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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067097 A3

(51) International Patent Classification[7]: G06F 1/00, G11B 20/00, H04L 9/32

(21) International Application Number: PCT/IB02/00127

(22) International Filing Date: 17 January 2002 (17.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
01200670.6 23 February 2001 (23.02.2001) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: KAMPERMAN, Franciscus, L., A., J.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: DEGUELLE, Wilhelmus, H., G.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

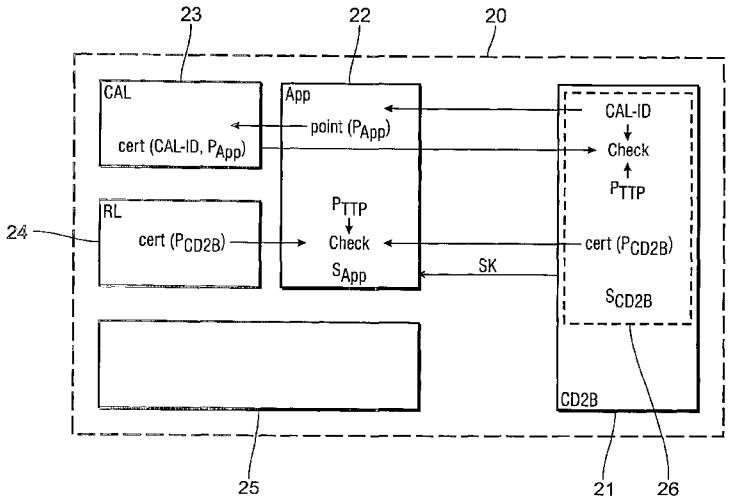
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
23 October 2003

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.

(54) Title: AUTHENTICATION METHOD AND DATA TRANSMISSION SYSTEM



(57) Abstract: The invention relates to a method for authenticating a first unit to a second unit and, in particular, to a method for transmitting data securely over a transmission channel from a security unit to an application unit. Known data transmission methods and systems use a revocation list stored in a security unit, e. g. in a CD drive, listing identifiers of revoked application units. In order to provide an environment for secure transmission of encrypted data and/or keys where the data and/or the keys are protected against copying, hacking and other misuse and which requires only a minimum storage capacity in the security unit a method for authenticating a first unit to a second unit is proposed according to the invention comprising the steps of: a) exchanging authentication data between said first unit and said second unit, said authentication data being retrieved from an authorisation list comprising a list identifier, and b) checking the authenticity of the authorisation list and the origin of the authentication data from a valid authorisation list.

WO 02/067097 A3