

(51) International Patent Classification:
G06F 21/44 (2013.01)(21) International Application Number:
PCT/EP2015/078896(22) International Filing Date:
8 December 2015 (08.12.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14197711.6 12 December 2014 (12.12.2014) EP(71) Applicant: **NAGRAVISION S.A.** [CH/CH]; Route de
Genève 22-24, 1033 Cheseaux-sur-Lausanne (CH).(72) Inventors: **HUNACEK, Didier**; ch. du Pré des Planches
16C, 1807 Blonay (CH). **MACCHETTI, Marco**; Via
Boccaccio 42, 22070 Casnate con Bernate (IT). **FISC-
HER, Nicolas**; Chemin Franconis 14, 1290 Versoix (CH).(74) Agent: **LEMAN CONSULTING S.A. 284**; Chemin de
Précossy 31, 1260 Nyon (CH).(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).

Published:

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

(54) Title: DEVICE KEYS PROTECTION

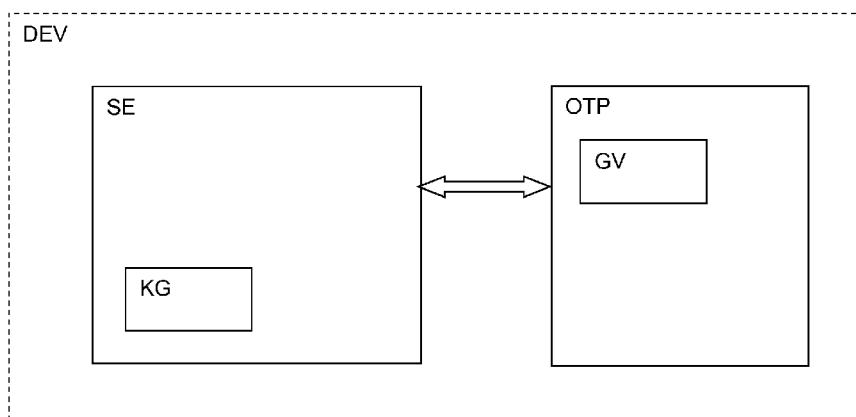


Fig. 1

(57) **Abstract:** A method to protect a device key in a device comprising at least one secure element locally connected to at least one time programmable memory storing a global value in form of a bit string comprising locked bits and unlocked bits. The locked bits are irreversibly pre-programmed in the one-time-programmable memory during an initialization phase of the device while the unlocked bits remaining in an initial state may be programmable by the secure element. The secure element is configured to generate, at initialization of the device, a device specific value by using the global value, program the device specific value previously obtained in the one time programmable memory, and erase the global value by programming the unlocked bits of the corresponding bit string. A further object of the disclosure includes a device configured to carry out the method.