PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

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

(51) International Patent Classification 6 :
H04L 9/32, 9/30

A3

(11) International Publication Number: **WO 99/27678**

(43) International Publication Date: 3 June 1999 (03.06.99)

(21) International Application Number: PCT/FI98/00928

(22) International Filing Date: 26 November 1998 (26.11.98)

(30) Priority Data:
974341 26 November 1997 (26.11.97) FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LEIWO, Jussipekka [FI/FI]; Hanuripolku 6 C 50, FIN–00420 Helsinki (FI).

(74) Agent: PATENT AGENCY COMPATENT LTD.; P.O. Box 156, FIN–00511 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

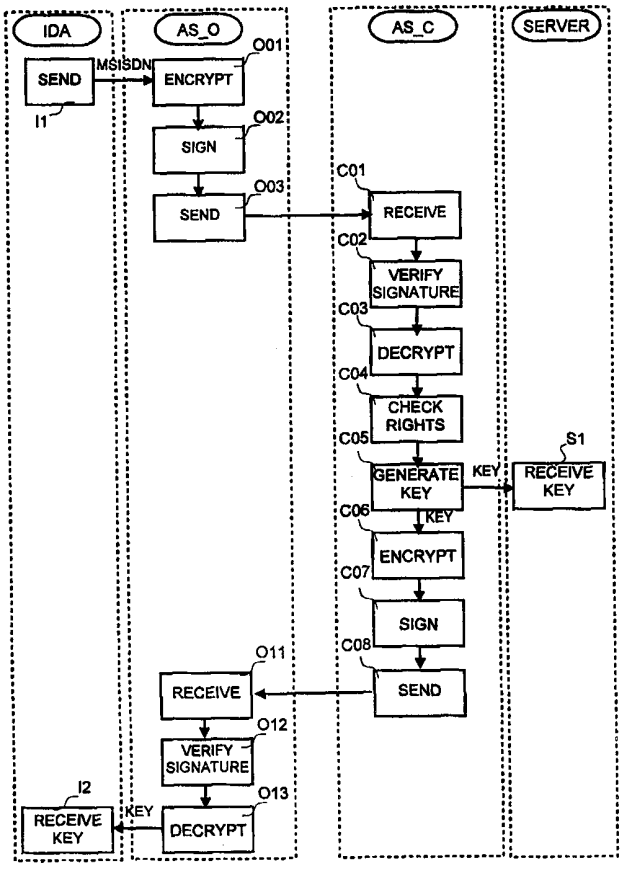
Published
With international search report.

(88) Date of publication of the international search report:
12 August 1999 (12.08.99)

(54) Title: SECURITY OF DATA CONNECTIONS

(57) Abstract

The invention concerns the security of the data connections of a telephone user. The basic idea of the invention is to forward the authentication of a telephone system to the leg between two private data networks connected via an arbitrating network. When establishing the connection, the private network connected to the telephone system forwards the authenticated subscriber identity to the other private network. To provide the identity forwarded with authenticity, the message containing the identity is signed. To provide encryption of the subscriber identity, the message is encrypted using a public key method. In response the second private network generates a session key to be used in the connection. This key is signed and encrypted using a public key method and sent to the first private network. During the connection, a symmetrical encryption method with the session key is used.



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		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00928

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32, H04L 9/30
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)

IPC6: 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2287160 A (FUJITSU LIMITED), 6 Sept 1995 (06.09.95), page 18, line 5 - page 21, line 6	1-27
	--	
A	WO 9605675 A1 (BRITISH TELECOMMUNICATIONS PBULIC LIMITED COMPANY), 22 February 1996 (22.02.96), claims 1,2,8, abstract	1-27
	--	
A	WO 9724831 A1 (MCI COMMUNICATIONS CORPORATION), 10 July 1997 (10.07.97), abstract	1-27
	--	
A	US 5386468 A (RYOTA AKIYAMA ET AL), 31 January 1995 (31.01.95), column 2, line 1 - line 29, abstract	1-27
	--	

[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" erlier 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 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 May 1999	29 -05- 1999
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 Bengt Romedahl/MN Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00928

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9523473 A2 (TELECOM FINLAND OY), 31 August 1995 (31.08.95), abstract --	1-27
A	US 5249230 A (THOMAS J. MIHM, JR.), 28 Sept 1993 (28.09.93), column 2, line 8 - line 47, abstract --	1-27
A	EP 0481121 A1 (SIEMENS AKTIENGESELLSCHAFT), 22 April 1992 (22.04.92), abstract --	1-27
A	GB 2279540 A (KOKUSAI DENSHIN DENWA KABUSHIKI KAISHA), 4 January 1995 (04.01.95), claims 1,2, abstract --	1-27
A	US 5546463 A (ANTHONY A. CAPUTO ET AL), 13 August 1996 (13.08.96), column 2, line 20 - column 3, line 35, abstract --	1-27
A	EP 0739105 A1 (CERTICOM CORP.), 23 October 1996 (23.10.96), column 3, line 5 - line 57, abstract -- --------	1-27

INTERNATIONAL SEARCH REPORT

Information on patent family members

03/05/99

International application No.
PCT/FI 98/00928

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2287160 A	06/09/95	GB 9425670 D	00/00/00
		JP 7245605 A	19/09/95
		US 5642420 A	24/06/97
WO 9605675 A1	22/02/96	AU 701309 B	28/01/99
		AU 3188795 A	07/03/96
		CA 2197676 A	22/02/96
		CN 1167553 A	10/12/97
		EP 0779003 A	18/06/97
		FI 970629 A	18/02/97
		GB 9416595 D	00/00/00
		JP 10504430 T	28/04/98
		NO 970692 A	14/04/97
		NZ 290931 A	25/03/98
WO 9724831 A1	10/07/97	AU 1425197 A	28/07/97
US 5386468 A	31/01/95	JP 6097931 A	08/04/94
WO 9523473 A2	31/08/95	AU 1707895 A	11/09/95
		EP 0749618 A	27/12/96
		FI 940734 A	17/08/95
		NO 963409 A	15/10/96
		US 5850430 A	15/12/98
US 5249230 A	28/09/93	NONE	
EP 0481121 A1	22/04/92	NONE	
GB 2279540 A	04/01/95	GB 9411680 D	00/00/00
		JP 6350598 A	22/12/94
		US 5544245 A	06/08/96
US 5546463 A	13/08/96	US 5778071 A	07/07/98
		US 5878142 A	02/03/99
EP 0739105 A1	23/10/96	AU 5266596 A	07/11/96
		CA 2174261 A	22/10/96
		US 5761305 A	02/06/98
		WO 9633565 A	24/10/96
		WO 9818234 A	30/04/98