PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32	A1	(11) International Publication Number: **WO 98/49805**
		(43) International Publication Date: 5 November 1998 (05.11.98)

(21) International Application Number: PCT/EP98/02273

(22) International Filing Date: 16 April 1998 (16.04.98)

(30) Priority Data:
1005912 25 April 1997 (25.04.97) NL

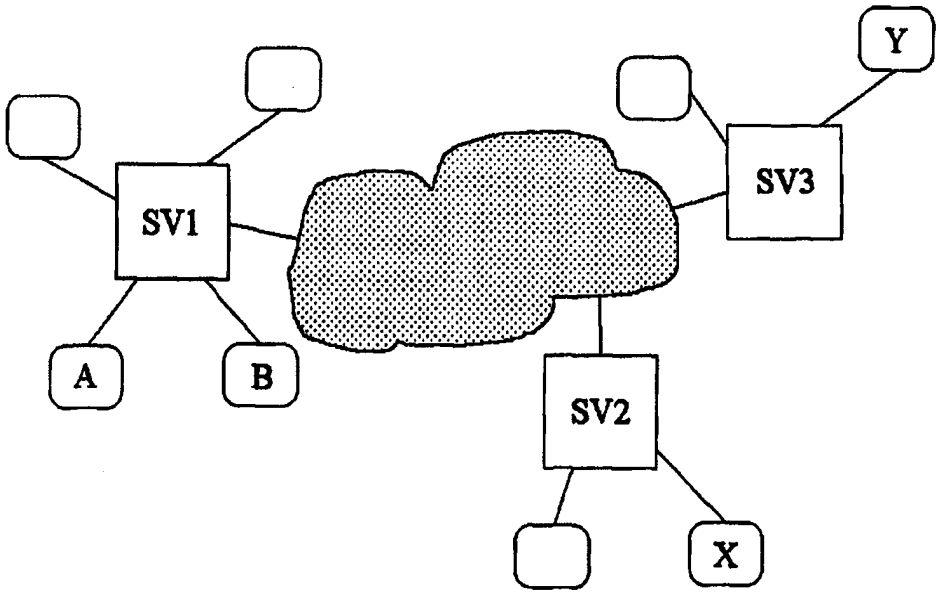
(71) Applicant *(for all designated States except US)*: KONINKLIJKE PTT NEDERLAND N.V. [NL/NL]; Stationsplein 7, NL–9726 AE Groningen (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: QUAK, Jacobus, Theodores, Willem [NL/NL]; Rembrandtkade 22, NL–3583 TW Utrecht (NL). KLEINHUIS, Geert [NL/NL]; Mindertfaen 1, NL–9264 TX Eernewoude (NL). DE BOER, Marten [NL/NL]; De Wiek 19, NL–9285 VD Buitenpost (NL).

(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, GW, 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, ML, MR, NE, SN, TD, TG).

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.

(54) Title: KEY DISTRIBUTION SYSTEM



(57) Abstract

Key distribution system for public key certificates. By a user A, registered at a server SV1, the public key of a user Y, registered at a server SV3, can be calculated from a public key of user Y signed with the secret key of SV3 ({Pky}SKsv3), a number of cross–certificates ({PKsv3}SKsv2, {PKsv2}SKsv1), and the public key (PKsv1) of server SV1. If the user must perform such a calculation himself, that would impose a substantial load on the processing capacity of his terminal. As an improvement, it is suggested, as a service to the users, to let the servers generate key certificates of external users not registered at the same server. The key certificates are thereto recertified into certificates which are digitally signed with the aid of the SK of the own server SV1 ({PKx}SKsv1) and are made available to the local users on request.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Title: Key distribution system.

A. BACKGROUND OF THE INVENTION

The invention relates to a key distribution system. Two cryptographic techniques exist for securing electronic communication: secret key systems and public/private (secret) key (PSK) systems. PSK systems are used in particular when the communication partners do not know each other beforehand.

In PSK systems, each user has a private (secret) key (SK) and a thereto related public key (PK). The PKs of the different users are available at a Trusted Third Party (TTP), incorporated in a TTP server (SV). The SK is known only to the user.

