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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 February 2002 (21.02.2002)

PCT

(10) International Publication Number
WO 02/15530 A2

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

(21) International Application Number: PCT/US01/25730

(22) International Filing Date: 15 August 2001 (15.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/225,796	15 August 2000 (15.08.2000)	US
60/239,019	4 October 2000 (04.10.2000)	US
09/930,029	14 August 2001 (14.08.2001)	US

(71) Applicant: **VIAQUO CORPORATION** [US/US]; 2460 N. First Street, Suite 280, San Jose, CA 95131 (US).

(72) Inventors: **SWEET, William, B.**; 3415 Oakwood Court, Morgan Hill, CA 95037 (US). **YU, John, J.**; 642 Troon Court, Milpitas, CA 95035 (US).

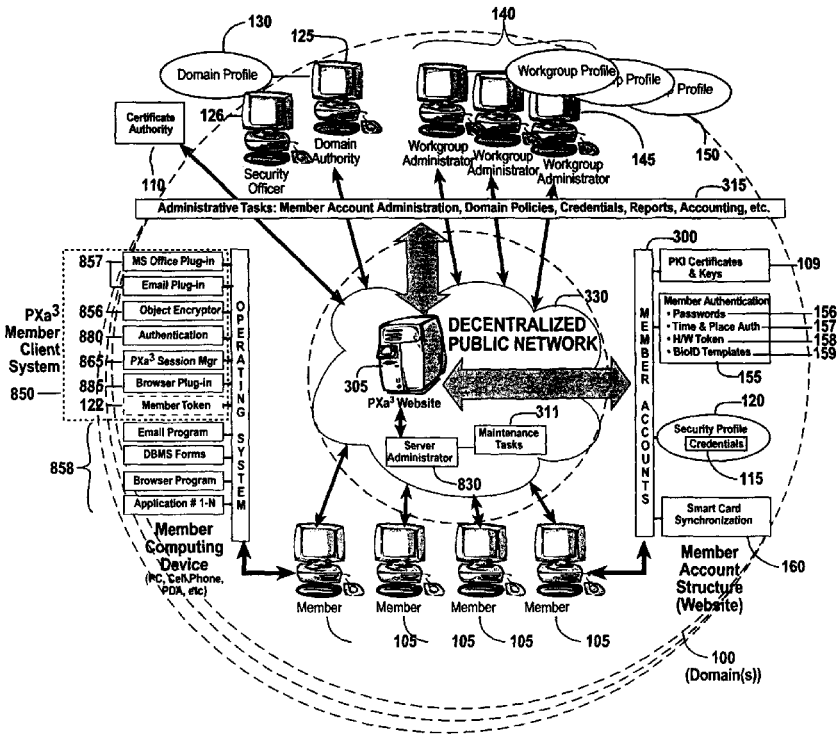
(74) Agents: **LAURIE, Ronald, S.** et al.; Skadden, Arps, Slate, Meagher & Flom LLP, 525 University Avenue, Palo Alto, CA 94301 (US).

(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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



(57) Abstract: The invention combines cryptographic key management technology with various authentication options and the use of a companion PKI system in a web-centric cryptographic key management security method and apparatus called (*PXa3™* Precise eXtensible Authentication, Authorization and Administration). The (*PXa3*) model uses a security profile unique to a network user and the member domain(s) he/she belongs to. A PXa3 server holds all private keys and certificates, the user's security profile, including credentials and the optional authentication enrollment data. The server maintains a security profile for each user, and administrators simply transmitted credential updates and other periodic maintenance updates to users via their PXa3 server-based member accounts. Domain and workgroup administrators also perform administrative chores via a connection to the (*PXa3*) web site, rather than on a local workstation. A member's security profile, containing algorithm access permissions, credentials, domain and maintenance values, a file header encrypting key, optional biometric templates, and domain-specific policies is contained in one of two places: either on a removable cryptographic token (e.g., a smart card), or on a central server-based profile maintained for each member and available as a downloadable "soft token" over any Internet connection.

WO 02/15530 A2

Published:
— *without international search report and to be republished upon receipt of that 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.