RTMPLS copy

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32	A2	(11) International Publication Number: WO 96/12362
		(43) International Publication Date: 25 April 1996 (25.04.96)

(21) International Application Number: PCT/NL95/00350

(22) International Filing Date: 12 October 1995 (12.10.95)

(30) Priority Data:
08/321,855 14 October 1994 (14.10.94) US

(71)(72) Applicant and Inventor: BRANDS, Stefanus, Alfonsus [NL/NL]; Ina Boudier-Bakkerlaan 143 III, NL-3582 XW Utrecht (NL).

(81) Designated States: AM, AU, BB, BG, BR, BY, CA, CN, CZ, EE, FI, GE, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MN, MX, NO, NZ, PL, RO, RU, SG, SI, SK, TJ, TM, TT, UA, UG, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
Without international search report and to be republished upon receipt of that report.

SG 9701604-2

(54) Title: SECRET-KEY CERTIFICATES

(57) Abstract

Cryptographic methods and apparatus are disclosed that enable formation and issuance of secret-key certificates. In contrast the well-known cryptographic technique of public-key certificates, where a public-key certificate is a digital signature of a certification authority on a public key, pairs consisting of a public key and a corresponding secret-key certificate can be generated by anyone. However, triples consisting of a secret key, a matching public key and a secret-key certificate corresponding to the public key, can only be generated when the certification authority is involved. Also described are applications of secret-key certificates to public-key directories and to restrictive blind issuing protocols.

