

Title (en)

METHOD FOR SECURE DATA LOADING BETWEEN TWO SECURITY MODULES

Title (de)

VERFAHREN ZUM GESICHERTEN LADEN VON DATEN ZWISCHEN SICHERHEITSMODULEN

Title (fr)

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

Publication

EP 1142193 A1 20011010 (FR)

Application

EP 00900603 A 20000118

Priority

- FR 0000099 W 20000118
- FR 9900462 A 19990118

Abstract (en)

[origin: FR2788649A1] The invention concerns a method for customizing a security module comprising a secure loading of an application key from a first security module to a set of second security modules, said first and second security modules comprising each at least a storage unit. The invention is characterised in that said method comprises steps which consist, at each loading, in: calculating in the first and second modules an operating key from a transport key identical for each second module of said set; using the operating key for encrypting the application key in the first module; then sending the application key to the second module, decrypted and verified in said module. The operating key is not recorded in the storage unit of the security modules. The invention is particularly applicable in the field of banking.

IPC 1-7

H04L 9/08

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP)

H04L 9/083 (2013.01)

Citation (search report)

See references of WO 0042731A1

Cited by

EP0242380B1

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)

FR 2788649 A1 20000721; CN 1199387 C 20050427; CN 1339206 A 20020306; EP 1142193 A1 20011010; WO 0042731 A1 20000720

DOCDB simple family (application)

FR 9900462 A 19990118; CN 00803434 A 20000118; EP 00900603 A 20000118; FR 0000099 W 20000118