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

Title (de)
VERFAHREN UND SYSTEM ZUR ERZEUGUNG EINES FORTGESCHRITTENEN SPEICHERSCHLÜSSELS IN EINER MOBILEN VORRICHTUNG OHNE SICHERE ELEMENTE

Title (fr)
PROCÉDÉ ET SYSTÈME POUR GÉNÉRER UNE CLÉ DE STOCKAGE ÉVOLUÉE DANS UN DISPOSITIF MOBILE SANS ÉLÉMENTS SÉCURISÉS

Publication
EP 3132406 A1 20170222 (EN)

Application
EP 14889340 A 20141202

Priority
- US 201461979113 P 20140414
- US 2014068000 W 20141202

Abstract (en)
[origin: WO2015160385A1] 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 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.

IPC 8 full level
G06Q 20/38 (2012.01)

CPC (source: EP KR RU US)
G06F 21/46 (2013.01 - KR); **G06Q 20/322** (2013.01 - KR); **G06Q 20/326** (2020.05 - EP KR RU US); **G06Q 20/3821** (2013.01 - EP KR); **G06Q 20/3823** (2013.01 - KR); **G06Q 20/3829** (2013.01 - EP KR RU US)

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)
BA ME

DOCDB simple family (publication)
WO 2015160385 A1 20151022; AU 2014391256 A1 20160707; AU 2014391256 B2 20170713; AU 2017245412 A1 20171102; AU 2019250276 A1 20191107; AU 2019250276 B2 20210401; CA 2933336 A1 20151022; CA 2933336 C 20180904; CN 106104605 A 20161109; CN 106104605 B 20200317; CN 111523884 A 20200811; CN 111523884 B 20230530; EP 3132406 A1 20170222; EP 3132406 A4 20171101; IL 246109 A0 20160731; IL 246109 B 20200331; JP 2017513248 A 20170525; JP 2018050300 A 20180329; JP 2020074566 A 20200514; JP 6224254 B2 20171101; JP 6703510 B2 20200603; JP 6889967 B2 20210618; KR 101903709 B1 20181004; KR 102150722 B1 20200902; KR 102151579 B1 20200903; KR 20160132105 A 20161116; KR 20180108907 A 20181004; KR 20200018729 A 20200219; MX 2016010086 A 20170427; MX 356939 B 20180620; NZ 721223 A 20180223; RU 2018113732 A 20190304; RU 2018113732 A3 20190304; RU 2653290 C1 20180507; RU 2682840 C2 20190321; SG 10201801008S A 20180328; SG 11201604876Y A 20160728; UA 117951 C2 20181025; ZA 201603938 B 20170927

DOCDB simple family (application)
US 2014068000 W 20141202; AU 2014391256 A 20141202; AU 2017245412 A 20171012; AU 2019250276 A 20191018; CA 2933336 A 20141202; CN 201480074686 A 20141202; CN 202010102477 A 20141202; EP 14889340 A 20141202; IL 24610916 A 20160608; JP 2016541581 A 20141202; JP 2017194490 A 20171004; JP 2020004636 A 20200115; KR 20167028484 A 20141202; KR 20187027712 A 20141202; KR 20207004059 A 20141202; MX 2016010086 A 20141202; NZ 72122314 A 20141202; RU 2016136503 A 20141202; RU 2018113732 A 20141202; SG 10201801008S A 20141202; SG 11201604876Y A 20141202; UA A201609401 A 20141202; ZA 201603938 A 20160609