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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 March 2005 (03.03.2005)

PCT

(10) International Publication Number
WO 2005/020542 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number:
PCT/US2004/025216

(22) International Filing Date: 4 August 2004 (04.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/639,903 12 August 2003 (12.08.2003) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **AISSI, Selim** [US/US]; 6870 SW 168th Place, Beaverton, OR 97007 (US). **WHEELER, David** [US/US]; 516 East Jasper Drive, Gilbert, AZ 85296 (US). **SRINIVASAN, Krishnamurthy** [US/US]; 6152 West Oakland Street, #274, Chandler, AZ 85226 (US).

(74) Agents: **VINCENT, Lester, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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, IT, 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).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

(54) Title: METHOD FOR USING TRUSTED, HARDWARE-BASED IDENTITY CREDENTIALS IN RUNTIME PACKAGE SIGNATURE TO SECURE MOBILE COMMUNICATIONS AND HIGH-VALUE TRANSACTION EXECUTION

(57) Abstract: A method for trusted package digital signature based on secure, platform bound identity credentials. The selection of a document to be electronically signed by a user via a computing device is made. A hash for the document is determined. The hash is encrypted with a private key of the user to create a digital signature. The document, an identification credential, and the digital signature are sent to a recipient computing device residing on a network. The identification credential comprises a digital file used to cryptographically bind a public key to specific trusted hardware attributes attesting to the identity and integrity of the trusted computing device. The trusted computing device includes a cryptographic processor.

WO 2005/020542 A1