



(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/GB2010/050313

(22) International Filing Date:
24 February 2010 (24.02.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0903714.4 4 March 2009 (04.03.2009) GB

(72) Inventor; and

(71) Applicant : **HAWKES, Michael Ian** [GB/GB]; Lyme House, Dunwood Lane, Rudyard Staffordshire ST13 8RH (GB).

(74) Agents: **FEARNSIDE, Andrew Simon** et al.; 15 Clare Road, Halifax, Yorkshire HX1 2HY (GB).

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

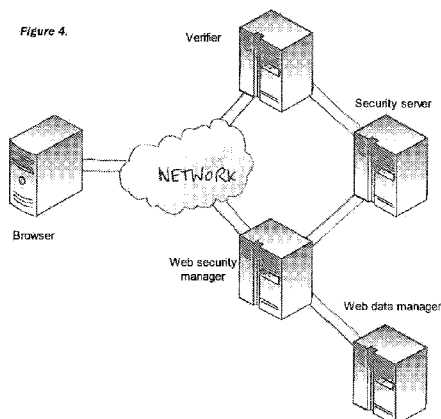
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND APPARATUS FOR SECURING NETWORK COMMUNICATIONS



(57) Abstract: A verifier (20) for verifying the authenticity of a communication sent via a communications network from a first network component (10) to a second network component (1000) including input means/apparatus arranged for receiving via the communications network an encrypted communication from a said first network component. The verifier has key means/apparatus operable to issue to a said second network component a key associated with the first network component on condition that the verifier has verified the encrypted communication to be decryptable using said key thereby to enable the second network component to decrypt encrypted communications from the first network component sent independently of the verifier apparatus.

