypted by the card issuer's key. The signature receiver after that transmits the signature to the card issuer. The card issuer decrypts the signature, debits the signature receiver and transmits the decrypted signature to the signature receiver. After that, the signature receiver can check the digital signature.

WO 2004/057547 A1

METHOD AND SYSTEM FOR TRANSMISSION OF DATA

Technical field

The present invention relates to a system and a method to, at a wireless telecommunication and data communication network, make earnings possible for a card issuer in a system which is based on open, standardized interfaces.

Prior art

Since some time back there are systems to create digital signatures by means of a mobile telephone, based on keys on so called smart cards in the mobile telephone and PKI (Public Key Infrastructure). There are two main approaches to realize these methods, on the one hand a solution which is based on SIM application tool combined with an OTA-platform (OTA = Over The Air) and on the other a solution based on WIM (Wireless Application Module).

In the first solution the card issuer, which is the mobile telephone operator, has full control over the signing process and all communication is executed via the operator's OTA-platform. By that, the operator has all possibilities to charge participants (that is, service providers, for instance banks) which want to use the signature function. The operator has for the same reason possibility to charge a CA (Certificate Authority) which wants to issue certificate based on keys on the smart card. The disadvantage with/of this solution is that it is not standardized.

In the latter solution the interfaces are standardized by WAP (Wireless Application Protocol) forum and is often considered to be the solution which will be the most successful. Here the interfaces are standardized, and the operator is transparent in communication sense to the participants which want to use the signing function. Of

that follows that the card issuer to-day has no technical possibility to charge participants which are using the signing function. There also are possibilities for a CA to issue certificate based on keys on the smart card, without the card issuer´s knowledge, and therefore neither earnings related to this are secured by the card issuer.

To-day's system to secure card issuer earnings at digital signatures is based on that the communication between the smart card in the mobile telephone and the service provider/CA is executed via some form of operator gateway, where billing data is generated (frequently based on so called SAT-technology (SIM Application Toolkit)+ OTA platform).

The solution which exists today to try to secure earnings for CA is to charge for revocation information. Such a solution is based on that CA = card issuer and does not function from a business point of view for systems where CA and card issuer are different parties. When some party is interested in validating/verifying a signature, this party turns to CA to get revocation information, not to the card issuer, so the card issuer has difficulties to get any earnings for the signatures which are created with/ by his card. It is true that CA frequently have based their certificates on the card issuer's device certificate (which usually informs about which party has made/issued the card, created key etc), but these are never revoked in the practice, so the card issuer hardly can base its business on revocation information for device certificate.

US 2002/0032860 shows a system in which an encrypted digital signature is transmitted from a customer, via a tradesman, to a financial institution. The financial institution decrypts the signature and transmits the

decrypted signature (+ account information) to the tradesman.

WO 99/00775 shows a system for payment. In a terminal is a "smart card". Between the terminal and an "acquirer" there is a two-way communication channel. This two-way communication channel connects the card issuer with the "acquirer", where the "acquirer" acts as an agent for the majority of card issuers and can, for instance, be a bank. One way is that a PIN-code is encrypted and is transmitted via an "acquirer" to the card issuer. The "acquirer" can not decrypt the PIN-code.

WO 01/45056 shows a system to perform card transactions. The buyer´s computer creates an encrypting number, which at least to some extent/part agrees with the card number. The encrypted number is given to a tradesman who forwards it to the card issuer, the computer of which can decrypt the number. Identification of the buyer is made via a separate link from the buyer to the card issuer.

WO 00/79724 shows a WIM-card containing the card manufacturer's private key. By this, certificate is signed. Verification of the signature is made by the card issuer.

US 2002/00056079 shows a method to load an application on a "smart card". The one which provides the application (the service provider) cannot decrypt "card attribute data", but has to transmit these (and ID for the application) further to the card issuer. The card issuer decrypts "card attribute data" and identifies the card. The card issuer then decides if the loading of the application shall be allowed or not, and informs about this to the service provider.

WO 01/22374 shows a method and system for secure payment. The idea of the method is that the card issuer is responsible for "authentication" of the card owner/holder and "authorization" of the card purchase. At a purchase an inquiry/request about payment is transmitted from the tradesman to the card holder. The card holder opens a link to the card issuer, (authenticated by the card issuer), and transmits information about the purchase and the tradesman via the link to the card issuer. The card issuer answers/ responds by transmitting payment information to the tradesman via the cardholder's computer. The tradesman's computer confirms the purchase. The card issuer confirms the payment when the card holder has been authenticated. All data which are transmitted are decrypted.

