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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2003 (24.04.2003)

PCT

(10) International Publication Number
WO 03/034772 A1

(51) International Patent Classification⁷: **H04Q 7/38**, H04L 9/32

(21) International Application Number: PCT/SE02/01765

(22) International Filing Date: 27 September 2002 (27.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0103485-9 19 October 2001 (19.10.2001) SE

(71) Applicant *(for all designated States except US)*: **SMART-TRUST SYSTEMS OY** [FI/FI]; P.O. Box 119, FIN-00511 Helsinki (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **THORSTENSSON, Tommy** [SE/SE]; Svartviksslingan 12, S-167 38 Bromma (SE). **REINHOLDSEN, Örjan** [SE/SE]; Adolf Lemons väg 19, S-187 76 Täby (SE). **SELLIN, Lars-Erik** [SE/SE]; Fem Fålars Brunn 3, S-125 35 Älvsjö (SE). **KILANDER, Ulf** [SE/SE]; Kulma Allé 46, S-135 53 Tyresö (SE).

(74) Agent: DR LUDWIG BRANN PATENTBYRÅ AB; Box 1344, S-751 43 Uppsala (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), 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, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (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, IE, IT, LU, MC, NL, PT, SE, 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.

WO 03/034772 A1

(54) Title: METHOD AND ARRANGEMENT IN A COMMUNICATIONS NETWORK

(57) Abstract: The present invention relates to a method and arrangement in a communications system and more specifically to digital signatures sent over bandwidth restricted connections. The objective of the present invention is to provide a way to enable a mobile public network user to use his/her mobile device (104) for performing digital signing of data suitable for being transferred partially over a bandwidth restricted radio link to a receiver (102) such as a payment server or similar. A digital signature is created within a mobile device (104) and transferred the over the radio access network (108) to the gateway (110), a certificate associated to the specific mobile device is retrieved by means of an agent (116) associated to the gateway (110), said retrieved certificate is attached to the digital signature by means of said agent (116); and said digital signature and attached certificate forwarded over the Internet (106) to the receiver (102).

METHOD AND ARRANGEMENT IN A COMMUNICATIONS NETWORK

FIELD OF THE INVENTION

The present invention relates to a method and arrangement in a communications system in accordance with the preambles of the independent claims. More specifically it relates to digital signatures sent over bandwidth restricted connections.

BACKGROUND OF THE INVENTION

To attain security in open networks, several security solutions have appeared. One example is Public key Infrastructure (PKI). PKI is a system to distribute and check keys that can be used to authenticate users, sign information and encrypt information. In a PKI system, two associated keys are used in connection with protecting information. One important feature of PKI systems is that it is computationally unfeasible to use knowledge of one of the keys to deduce the other key, such keys being called asymmetric keys. In a typical PKI system, a set of two such keys are assigned to an owner. One of the keys is maintained private while the other is freely published. When the keys are used for encryption of information, the information is encrypted with the public key and only the owner having the private key can decrypt it. As only the owner possesses the private key, the keys can be used for digital signatures when used in the opposite way. Thus, when the keys are used for signing, the information is encrypted with the private key by the owner and the signature can be verified by the public key.

A PKI distributes one or several public keys. A central element of a Public Key Infrastructure are public key certificates, which are needed to provide assurance of the validity of public keys. A trusted third party issues certificates and is called a certification authority (CA). The CA uses its good name to guarantee the correctness of a public key by signing a certificate including the public key and other information.

According to International Organization for Standardization (ISO) 7498-2, a digital signature is data appended to, or cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient.

A recipient of a digitally signed message (relying party), in this document referred to as the receiver, is someone that wants to prove the source and integrity of the message and verify the sender of that particular message. With a trusted third party in a PKI the recipient may know that the public key provided to him/her is the right one and is corresponding to the senders identity. This is assured by the trusted third party through a Certificate.

Digital signatures made by means of said public key processes, are generated by means of the private key with a mathematical algorithm and the signature can be verified with the associated public key. The private key can be controlled only by the signer that owns the key so that nobody is able to sign in the name of the signer. The public key, on the other hand may be published so that anybody can verify the signature. The private key is usually protected through a Personal Identification Number (PIN) so that for making a signature, knowledge of the PIN and possession of the private key are required.

