



(51) International Patent Classification:
H04L 9/20 (2006.01)

(21) International Application Number:
PCT/IB2021/052201

(22) International Filing Date:
17 March 2021 (17.03.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/843,980 09 April 2020 (09.04.2020) US

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York, New York 10504 (US).

(71) Applicants (*for MG only*): **IBM ISRAEL SCIENCE AND TECHNOLOGY LTD.** [IL/IL]; Haifa University Campus, 165 Aba Khoushy Ave, Mount Carmel, 3498825 Haifa (IL). **IBM (CHINA) INVESTMENT COMPANY LTD.** [CN/CN]; 25/F, Pangu Plaza, No.27, Central North 4th Ring Road, Chaoyang District, Beijing 100101 (CN).

(72) Inventors: **VISEGRADY, Tamas**; IBM Research GmbH, Saeumerstrasse 4, Rueschlikon, 8803 Zurich (CH). **DRAGONE, Silvio**; IBM Research GmbH, Saeumerstrasse 4, Rueschlikon, 8803 Zurich (CH). **OSBORNE, Michael**; IBM Research GmbH, Saeumerstrasse 4, Rueschlikon, 8803 Zurich (CH). **PALMER, Elaine**; IBM, 5 Bedford Farms Drive, Bedford, New Hampshire 03110-6531 (US).

(74) Agent: **GILBOA, Eyal**; IBM Israel Science And Technology Ltd., Haifa University Campus, 165 Aba Khoushy Ave, Mount Carmel, 3498825 Haifa (IL).

(54) Title: KEY ATTRIBUTE VERIFICATION

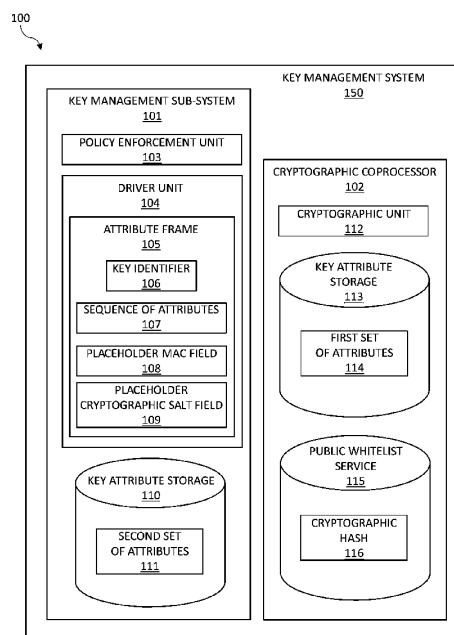


FIG. 1

(57) Abstract: A key identifier that identifies a cryptographic key is transmitted to a cryptographic coprocessor. A first set of attributes is received from the cryptographic coprocessor. The first set of attributes and a second set of attributes are serialized into a first sequence of attributes. The first sequence of attributes are stored to an attribute frame. One or more attributes in the second set of attributes are associated with the cryptographic key and originate from a key attribute storage of the key management system. The second set of attributes is different from the first set of attributes. The first sequence of attributes is transmitted to the cryptographic coprocessor. A first message authentication code (MAC) calculated from the first sequence of attributes is received from the cryptographic coprocessor. The attribute frame is verified by comparing the first MAC, or a value derived from the first MAC, to a reference value.



(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, 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))