

Title (en)

PUBLIC KEY CRYPTOGRAPHIC METHOD AND SYSTEM, CERTIFICATION SERVER AND MEMORIES ADAPTED FOR SAID SYSTEM

Title (de)

KRYPTOGRAPHISCHE VORRICHTUNG UND VERFAHREN MIT ÖFFENTLICHEM SCHLÜSSEL UND ZERTIFIZIERUNGS-SERVER SOWIE AN DIESE VORRICHTUNG ANGEPASSTE SPEICHER

Title (fr)

SYSTEME ET PROCEDE CRYPTOGRAPHIQUE A CLE PUBLIQUE ET SERVEUR DE CERTIFICATION, MEMOIRES ADAPTEES POUR CE SYSTEME

Publication

**EP 1794926 A1 20070613 (FR)**

Application

**EP 05804306 A 20050928**

Priority

- FR 2005002396 W 20050928
- FR 0410307 A 20040929

Abstract (en)

[origin: WO2006035159A1] The invention relates to a public key cryptographic method and system, a certification server and memories adapted for said system. In said public key cryptographic system, there is insufficient information contained in an electronic public key certificate alone to retrieve the public key. The inventive system comprises at least a second memory (52, 72) in which complementary information is stored, which can be used to retrieve the public key when used together with the information contained in the certificate. According to the invention, access to said complementary information is reserved to a limited number of authorised terminals among the group of terminals that can verify the certificate signature.

IPC 8 full level

**H04L 9/32** (2006.01)

CPC (source: EP US)

**H04L 9/3263** (2013.01 - EP US)

Citation (search report)

See references of WO 2006035159A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

**FR 2875977 A1 20060331**; EP 1794926 A1 20070613; US 2008159543 A1 20080703; WO 2006035159 A1 20060406

DOCDB simple family (application)

**FR 0410307 A 20040929**; EP 05804306 A 20050928; FR 2005002396 W 20050928; US 66399105 A 20050928