

Title (en)

COMMUNICATION METHOD WITH ENCRYPTION KEY ESCROW AND RECOVERY

Title (de)

KOMMUNIKATIONSVERFAHREN MIT SCHLÜSSELHINTERLEGUNG UND SCHLÜSSELRÜCKGEWINNUNG

Title (fr)

PROCEDE DE COMMUNICATION AVEC SEQUESTRE ET RECUPERATION DE CLE DE CHIFFREMENT

Publication

**EP 1254534 A1 20021106 (FR)**

Application

**EP 01904002 A 20010130**

Priority

- FR 0100285 W 20010130
- FR 0001185 A 20000131

Abstract (en)

[origin: FR2804561A1] The invention concerns a method whereby the entity starting a communication session generates a session key (KS) using a pseudo-random generator initialised by the secret key (Sa) of the entity and an initial value (VI). The message is encrypted by the session key. The latter can be retrieved by the escrow authority (Ta), which archives the secret key (Sa) and can recover the initial value (VI). The invention is applicable to secure communications.

IPC 1-7

**H04L 9/08**

IPC 8 full level

**H04L 9/08** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)

**H04L 9/0841** (2013.01 - EP US); **H04L 9/0894** (2013.01 - EP US); **H04L 9/14** (2013.01 - EP US)

Citation (search report)

See references of WO 0156222A1

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

**FR 2804561 A1 20010803**; **FR 2804561 B1 20020301**; EP 1254534 A1 20021106; JP 2003521197 A 20030708; US 2003012387 A1 20030116; WO 0156222 A1 20010802

DOCDB simple family (application)

**FR 0001185 A 20000131**; EP 01904002 A 20010130; FR 0100285 W 20010130; JP 2001555258 A 20010130; US 18159802 A 20020718