Title (en)

ANONYMOUS AUTHENTICATION METHOD BASED ON AN ASYMMETRIC CRYPTOGRAPHIC ALGORITHM

Title (de)

ANONYMES AUTHENTIFIZIERUNGSVERFAHREN BASIEREND AUF EINEM ASYMMETRISCHEN VERSCHLÜSSELUNGSALGORITHMUS

Title (fr)

PROCEDE D'AUTHENTIFICATION ANONYME BASE SUR UN ALGORITHME CRYPTOGRAPHIQUE DE TYPE ASYMETRIQUE

Publication

EP 1774699 A1 20070418 (FR)

Application

EP 05793306 A 20050720

Priority

- FR 2005001868 W 20050720
- FR 0408572 A 20040803

Abstract (en)

[origin: WO2006024732A1] The invention relates to an anonymous authentication method based on an asymmetric cryptographic algorithm. The inventive method is used by an authentication entity (B) to authenticate a client entity (A) using a public-key encryption (ASYM (PB, R))/decryption (ASYM(SB, R')) algorithm which is implemented at the client entity end and the authentication entity end respectively. At the client entity end, the inventive method comprises the following steps: generation of a cryptogram (R'), consisting in encrypting a message (R) containing an identification datum (idA) for the identification of said entity, a secret datum (KA) and an authentication counter value (CA, CB), thereby guaranteeing that the authentication is not performed a second time; and sending of the cryptogram to the authentication entity. At the authentication entity end, the method comprises the following steps: decryption of the cryptogram; using a database (BD) to save a record comprising at least the client entity identification datum, for each client entity to be authenticated; determination of the record corresponding to the decrypted identification datum; and verification of the correspondence between the decrypted secret datum and the secret datum of the client entity obtained from the record.

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP US)

H04L 9/32 (2013.01 - US); **H04L 9/3236** (2013.01 - EP); H04L 2209/42 (2013.01 - EP)

Citation (search report)

See references of WO 2006024732A1

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 2874144 A1 20060210; EP 1774699 A1 20070418; US 2009019282 A1 20090115; WO 2006024732 A1 20060309

DOCDB simple family (application)

FR 0408572 A 20040803; EP 05793306 A 20050720; FR 2005001868 W 20050720; US 65929605 A 20050720