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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2003 (05.06.2003)

PCT

(10) International Publication Number
WO 03/047161 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/NO02/00446

(22) International Filing Date:
26 November 2002 (26.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20015812 28 November 2001 (28.11.2001) NO

(71) Applicant *(for all designated States except US)*: **TELENOR ASA** [NO/NO]; Snarøyveien 30, N-1331 Fornebu (NO).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **SANDBERG, Leif** [SE/SE]; Jäntans väg 14, S-132 35 Saltsjö-Boo (SE).

(74) Agent: **OSLO PATENTKONTOR AS**; Postboks 7007 M, N-0306 Oslo (NO).

(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, SC, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations 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, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, 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)*

— *of inventorship (Rule 4.17(iv)) for US only*

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 FOR REGISTERING AND ENABLING PKI FUNCTIONALITIES

(57) Abstract: The present invention discloses a method of registering and activation of PKI functionalities in SIM (Subscriber Identity Module) cards by preprinting a number of sealed envelopes each containing an activation code hidden when unopened and a reference number or code visibly printed on the envelope. The reference number or code and the associated activation code of each envelope are stored in a table in a security server being integrated in or connected to the PKI. The user is provided one of the sealed envelopes together with an application form. The user is requested to fill in the reference code or number on the application form together with personal data, and this is transferred to the PKI and the security server. When the registration is approved by the PKI, approval information is transmitted to the user, requesting him to enter the activation code in his terminal. Simultaneously, the activation code associated with the reference code or number in the table and a Smart Card identity corresponding to the Smart Card of the user, are provided to an Activation Module in the PKI. Upon entering of the activation code in the terminal, the activation code together with the Smart Card identity is transmitted from the terminal to the Activation Module. Upon receipt of the activation code and the Smart Card identity, the Activation Module determines if the received activation code and Smart Card identity match those previously provided by the security server, and if so, the Activation Module executes the necessary procedure for enabling the PKI part of the Smart Card.

WO 03/047161 A1

METHOD FOR REGISTERING AND ENABLING PKI FUNCTIONALITIES

Field of the invention

The present invention is related to PKI (Public Key Infrastructure), particularly to registering and activation of PKI (Public Key Infrastructure) functionalities in SIM (Subscriber Identity Module) cards.

Background of the invention

To realize the full potential of communication networks, there has to exist a standardized system so that the users can engage in electronic transactions with the same degree of trust as associated with paper-based transactions.

For this reason, PKI has been developed as the primary platform for global commerce and communications. PKI insures that sensitive electronic communications are private and protected from tampering. PKI is used for digital signatures, authentication and encryption.

PKI is based on the use of cryptography, which means scrambling of information by a mathematical formula and a virtual key, so that only an authorized party using a related key can decode it. A PKI uses pairs of cryptographic keys provided by a trusted third party known as a Certification Authority (CA). Central to the workings of a PKI, a CA issues digital certificates that identify the holder's identity. A CA maintains accessible directories of valid certificates, and a list of certificates it has revoked.

Traditionally, PKI functionalities have been used by data terminals with the certificate and keys stored in an external Smart Card. However, as cellular phones merge to data terminals, there will be a need for PKI functions also in the phones. The certificate and keys will then normally be

stored in the subscriber card, e.g. in the SIM (Subscriber Identity Module) card as for GSM phones.

For the PKI system to be trusted, there has to exist a secure routine when registering new users by issuing digital certificates. One has to be 100% sure that the one requesting digital certificates is who he or she claims to be. This is normally done in that the user in person shows up at an office, e.g. at a post office, fills in a form and identifies himself by a trusted identification like a passport. When the counter clerk at the post office has verified the identification information, the data form is transmitted electronically to a CA. The CA controls and whitewashes the data and issues a PKI card, either in the form of a SIM card or a Smart Card, together with an activation code. The PKI card and the activation code are now sent by registered mail to the user. Again, the user personally has to appear in the post office and identify himself by, e.g., his passport, for being allowed to receive the mail.

This two-time appearance at an office has turned out to be a problem for the spreading of PKI, simply because people seem to have a resistance against making use of new technology with high entrance thresholds meaning that great initial efforts have to be made. Also, the process is naturally time consuming, and at least one week will lapse from the certificate is ordered to the user has got access to PKI functions.

From the issuer of digital certificates point of view, the costs of the issuing process are relatively high, especially because of the execution and sending of the registered mail.

Thus, there is a need for simplifying the issuing process for the benefit for both the issuer and the user.

Summary of the invention

It is an object of the present invention to provide a method that eliminates the drawbacks described above. The features defined in the claims enclosed characterize this method.

More specifically, the present invention provides a method of a Public Key Infrastructure (PKI) for registering a user of the PKI and enabling a PKI part of a Smart Card of the user by preprinting a number of sealed envelopes each containing an activation code hidden when unopened and a reference number or code visibly printed on the envelope. The reference number or code and the associated activation code of each envelope are stored in a table in a security server being integrated in or connected to the PKI. The user is provided one of the sealed envelopes together with an application form. The user is requested to fill in the reference code or number on the application form together with personal data, and this is transferred to the PKI and the security server.

