


 RSTMP
copy

56 9700728-0

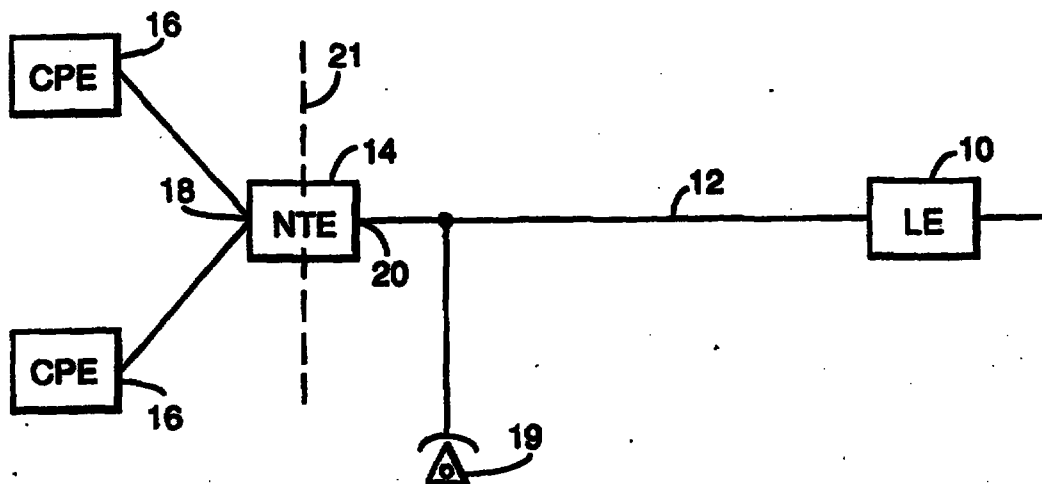
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/32, H04Q 3/00		A1	(11) International Publication Number: WO 96/05675
			(43) International Publication Date: 22 February 1996 (22.02.96)
(21) International Application Number: PCT/GB95/01937		ROBERTS, David, Anthony [GB/GB]; 7 Rowanmayes Close, Ipswich IP2 9SX (GB). STIRLAND, Mark, Jonathan [GB/GB]; Albert Villa, Dockamere, Bramford, Ipswich IP1 1UX (GB). SWALE, Richard, Paul [GB/GB]; 4 Fairbairn Avenue, Kesgrave, Ipswich, Suffolk IP5 7YS (GB). (74) Agent: PRATT, David, Martin; BT Group Legal Services, Intellectual Property Dept., 13th floor, 151 Gower Street, London WC1E 6BA (GB). (81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, 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), ARIPO patent (KE, MW, SD, SZ, UG).	
(22) International Filing Date: 16 August 1995 (16.08.95)			
(30) Priority Data: 9416595.8 17 August 1994 (17.08.94) GB			
(71) Applicant (for all designated States except US): BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).			
(72) Inventors; and (75) Inventors/Applicants (for US only): HARDING, Peter, Maxwell [GB/GB]; 79 The Seafront, Hayling Island, Hants PO10 7HQ (GB). HICKS, Richard, Middleton [GB/GB]; 21 Birchwood Drive, Rushmere & Andrew, Ipswich, Suffolk IP5 7EB (GB). KINGAN, Jonathan, James [GB/GB]; 20 Warwick Road, Ipswich, Suffolk IP4 2QD (GB). MEYERSTEIN, Michael, Victor [GB/GB]; 27 Mayfields, Martlesham Heath, Ipswich, Suffolk IP5 7TU (GB). NOLDE, Keith, Eric [GB/GB]; 10 Whitethorn Road, Warren Heath, Ipswich IP3 8SS (GB). RABSON, John [GB/GB]; Limes Farm House, Eyke, Woodbridge, Suffolk IP12 2QG (GB). RANGER, Jonathan, Crispin [GB/GB]; 189 Humber Douly Lane, Ipswich, Suffolk IP4 3PD (GB).			

Published

With international search report.

(54) Title: USER AUTHENTICATION IN A COMMUNICATIONS NETWORK



(57) Abstract

An authentication system of a terminal on a public switched telephone network comprises a security node associated with a local exchange (10) and a network terminal (14). For one-way authentication, the terminal (14) responds to a call initiation by sending a unique authentication code (R) comprising a number (m) and a secret key (S_i) encrypted according to a first algorithm (F), the secret key being specific to the terminal. The security node constructs the expected authentication code (E) from the number (m), using the first algorithm (F) and a second key which is a function of a terminal identification number (TN), and compares the expected code (E) with the received code (R). In two-way authentication, the security node responds to the call initiation by sending a transaction number (n) to the terminal (14) encrypted according to a second algorithm (f_i). The terminal (14) generates the authentication code (R) as a function of the first algorithm (F), the secret key (S_i) and the transaction number (n). The authentication code (R) is sent back to the security node. An expected code (E) is compared with the received one (R) in the same way. In both cases, a match between expected and received authentication codes (E and R) constitutes authentication of the terminal (14), allowing the user access to the network.

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.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

9700728-0