The digital signatures can be generated in a computer, e.g. in a PC, by means of computer programs consisting of such a mathematical algorithm. The private key is usually stored on a hard disk or a diskette and downloaded into the main memory for generating the signature. Mostly, the private key is stored encoded and protected via a PIN, which the owner has to enter when signing by means of the computer program. This will ensure that only the owner of the private key can use the private key for signing. Since no additional software is required, this process is advantageous in regard to costs.

Digital signatures are widely used in the fixed Internet world, which is a public open network.. One way to use digital signing is to send a signing request from a signature recipient to a computer of a user. The user receives the request and signs it by using his private key, e.g. in a smart card within the computer, containing the necessary private key. The signature is sent back to the signature recipient in a message. Optionally the client may attach the user's certificate to the message sent back to the signature recipient.

The use of digital signatures in the mobile Internet word or other public network is becoming more and more common. The European patent application EP 102784 shows a process for digital signing of a message and describes the use of a mobile radio telephone net for transmitting signed messages. However, this document is silent about attaching certificates to such a message.

A certificate comprises lots of information and requires a great deal of bandwidth when transferred and a lot of memory capacity for storing. As the storage capacity of mobile devices is limited and the bandwidth of the radio communication channel it uses for the transfer to the recipient is restricted there are problems with storing the certificate and transferring the digital signature and added certificate over radio connection to the recipient when using a mobile device to perform the digital signing, adding the correspondent certificate to it and transfer it to the recipient that requested the digital signature.

SUMMARY OF THE INVENTION

The object of the present invention is to provide a way to enable a mobile Internet or other public network user to use his/her mobile device for performing digital signing of data suitable for being transferred over a bandwidth restricted radio link to a receiver such as a signature recipient application, e.g. a payment server or similar.

The problem is solved by a method having the features of claim 1 and a device having the features of claim 8.

The method, comprising the steps of transferring a digital signature over the radio access network to the gateway, retrieving a certificate associated to the specific mobile device by means of an agent associated to the gateway, attaching said certificate to the digital signature by means of said agent; and forwarding said digital signature and attached certificate over the Internet or other public network to the receiver, makes it possible to transfer the digital signature without the certificate over the bandwidth restricted radio link.

Thanks to that the agent, associated to the gateway, has access to a directory wherein certificates are stored and that the agent has means for retrieving a certificate associated to a specific mobile device and attach it to the digital signature when transferring it on to the receiver, associated certificates do not have to be transferred over the bandwidth restricted radio link.

Preferred embodiments are shown in the independent claims.

An advantage of the present invention is that certificates do not have to be stored on a signature client with limited storage capacity, nor transmitted over a communication channel with restricted bandwidth and receivers may still receive digital signatures with certificates attached in the same way as receiving digital signatures from fixed Internet or other public network clients with sufficient storage capacity and bandwidth.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating an exemplary digital signature system according to the present invention.

Figure 2 is a block diagram depicting a mobile device according to the present invention.

Figure 3 is a signalling sequence diagram showing an example of the signing method according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 is a block diagram illustrating an exemplary digital signature system 100 wherein a receiver such as a signature recipient application 102 wishes to ensure that a mobile end-user is who he/she claims to be. The system comprises a mobile device 104 such as e.g. a Mobile Station, adapted to be used by an end-user. In this example the mobile device 104 is accessible to the public network Internet 106 over a mobile access network 108 and via a wireless public network gateway i.e. in this example a wireless Internet gateway 110 constituting an entry into the public network, i.e. in this example the Internet 106.

The digital signature system 100 uses asymmetric cryptography, as being part of a PKI, for performing digital signatures. A pair of keys, consisting of a private key and a public key, is assigned to the user. The key pair is associated to a certificate, e.g. a X.509 certificate, through a certification process, whereby the public key is bound to an identity and thereby also the private key. X.509 is a standard by the International Telecommunications Union (ITU) specifying the contents of a digital certificate. The certificate issuing in a PKI is performed by a CA, Certificate Authority. Hence, the certificate is a trusted source for the RECEIVER to receive the signer identity or other certified information. A mobile user identity may be e.g. a name, birthday number, Mobile Station International ISDN Number (MSISDN) and/or Integrated Circuit Card Identification number (ICCID).

