Title (en)

BILATERAL AUTHENTICATION AND ENCRYPTION SYSTEM

Title (de)

VORRICHTUNG ZUR BILATERALEN AUTHENTIFIZIERUNG UND VERSCHLÜSSELUNG

Title (fr)

SYSTEME ET PROCEDE BILATERAUX D'AUTHENTIFICATION ET DE CHIFFRAGE

Publication

EP 0966813 A2 19991229 (EN)

Application

EP 98939048 A 19980309

Priority

- US 9804408 W 19980309
- US 81345797 A 19970310

Abstract (en)

[origin: WO9847258A2] A bilateral system for authenticating remote transceiving stations through use of station identifiers (IDs), and through use of passwords which are used only one time, and thereafter exchanging messages through use of an encrytion key which is changed after each system connection. Upon authentication, each of the stations independently creates a secret session encryption key in response to the other station's unique station identifier that is exchanged over a communication link in cleartext. The station identifiers are used as tags to look up a unique static secret and a unique dynamic secret which are known only by the two stations, but which are not exchanged over the communication link. The secrets are independently combined by a bit-shuffle algorithm, the result of which is applied to a secure hash function to produce a message digest. The secret session encryption key, a one-time password for the originating station, a one-time password for the receiving station, and a pseudo-random change value for updating the dynamic secret are derived from the message digest. The dynamic secret is updated by the pseudo-random change value and a prime constant after each system connection, thus causing the message digest to be updated upon the occurrence of a new system connection. Further, the system IDs also may be altered by a component of the message digest upon the occurrence of a new system connection to provide an additional protection against playback impersonation.

IPC 1-7

H04L 9/32

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/14** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

H04L 9/0822 (2013.01); **H04L 9/0891** (2013.01); **H04L 9/3226** (2013.01); H04L 2209/34 (2013.01)

Citation (search report)

See references of WO 9847258A2

Designated contracting state (EPC)

DE FI FR GB

DOCDB simple family (publication)

WO 9847258 A2 19981022; **WO 9847258 A3 19990121**; CA 2294170 A1 19981022; EP 0966813 A2 19991229; JP 2002508892 A 20020319

DOCDB simple family (application)

US 9804408 W 19980309; CA 2294170 A 19980309; EP 98939048 A 19980309; JP 54388498 A 19980309