



- (51) International Patent Classification:
H04L 9/00 (2006.01)
- (21) International Application Number:
PCT/SG2014/000592
- (22) International Filing Date:
12 December 2014 (12.12.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
201309317-4 17 December 2013 (17.12.2013) SG
- (71) Applicant: AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH [SG/SG]; 1 Fusionopolis Way, #20-10, Connexis, Singapore 138632 (SG).
- (72) Inventors: CHAN, Aldar Chun Fai; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis, South Tower, Singapore 138632 (SG). WONG, Jun Wen; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis, South Tower, Singapore 138632 (SG). ZHOU, Jianying; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis, South Tower, Singapore 138632 (SG). TEO, Joseph Chee Ming; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis, South Tower, Singapore 138632 (SG).
- (74) Agent: VIERING, JENTSCHURA & PARTNER LLP; P.O. Box 1088, Rochor Road, Rochor Post Office, Singapore 911833 (SG).
- (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, 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.

[Continued on next page]

(54) Title: ENTITY AUTHENTICATION IN NETWORK

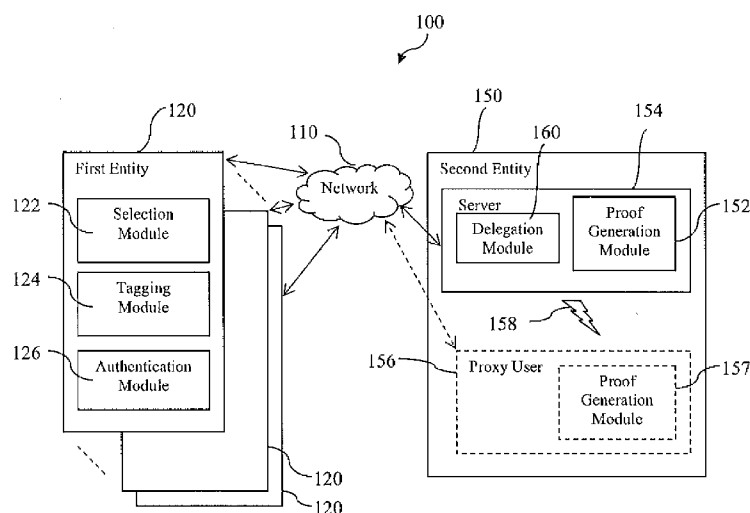


FIG. 1

(57) Abstract: There is provided an entity authentication method for a network including a first entity and a second entity, the method including: selecting, at the first entity, one or more pieces of data processed by the first entity to be used for authenticating the second entity; tagging, at the first entity, each of the one or more pieces of data selected with a respective tag generated based on a first secret key of the first entity; sending, from the first entity, a set of authentication data comprising the one or more pieces of data and the respective tags to the second entity; and authenticating, by the first entity, the second entity using a challenge-response authentication technique based on the set of authentication data and the first secret key. There is also provided a corresponding system with entity authentication for a network, and an entity in a network with entity authentication.



(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, ST, 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))*