The receiver

The receiver may for example be an internet bank application, a payment server or any application in the need of authentication (ensuring the identity of another party) or non-repudiation (preventing the denial of previous action). The receiver 102 is connectable to the Internet 106 and is able to communicate with the mobile device 102 of the end user. The receiver 102 is typically implemented as a software application, such as e.g. an internet web server application, running on a computer hardware. The receiver 102 has the ability to verify the digital signature.

The mobile device

The mobile device 104, depicted in **Figure 2**, may be a mobile station, a pager, a Personal Digital Assistant (PDA), etc. that the user wishes to use for proving for the receiver that he/she is who he/she claims to be, or ensuring the commitment of an action such as signing a payment transaction. The mobile device 104 comprises a transmitting and a receiving means 212 for radio communication with mobile access network 108. The mobile device 104 comprises a client software 204 such as e.g. a WAP User Agent or wireless Internet browser which may be placed on e.g. the mobile equipment or a smart card of the mobile device 104, which may be a SIM card if the mobile device 104 is a GSM Mobile Station. The client software 204 is adapted for communicating with the mobile Internet gateway 110. The mobile device 104 further comprises a signing means 206 with the ability to perform digital signatures by means of mathematical algorithms on data sent to the mobile device 104. The signing means 206 and the user's private key which e.g. is used for signing of data, is preferably located in a tamper proof device such as a smart card. The mobile device 104 further comprises a displayer 210 wherein messages to be signed may be displayed and input means, e.g. a keyboard, by means of which the user may enter a PIN code for access to the private key for performing the signature.

The wireless public network gateway and the agent

Referring to Figure 1, the wireless internet gateway 110, from now on called the gateway, is the entry to the public network, in this example the Internet 106, for the mobile device 104 or more specific the mobile station based client software 204 as shown in Figure 2.

The mobile client 204 communicates with a server within the gateway 110. According to the present invention a so-called certificate agent 116 is associated to the gateway 110. This agent is adapted to assisting the mobile device 104, in its performance of the digital signature procedure, by handling certificates. The agent 116 is able to access a directory 114, e.g. via the Internet, which directory 114 contains certificates, each of them associated to a mobile user e.g. by means of the identity of the mobile device 104 or the identity of the smart card of the mobile device 104. More than one certificate may be associated to one mobile device. The certificate(s) are put into the directory by the Certificate Authority when issuing the certificate(s). This is however outside the scope of this document.

The directory 114 may be a X.500 directory accessed by means of a X.500 directory protocol (X.500 is a Directory Standard defined by ISO and the ITU) or a Lightweight Directory Access Protocol (LDAP) (defined in RFC 2251).

Upon receipt in the gateway 110 of a signed message on its way from the user to the receiver 102, the signed message is forwarded to the agent 116. The agent 116 then retrieves the specific mobile user certificate in the directory 114 by matching a user identity, such as the Mobile Station International ISDN Number (MSISDN) and/or Integrated Circuit Card Identification number (ICCID), as a search criteria. The agent 116 attaches the certificate(s) to the signed message, returns the message back to the gateway that forwards it to the receiver 102.

The cryptographic message

The digital signature as well as certificates may be contained within a cryptographic message structure such as e.g. PCKS#7, referred to in RFC 2315 as Cryptographic Message Syntax Version 1.5. (RFC is short for Request for Comments, a series of notes about the Internet.)

Signing procedure

Referring to Figure 1, an exemplary scenario could be a mobile user that wishes to e.g. buy a CD at a web site or pay a bill in an Internet bank.. The receiver 102 requests for a signature from the mobile device 104 of the user to ensure that a mobile end-user is who he/she claims to be. The user signs the message e.g. by means of the smart card of the mobile device 104. Instead of transferring the associated certificate from the mobile device 104 to the receiver 102 over a radio carrier with limited bandwidth each time a signing is performed as in prior art, the certificate is in the invention attached to the digital signature created on the mobile device, by the certificate agent 116 associated to the wireless Internet gateway . The completed signature is then forwarded to the receiver 102 which verifies it.

