Title (en)

MULTIPLE-LEVEL ELECTRONIC SIGNATURE METHOD

Title (de)

VERFAHREN ZUR ERZEUGUNG MEHRSTUFIGER DIGITALSIGNATUREN

Title (fr)

PROCEDE DE SIGNATURE ELECTRONIQUE A NIVEAUX MULTIPLES

Publication

EP 1344344 A1 20030917 (FR)

Application

EP 01999076 A 20011122

Priority

- FR 0103679 W 20011122
- FR 0015529 A 20001130

Abstract (en)

[origin: WO0245338A1] The invention concerns an electronic public key signature method comprising a secret key s compatible with a verifying public key v. It consists in: generating a new secret key s' consisting of s and partial secret key, sl, , sj, , sn, in generating a new verifying public key v' consisting of v and reserve public keys, vl, , vj, vn, the secret keys (s, sl, , sj) being compatible with the keys (v, vl, , vj) and the secret key s' being compatible with any one key (v, vl, , vj) j ranging between 1 and n, signing the message m with the secret key s'. The invention aims at generating an electronic signature resistant to coercive attempts forcing disclosure of secret keys. This is achieved by varying the signature verification criteria.

IPC 1-7

H04L 9/32

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP)

H04L 9/3247 (2013.01)

Citation (search report)

See references of WO 0245338A1

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)

WO 0245338 A1 20020606; AU 2201302 A 20020611; EP 1344344 A1 20030917; FR 2817422 A1 20020531; FR 2817422 B1 20030214

DOCDB simple family (application)

FR 0103679 W 20011122; AU 2201302 A 20011122; EP 01999076 A 20011122; FR 0015529 A 20001130