Title (en)

VOICE AND DATA ENCRYPTION METHOD USING A CRYPTOGRAPHIC KEY SPLIT COMBINER

Title (de)

VERFAHREN ZUR SPRACH- UND DATENVERSCHLÜSSELUNG UNTER VERWENDUNG EINES KRYPTOGRAPHISCHEN TEILSCHLÜSSEL KOMBINIERERS

Title (fr)

CRYPTAGE VOIX ET DONNEES AU MOYEN D'UN COMBINEUR DE FRACTIONS DE CLES CRYPTOGRAPHIQUES

Publication

EP 1161812 A1 20011212 (EN)

Application

EP 00914874 A 20000310

Priority

- US 0006110 W 20000310
- US 12408699 P 19990311

Abstract (en)

[origin: WO0054455A1] A cryptographic key split combiner, which includes a number of key split generators (42, 48, and 56) for generating cryptographic key splits (32, 34, 36, 38, and 64) and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key (62), and a process for forming cryptographic keys. Each of the key split generators (42, 48 and 56) generates key splits (32, 34, 36, 38, and 64) from seed data (40, 44, 46, 50, 52, 54, 58, and 60). The key split generators may include a random split generator (42) for generating a random key split (32) based on reference data (40) and encryption date/time (44). Other key split generators may include a token split generator (48) for generating a token key split (34) based on label data (46) and organization data (50), a console split generator (56) for generating a console key split (36) based on current maintenance data (52) and previous maintenance data (54), and a biometric split generator for generating a biometric key split (38) based on biometric data (58). All splits may further be based on static data, which may be updated, for example by modifying a prime number divisor of the static data. The label data may be read from a storage medium, and may include user authorization data. The label data may be associated with label categories and sub-categories of addresses, which are meaningful to a user who is specifying or determining the intended recipient(s) of the encrypted information or object. An array associated with a software component object may use key splits (32, 34, 36, 38, and 64) which determine which methods and properties are allowed and control access to the memory address for those allowed methods and properties. The resulting cryptographic key (62) may be, for example, a stream of symbols, at least one symbol block, or a key matrix.

IPC 1-7

H04L 9/08

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/08** (2006.01); **H04L 9/22** (2006.01)

CPC (source: EP)

H04L 9/0866 (2013.01); **H04L 9/0869** (2013.01)

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

DOCDB simple family (publication)

WO 0054455 A1 20000914; AU 3620400 A 20000928; AU 753951 B2 20021031; BR 0008595 A 20020108; CA 2368307 A1 20000914; CA 2368307 C 20070522; EP 1161812 A1 20011212; EP 1161812 A4 20040414; HK 1040023 A1 20020517; JP 2002539489 A 20021119; JP 4615128 B2 20110119; MX PA01009051 A 20040405

DOCDB simple family (application)

US 0006110 W 20000310; AU 3620400 A 20000310; BR 0008595 A 20000310; CA 2368307 A 20000310; EP 00914874 A 20000310; HK 02101235 A 20020220; JP 2000604568 A 20000310; MX PA01009051 A 20000310