20000 5252

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 99/57846

(43) International Publication Date: 11 November 1999 (11.11.99)

(21) International Application Number: PCT/IB99/00910

(22) International Filing Date: 6 May 1999 (06.05.99)

(30) Priority Data:

60/084,410	6 May 1998 (06.05.98)	US
09/129,795	6 August 1998 (06.08.98)	US

(71) Applicant: KYBERPASS CORP. [CA/CA]; Suite 110, One Antares Drive, Nepean, Ontario K2E 8C4 (CA).

(72) Inventor: HAVERTY, Rand; 314 Clemow Avenue, Ottawa, Ontario K1S 2B8 (CA).

(81) Designated States: AU, CA, CN, JP, SG, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

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: USER AUTHENTICATION USING A VIRTUAL PRIVATE KEY

(57) Abstract

A method, computer system, and program product provides for authentication of user messages using PKI technology in environments where limited capacity prevents direct PKI technology use, and strong security is provided using magnetic swipe cards or the like, and a passphrase is used for enhanced security and to avoid the need for special purpose devices. The invention is advantageous where there are limitations on the space available for PKI credentials, such as in the userid and password fields of a remote access protocol. PKI techniques are used without transferring lengthy keys or certificates once an initial registration process is complete. A secret key is used. A digest is computed of the secret key, the user's certificate serial number, and a time stamp. The digest, together with the user's certificate serial number and the time stamp, forms a compact message that may be transmitted. Private keys and secret keys are not sent during authentication. Replay attacks are prevented.