Assume that a user A and a user B are registered at a server SV1. User A has a secret code, SKa, his public key, PKa, being stored in the server SV1. User B also has a secret key, SKb, his public key also being stored in the server SV1. The server makes certificates of the public user keys PKa, PKb, etc. available to users who ask for them. The certificate of a PK comprises the PK, provided with a digital signature, making use of the SK of the server; such key certificates are hereinafter represented as {PKa}SKsv1, {PKb}SKsv1, etc., where SKsv1 represents the secret key of server SV1. In this way, users can avail themselves of PKs which are certified by means of the digital signature of the TTP server where they are registered, whereby their integrity is guaranteed. By means of the public key of the server, PKsv1, which is made available to every user registered at SV1, user A, for example, can extract PKb from the received key certificate {PKb}SKsv1 (PKb = {{PKb}SKsv1}PKsv1) in order to subsequently encrypt with PKb a message which is to be sent to user B.

Users who are registered at the same TTP server can make use of key certificates which are certified by means of the SK of that same TTP server, for example {PKa}SKsv1, {PKb}SKsv1, {PKc}SKsv1, etc. All users can extract reliable keys, PKa, PKb, PKc, from the received certificates, namely by means of the PK of the server where they are registered. It is different if there are more servers and users whoare not registered at the same server. For example, user A is registered at server SV1 and user X at server SV2. In order to send an encrypted message to X which can be deciphered by X with the aid of his SK, SKx, A requires PKx. That is administered by his SV2. A, however, does not have a relationship with SV2. User A requests his own server, SV1, to

send him a certificate of PKx. SV1 routes said request to server SV2, which thereupon sends a certificate of PKx, {PKx}SKsv2, to SV1. Said certificate is thus certified by means of the SK of SV2. SV1 sends the certificate, {PKx}SKsv2, to user A. User A, however, does not have the PK of SV2 at its disposal, and therefore can not extract PKx from {PKx}SKsv2. SV1 therefore also sends to A a cross-certificate of SV1 and SV2: {PKsv2}SKsv1. A then uses that, together with PKsv1, to extract PKx from {PKx}SKsv2: PKx = {{{PKx}SKsv2} {PKsv2}SKsv1 PKsv1.

The more servers which need to be accessed to obtain the PK of an "external" user X not registered at the same TTP server, the greater the computational capacity that will required of A to extract (calculate) PKx before being able to communicate with X. For n servers, the PKx is calculated from:

PKx = {{...{{{PKx}SKsvn}PKsvn}SKsvn-1}PKsvn-1}SKsvn-2}PKsvn-2}...}SKsv1}PKsv1.

It is clear that such a process can require a considerable amount of time.

B. SUMMARY OF THE INVENTION

The invention seeks to bring about an improvement in the above, whereby the speed of communication can be increased considerably, and whereby the computational capacity of the user terminals can be restricted. Further, the application software (and application hardware) of the user can be less sophisticated.

According to the invention, it is provided that in one or more local servers, for example batch-wise, that is, at set times, locally useable certificates are created and stored of public keys of external users not registered at that same local server: re-certification of the PKs of external users. The PKs re-certified in this way are formed by the PKs of said external users, but certified with the SK of the own server SV1: {PKx}SKsv1. Said certificates can then, just as the certificates of the local users, be made available to the local users registered at the SV upon request. From such a certificate, {PKx}SKsv1, the local user can extract the key of an external user X, making use of the public key of his own server, PKsv1. Hereby the user does not need to perform a complex calculation, in the form of PKx = {{...{{{PKx}SKsvn}PKsvn}SKsvn-1}PKsvn-1}SKsvn-2}PKsvn-2}...}SKsv1}PKsv1, but can suffice with the calculation PKx =

{{PKx}SKsv1}PKsv1, the same as the calculation for extracting keys of local users.

C. EXEMPLARY EMBODIMENT

FIG. 1 shows a network with a number of TTP servers SV1, SV2 and SV3. Users A, B, X and Y are connected to the servers. A has a secret key SKa, his public key, PKa, being stored in the server SV1. B has a secret key SKb, his public key also being stored in the server SV1. X has a secret key SKx, his public key PKx being stored in server SV2. Finally, Y has a secret key SKy, his public key, PKy, being stored in server SV3. Certificates of the public user keys PKa and PKb are made available by server SV1, certificates of PKx by server SV2, and certificates of PKy by server SV3. The servers themselves respectively have secret keys SKsv1, SKsv2 and SKsv3, and public keys PKsv1, PKsv2 and PKsv3.

If user A wishes to send a message to user B, user A requires key PKb, so that user B can decipher the received message, which is encrypted with PKb, with the aid of his own private key SKb. A therefore requests the key certificate {PKb}SKsv1 at server SV1. A calculates PKb from the received certificate with the aid of PKsv1: PKb = {{PKb}SKsv1}PKsv1.

