

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 January 2001 (04.01.2001)

PCT

(10) International Publication Number
WO 01/01627 A3

(51) International Patent Classification⁷: H04L 9/08, 9/32

(21) International Application Number: PCT/US00/18546

(22) International Filing Date: 29 June 2000 (29.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/141,571	29 June 1999 (29.06.1999)	US
60/167,453	23 November 1999 (23.11.1999)	US
60/188,834	10 March 2000 (10.03.2000)	US
09/574,687	17 May 2000 (17.05.2000)	US

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

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

(74) Agents: FARN, Michael, W. et al.; Fenwick & West LLP, Two Palo Alto Square, Palo Alto, CA 94306 (US).

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, 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, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

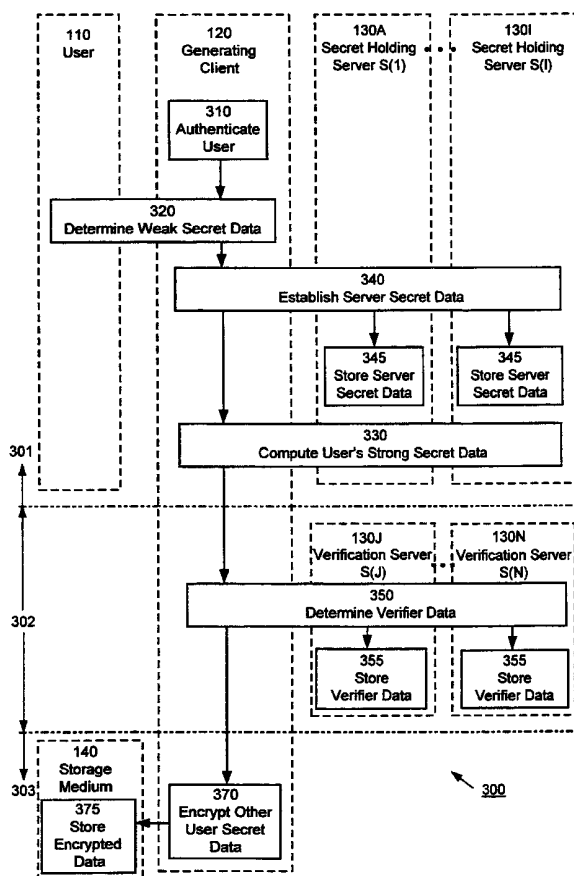
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

[Continued on next page]

(54) Title: SERVER-ASSISTED REGENERATION OF A STRONG SECRET FROM A WEAK SECRET



(57) Abstract: Methods for regenerating a strong secret for a user, based on input of a weak secret, such as a password, are assisted by communications exchanges with a set of independent servers. Each server holds a distinct secret value (i.e., server secret data). The strong secret is a function of the user's weak secret and of the server secret data, and a would-be attacker cannot feasibly compute the strong secret without access to both the user's weak secret and the server secret data. Any attacker has only a limited opportunity to guess the weak secret, even if he has access to all messages transmitted in the generation and regeneration processes plus a subset (but not all) of the server secret data.

WO 01/01627 A3



(88) Date of publication of the international search report:
11 October 2001

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.

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 00/18546

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 H04L9/08 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

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)

WPI Data, PAJ, EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PERLMAN R ET AL: "Secure password-based protocol for downloading a private key" PROCEEDINGS 1999 NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, PROCEEDINGS OF THE INTERNET SOCIETY 1999 NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, SAN DIEGO, CA, USA, 3-5 FEB. 1999, pages 3-11, XP000987305 1999, Reston, VA, USA, Internet Soc, USA ISBN: 1-891562-04-5 cited in the application page 6, left-hand column, line 11 - line 27 --- -/--	1,4,8, 10,21,22



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.

* & * document member of the same patent family

Date of the actual completion of the international search

7 March 2001

Date of mailing of the international search report

19/03/2001

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

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/18546

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LI GONG: "INCREASING AVAILABILITY AND SECURITY OF AN AUTHENTICATION SERVICE" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, US, IEEE INC. NEW YORK, vol. 11, no. 5, 1 June 1993 (1993-06-01), pages 657-662, XP000399661 ISSN: 0733-8716 cited in the application page 658, right-hand column, line 32 - line 41 page 659, left-hand column, paragraph 1 - right-hand column, line 31 -----	1,8,49, 56,97, 104
P,X	FORD W ET AL: "Server-assisted generation of a strong secret from a password" PROCEEDINGS IEEE 9TH INTERNATIONAL WORKSHOPS ON ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES (WET ICE 2000), PROCEEDINGS OF WET ICE 2000. 9TH IEEE INTERNATIONAL WORKSHOPS ON ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATI, pages 176-180, XP002162294 2000, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-7695-0798-0 page 177, left-hand column, line 3 -page 178, paragraph 2 -----	21,69