The cardholder's computer can be a mobile telephone. The card issuer has control over the information flow to the card holder during the transfer of the payments.

SUMMARY OF THE INVENTION

The present invention relates to a system and a method to create digital signatures by means of a mobile telephone, which system is based on keys in so called smart cards in a mobile telephone and PKI.

Today's system for securing card issuer earnings at digital signatures is based on that the communication between the smart card in the mobile telephone and the service provider is executed via some form of operator interface where the debiting data is generated. The invention results in that a standardized system with open solutions instead can be used, that is, in the whole interaction between the service provider and the user.

A distinctive feature of the invention is that when a digital signature has been created on a smart card in a mobile unit, the digital signature is encrypted (not the

signed amount of data) with/by a key which belongs to the card issuer before the signature leaves the smart card. The encrypted signature is transmitted/transferred to the receiver in the same way as if it had not been encrypted by /with the card issuer's key. The receiver transmits the signature to the card issuer, which is the only one that can decrypt the signature. The card issuer decrypts the signature, debits the signature receiver and transmits the decrypted signature to the signature receiver. Only after that, the signature receiver can evaluate/check the decrypted signature.

One advantage with/of the invention is that verification of the digital signature is made in a standardized system with open solutions, that is, in the whole interaction between service provider/CA and user.

Another advantage with/of the invention is that the digital signature is encrypted after it has been created, so that only the card issuer can decrypt it.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention now will be described in details in the following with reference to enclosed drawings, in which

Figure 1 shows a survey of a mobile system which verifies signatures on smart cards,

Figure 2 shows verification system/systems of how a digital signature can be verified,

Figure 3 shows a signal diagram of how the signature can be verified,

Figure 4 shows a flow chart of how the signature is verified.

DESCRIPTION OF PREFERRED EMBODIMENTS

The invention aims at securing the card issuer´s earnings for systems which are based on WIM or other future systems with open interfaces.

Figure 1 shows a survey of a system 100 for mobile communication, the mobile system, which can verify signatures on smart cards. The mobile system 100 consists of a smart card SK 102 which contains/includes a function A to create a digital signature DS on an amount of data, and a function B which encrypts the digital signature by/with a card issuer´s key KN and gets an encrypted digital signature. A mobile terminal ME 104 with a card reader where the smart card is placed. A mobile communication network 106 via which communication between mobile terminal/smart card and a signature receiver SM 112 is executed. The mobile communication network includes typically base stations, transmission, exchanges and databases. The mobile communication network also can be a short distance communication network (based on, for instance, Blue Tooth). A gateway or proxy 108 which connects the mobile communication network with an Internet 110. Internet (data communication network) is used for the communication between mobile terminal/smart card and the signature receiver. Such a data communication network also can be used for communication between the signature receiver and a card issuer server 118. There are two main types of signature receivers: Certificate Authority 114 (certificate-issuer) or a Service Provider 116 (service-provider). At/with these there are different servers and databases/catalogs. From the signature receiver, the encrypted digital signatures are transmitted to the card issuer server. The card issuer server decrypts the digital signatures and after that returns the decrypted digital signatures to the signature receiver.

Figure 2 shows a verification system 200 of how a signature can be verified, and Figure 3 shows a signal diagram 300 over how the signature can be verified. The signal diagram shows examples of which type of signal management that is applied between the different units in the verification system. In the verification system is included a smart card module SKM 202 to create digital signatures (WIM), a mobile terminal 104, some type of mobile communication network ME 106, for instance GSM + possible WAP-gateway, the signature receiver SM 112, and card issuer KU 210 which provides the card issuer server 118.

The following communication can be executed between the different units:

Step 1: The signature receiver SM 112 transmits 302 a signing enquiry/request to the mobile terminal ME 104.

Step 2: The mobile terminal ME 104 attends to the signing enquiry/request. After that, the mobile terminal ME request 304 that a smart card module SKM 202 shall create a digital signature.

Step 3: The smart card module SKM 202 makes use of the function A, which creates a digital signature DS and the function B, which encrypts the digital signature and then will have an encrypted digital signature KDS. After that, the encrypted digital signature is transmitted 306 to the mobile terminal ME 104.

Step 4: The mobile terminal ME 104 transmits 308 with the encrypted digital signature KDS to the signature receiver SM 112.

Step 5: The signature receiver SM 112 forwards/further transmits 310 the encrypted digital signature KDS to a card issuer KU 210.

Step 6: The card issuer KU 210 decrypts the encrypted digital signature KDS and gets a decrypted digital signature DDS, debits the signature receiver for this, and transmits 312 the decrypted signature to the signature receiver 112.

