(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年4 月1 日 (01.04.2004)

PCT

(10) 国際公開番号
WO 2004/028079 A1

(51) 国際特許分類[7]: H04L 9/32, 9/08, G06F 15/00

(21) 国際出願番号: PCT/JP2003/011802

(22) 国際出願日: 2003 年9 月17 日 (17.09.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-273903 2002 年9 月19 日 (19.09.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 大森 和雄 (OMORI,Kazuo) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 本城 哲 (HONJO,Akira) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 末吉 正弘 (SUEYOSHI,Masahiro) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 花木 直文 (HANAKI,Naofumi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 舘野 啓 (TATENO,Kei) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

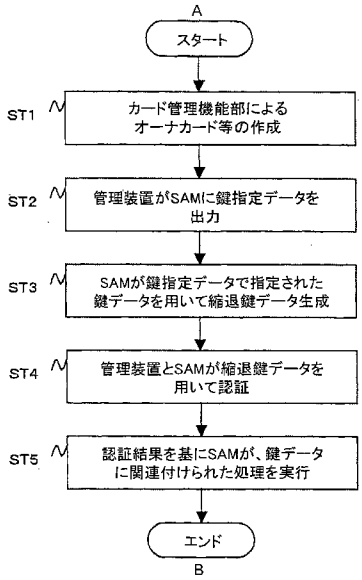
(74) 代理人: 佐藤 隆久 (SATOH,Takahisa); 〒111-0052 東京都 台東区 柳橋２丁目４番２号 宮木ビル４階 創進国際特許事務所 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK,

[続葉有]

(54) Title: DATA PROCESSING METHOD, ITS PROGRAM AND ITS DEVICE

(54) 発明の名称: データ処理方法、そのプログラムおよびその装置



A...START
ST1...CARD MANAGEMENT FUNCTIONAL UNIT CREATES OWNER CARD.
ST2...MANAGEMENT DEVICE OUTPUTS KEY SPECIFICATION DATA TO SAM.
ST3...SAM GENERATES DEGENERATE KEY DATA USING KEY DATA SPECIFIED BY KEY SPECIFICATION DATA.
ST4...MANAGEMENT DEVICE AND SAM PERFORM AUTHENTICATION USING DEGENERATE KEY DATA.
ST5...SAM EXECUTES PROCESSING ASSOCIATED WITH KEY DATA ACCORDING TO AUTHENTICATION RESULT.
B...END

(57) Abstract: A management device (20) outputs key specification data, read from a card, to an SAM unit (9a). The SAM unit (9a) generates degenerate key data using two-way authentication key data specified by the key specification data. The management device (20) and the SAM unit (9a) perform authentication using the degenerate data. When the SAM unit (9a) authenticates the management device (20), the SAM unit (9a) executes a processing associated with one or more sets of two-way authentication key data used for generating the degenerate key data.

(57) 要約: 管理装置２０が、カードから読み込んだ鍵指定データをＳＡＭユニットに９ａに出力する。ＳＡＭユニット９ａが、鍵指定データが指定する相互認証鍵データを用いて縮退鍵データを生成する。管理装置２０とＳＡＭユニット９ａとで縮退鍵データを用いて認証を行う。ＳＡＭユニット９ａが管理装置２０の正当性を認めると、上記縮退鍵データの生成に用いられた単数または複数の相互認証鍵データに関連付けられた処理を実行する。

WO 2004/028079 A1

DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, 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) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。