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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 September 2004 (16.09.2004)

PCT

(10) International Publication Number
WO 2004/079986 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number:
PCT/IB2004/000626

(22) International Filing Date: 3 March 2004 (03.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03405143.3 4 March 2003 (04.03.2003) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BUHLER, Peter** [DE/CH]; Muehlestrasse 39, CH-8803 Rueschlikon (CH). **OSBORNE, Michael** [GB/CH]; Apfelmatte 13, CH-8804 Au (CH). **MAEDER, Roman** [CH/CH]; Ruetihofstrasse 61, CH-8049 Zurich (CH). **KURSAWE, Klaus** [DE/BE]; Departement Elektrotechniek - ESAT, Kastelpark Arenberg 10, B-3001 Leuven-Heverlee (BE).

(74) Agents: **KLETT, Peter, M.** et al.; IBM Research GmbH, Zurich Research Laboratory, Intellectual Property Law, Saeumerstrasse 4 / Postfach, CH-8803 Rueschlikon (CH).

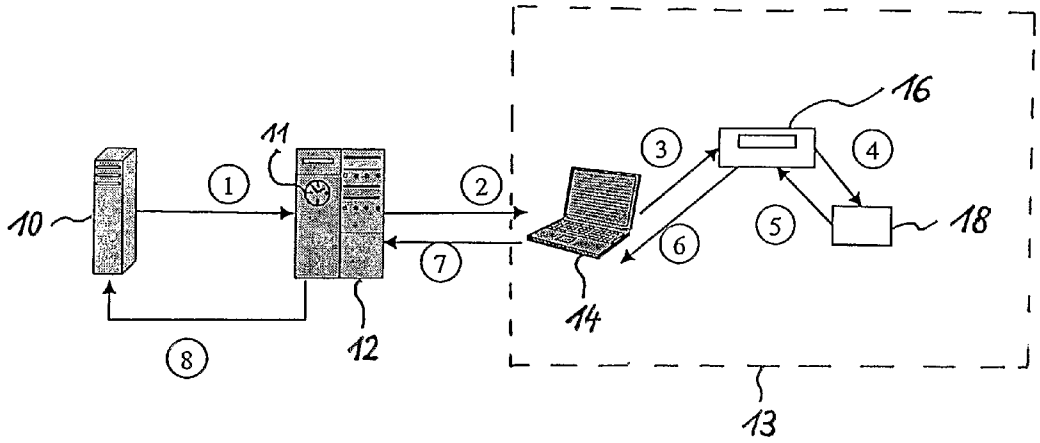
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, 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, 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*

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: LONG-TERM SECURE DIGITAL SIGNATURES



(57) Abstract: The present invention relates to digitally signing of electronic documents which are to be kept secure for a very long time, thereby taking into account future cryptographic developments which could render current cryptographic key-lengths insufficient. In accordance with the invention a double signature is issued for each document. A first digital signature (DTS) ensures the long time security, whilst a second digital signature (DUS) ensures the involvement of an individual user. Thereby, the second digital signature is less computationally intensive in its generation than the first digital signature.

WO 2004/079986 A1