In Figure 4 a flow chart 400 over how the signature is verified is shown, consequently a more detailed procedure than has earlier been described. The service provider 116, which also is the signature receiver SM 112, transmits 402 a signing enquiry/request to the user's mobile terminal ME 104, which, for instance, includes/contains the data which shall be signed.

The mobile terminal ME 104 starts 404 a dialog with a user. The user decides 406 to sign the content and enters 408 information (most often a PIN-code) which is required to unlock the signing key SN. The mobile terminal requests 410 that the smart card module SKM 202 shall create a digital signature DS for the content, by one of the private keys PN for signing on the card.

The function A creates 412 a digital signature DS for the content in the smart card module SKM 202. The function B encrypts 414 the digital signature DS by the card issuer's key KN. After that, the encrypted digital signature KDS is transmitted 416 to the mobile terminal ME 104.

The mobile terminal ME 104 formats/creates 418 an answer to the signature inquiry/request and encloses 420 the encrypted digital signature KDS to the signature

receiver SM 112. Information about which party the card issuer is, is also enclosed.

The signature receiver SM 112 transmits 422 the encrypted digital signature KDS to the card issuer KU 210.

The card issuer KU 210 decrypts 424 the encrypted digital signature, debits 426 the signature receiver SM 112 for this, and transmits 428 the decrypted digital signature DDS to the signature receiver SM 112.

The invention is not limited to use with any/some specific protocols or frameworks, but since it is in the first phase is expected to be used together with WIM and WPKI according to WAP forum, here follows a (somewhat simplified of the steps 1-5) description of what this case can look like:

The service provider transmits a signing inquiry/ request to the user´s mobile terminal by means of the function "signText". A description of "signText" is to be found in "WMLScript Crypto Library" WAP-161-WMLScriptCrypto-20010620-a, WAP forum.

The mobile terminal starts a dialog towards the user, and the user decides to sign the content and enters information (most often a PIN-code) which is required to unlock the signing key. The mobile terminal request that WIM shall create a digital signature for the content by transmitting the command "Compute Digital Signature" to WIM, see "Wireless Identity Module" WAP-260-WIM-20010712-a, WAP forum.

The WIM-application creates a signature for/to the content. An additional function on the smart card encrypts the signature with/by the card issuer's key. After that,

the encrypted signature is transmitted to the mobile terminal in the command answer to "Compute Digital Signature".

The mobile terminal formats/creates a result of "signText", where the encrypted signature is enclosed as the object "Signature". A certificate or a certificate-ULR is also added, where the certificate includes additional information about which party the card issuer is. The result of "signText" is transmitted from the mobile terminal to the signature receiver. The signature receiver transmits the encrypted signature to the card issuer.

The card issuer decrypts the signature, debits the signature receiver for this, and transmits the decrypted signature to the signature receiver.

Note that it is only the signature, not the signed content, that is encrypted in Step 3, and which is transmitted to the card issuer in Step 5. Because the signature is based on a one-way function of the signed content, it is insensitive information from a security point of view, even if the signed content is of confidential nature.

The signature receiver must get to know that the signature is encrypted, and where to turn to get it decrypted. The best way probably is to let the information exist explicitly or implicitly in the user- or device certificate (sometimes a URL is transmitted instead which point at the certificate) which, according to Step 4, is transmitted to the service provider, even if there are other possibilities.

One important quality of the invention is that it probably can be used for WAP (WIM, signtext) without

changes in the mobile terminal or WAP GW, the encrypted signature is transmitted transparently as a non-encrypted signature. The adjustments are made in WIM (however not in the interface towards the mobile terminal) and in origin server/PKI-portal (however not in the interface towards WAP GW).

The method can be used both with symmetric and asymmetric card issuer encryption of the digital signature. In the symmetric case, the secret key which has been placed on the smart card to encrypt the signatures, is only known by/to the card issuer. In the asymmetric case, the signature is encrypted by a public key, the corresponding private key of which only is known by the card issuer.

Note that a card issuer key per card should be used, and not a card issuer key for several cards. This in order to minimize the damage if the key becomes known.

One possible variant of the method is that a service provider/signature receiver buys "permanent" access to the card issuer key of certain cards, and is allowed to use it under an agreement. In that case the communication with the card issuer in Step 5 and 6 is not needed for each signature.

The method also can be used where digital signatures created on a smart card are used in any step to create a secure data transport, for instance WTLS (Wireless Transport Layer Security) or SSL (Secure Sockets Layer). This might, in the WTLS-case, imply that the answer to Sign H (handshake-msg) would be encrypted with/by the card issuer's key, whereupon it is transmitted to the server in "Certificate verify", whereupon the server has to transmit the content in "Certificate verify" to the card issuer to get the signature decrypted.

