(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 December 2005 (01.12.2005)

PCT

(10) International Publication Number
WO 2005/114903 A1

(51) International Patent Classification[7]: H04L 9/30

(21) International Application Number:
PCT/SG2005/000154

(22) International Filing Date: 20 May 2005 (20.05.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/573,524 21 May 2004 (21.05.2004) US

(71) Applicant *(for all designated States except US)*: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 20 Biopolis Way, #07-01 Centros, Singapore 138668 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LAKSHMI-NARAYANAN, Anantharaman** [IN/SG]; c/o Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

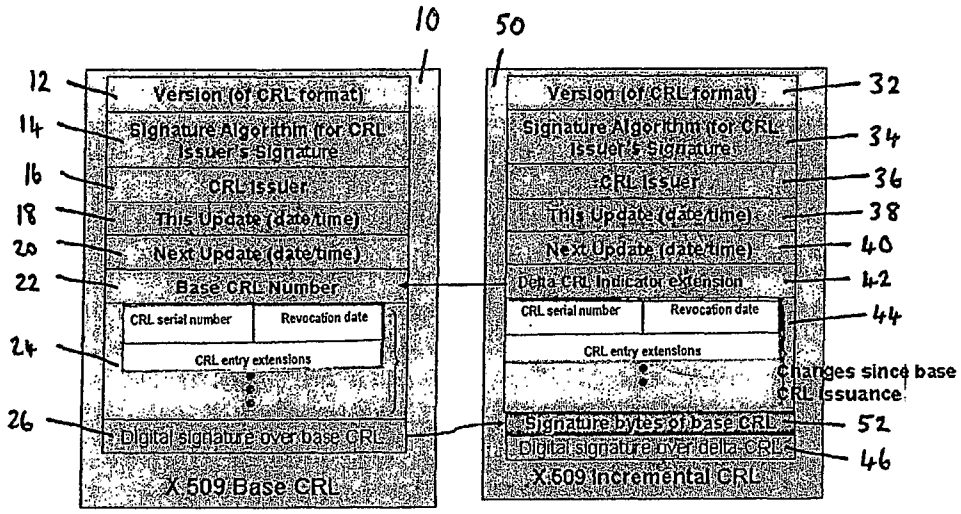
(74) Agent: **ELLA CHEONG SPRUSON & FERGUSON (SINGAPORE) PTE LTD**; P.O. Box 1531, Robinson Road Post Office, Singapore 903031 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: COMMUNICATIONS NETWORK SECURITY CERTIFICATE REVOCATION



(57) Abstract: The distribution of security certificate revocation information on a communications network is disclosed. An issuer node (82) of said network periodically generates data representative of base certificate revocation lists (CRLs) (10). The issuer node (82) periodically generates data representative of incremental CRLs (50), the incremental CRL data (50) including attributes for a current list of revoked certificates and a digital signature of the most-recent base CRL (10). A relying node (86) requests current incremental CRL data (50) from the issuer node (82). The relying node (86) reconstructs said most-recent base CRL by iteratively updating the list of revoked certificates present in the previous base CRL data held with the list of revoked certificates held by any intervening incremental CRL data (50). Additional forms of milestone CRL data (60) and augmented CRL data (70) are also disclosed.

WO 2005/114903 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.