When the registration is approved by the PKI, approval information is transmitted to the user, requesting him to enter the activation code in his terminal. Simultaneously, the activation code associated with the reference code or number in the table and a Smart Card identity corresponding to the Smart Card of the user, are provided to an Activation Module in the PKI. Upon entering of the activation code in the terminal, the activation code together with the Smart Card identity is transmitted from the terminal to the Activation Module. Upon receipt of the activation code and the Smart Card identity, the Activation Module determines if the received activation code and Smart Card identity match those previously provided by the security server, and if so, the Activation Module executes the necessary procedure for enabling the PKI part of the Smart Card.

Detailed description of an example embodiment

The present invention will now be described by an example embodiment where a user is about to order a SIM card with PKI functionality to his GSM phone.

As before, the user has to show up in person in authorized offices, like a post office, a bank or at the telephone operator, to which the user is subscribed.

At the authorized office, the user will receive a preprinted sealed envelope together with an application form he is asked to fill in. A reference number printed on a noticeable place thereon identifies the envelope. The form and the sealed envelope that the user receive at the office is uniquely associated with each other in that the mentioned reference number also is printed on the form, or is one of the data the user is asked to fill in.

After filling the form, an officer will check if the given personalia matches those on an identity card the user has to produce and that the reference number corresponds to the one printed on the envelope. If the personalia and the number are OK, the form is forwarded to further execution, and the user will be asked to keep the envelope unsealed until he has received his new SIM card.

The sealed envelope contains an activation code that is invisible when the envelope is unopened. Data concerning all the preprinted envelopes are stored, e.g., in a table within a security server connected to or integrated in the PKI. For each envelope, at least the corresponding reference number, activation code and a status are stored so that once the security server knows the reference number or code of an application form, it also knows the activation code that is given to the user in the envelope together with the application form, and in which stage of execution the application presently is. The status may be one of the

following: unused, under consideration, approved, but not activated, activated, not approved. Initially, the status is set to "unused".

Turning to the user example, the form data is read, preferably electronically, and transferred to the security server. Simultaneously, the status of the envelope stored in the table is changed from "unused" to "under consideration". The form data, which in this example should be considered as an application for a PKI SIM card, is executed by a PKI server under control of a CA in a way according to the state of the art, which should be known to a person skilled in the art. Additionally, the status of the envelope will be changed in the security server according to the result of the execution. If the application is refused, the corresponding status is changed to "not approved". In contrast, if the application is approved, the corresponding status is naturally changed to "approved".

The result of the execution of the application will then be sent to the user in a message via a communication network, preferably carried by SMS or similar, and alternatively by e-mail or mail. A new SIM card may be sent to the user, but it is not necessary to use registered mail because the user will be able to prove his identity by using the activation code hidden in the envelope. Alternatively, if the user already has a SIM card with PKI functionality installed, but till now not accessible, no new SIM card will be necessary to issue. Simultaneously, the security server will provide an Activation Module with the activation code associated with the reference number or code together with necessary identity information regarding the corresponding SIM card.

A message representing a positive result will, e.g., read as follows: "Your application has been approved, please open the sealed envelope and use the activation code inside on your SIM card".

However, before the user may enter the activation code, a "SIM PKI menu" must be enabled. When the "SIM PKI menu" is enabled, the user enters the activation code in his handset to enroll to the service. The activation code is sent by SMS to the PKI together with the SIM card identity. The user may have 3 attempts to enter this code correctly.

The Activation Module fetches the activation code and the SIM card identity and verifies if it matches the activation code and the SIM card identity that already have been provided from the security server. The Activation Module then transmits a "Generate PKI keys enabling command" back to the SIM, and the key generation application in the SIM will generate a key pair comprising one private key and one verification public key.

The verification public key (VPuK) is transmitted by SMS to the Activation Module, and the SMS is preferably encrypted according to GSM 03.48 for protection of sensitive information.

The user is then requested to choose a PIN_SIGNKEY, which is a personal self-chosen signing PIN used for, e.g., transaction signing and authentication.

In the case of successful verification, the Activation Module connects to the CA to issue a valid certificate with the public key associated with the user. This certificate is at the same time sent to a certification directory.

A confirmation of successful certification is sent back to the user and the PKI menu will then be disabled in the SIM. Consequently, the PKI functions in the SIM card are enabled.

The present invention provides a method for registering and activation of PKI (Public Key Infrastructure) functionalities making it unnecessary for a user to show up in person

at an authorized office more than once. Sending of items and data associated with the PKI functionalities after the first identity confirmation will not be necessary, as the user will be in possession of the activation code before his identity is assigned to the activation code, inter alia, in the RA. This guarantees that the right person is in possession of the right activation code already at the time of the first personal appearance.

