Title (en)

IDENTITY BASED BROADCAST ENCRYPTION

Title (de)

IDENTITÄTSBASIERTE BROADCAST-VERSCHLÜSSELUNG

Title (fr)

CHIFFREMENT BROADCAST BASE SUR IDENTITE

Publication

EP 2127197 A2 20091202 (FR)

Application

EP 08762146 A 20080225

Priority

- FR 2008050305 W 20080225
- FR 0701451 A 20070228

Abstract (en)

[origin: FR2913154A1] The method involves generating a symmetric encryption key (k) by an encryption key generator (23) and generating a cryptogram (Hdr) associated to the encryption key based on a public key, identity parameters of receiver entity and an integer chosen by a transmitting entity (2). The cryptogram is generated so as to provide access to the encryption key by combination with the public key, the parameters and a private key of receiver entity. A message is encrypted in the entity (2) using the encryption key, and the cryptogram and the encrypted message(C-M) are broadcasted from the entity (2). Independent claims are also included for the following: (1) an encryption device, comprising a memory (2) a decryption device, comprising a memory for containing a public key (3) a computer program for encryption device, comprising instructions for implementing encryption operation of identity based cryptographic method (4) a computer program for decryption device, comprising instructions for implementing decryption operation of identity based cryptographic method (5) a data medium for recording a program for implementing decryption operation of identity based cryptographic method.

IPC 8 full level

H04L 9/30 (2006.01); **H04L 9/08** (2006.01)

CPC (source: EP US)

H04L 9/0833 (2013.01 - EP US); **H04L 9/3073** (2013.01 - EP US); H04L 2209/601 (2013.01 - EP US); Y04S 40/20 (2013.01 - EP)

Citation (search report)

See references of WO 2008113950A2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR

DOCDB simple family (publication)

FR 2913154 A1 20080829; EP 2127197 A2 20091202; US 2010098253 A1 20100422; WO 2008113950 A2 20080925; WO 2008113950 A3 20081127

DOCDB simple family (application)

FR 0701451 A 20070228; EP 08762146 A 20080225; FR 2008050305 W 20080225; US 52911708 A 20080225