The method also would be possible to use in corresponding non-mobile connections to secure card issuer earnings.

Example 1

There is operator which issues SIM with WIM (SWIM) which also points at a device certificate (SWIM does not hold the public key) with RSA-keys. The operator's idea partly is based on the principle that the party who wants to issue a certificate based on keys on SWIM shall pay a fee to the operator for this. One method for this is that the operator creates a database with device certificates and charges the one who requests a device certificate as basis to create a user certificate. In principle anybody can issue a user certificate if the above invention is not used. By the suggested method, two signatures of/by users inquire/request (in that way the public key can be calculated, device certificate is not necessary). The invention prevents this, by only parties having agreements with the operator being allowed to have signatures decrypted. The operator then can charge a small sum for each signature that has been made, which as such is a business possibility. This in its turn makes possible that the operator might allow external CA (Certificate Authority) to issue "public" certificates (public in this context means that the user will have full access to his/her certificate and it is associated to an official CPS etc), without it, for that reason, being uninteresting for/to other parties to issue certificates for the same user connected to the same SWIM.

Example 2

The operator issues SIM with WIM (SWIM) and the operator issues "public" user certificates to it as the holder of SWIM (public in this context means that the user will have full access to his/her certificate and it is

invention, the operator can get possibility to create earnings at each signature which is made by means of the SWIM.

PATENT CLAIMS

1. Verification system (200) to verify signatures on a smart card (102, 202), which verification system includes at least one mobile terminal (104) with at least one card reader for at least one smart card (102, 202), at least one signature receiver (112) and at least one card issuer server (118), c h a r a c t e r i z e d in that the smart card/mobile terminal is in connection with the signature receiver via at least one mobile communication network (106) which in its turn is in connection with the card issuer server, that it in the smart card first is created (412) a signature, next step the signature is encrypted (414), after that the encrypted signature is transmitted (306, 416, 308, 420, 310, 422) to the card issuer server via the mobile terminal and the signature receiver, that in the card issuer server the signature is decrypted (424), after that the decrypted signature is returned (312, 428) to the signature receiver, and that in the signature receiver the decrypted signature is evaluated/checked.

2. Verification system to verify signatures on a smart card as claimed in patent claim 1, c h a r a c t e r i z e d in that the mobile communication network includes base stations, transmission, exchanges and databases.

3. Verification system to verify signatures on a smart card as claimed in patent claim 1, c h a r a c t e r i z e d in that the mobile communication network is a short distance communication network.

4. Verification system to verify signatures on a smart card as claimed in any of the patent claims 1-3, c h a r a c t e r i z e d in that between the mobile communication network and the signature receiver is a

gateway (108) and a data communication network (110) which are connected with each other.

5. Verification system to verify signatures on a smart card as claimed in patent claim 4, c h a r a c t e r i z e d in that the data communication network is used for communication between the mobile terminal/the smart card and the signature receiver.

6. Verification system to verify signatures on a smart card as claimed in any of the previous/above given patent claims, c h a r a c t e r i z e d in that the signature receiver is certificate issuer (114).

7. Verification system to verify signatures on a smart card as claimed in any of the patent claims 1-5, c h a r a c t e r i z e d in that the signature receiver is a service provider (116).

8. Procedure (200, 300, 400) to verify signatures on a smart card consisting of a verification system (100) which includes at least one mobile terminal (104) with at least one card reader for at least one smart card (102, 202), at least one signature receiver (112) and at least one card issuer server (118), c h a r a c t e r i z e d in that the smart card/the mobile terminal is in connection with the signature receiver via at least one mobile communication network (106) which in its turn is in connection with the card issuer server, that the procedure includes to create (412) a signature, to encrypt (414) the signature in the smart card, to transmit (306, 416, 308, 420, 310, 422) the encrypted signature to the card issuer server via the mobile terminal and the signature receiver, to decrypt (424) the signature, to return (312, 428) the decrypted signature to the signature receiver that these steps of procedure are executed in the card issuer server, to

evaluate/check the decrypted signature in the signature receiver.

9. Procedure to verify signatures on a smart card as claimed in patent claim 8, c h a r a c t e r i z e d in that before creating a signature the procedure includes a first step; to transmit (302, 402) a signing/signature inquiry/request from the signature receiver to the mobile terminal.

10. Procedure to verify signatures on a smart card as claimed in patent claim 8, c h a r a c t e r i z e d in that before the step to create a signature, in the mobile terminal, the procedure includes a second step; to attend to the signing inquiry/request, to request (304, 404) that the smart card shall create a digital signature.