According to the prior art, the communication between A and X would take place as follows:

In order to be able to communicate with X, A requires PKx. The certificate thereof, {PKx}SKsv2, is registered in SV2. A requests his own local server SV1 to send him {PKx}SKsv2. SV1 requests said certificate {PKx}SKsv2 from SV2, and sends said certificate on to user A. Since A does not have PKsv2 at its disposal, SV1 also sends a cross-certificate {PKsv2}SKsv1, present in said server, to A. Initially, A already has PKsv1 (i) at its disposal and can now, with the aid of the cross-certificate {PKsv2}SKsv1 (ii) received from SV1, extract PKx from the certificate {PKx}SKsv2 (iii) received via SV1 from SV2: PKx = {{{PKx}SKsv2}(iii) {PKsv2}SKsv1}(ii) PKsv1(i).

The more servers which need to be accessed for obtaining the PK of an external user, the greater the computational capacity which will be required of A. Thus, in communication between user A and user Y, connected to server SV3 (via server SV2), the public key of Y, PKy, must be calculated from: PKy = {{{{PKy}SKsv3}(iv) {PKsv3}SKsv2}(iii)

{PKsv2}SKsv1}(ii) PKsv1(i).

Herein, part (iv) is the certificate of the public key PKy of user Y supplied by server SV3 to server SV2, certified by the secret key of SV3, SKsv3. In this case, two cross-certificates are required in order to enable user A to calculate PKy from {PKy}SKsv3, namely the cross-certificate {PKsv3}SKsv2 (iii) and the cross-certificate (PKsv2}SKsv1 (ii), together with the public key PKsv1 (i) already present at A of its own server SV1. It is clear that such a calculation can require a considerable amount of time. Furthermore, the user software and hardware must be relatively complex.

The invention is based on the insight that re-certifying non-local key certificates by means of cross-certificates can be more expediently performed by the key distribution system, that is to say by the servers, than by the users.

According to the invention, it is provided for that the user does not need to calculate the public key of an external (non-local) user from a series of cross-certificates, but that the key certificates of non-local users also are made available in the same form, namely certified with the same digital signature of the local server, as the key certificates of the local users. It is suggested that making key certificates of non-local users available to local users be offered as service. Such a service allows users to save substantially on the processing possibilities of their local terminals. Further, the administration of the certificates also becomes easier, partly because key changing becomes easier.In the implementation of the suggested service, two options are possible:

1. periodically, locally useable key certificates, re-certified with the SK of the local TTP server, are made batch-wise of the external users or a relevant group thereof;
2. the moment the local user requests it, a locally useable key certificate of the desired external PK, re-certified with the SK of the local server, is generated by the local server.

The advantage of option 1 is that, provided a key certificate has been made of the desired external user, said certificate no longer needs to be generated the moment there is a demand for it. A disadvantage is that many certificates are generated for which there is no or only little demand, while nevertheless storage capacity on the local server is necessary thereto. Further, such files present on

the servers must be kept up to date. The advantage of the second option is that the certificates are always "fresh" and that no storage capacity is required for large numbers of certificates. A disadvantage is that the server will only start calculating a requested certificate the moment there is demand for it.

D. CLAIMS

1. Key distribution system for distributing public keys via servers (SV1, ...), where users (A, ...) are registered; where key certificates ({PKa}SKsv1, ...) are made available by the servers, that is to say, public keys (PKa, ...) which are digitally signed with the aid of the secret key (SKsv1) of the server, characterised in that a local server (SV1) makes available to its own users (A, B) recertified key certificates ({PKx}SKsv1) of users (X, Y) not registered at said local server, that is to say, public keys (PKx) of non-own users (X, Y), being digitally signed with the aid of the secret key (SKsv1) of the local server (SV1).

2. System according to Claim 1, characterised in that the local server (SV1) generates the key certificates ({PKx}SKsv1, {PKy}SKsv1) of users (X, Y), not registered at said server (SV1), at moments which are independent of the moments at which users (A, B, ...) registered at said local server (SV1), request such key certificates.

3. System according to Claim 1, characterised in that the local server (SV1) generates the key certificate ({PKx}SKsv1) of a user (X) not registered at said server (SV1) as soon as an own user (A, B, ...) requests said key certificate.