The signing method according to the present invention will now be described more in detail referring to the signalling diagram in **Figure 3.**

The method comprises the following steps:

Step 300 For the receiver 102 to be able to receive a digital signature from the mobile user, the receiver 102 sends a signing request message such as a message in a predefined and agreed protocol including a calling mechanism to the signature capability of the mobile device. The message is sent to the mobile user, i.e. to the mobile client 204 within the user's mobile device 104 as referred to in figure 2, via the gateway 110. The receiver 102 may also add Instructions/parameters for the agent 116 indicating what service to be performed. The possible instructions/parameters are embedded in the signature request message together with the signature request as well as in a subsequent message from the mobile device 104 to the gateway 110 together with the digital signature. The agent 116 will later in step 306 act in accordance with the Instructions/parameters.

Example of input parameters are:

- What type of output format of the cryptographic message is requested, e.g. PKCS#7 or WAP SignedString?
- Should the content be sent back to the receiver 102 with the PKCS#7 message?

Step 301 The gateway 110 receives the message and forwards it to the signing means 206 within the mobile device 104.

Step 302 The mobile device 104 receives the signature request message. The signing means 206 may display the text to be signed in the displayer 210 of the mobile device 104 and prompting the user for his/her PIN. The user enters his/her signing Personal Identification Number (PIN) to the signing means 206 by means of the input means. The signing means 206 obtains the PIN and verifies the PIN. If the correct PIN is entered, the signing means 206 is allowed to access the private key for performing the cryptographic calculation forming the digital signature. The signing means 206 returns the digital signature to the mobile client software 204 which in turn sends the digital signature over the bandwidth restricted mobile access network 108 to the gateway 110, possibly together with parameters provided in the original message from the receiver 102 .The digital signature is transferred in a message.

Step 303 The gateway 110 receives the digital signature message and relays it to the agent 116.

Step 304 After receiving the digital signature message, the agent 116 accesses the directory 114.

Step 305 It retrieves the certificate or certificates of the specific user by means of e.g. an identity of the mobile device 104 or the identity of the smart card such as Mobile Station International ISDN Number (MSISDN) or Integrated Circuit Card Identification number (ICCID), from which the signature carrying message came.

Step 306 If parameters/instructions is included in the message, the agent 116 performs different operations in accordance with these parameters/instructions. One typical instruction would be that the agent 116 attaches the certificates and creates a PKCS#7 message structure containing the certificate and the digital signature. The new message structure, e.g. PKSC#7, is passed back to the gateway 110. If a user has multiple certificates, all certificates may be sent.

Step 307 The gateway 110 forwards the signature and certificate, comprised in a message to the receiver 102.

The method is implemented by means of a computer program product comprising the software code means for performing the steps of the method. The computer program product is run on a computer placed in the gateway domain and implements a certificate handling entity within the digital signature system. The computer program is loaded directly or from a computer usable medium, such as a floppy disc, a CD, the Internet etc.

The present invention is not limited to the above-described preferred embodiments. Various alternatives, modifications and equivalents may be used. Therefore, the above embodiments should not be taken as limiting the scope of the invention, which is defined by the appending claims.

CLAIMS

1. Method for performing a digital signature by means of a mobile device (104), which signature is to be transferred from the mobile device (104) via a mobile access network (108), a wireless public network gateway (110) and a public network (106) to a receiver (102), the method comprising the steps of:
   - *creating* (305) a digital signature within the mobile device (104);
   - *transferring* (306) the digital signature over the mobile access network (108), to the gateway (110);

   the method is **characterised** by comprising the further steps of:
   - *retrieving* (307) a certificate associated to the specific mobile device (104) in an agent (116) associated to the gateway (110);
   - *attaching* (307) said certificate to the digital signature by means of said agent (116);
   - *forwarding* (308) said digital signature and attached certificate over the public network to the receiver (102).

2. The method according to claim 2, wherein it comprises the further step to be taken after the step of transferring (306) the digital signature over the mobile access network (108):
   - the gateway (110) *relaying* the received digital signature to the agent (116) associated to the gateway (110).

