



(51) International Patent Classification:

H04L 9/32 (2006.01) *G06Q* 20/42 (2012.01)
G06F 21/42 (2013.01) *H04W* 12/06 (2009.01)
H04L 29/06 (2006.01)

(21) International Application Number:

PCT/GB2014/051749

(22) International Filing Date:

6 June 2014 (06.06.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

1310468.2 12 June 2013 (12.06.2013) GB

(71) Applicant: **CRYPTOMATHIC LTD** [GB/GB]; 329
 Cambridge Science Park, Milton Road, Cambridge, Cam-
 bridgeshire CB4 0WG (GB).

(72) Inventors: **FORGET, Guillaume**; c/o Cryptomathic
 GmbH, Bretonischer Ring 7, 85630 Grasbrunn (DE). **PED-
 ERSEN, Torben Pryds**; c/o Cryptomathic A/S, Jaeger-
 gardsgade 118, DK-8000 Aarhus C (DK).

(74) Agent: **MARKS & CLERK LLP**; 62-68 Hills Road,
 Cambridge, Cambridgeshire CB2 1LA (GB).

(81) Designated States (unless otherwise indicated, for every
 kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
 BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
 DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
 HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
 KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
 MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
 OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
 SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
 TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
 ZW.

(84) Designated States (unless otherwise indicated, for every
 kind of regional protection available): ARIPO (BW, GH,
 GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
 UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
 TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
 EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
 MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
 TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
 KM, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the
 claims and to be republished in the event of receipt of
 amendments (Rule 48.2(h))

(54) Title: SYSTEM AND METHOD FOR ENCRYPTION

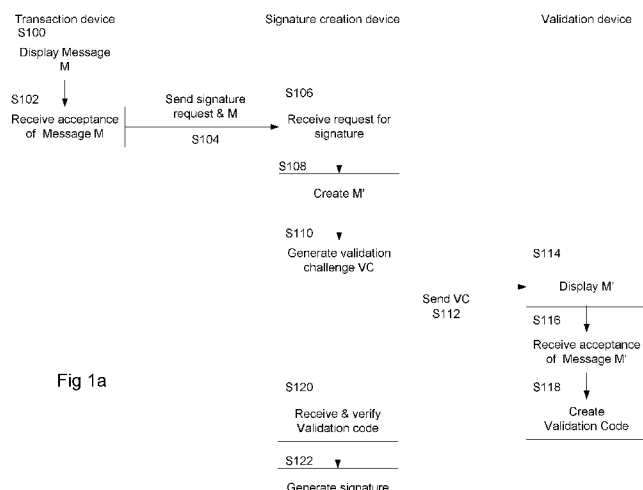


Fig 1a

(57) Abstract: A method and system for generating a signature for a user are described. The system comprises a signature server, an initial transaction device for a user and a validation device for a user. The initial transaction device is configured to display a first message M and send a request to the signature server to create a signature for said first message M. The signature server is configured to generate a validation challenge using a second message M' which is based on said first message M' and a first secret shared between said user and said signature server and send said validation challenge to the validation device. The validation device is configured to regenerate said second message M' using said first shared secret, display said second message M', receive user confirmation that the displayed second message M' corresponds to said first message M, generate a validation code confirming the request to create a signature; and send said validation code to said signature server. Thereafter, said signature server generates the signature for the user for the first message M.

