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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 July 2004 (08.07.2004)

PCT

(10) International Publication Number
WO 2004/057796 A1

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

(21) International Application Number:
PCT/GB2003/005107

(22) International Filing Date:
24 November 2003 (24.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0229894.1 21 December 2002 (21.12.2002) GB

(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)*: **OWLETT, John** [GB/GB]; 26 Ranelagh Gardens, Southampton, Hampshire SO15 2TH (GB). **THOMPSON, George** [GB/GB]; 37 Pyrford Close, Waterlooville, Hampshire PO7 6BT (GB). **WALTON, Keith, Andrew** [GB/GB]; 48 Kenilworth Avenue, London SW19 7LW (GB).

(74) Agent: **LITHERLAND, David, Peter**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

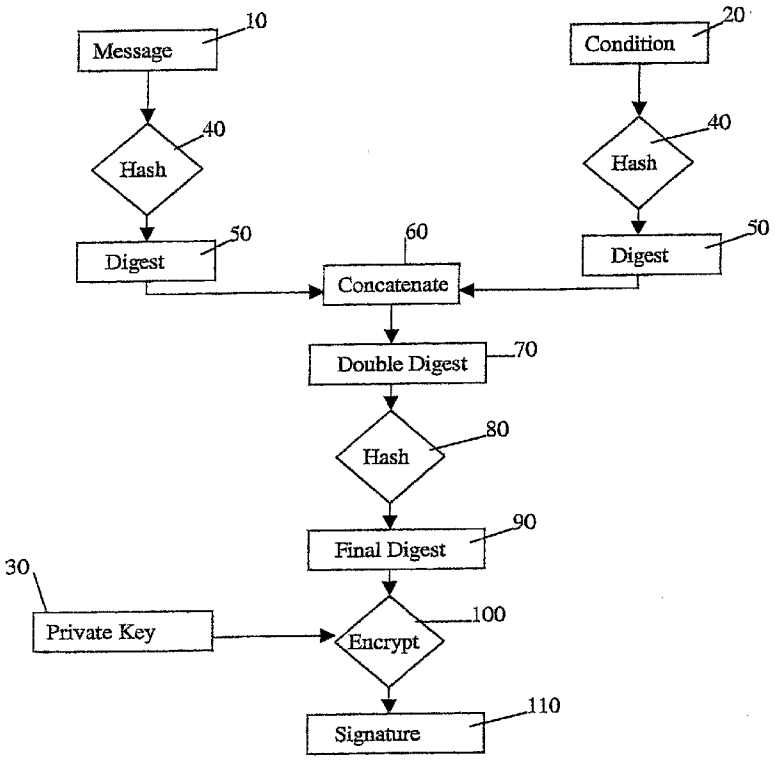
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, 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 *(regional)*: ARIPO patent (BW, 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*

[Continued on next page]

(54) **Title:** METHODS, APPARATUS AND COMPUTER PROGRAMS FOR GENERATING AND/OR USING CONDITIONAL ELECTRONIC SIGNATURES FOR REPORTING STATUS CHANGES



(57) **Abstract:** Provided are methods, apparatus and computer programs for generating and using conditional electronic signatures enabling the parties to an online communication or transaction to link conditions unambiguously with signed data items, and enabling verification of the authenticity of the data item and conditions and verification of the identity of the signing party. A data item and one or more conditions are separately hashed, the resulting digests (hash values) are concatenated, and the concatenand is further hashed to produce a final digest. The final digest is encrypted using the private key of a public/private key encryption scheme to produce a conditional digital signature. The data item and conditions can each be verified. Verification includes decrypting the conditional signature and comparing the decrypted result with a separately generated final digest. A solution is also disclosed for propagating information to interested parties when a first is countermanded at a second review.

WO 2004/057796 A1

— *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.