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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 March 2006 (09.03.2006)

PCT

(10) International Publication Number
WO 2006/024816 A2

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

(21) International Application Number:
PCT/GB2005/003199

(22) International Filing Date: 16 August 2005 (16.08.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0419479.1 2 September 2004 (02.09.2004) GB

(71) Applicant *(for all designated States except US)*: **CRYPTOMATHIC LTD** [GB/GB]; 329 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire CB4 0WG (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TULIANI, Jonathan, Roshan** [GB/GB]; 206 The Rowans, Milton, Cambridge, Cambridgeshire CB4 6ZL (GB). **BURSELL, Michael** [GB/GB]; c/o Cambridge Sciense Park, Milton Road, Cambridge, Cambridgeshire CB4 0WG (GB).

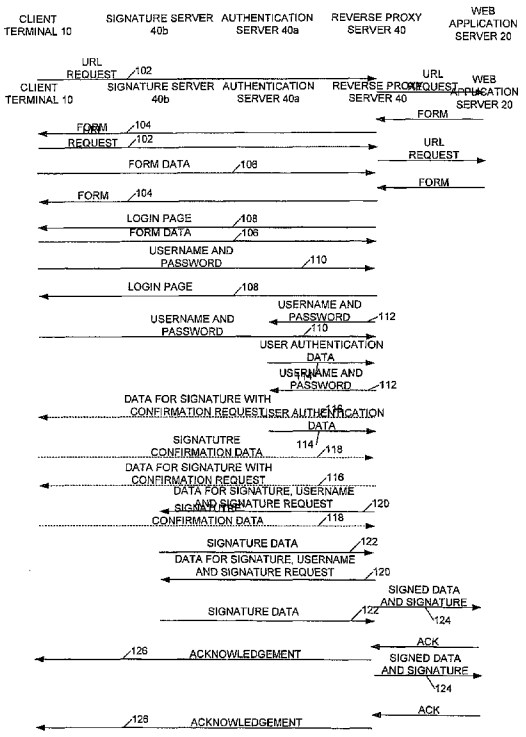
(74) Agent: **MARKS & CLERK**; 66-68 Hills Road, Cambridge CB2 1LA (GB).

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

[Continued on next page]

(54) Title: DATA CERTIFICATION METHODS AND APPARATUS



(57) Abstract: This invention generally relates methods, computer program code, data processing apparatus, and signals for certifying data, in particular by means of an electronic signature. Embodiments of the invention can be implemented on a user terminal without the need for dedicated hardware or software and may be termed "zero-footprint" data certification methods. A method of providing an electronic signature to-a-server; the method comprising receiving data for said server at a proxy system for said server; reading said received data to identify a signature request; obtaining a signature for a portion of said received data associated with said request responsive to said request, and providing said signature from said proxy system to said server. The use of a signature-enabled reverse proxy enables the use of a zero footprint user terminal, that is without the need to add additional functionality to the terminal for the purposes of signature creation in the context of a distributed application architecture.

WO 2006/024816 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.