11. Procedure to verify signatures on a smart card as claimed in patent claim 8, c h a r a c t e r i z e d in that the step to create a signature, the procedure includes a third step; to use a function A to create (412) a digital signature, to in the step to encrypt the signature use a function B to encrypt (414) the digital signature, and to after that transmit (306, 416) the encrypted digital signature to the mobile terminal.

12. Procedure to verify signatures on a smart card as claimed in patent claim 8, c h a r a c t e r i z e d in that after the step to encrypt the signature, the procedure includes a fourth step ; to transmit (308, 420) the encrypted digital signature from the mobile terminal to the signature receiver.

13. Procedure to verify signatures on a smart card as claimed in patent claim 8, c h a r a c t e r i z e d in

that, after the step to encrypt the signature, the procedure includes a fifth step ; to transmit (310, 422) the encrypted digital signature from the signature receiver to card issuer server.

14. Procedure to verify signatures on a smart card as claimed in patent claim 8, c h a r a c t e r i z e d in that, in the step to decrypt the encrypted signature, the procedure includes a sixth step; to decrypt (424) the encrypted digital signature, to debit (426) the signature receiver for this, and to transmit (312, 428) the decrypted digital signature to the signature receiver.

15. Procedure to verify signatures on a smart card as claimed in patent claim 10, c h a r a c t e r i z e d in that the second step of procedure includes to start (404) a dialog with a user, that the user decides (406) to sign the content and enters (408) a PIN-code to unlock the signing key SN, to request (310, 410) that the smart card shall create the digital signature by one of the private keys for signing on the card.

16. Procedure to verify signatures on a smart card as claimed in patent claim 11, c h a r a c t e r i z e d in that in the function B the digital signature is encrypted (414) by/with the card issuer's key.

17. Procedure to verify signatures on a smart card as claimed in patent claim 12, c h a r a c t e r i z e d in that the fourth step of procedure includes that the mobile terminal formats/creates (418) an answer to the signature inquiry/request and encloses (308, 420) the encrypted digital signature and information about which party the card issuer is.

18. Computer program including program steps for execution of the steps in a procedure according to any of the patent claims 8-17.

19. Computer with readable medium including instructions for execution of the steps in procedure according to any of the patent claims 8-17.

