

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
09 April 2020 (09.04.2020)



(10) International Publication Number
WO 2020/072550 A1

(51) International Patent Classification:

G06Q 20/32 (2012.01) H04W 12/06 (2009.01)
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/US2019/054149

(22) International Filing Date:

01 October 2019 (01.10.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/740,352 02 October 2018 (02.10.2018) US
16/205,119 29 November 2018 (29.11.2018) US
16/590,153 01 October 2019 (01.10.2019) US

(71) Applicant: CAPITAL ONE SERVICES, LLC [US/US];
1680 Capital One Drive, McLean, VA 22102 (US).

(72) Inventors: RULE, Jeffrey; 3906 Laird Place, Chevy
Chase, MD 20815 (US); ILINCIC, Rajko; 4428 Sleaford
Road, Annandale, 22003 (US).

(74) Agent: KASNEVICH, Andrew, D. et al.; Hunton Andrews
Kurth LLP, 2200 Pennsylvania Ave, NW, Washington, DC
20037 (US).

(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, 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, 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, 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))

(54) Title: SYSTEMS AND METHODS FOR CRYPTOGRAPHIC AUTHENTICATION OF CONTACTLESS CARDS

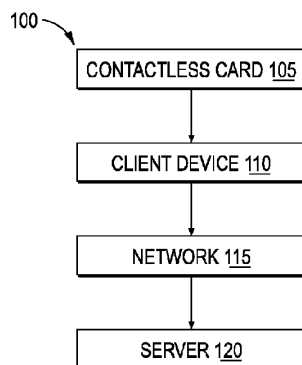


FIG. 1A

(57) Abstract: Example embodiments of systems and methods for data transmission between a contactless card and a client application are provided. A card key may be generated using a master key and identification number. A first and second session key may be generated using the card key and portions of the counter. A cryptographic result including the counter may be generated using one or more cryptographic algorithms and the card key. A cryptogram may be generated using the first session key and encrypted using the second session key. The application may transmit one or more messages to the first applet of the contactless card. The first applet may be configured to establish one or more communication paths to the second applet based on receipt of the one or more messages from the client device. The second applet may be deactivated by the first applet via the one or more communication paths.

WO 2020/072550 A1