(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2004 (23.12.2004)

PCT

(10) International Publication Number
WO 2004/111752 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/NL2004/000422

(22) International Filing Date: 14 June 2004 (14.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/NL03/00436 13 June 2003 (13.06.2003) NL

(71) Applicant *(for all designated States except US)*: **ORBID LIMITED** [IE/IE]; Wil House, c/o Oonagh Hayes, Shannon Business Park, Co Clare Shannon (IE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TEL, Teunis** [NL/NL]; 13 Esserlaan, NL-9722 SK Groningen (NL). **WARD, Scott, MacDonald** [US/NL]; 31 Zuidlaan, NL-2111 GB Aerdenhout (NL).

(74) Agent: **MERTENS, H., V.**; Exter Polak & Charlouis B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

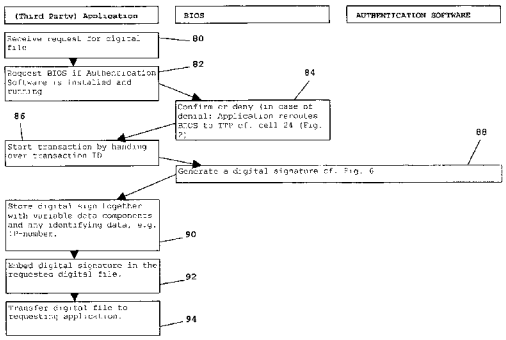
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
17 March 2005

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR PERFORMING A TRANSACTION AND FOR PERFORMING A VERIFICATION OF LEGITIMATE ACCESS TO, OR USE OF DIGITAL DATA



(57) Abstract: A method for performing an electronic transaction is disclosed. The method provides authentication data and authentication software to an electronic device and preferably stored in a secure storage location or other location inaccessible to the user or the operating system of the device. When digital data is requested from a transaction party that requests a digital signature, the authentication software is activated to generate said digital signature from the authentication data. Next, the digital signature is provided to the other transaction party, which then provides the requested digital data. The digital signature may be embedded in the requested and provided digital data. Further, a method for performing a verification of legitimate use of digital data is disclosed. Digital data digitally signed according to the present invention may only be accessed if the embedded digital signature is identical to a regenerated digital signature that is regenerated by the authentication software, using user inaccessible authentication data installed on the device. If the embedded and regenerated digital signatures are not identical, the data may not be accessed and an error signal is generated.

WO 2004/111752 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.