

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
11 August 2022 (11.08.2022)



(10) International Publication Number
WO 2022/169457 A1

(51) International Patent Classification:

H04L 29/06 (2006.01) H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:

PCT/US2021/016770

(22) International Filing Date:

05 February 2021 (05.02.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: VISA INTERNATIONAL SERVICE
ASSOCIATION [US/US]; P.O. Box 8999, San Francisco,
California 94128 (US).

(72) Inventors: CHEN, Yuexi; P.O. Box 8999, San Francisco,
California 94128 (US). KEKICHEFF, Marc; P.O. Box
8999, San Francisco, California 94128 (US).

(74) Agent: JEWIK, Patrick et al.; 1100 Peachtree Street, NE
Suite 2800, Atlanta, Georgia 30309 (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, 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).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a
patent (Rule 4.17(ii))

Published:

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

(54) Title: MOBILE DEVICE SECRET PROTECTION SYSTEM AND METHOD

(57) Abstract: A method is disclosed. The method includes transmitting, by
a user device to an access device, a digital certificate and a seed. The access
device encrypts the seed and a first access device key with a public key from
the digital certificate to form encrypted data. The method also includes receiving
from the access device, the encrypted data, decrypting the encrypted
data using a private key corresponding to the public key to obtain the seed
and the first access device key, verifying that the seed received from the access
device matches the seed sent to the access device, encrypting a secret or
derivative thereof with the first access device key to form an encrypted secret
or derivative thereof, and transmitting to the access device, the encrypted
secret or derivative thereof.

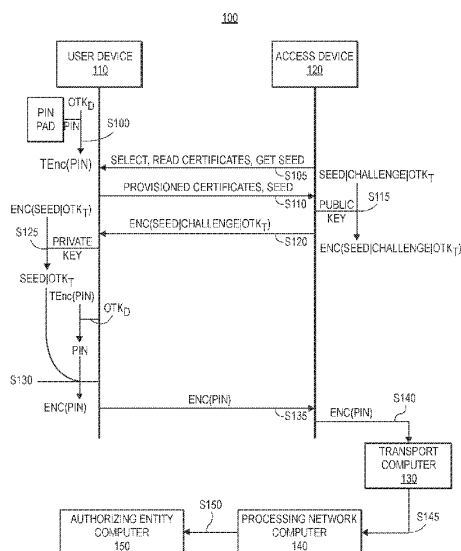


FIG. 1