

(10) International Publication Number
WO 2015/160385 A1(43) International Publication Date
22 October 2015 (22.10.2015)(51) International Patent Classification:
G06Q 20/38 (2012.01)(21) International Application Number:
PCT/US2014/068000(22) International Filing Date:
2 December 2014 (02.12.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/979,113 14 April 2014 (14.04.2014) US(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, New York 10577 (US).(72) Inventors: **COLLINGE, Mehdi**; 8, Rue Cesar Franck, B-1420 Braine-l'Alleud (BE). **RADU, Cristian**; Rue de Tourinnes 2, B-1320 Beauvechain (BE).(74) Agent: **WIELAND III, Charles F.**; Buchanan Ingersoll & Rooney PC, P.O. Box 1404, Alexandria, Virginia 22313-1404 (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, 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.

(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))
- 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))

(54) Title: METHOD AND SYSTEM FOR GENERATING AN ADVANCED STORAGE KEY IN A MOBILE DEVICE WITHOUT SECURE ELEMENTS

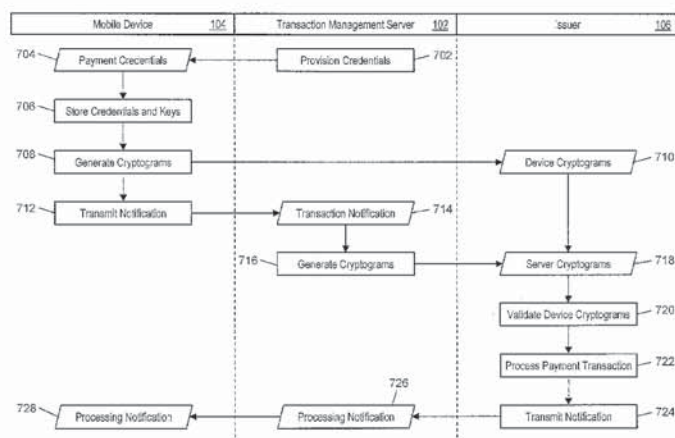


FIG. 7

(57) **Abstract:** A method for building an advanced storage key includes: storing, in a memory of a mobile device, at least (i) device information associated with the mobile device, (ii) program code associated with a first program, the code including an instance identifier, and (iii) program code associated with a second program, the code including a first key; generating a device fingerprint as associated with the mobile device based on the device information via execution of the code associated with the first program; generating a random value via execution of the code associated with the first program; building a diversifier value based on the generated device fingerprint, the generated random value, and the instance identifier included in the code associated with the first program; and decrypting the built diversifier value using the first key stored in the code associated with the second program via execution of the code associated with the second program to obtain a storage key.

METHOD AND SYSTEM FOR GENERATING AN ADVANCED STORAGE KEY IN A MOBILE DEVICE WITHOUT SECURE ELEMENTS

RELATED APPLICATIONS

[0001] This application claims the benefit, under 35 U.S.C. 119(e), of prior-filed Provisional Patent Application Nos. 61/910,819 filed December 2, 2013; 61/951,842 filed March 12, 2014; 61/955,716 filed March 19, 2014; 61/979,132 filed April 14, 2014; and 61/980,784 filed April 17, 2014; 61/979,122 filed April 14, 2014; 61/996,665 filed May 14, 2014; and, in particular, Provisional Patent Application No. 61/979,113 filed April 14, 2014, each herein incorporated by reference in their entirety.

FIELD

[0002] The present disclosure relates to the generation of an advanced storage key for use in a mobile device without a requiring secure element, and more specifically the use of multiple values to build an advanced storage key in a mobile device without a secure element for use in the secure storage of data in the mobile device.

BACKGROUND

[0003] Advances in mobile and communication technologies have created tremendous opportunities, one of which is providing the user of a mobile computing device with the ability to initiate and pay for payment transactions using their mobile device. One such approach to enable such actions on a mobile device has been the use of near field communication (NFC) technology to securely transmit payment details from the mobile device to a nearby contactless point of sale (POS) terminal. In order to achieve this, mobile phones with secure element hardware, such as a secure element (SE) chip, are used to securely store the payment credentials. A secure element is a special that may be included in some NFC-enabled devices that is a temper-resistant platform that may securely host applications and their confidential data.