



(51) International Patent Classification:

<i>G06F 21/35</i> (2013.01)	<i>G06Q 20/38</i> (2012.01)
<i>G06F 21/40</i> (2013.01)	<i>H04L 9/32</i> (2006.01)
<i>G06F 21/64</i> (2013.01)	

(21) International Application Number:

PCT/EP2018/085602

(22) International Filing Date:

18 December 2018 (18.12.2018)

(25) **Filing Language:** English

English

(26) **Publication Language:** English

English

(30) Priority Data:

17208564.9 19 December 2017 (19.12.2017) EP

(71) Applicant: RIDDLE & CODE GMBH [AT/AT]; ORBI

Tower, Thomas-Klestil-Platz 13, 1030 Wien (AT).

(72) **Inventor: FÜRSTNER, Thomas**; FL01 Santa Maria, 17,

Ward Street, II-Madliena, SWQ-1102 (MT).

(74) Agent: SONN & PARTNER PATENTANWÄLTE;

Riemergasse 14, 1010 Vienna (AT).

(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,

HR, HU, ID, IL, IN, IR, IS, 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, 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))*
- *of inventorship (Rule 4.17(iv))*

Published:

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

(54) Title: DONGLES AND METHOD FOR PROVIDING A DIGITAL SIGNATURE

- (57) **Abstract:** Set (s) of two or more dongles (a,b,c) for providing a digital signature (S_i), wherein each dongle (a,b,c) holds a secret key (K_i) wherein each dongle (a,b,c) is configured to receive a message (M), to compute (28,36) a digital signature (S_i) of the received message (M) using the secret key (K_i), and to transmit the computed digital signature (S_i), characterised in that at least one of the dongles (a) is configured to, before computing (28) the digital signature (S_a), verify (26) the presence of at least one other dongle (b,c) belonging to the set (s), and to compute (28) the digital signature (S_a) only upon successful verification of the presence of one or more other dongles (b,c).

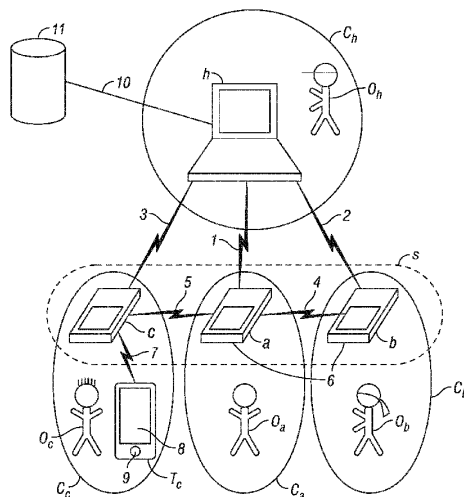


FIG. 1