3. The method according to any of the claims 1-2, wherein the step of retrieving a certificate comprises the further step of:
   - the agent (116) *accessing* a directory (114) adapted for storing certificates associated to mobile devices.

4. The method according to claim 3, wherein the step of retrieving a certificate comprises the further step of:

- *identifying* the certificate associated to the specific mobile device (104) among the stored certificates within said directory (114) by means of an identity of the mobile device (104) or the identity of the smart card.

5. The method according to any of the claims 1-4, comprising the further step of:
   - the agent (116) *creating* a PKCS#7 message structure containing said certificate and the digital signature before forwarding it to the receiver (102).

6. A computer program product directly loadable into the internal memory of a processing means within a computer placed in a wireless public network gateway domain, comprising the software code means for performing the steps of any of the claims 1-5.

7. A computer program product stored on a computer usable medium, comprising readable program for causing a processing means in a computer placed in the gateway domain, to control an execution of the steps of any of the claims 1-5.

8. A certificate agent (116) for assisting a mobile device (104) to perform a digital signature to be sent to a receiver (102), the agent (116) being associated to a wireless public network gateway (110) via which gateway (110) said digital signature is transferred on its way to the receiver (102), the agent (116) comprising means for receiving the digital signature sent from the mobile device (104) over a mobile access network (108) to the gateway (110), **characterised** in that the agent (116) further comprises:
   - means for accessing a directory (114) adapted for storing certificates associated to mobile devices;
   - means for retrieving a certificate associated to the specific mobile device (104) from said directory (114);

9. The agent (116) according to claim 8, wherein it comprises:

- means for identifying the certificate associated to the specific mobile device (104) among the stored certificates within the directory (114) by means of an identity of the mobile device (104) or the identity of the smart card.

10. The agent (116) according to any of the claims 8-9, wherein it comprises:
    - means for attaching said certificate to the digital signature.

11. The agent (116) according to any of the claims 8-10, wherein it comprises:
    - means for creating a PKCS#7 message structure containing said certificate and the digital signature before forwarding it to the receiver (102).

12. The agent (116) according to any of the claims 8-11, wherein it comprises:
    - means for forwarding said digital signature and attached certificate via the gateway (110) and over the public network (106) to the receiver (102).

