Title (en)

AUTO-RECOVERABLE AUTO-CERTIFIABLE CRYPTOSYSTEMS

Title (de)

VERSCHLÜSSELUNGSSYSTEME MIT SELBSTRÜCKGEWINNUNG UND SELBSTZERTIFIZIERUNG

Title (fr)

SYSTEME CRYPTOGRAPHIQUE AUTORECUPERABLE ET AUTOCERTIFIABLE

Publication

EP 0997017 A2 20000503 (EN)

Application

EP 98937934 A 19980521

Priority

- US 9810392 W 19980521
- US 86483997 A 19970528
- US 87818997 A 19970618
- US 92050497 A 19970829
- US 93263997 A 19970917
- US 95935197 A 19971028

Abstract (en)

[origin: WO9854864A2] A method is provided for an escrow cryptosystem that is overhead-free, does not require a cryptographic tamper-proof hardware implementation (i.e., can be done in software), is publicly verifiable, and cannot be used subliminally to enable a shadow public key system. A shadow public key system is an unescrowed public key system that is publicly displayed in a covert fashion. The keys generated by the method are auto-recoverable and auto-certifiable (abbrev. ARC). The ARC Cryptosystem is based on a key generation mechanism that outputs a public/private key pair, and a certificate of proof that the key was generated according to the algorithm. Each generated public/private key pair can be verified efficient ly to be escrowed properly by anyone. The verification procedure does not use the private key. Hence, the general public has an efficient way of making sure that any given individual's private key is escrowed properly, and the trusted authorities will be able to access the private key if needed. Since the verification can be performed by anyone, there is no need for a special trusted entity, known in the art as a "trusted third party". The cryptosystem is overhead free since there is no additional protocol interact ion between the user who generates his or her own key, and the certification authority or the escrow authorities, in comparison to what is required to submit the public key itself in regular certified public key systems. Furthermore, the system is designed so that its internals can be made publicly scrutinizable (e.g., it can be distributed in source code form). This differs from any schemes which require that the escrowing device be tamper-proof hardware.

IPC 1-7

H04L 9/30

IPC 8 full level

H04L 9/08 (2006.01); **G09C 1/00** (2006.01)

CPC (source: EP KR)

H04L 9/0894 (2013.01 - EP); **H04L 9/30** (2013.01 - KR); **H04L 9/3013** (2013.01 - EP); **H04L 9/3263** (2013.01 - EP)

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 9854864 A2 19981203; **WO 9854864 A3 19990514**; AU 737037 B2 20010809; AU 8656498 A 19981230; BR 9809664 A 20000905; CA 2290952 A1 19981203; CN 1241353 C 20060208; CN 1262007 A 20000802; CZ 9904106 A3 20010815; EP 0997017 A2 20000503; IL 132961 A0 20010319; JP 2002500842 A 20020108; KR 20010013155 A 20010226; NO 995811 D0 19991126; NO 995811 L 20000127; NZ 501273 A 20010928; PL 338018 A1 20000925

DOCDB simple family (application)

US 9810392 W 19980521; AU 8656498 A 19980521; BR 9809664 A 19980521; CA 2290952 A 19980521; CN 98806690 A 19980521; CZ 410699 A 19980521; EP 98937934 A 19980521; IL 13296198 A 19980521; JP 50076699 A 19980521; KR 19997011138 A 19980521; NO 995811 A 19991126; NZ 50127398 A 19980521; PL 33801898 A 19980521