Title (en)

A KEY-AGREEMENT SYSTEM AND METHOD

Title (de)

VORRICHTUNG UND VERFAHREN ZUR SCHLÜSSELÜBEREINKUNFT

Title (fr)

SYST ME ET PROC D D'AGR MENT DE CL S

Publication

EP 1095483 A1 20010502 (EN)

Application

EP 99928197 A 19990705

Priority

- IL 9900361 W 19990705
- IL 12522298 A 19980706

Abstract (en)

[origin: WO0005836A1] A method for carrying out a key distribution process, whereby each member (Useri) who uses the services of a Certifying Authority (CA) is provided with a member's public key (PUi) and a member's private key (si), wherein said process is effected over a finite group of points comprising the steps of: (1) permitting said Certifying Authority to select a generating group-point (G); (2) to generate a random Certifying Authority private key (d); (3) to generate a Certifying Authority public key (PS) (PS=d*G); (4) permitting said member (Useri) to generate a first member's random value (xi) and calculate a first intermediate member's public key (xi*G); (6) permitting said Certifying Authority to calculate said member's public key (PUi) and member's intermediate private key (pi), wherein: a second member's random value (yi) is generated and a second intermediate member's public key (yi*G) is calculated, said member's public key (PUi) is calculated: PUi = xi*G + yi*G, a member's temporary value (H(IDi, PUi)) is calculated by operating with a hash transformation (H), said member's intermediate private key (pi) is calculated (pi=H(IDi, PUi)*d +yi); (7) permitting said member to generate said member's private key (si) (si=pi+xi).

IPC 1-7

H04L 9/08; H04L 9/30

IPC 8 full level

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

CPC (source: EP)

H04L 9/083 (2013.01); **H04L 9/0844** (2013.01); **H04L 9/3013** (2013.01)

Citation (search report)

See references of WO 0005836A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 0005836 A1 20000203; AU 4530799 A 20000214; CA 2336372 A1 20000203; EP 1095483 A1 20010502; IL 125222 A0 19990312

DOCDB simple family (application)

IL 9900361 W 19990705; AU 4530799 A 19990705; CA 2336372 A 19990705; EP 99928197 A 19990705; IL 12522298 A 19980706