1/3

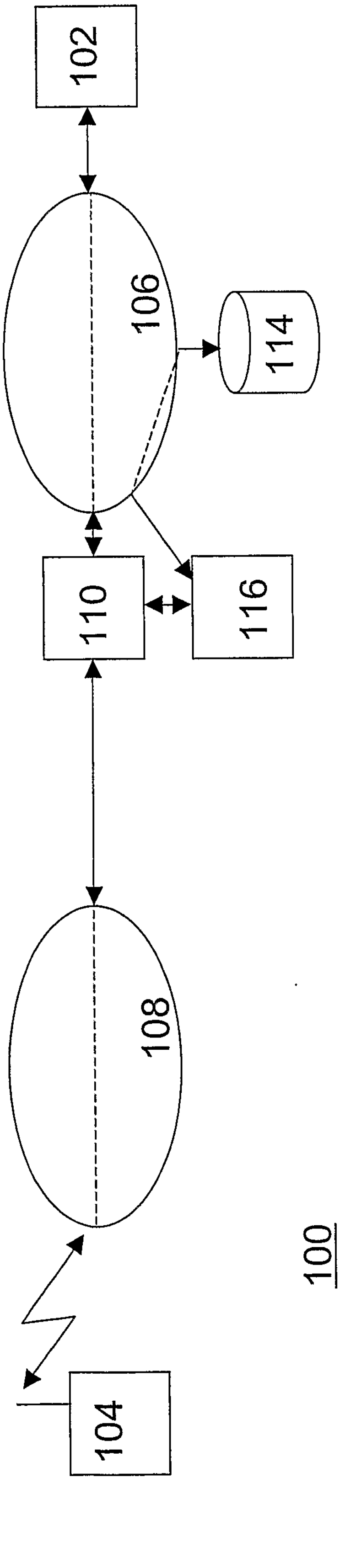


Fig. 1

Fig. 2

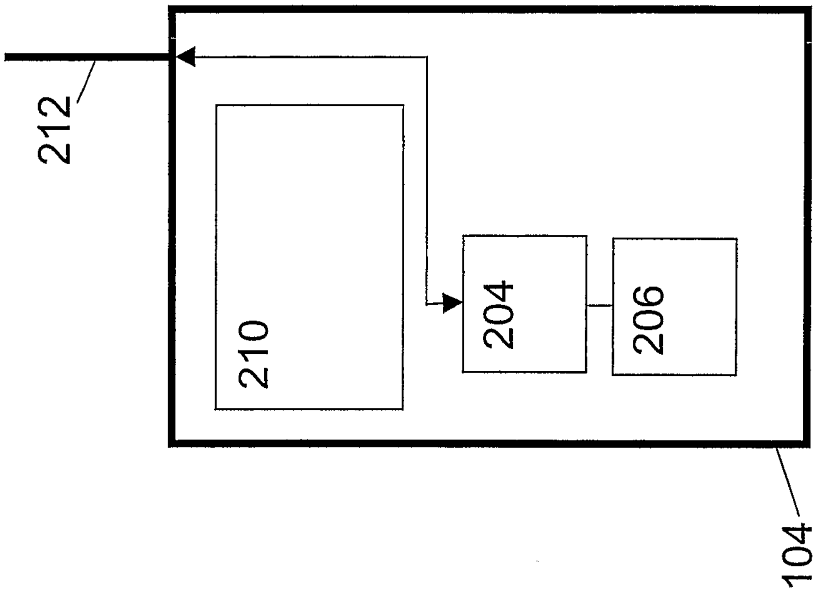
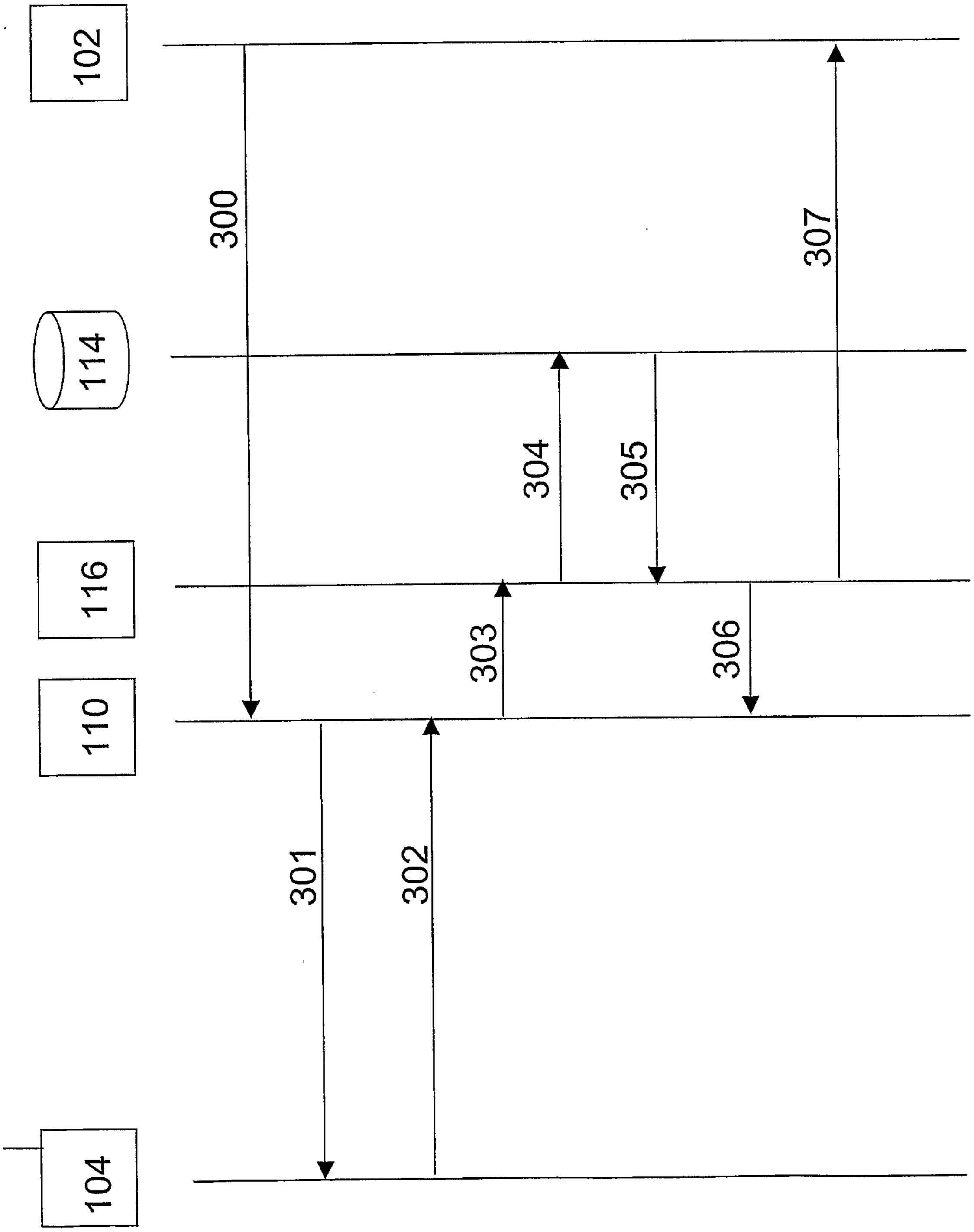


