

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 February 2002 (28.02.2002)

PCT

(10) International Publication Number
WO 02/017555 A3

(51) International Patent Classification⁷: H04L 29/06, 9/32

(74) Agents: RADLO, Edward, J. et al.; Fenwick & West LLP,
Two Palo Alto Square, Palo Alto, CA 94306 (US).

(21) International Application Number: PCT/US01/25927

(22) International Filing Date: 16 August 2001 (16.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/226,429 18 August 2000 (18.08.2000) US
09/921,265 1 August 2001 (01.08.2001) US

(71) Applicant: VERISIGN, INC. [US/US]; 1350 Charleston
Road, Mountain View, CA 94043 (US).

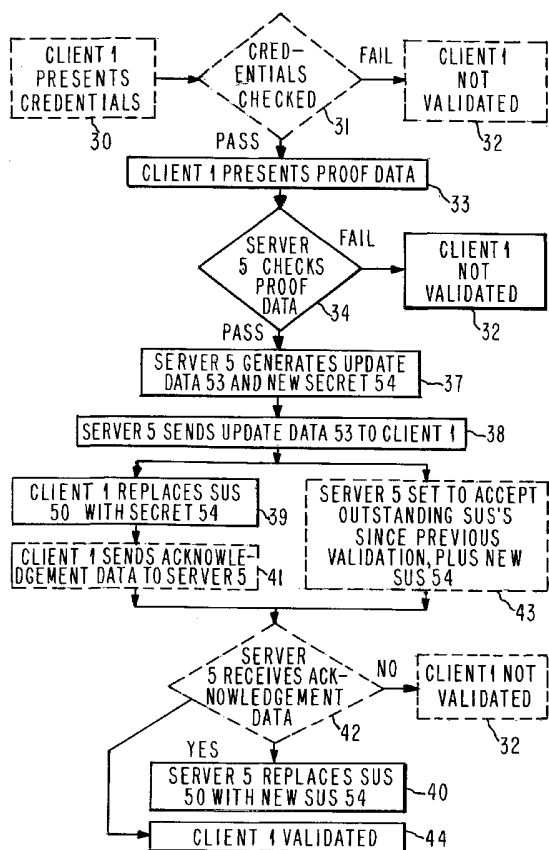
(72) Inventor: FORD, Warwick; 6 Ellery Square, Cambridge,
MA 02138 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, 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, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, 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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: COUNTERING CREDENTIALS COPYING



(57) Abstract: Systems, methods and computer readable media for enabling a server device (5) to validate one or more client devices (1). A shared unpredictable secret (50) is generated. The shared unpredictable secret (50) is stored in the client device (1) and in the server device (5). The client device (1) proves possession of a correct shared unpredictable secret (50) to the server device (5). The shared unpredictable secret (50) is replaced by a new shared unpredictable secret (54) each time the client device (1) is validated by the server device (5).



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.

(88) Date of publication of the international search report:

3 January 2003

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 01/25927

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 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 7 H04L G06F

Documentation searched other than minimum documentation 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)

EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	OORSCHOT VAN ET AL: "HANDBOOK OF APPLIED CRYPTOGRAPHY" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 395-397, XP002134672 ISBN: 0-8493-8523-7	1,2,5,7, 8,16-19
Y	the whole document	3,4,6,9
Y	US 5 815 665 A (BALAZ RUDOLPH ET AL) 29 September 1998 (1998-09-29) abstract column 2, line 31 -column 3, line 4 column 4, line 15 - line 27 --- -/--	3,4

☒ 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 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.

Z document member of the same patent family

Date of the actual completion of the international search

27 August 2002

Date of mailing of the international search report

04/09/2002

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

Bertolissi, E

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/25927

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 661 807 A (GUSKI RICHARD HENRY ET AL) 26 August 1997 (1997-08-26) abstract figure 4	6
A	--- LAMPORT L: "PASSWORD AUTHENTICATION WITH INSECURE COMMUNICATION" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, US, vol. 24, no. 11, 1 November 1981 (1981-11-01), pages 770-772, XP000577349 ISSN: 0001-0782 abstract ---	1-19
Y	--- US 6 029 150 A (KRAVITZ DAVID WILLIAM) 22 February 2000 (2000-02-22) abstract column 7, line 9 - line 63 -----	9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 01/25927

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5815665	A	29-09-1998	NONE	
US 5661807	A	26-08-1997	EP 0636963 A2	01-02-1995
			JP 3053527 B2	19-06-2000
			JP 7107086 A	21-04-1995
			US 5592553 A	07-01-1997
US 6029150	A	22-02-2000	AU 4588197 A	24-04-1998
			EP 0944882 A1	29-09-1999
			WO 9814921 A1	09-04-1998