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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 March 2004 (04.03.2004)

PCT

(10) International Publication Number
WO 2004/019254 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/US2003/026414

(22) International Filing Date: 19 August 2003 (19.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/225,504 20 August 2002 (20.08.2002) US

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

(72) Inventors: **AISSI, Selim**; 6870 SW 168th Place, Beaverton, OR 97007 (US). **SMITH, Ned**; 375 SW Delta Drive, Beaverton, OR 97006 (US). **WISEMAN, Willard**; 57109 Timber Road, Vernonia, OR 97064 (US).

(74) Agents: **REED, Julie** et al.; Marger, Johnson & McCollom, 1030 SW Morrison Street, Portland, OR 97205 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, 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, UZ, VC, VN, YU, ZA, ZM, ZW.

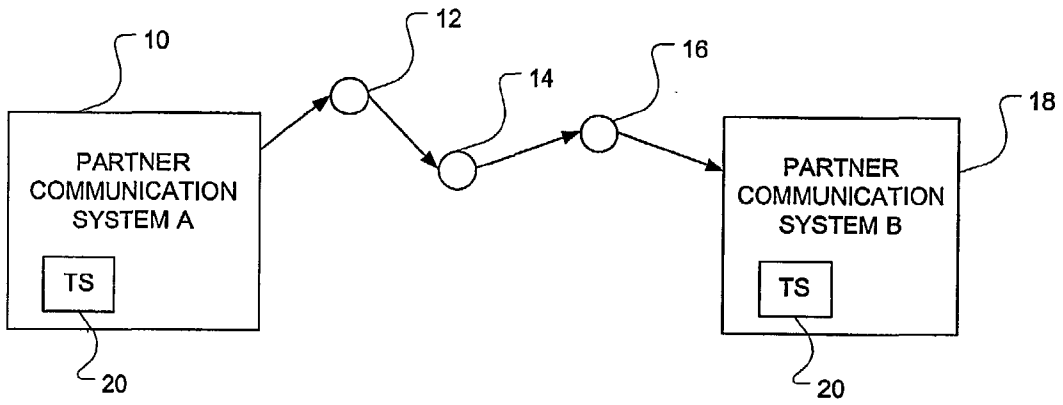
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, 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*

(88) Date of publication of the international search report:
20 October 2005

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: HARDWARE-BASED CREDENTIAL MANAGEMENT



(57) Abstract: A credential management device has a protected domain and a credential manager to perform credential transactions. A credential transaction may comprise determining if a platform is operating in a trusted mode and releasing an operation credential if the platform is operating in a trusted mode. A credential transaction may comprise validating incoming credentials from other platforms.

WO 2004/019254 A3