Title (en)

METHOD FOR ENCODING LONG MESSAGES FOR RSA ELECTRONIC SIGNATURE SCHEMES

Title (de)

VERFAHREN ZUR KODIERUNG LANGER NACHRICHTEN FÜR AUF RSA BASIERENDE DIGITALSIGNATURMETHODEN

Title (fr)

PROCEDE D'ENCODAGE DE MESSAGES LONGS POUR SCHEMAS DE SIGNATURE ELECTRONIQUE A BASE DE RSA

Publication

EP 1325584 A1 20030709 (FR)

Application

EP 01972217 A 20010926

Priority

- FR 0102983 W 20010926
- FR 0012351 A 20000928

Abstract (en)

[origin: WO0228010A1] The RSA encryption algorithm is the most used public key encryption algorithm. The invention concerns a novel message encoding method for signing arbitrarily long messages, without using the hash function. The invention is easily applicable in an electronic component such as a smart card.

IPC 1-7

H04L 9/30

IPC 8 full level

H04L 9/30 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)

H04L 9/302 (2013.01 - EP US); **H04L 9/3249** (2013.01 - EP US)

Citation (search report)

See references of WO 0228010A1

Designated contracting state (EPC)

DE ES FR GB IT

DOCDB simple family (publication)

WO 0228010 A1 20020404; AU 9200301 A 20020408; CN 1393081 A 20030122; EP 1325584 A1 20030709; FR 2814619 A1 20020329; FR 2814619 B1 20021115; US 2003165238 A1 20030904

DOCDB simple family (application)

FR 0102983 W 20010926; AU 9200301 A 20010926; CN 01802931 A 20010926; EP 01972217 A 20010926; FR 0012351 A 20000928; US 13093702 A 20020524