

Title (en)
METHOD FOR MAKING SECURE THE PRE-INITIALISING PHASE OF A SILICON CHIP INTEGRATED SYSTEM, IN PARTICULAR A SMART CARD AND INTEGRATED SYSTEM THEREFOR

Title (de)
VERFAHREN ZUR SICHERUNG DER VORINITIALISIERUNGSPHASE EINES MIT EINEM ELEKTRONISCHEN CHIP VERSEHENEN SYSTEMS, INSBESONDERE EINER CHIPKARTE, UND EINGEBETTETES SYSTEM ZUR DURCHFÜHRUNG DES VERFAHRENS

Title (fr)
PROCEDE DE SECURISATION DE LA PHASE DE PRE-INITIALISATION D'UN SYSTEME EMBARQUE A PUCE ELECTRONIQUE, NOTAMMENT D'UNE CARTE A PUCE, ET SYSTEME EMBARQUE METTANT EN OEUVRE LE PROCEDE

Publication
EP 1234284 A1 20020828 (FR)

Application
EP 01943588 A 20010608

Priority
• FR 0101774 W 20010608
• FR 0007319 A 20000608

Abstract (en)
[origin: FR2810139A1] The invention relates to a secure method for the pre- initializing phase of smart card (CP) with mutual authentication of the card, recording of a symmetric secret key (Km) and an asymmetric public key (Kpq), and a security access module (3) storing the same secret key and the asymmetric public key (Kpq) corresponding to the public key. The card (CP) and security access module (SAM) (3) supply random numbers (Nac). The SAM authenticates itself by transmitting a cryptogram (SR) to the card derived from two random numbers, using an asymmetric algorithm. The card authenticates itself by calculating a secret session key derived from the random numbers using a symmetric algorithm and the secret key and in transmitting to the SAM a cryptogram (CC) derived from the second random number, using the symmetric algorithm and the session key. The dedicated key (KF) is transmitted to the card encrypted using the session key. An Independent claim is made for an integrated system for implementing the method.

IPC 1-7
G07F 7/10

IPC 8 full level
G06K 17/00 (2006.01); **G06K 19/07** (2006.01); **G06K 19/10** (2006.01); **G07F 7/10** (2006.01); **H04L 9/08** (2006.01); **H04L 9/10** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)
G06Q 20/105 (2013.01 - EP US); **G06Q 20/341** (2013.01 - EP US); **G06Q 20/3558** (2013.01 - EP US); **G06Q 20/40975** (2013.01 - EP US); **G07F 7/0826** (2013.01 - EP US); **G07F 7/1008** (2013.01 - EP US); **H04L 9/0625** (2013.01 - EP US); **H04L 9/0844** (2013.01 - EP US); **H04L 9/0897** (2013.01 - EP US); **H04L 9/3249** (2013.01 - EP US); **H04L 9/3273** (2013.01 - EP US)

Citation (search report)
See references of WO 0195274A1

Designated contracting state (EPC)
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)
FR 2810139 A1 20011214; FR 2810139 B1 20020823; CN 1172477 C 20041020; CN 1386249 A 20021218; EP 1234284 A1 20020828; JP 2003536304 A 20031202; JP 3773488 B2 20060510; TW 513681 B 20021211; US 2002107798 A1 20020808; US 7602920 B2 20091013; WO 0195274 A1 20011213; WO 0195274 A8 20020214

DOCDB simple family (application)
FR 0007319 A 20000608; CN 01801950 A 20010608; EP 01943588 A 20010608; FR 0101774 W 20010608; JP 2002502735 A 20010608; TW 90113952 A 20010608; US 4902502 A 20020208