

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

(19) World Intellectual Property  
Organization  
International Bureau

(43) International Publication Date  
25 November 2021 (25.11.2021)



(10) International Publication Number  
**WO 2021/236446 A1**

(51) International Patent Classification:

G06F 21/54 (2013.01) G06F 21/57 (2013.01)  
G06F 21/14 (2013.01) H04L 9/06 (2006.01)  
G06F 21/51 (2013.01)

(21) International Application Number:

PCT/US2021/032475

(22) International Filing Date:

14 May 2021 (14.05.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/027,208 19 May 2020 (19.05.2020) US

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

(72) Inventors: AGRAWAL, Shashank; P.O. Box 8999, San  
Francisco, California 94128 (US). ALPIREZ BOCK, Es-  
tuardo; P.O. Box 8999, San Francisco, California 94128  
(US). CHEN, Yilei; P.O. Box 8999, San Francisco, Califor-  
nia 94128 (US). WATSON, Gaven James; 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,

(54) Title: SYSTEMS AND METHODS FOR WHITEBOX DEVICE BINDING

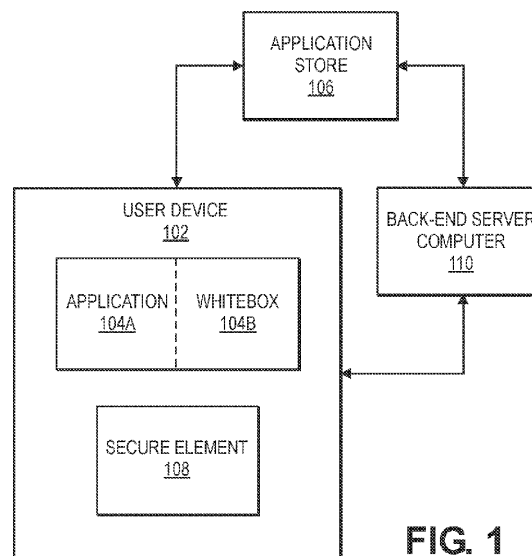


FIG. 1

(57) Abstract: A method is disclosed. The method includes receiving, by a user device, an encrypted message from a server computer. The encrypted message is a message encrypted with a master secret key or a key derived from the master secret key. The user device signs the encrypted message with a secure element private key. The user device, using a whitebox, cryptographically recovers a secure element public key from a certified key using a server computer public key. The certified key is certified by the server computer and based on at least the secure element public key. The user device, using the whitebox, cryptographically recovers the encrypted message from the signed encrypted message using the secure element public key. The user device, using the whitebox, decrypts the encrypted message using the master secret key or the key derived from the master secret key in the whitebox to obtain the message.

[Continued on next page]

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 the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

**Published:**

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