Title (en)

CONTROL SYSTEM AND METHOD USING IDENTITY OBJECTS

Title (de)

STEUERSYSTEM UND -VERFAHREN UNTER VERWENDUNG VON IDENTITÄTSOBJEKTEN

Title (fr)

SYSTÈME DE COMMANDE ET PROCÉDÉ UTILISANT DES OBJETS D'IDENTITÉ

Publication

EP 2038799 A2 20090325 (EN)

Application

EP 07810186 A 20070628

Priority

- US 2007015430 W 20070628
- US 81950706 P 20060707
- US 55703906 A 20061106
- US 55704106 A 20061106

Abstract (en)

[origin: WO2008008243A2] An object known as an identity object comprises a public key and a private key pair and at least one certificate issued by a certificate authority that certifies that the public key of the pair is genuine. In one embodiment, this object may be used as proof of identification by using the private key to sign data provided to it or signals derived from the data. An identity object may be stored in a non-volatile memory as proof of identity, where the memory is controlled by a controller. Preferably, a housing encloses the memory and the controller. In another embodiment, an identity object may be stored in a non-volatile memory of a memory system as proof of identity. The memory system is removably connected to a host device. After the host device has been successfully authenticated, the private key of the object is used to encrypt data from the host device or signals derived from said data, and the at least one certificate and the encrypted data or signals are sent to the host device. In yet another embodiment, after an entity has been authenticated by a control data structure of the memory system, the public key of the identity object and the at least one certificate to certify the public key are provided to the entity. In one practical application of this embodiment, if encrypted data encrypted by means of the public key of the identity object is received from the entity, the memory system will then be able to decrypt the encrypted data using the private key in the identity object. The identity object and the at least one certificate are stored in a non-volatile memory where the memory is controlled by a controller. Preferably, a housing encloses the memory and the controller. In one more embodiment, an identity object may be stored in a non-volatile memory of a memory system. The memory system is removably connected to a host device. After the host device has been successfully authenticated, the public key of the identity object and the at least one certificate to certify the public key are provided to the host device. When encrypted data encrypted by means of the public key of the identity object is received from the host device, the memory system decrypts the encrypted data using the private key in the identity object.

IPC 8 full level

G06F 21/34 (2013.01); **G06F 21/62** (2013.01); **G06F 21/64** (2013.01); **G06F 21/72** (2013.01); **G06F 21/77** (2013.01); **G06F 21/86** (2013.01)

CPC (source: EP KR)

G06F 12/00 (2013.01 - KR); **G06F 15/00** (2013.01 - KR); **G06F 21/00** (2013.01 - KR); **G06F 21/34** (2013.01 - EP); **G06F 21/6218** (2013.01 - EP); **G06F 21/64** (2013.01 - EP); **G06F 21/72** (2013.01 - EP); **G06F 21/77** (2013.01 - EP); **G06F 21/86** (2013.01 - EP); **H04L 9/14** (2013.01 - KR)

Citation (search report)

See references of WO 2008008243A2

Cited by

US9143513B2

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 MT NL PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA HR MK RS

DOCDB simple family (publication)

WO 2008008243 A2 20080117; **WO 2008008243 A3 20080228**; EP 2038799 A2 20090325; JP 2009543210 A 20091203; JP 4972165 B2 20120711; KR 20090034332 A 20090407; TW 200822669 A 20080516

DOCDB simple family (application)

US 2007015430 W 20070628; EP 07810186 A 20070628; JP 2009518355 A 20070628; KR 20097000391 A 20090108; TW 96124586 A 20070706