From a user's point of view, the present invention allows for less effort in providing PKI functionalities. From an issuer's point of view, the present invention will most likely increase the number of PKI users. In addition, the costs per registration will decrease as the execution time will decrease and the need of registered mail will be eliminated.

Patent claims

1. Method of a Public Key Infrastructure (PKI) for registering a user of the PKI and enabling a PKI part of a Smart Card of the user, said Smart Card associated with a terminal, said terminal connected to a communication network providing access to the PKI, for the purpose of registering, the user is requested to fill personal data in an application form and to identify himself by a valid identity card, the data is verified against the identity card and electronically transferred to the PKI for approval of the registering,
characterized in the following steps:

a) preprinting a number of sealed envelopes each containing an activation code hidden when unopened and a reference number or code visibly printed on the envelope, the reference number or code and the associated activation code of each envelope are stored in a table in a security server being integrated in or connected to the PKI,

b) providing one of the sealed envelopes to the user together with the application form on which the reference number or code possibly may be preprinted,

c) requesting the user to fill the reference code or number on the application form if the reference number is not already preprinted thereon,

d) transferring the reference code or number together with said personal data to the PKI and the security server,

e) when the registering is approved by the PKI, transmitting approval information to the user requesting him to enter the activation code in his

terminal and providing the activation code associated with the reference code or number in the table and a Smart Card identity corresponding to the Smart Card of the user to an Activation Module in the PKI,

f) upon entering of the activation code, transmitting the activation code from the terminal to the Activation Module together with the Smart Card identity, and upon receiving the activation code and the Smart Card identity:

g) determining if the received activation code and Smart Card identity match those previously provided by the security server, and if so, enabling the PKI part of the Smart Card.

2. Method as defined in claim 1, c h a r a c t e r i z e d i n that said communication network is a GSM or 3G network, said terminal is a GSM or 3G mobile telephone, and said Smart Card is a SIM card.

3. Method as defined in claim 2, c h a r a c t e r i z e d i n that said Smart Card identity is an MSISDN and ICCID.

4. Method as defined in any of the preceding claims, c h a r a c t e r i z e d i n that said PKI functions are stored in said Smart Card, but hidden for the user until enabling.

5. Method as defined in any of the preceding claims, c h a r a c t e r i z e d i n that the approval information is transmitted via SMS, e-mail or mail.

6. Method as defined in any of the preceding claims, c h a r a c t e r i z e d i n that for each of the

sealed envelopes, a status is stored in the table together with the reference number or code and the activation code.

7. Method as defined in claim 6,
c h a r a c t e r i z e d i n that the status initially is set to "unused" and changed to "under consideration" during step d), "approved but not activated" in the case of approval during step e), "not approved" in the case of non-approval during step e), and "activated" in the case of a match in step g).

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 02/00446

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: 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: 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6061791 A (MOREAU, T.), 9 May 2000 (09.05.00), the whole document ---	1-7
P,A	EP 1162781 A2 (TRW INC.), 12 December 2001 (12.12.01), the whole document ---	1-7
P,A	WO 02060210 A1 (TELENOR ASA), 1 August 2002 (01.08.02), the whole document ---	1-7
P,A	EP 1185027 A2 (HITACHI, LTD.), 6 March 2002 (06.03.02), the whole document --- --------	1-7

☐ 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	Date of mailing of the international search report
27 February 2003	03 -03- 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 Rune Bengtsson /OGU Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

30/12/02

International application No.
PCT/NO 02/00446

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6061791 A	09/05/00	AU 733803 B	24/05/01
		AU 7202698 A	08/12/98
		BR 9809272 A	27/06/00
		EP 1000481 A	17/05/00
		WO 9852316 A	19/11/98
EP 1162781 A2	12/12/01	EP 1162779 A	12/12/01
		EP 1162780 A	12/12/01
		EP 1162782 A	12/12/01
		EP 1162783 A	12/12/01
		EP 1162807 A	12/12/01
		EP 1164745 A	19/12/01
		EP 1175037 A	23/01/02
		EP 1175038 A	23/01/02
		EP 1175039 A	23/01/02
		JP 2002033726 A	31/01/02
		JP 2002049311 A	15/02/02
		JP 2002057660 A	22/02/02
		JP 2002057661 A	22/02/02
		JP 2002064485 A	28/02/02
		JP 2002082913 A	22/03/02
		JP 2002123492 A	26/04/02
		JP 2002124944 A	26/04/02
		JP 2002135244 A	10/05/02
		JP 2002135245 A	10/05/02
		US 2002138724 A	26/09/02
		US 2002141592 A	03/10/02
		US 2002144111 A	03/10/02
		US 2002176582 A	28/11/02
WO 02060210 A1	01/08/02	NO 313480 B	07/10/02
		NO 20010427 A	25/07/02
EP 1185027 A2	06/03/02	JP 2002072876 A	12/03/02
		US 2002046340 A	18/04/02