1/3

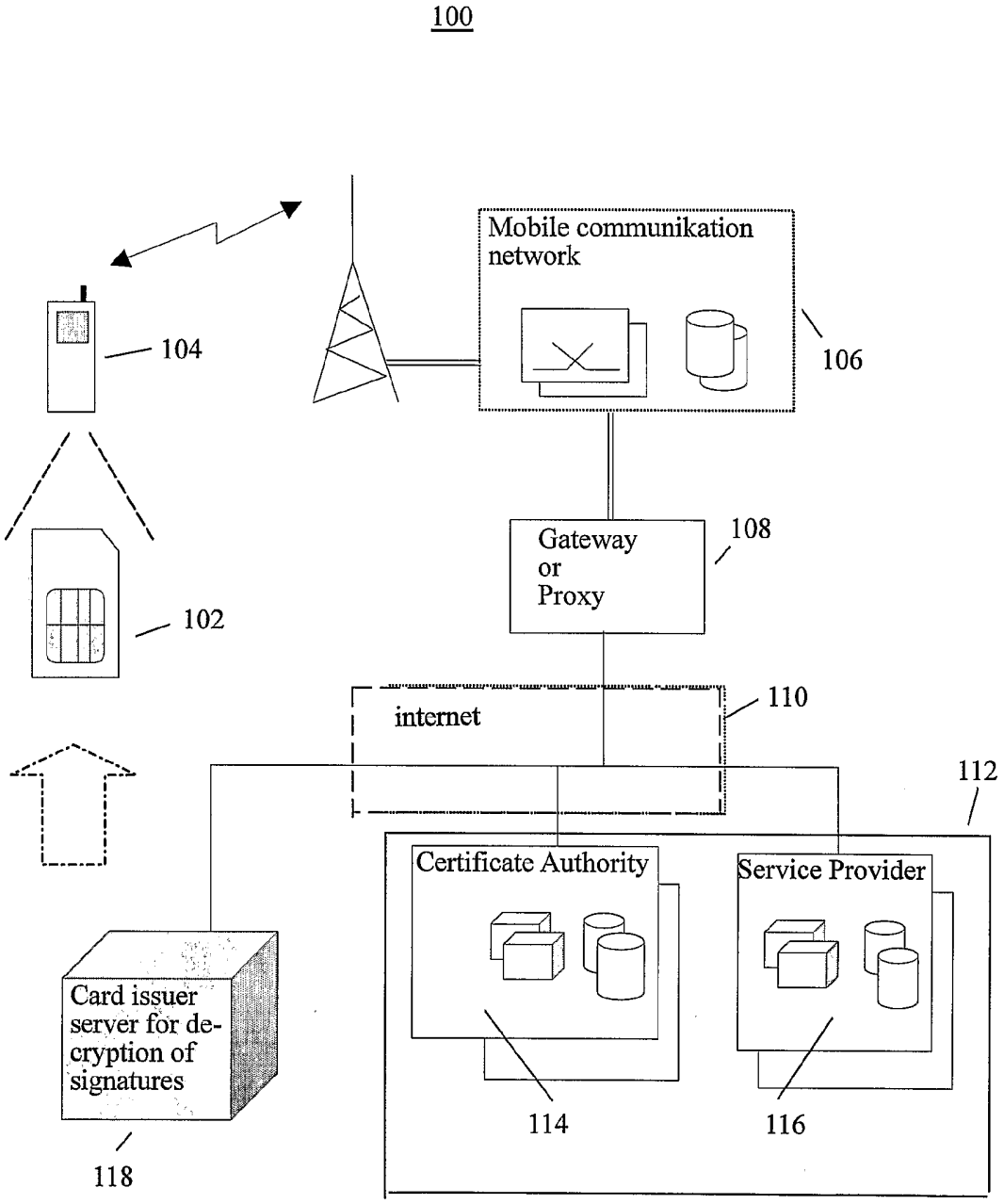

100
Mobile communikation network
106
104
102
Gateway or Proxy
108
internet
110
112
Certificate Authority
Service Provider
Card issuer server for de-cryption of signatures
114
116
118

Fig. 1

2/3

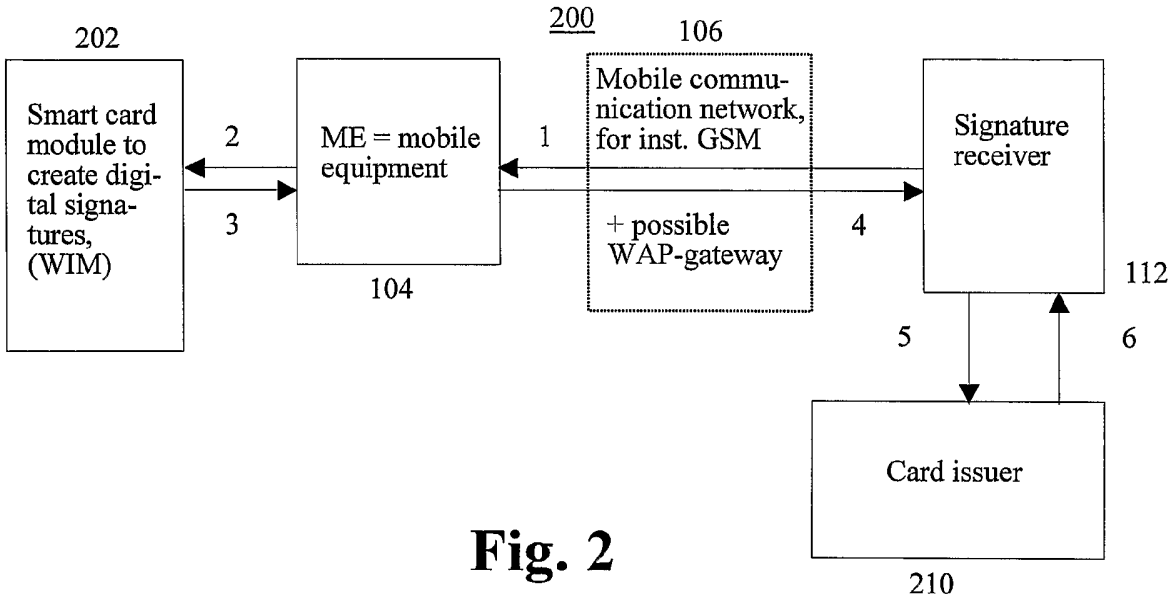

200
202
106
Smart card module to create digital signatures, (WIM)
2
3
ME = mobile equipment
104
1
Mobile communication network, for inst. GSM
+ possible WAP-gateway
4
Signature receiver
112
5
6
Card issuer
210

