

(51) International Patent Classification:
G06F 21/02 (2006.01)(21) International Application Number:
PCT/EP2011/006059(22) International Filing Date:
2 December 2011 (02.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10015270.1 3 December 2010 (03.12.2010) EP(71) Applicant (for all designated States except US): **NOVO-MATIC AG** [AT/AT]; Wiener Strasse 158, A-2352 Gumpoldskirchen (AT).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HUEBER, Andreas** [AT/AT]; Wiener Strasse 158, A-2352 Gumpoldskirchen (AT). **NAGL, Gerhard** [AT/AT]; Wiener Strasse 158, A-2352 Gumpoldskirchen (AT). **NOWAK, Robert** [AT/AT]; Wiener Strasse 158, A-2352 Gumpoldskirchen (AT). **MUDRY, Igor** [AT/AT]; Wiener Strasse 158, A-2352 Gumpoldskirchen (AT).(74) Agents: **LORENZ-SEIDLER-GOSSEL** et al.; Widenmayerstrasse 23, 80538 München (DE).

(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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

[Continued on next page]

(54) Title: DEVICE FOR AND METHOD OF HANDLING SENSITIVE DATA

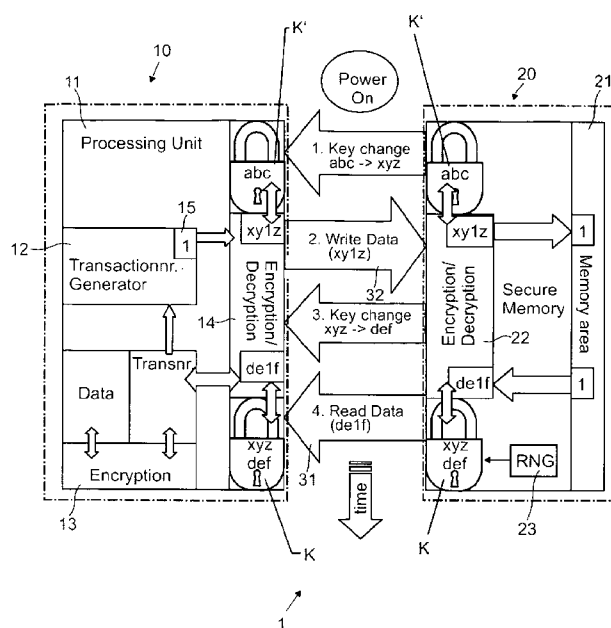


FIG. 1

(57) Abstract: The invention is related to a device for handling sensitive data comprising at least one first integrated circuitry for forming a first trust zone and at least one second integrated circuitry for forming a second trust zone wherein the first integrated circuitry comprises at least one secure processing unit adapted for processing sensitive data, the second integrated circuitry comprises at least one persistent memory area within its trust zone for storing the sensitive data wherein the second integrated circuitry is separated from the first integrated circuitry, the processing unit of the first integrated circuitry is adapted to transfer the sensitive data from the first trust zone to the second trust zone for securely storing said data in the persistent memory area of the second trust zone, the second integrated circuitry is adapted to transfer the sensitive data stored in its persistent memory area to the processing unit of the first trust zone, wherein the first and the second integrated circuitry comprise crypto means for securely transferring the sensitive data based on a symmetrical crypto method using a secure key, and wherein the second integrated circuitry comprises means for initiating a new key generation to replace the active secure key.



Published:

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

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))