Fig. 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/01765

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, 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: H04Q

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9922486 A1 (BROKAT INFOSYSTEMS AG), 6 May 1999 (06.05.99), page 1 - page 17, abstract --	10,12
Y	EP 0782296 A2 (NCR INTERNATIONAL INC.), 2 July 1997 (02.07.97), page 1 - page 6, abstract --	1-9,11
Y	WO 9712460 A1 (DOCUMENT AUTHENTICATION SYSTEMS INC.), 3 April 1997 (03.04.97), page 4 - page 6, abstract --	1-12

☒ Further documents are listed in the continuation of Box C. ☒ 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 16 January 2003	Date of mailing of the international search report 20 -01- 2003
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 Behroz Moradi /itw Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/01765

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,Y	US 6223291 B1 (L.C.PUHL ET AL), 24 April 2001 (24.04.01), column 2, line 36 - column 7, line 21, figures 1-5, abstract --	1-12
A	US 5970475 A (R.L.BARNES ET AL), 19 October 1999 (19.10.99), column 3, line 5 - column 4, line 26, abstract -- --------	1-9,11

INTERNATIONAL SEARCH REPORT

Information on patent family members

30/12/02

International application No.
PCT/SE 02/01765

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9922486 A1	06/05/99	AT 213575 T	15/03/02
		AU 735091 B	28/06/01
		AU 1557499 A	17/05/99
		CA 2308386 A	06/05/99
		DE 19747603 A,C	20/05/99
		DE 59803145 D	00/00/00
		EP 1027784 A,B	16/08/00
		ES 2173652 T	16/10/02
		JP 2001522057 T	13/11/01
		NO 20002182 A	23/06/00
EP 0782296 A2	02/07/97	JP 9219701 A	19/08/97
		US 5774552 A	30/06/98
WO 9712460 A1	03/04/97	AU 714220 B	23/12/99
		AU 7105896 A	17/04/97
		BR 9610720 A	21/12/99
		CA 2232170 A	03/04/97
		CN 1202288 A	16/12/98
		CZ 9800787 A	14/10/98
		EP 0850523 A	01/07/98
		HU 9802232 A	28/01/99
		IL 123663 A	10/03/02
		JP 11512841 T	02/11/99
		NO 981170 A	13/05/98
		NZ 318941 A	29/07/99
		PL 182163 B	30/11/01
		PL 326075 A	17/08/98
		TR 9800462 T	00/00/00
		US 5748738 A	05/05/98
		US 6237096 B	22/05/01
		US 6367013 B	02/04/02
		US 2001002485 A	31/05/01
US 6223291 B1	24/04/01	AU 3498600 A	16/10/00
		CN 1345494 T	17/04/02
		EP 1166490 A	02/01/02
		WO 0059149 A	05/10/00
US 5970475 A	19/10/99	AU 8901398 A	03/05/99
		EP 0996917 A	03/05/00
		WO 9919819 A	22/04/99