Fig. 2

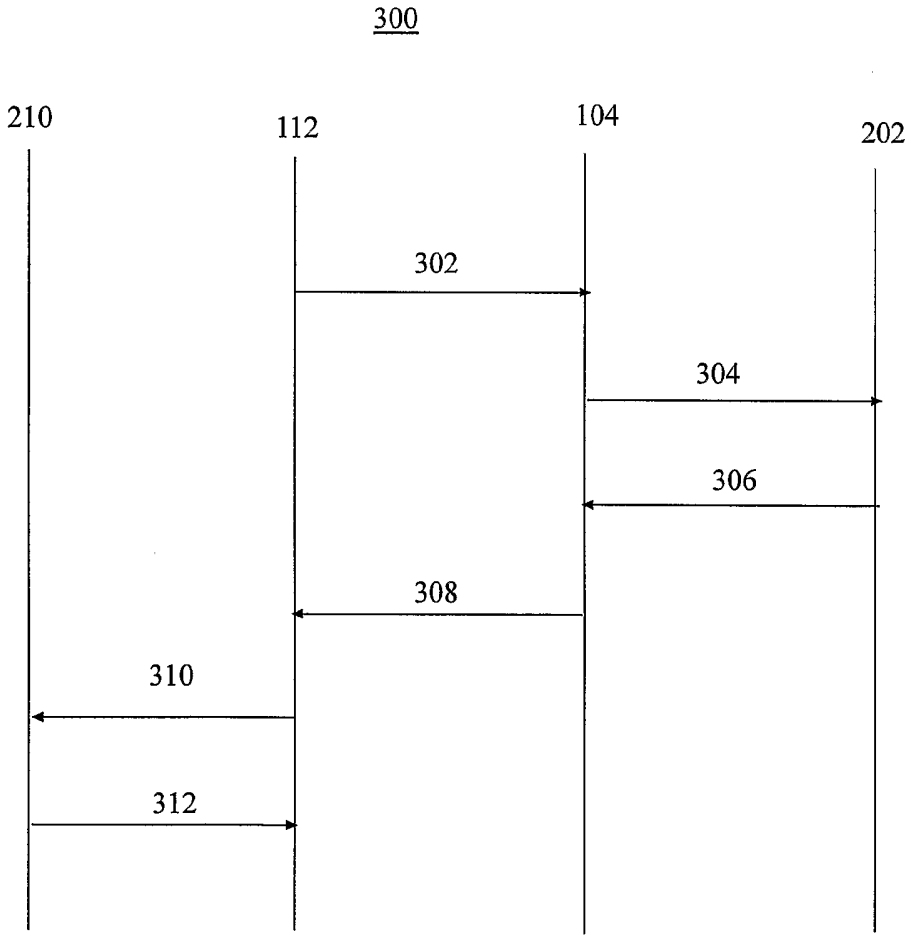

300
210
112
104
202
302
304
306
308
310
312

Fig. 3

3/3

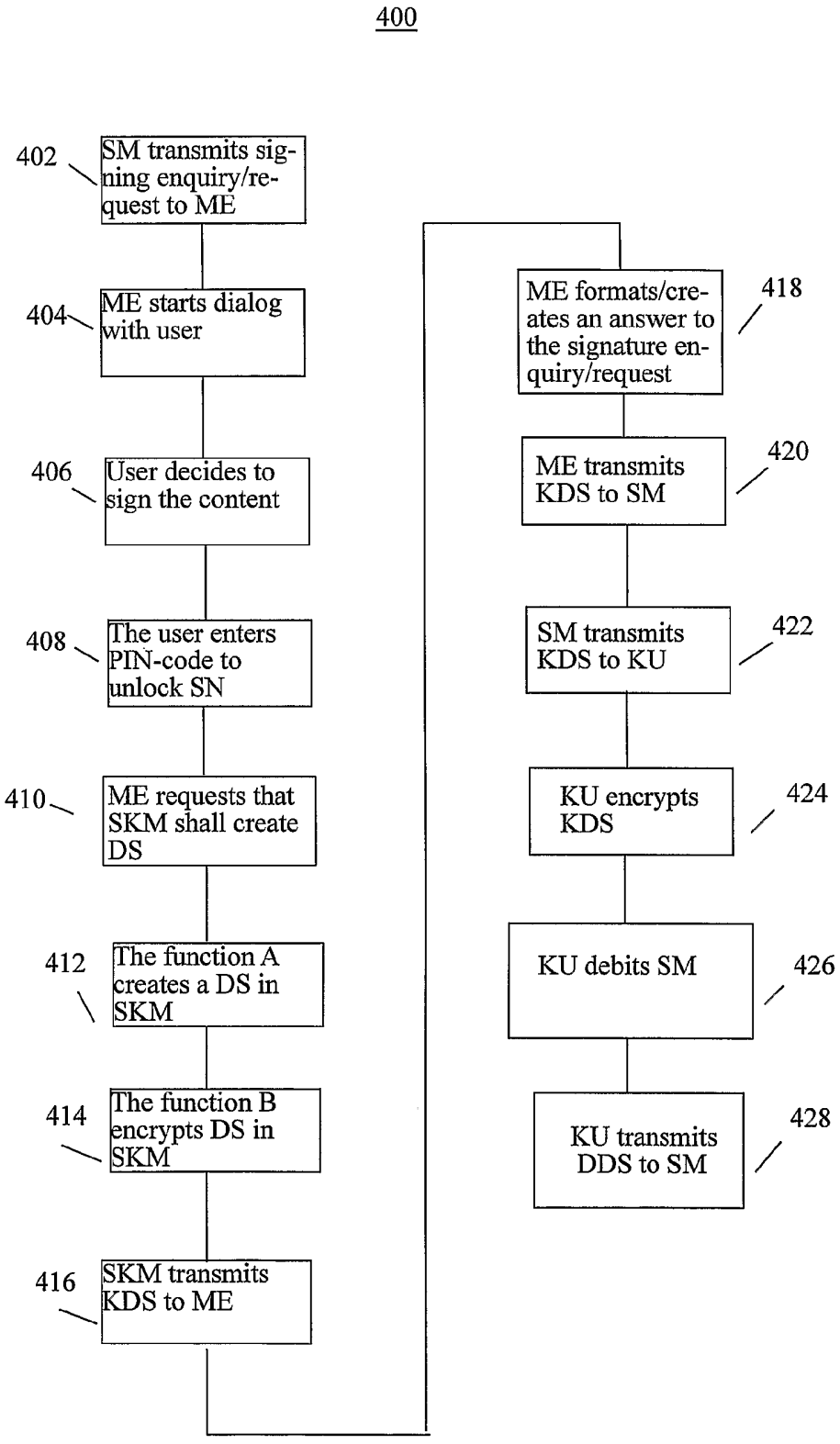

400
402
SM transmits signing enquiry/request to ME
404
ME starts dialog with user
406
User decides to sign the content
408
The user enters PIN-code to unlock SN
410
ME requests that SKM shall create DS
412
The function A creates a DS in SKM
414
The function B encrypts DS in SKM
416
SKM transmits KDS to ME
418
ME formats/creates an answer to the signature enquiry/request
420
ME transmits KDS to SM
422
SM transmits KDS to KU
424
KU encrypts KDS
426
KU debits SM
428
KU transmits DDS to SM

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 2003/001980

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G07F 7/10, G07F 19/00, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G07F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2375872 A (VODAFONE GROUP LIMITED (INCORPORATED IN THE UNITED KINGDOM)), 27 November 2002 (27.11.2002), page 5 - page 6	1-19
	--	
A	WO 9852151 A1 (ACCESS SECURITY SWEDEN AB), 19 November 1998 (19.11.1998), fig. 5 and adherent text	1-19
	--	
A	US 2002077993 A1 (IMMONEN ET AL), 20 June 2002 (20.06.2002), whole document	1-19
	--	