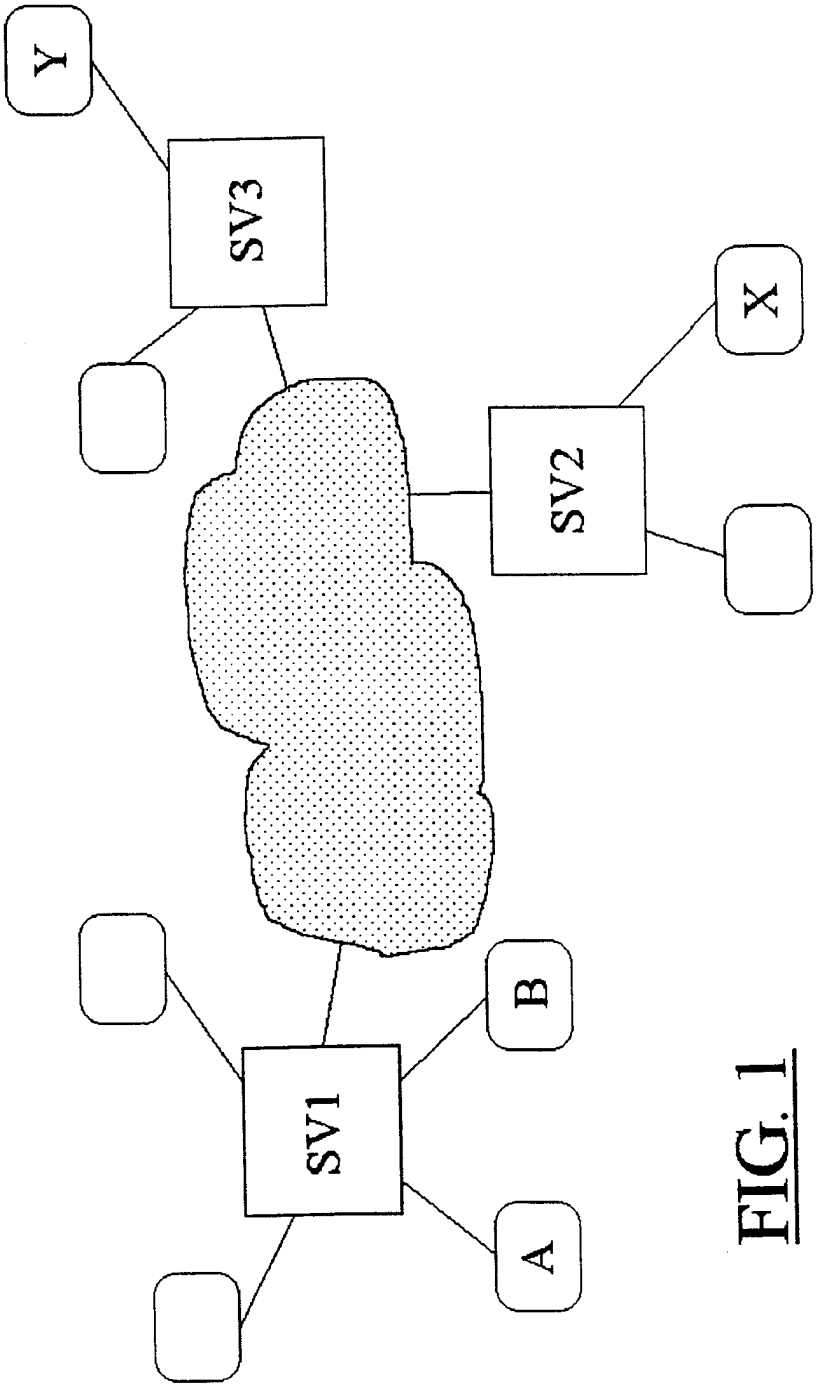


FIG. 1

INTERNATIONAL SEARCH REPORT

Ir ational Application No
PCT/EP 98/02273

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

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)
IPC 6 H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TARDO J J ET AL: "SPX: global authentication using public key certificates" PROCEEDINGS. 1991 IEEE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY (CAT. NO.91CH2986-8), OAKLAND, CA, USA, 20-22 MAY 1991, pages 232-244, XP000220797 ISBN 0-8186-2168-0, 1991, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC. PRESS, USA see page 237, left-hand column, line 28 - right-hand column, line 36 -----	1

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in 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 document 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 publicationdate 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 theinternational search	Date of mailing of the international search report
28 August 1998	04/09/1998
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Holper, G

1