A	US 6223291 B1 (PUHL ET AL), 24 April 2001 (24.04.2001), whole document	1-19
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 March 2004	15 -03- 2004
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Inger Löfving / MRo Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 2003/001980

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5903882 A (ASAY ET AL), 11 May 1999 (11.05.1999), whole document -- --------	1-19

GB	2375872	A	27/11/2002	GB	0112480	D	00/00/0000
WO	9852151	A1	19/11/1998	AU	741873	B	13/12/2001
				AU	7560298	A	08/12/1998
				CN	1256775	T	14/06/2000
				EP	0981804	A	01/03/2000
				EP	1024777	A	09/08/2000
				HU	0001872	A	28/09/2000
				IL	132689	D	00/00/0000
				JP	2001525093	T	04/12/2001
				NO	995529	A	10/01/2000
				NZ	501074	A	01/02/2002
				PL	336938	A	17/07/2000
				SE	512748	C	08/05/2000
				SE	9701814	A	16/11/1998
US	2002077993	A1	20/06/2002	NONE			
US	6223291	B1	24/04/2001	AU	3498600	A	16/10/2000
				CN	1345494	T	17/04/2002
				EP	1166490	A	02/01/2002
				WO	0059149	A	05/10/2000
US	5903882	A	11/05/1999	AU	5515398	A	03/07/1998
				BR	9714400	A	18/04/2000
				CA	2274897	A	18/06/1998
				CN	1244936	A	16/02/2000
				EP	0965111	A	22/12/1999
				JP	2001507145	T	29/05/2001
				US	2001011255	A	02/08/2001
				WO	9826385	A	18/06/1998