(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
2005 年7 月21 日 (21.07.2005)

PCT

(10) 国際公開番号
WO 2005/067199 A1

(51) 国際特許分類[7]: H04L 9/14, 9/32

(21) 国際出願番号: PCT/JP2004/005881

(22) 国際出願日: 2004 年4 月23 日 (23.04.2004)

(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 2003-432476
2003 年12 月26 日 (26.12.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３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): 大越 丈弘 (OHKOSHI, Takehiro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 山田 敬喜 (YAMADA, Keiki) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP). 牧田 覚 (MAKITA, Satoru) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内 Tokyo (JP).

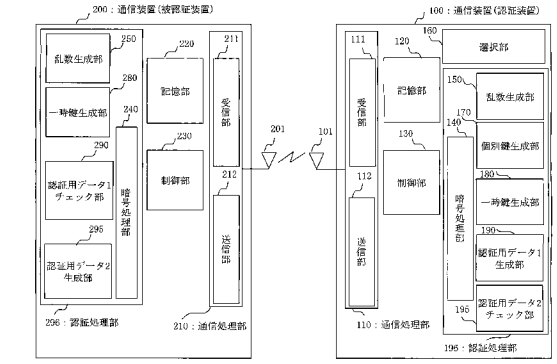
(74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM,

[続葉有]

(54) Title: AUTHENTICATEE DEVICE, AUTHENTICATOR DEVICE, AND AUTHENTICATION METHOD

(54) 発明の名称: 被認証装置及び認証装置及び認証方法



200...COMMUNICATION DEVICE (AUTHENTICATEE DEVICE)
250...RANDOM NUMBER GENERATION SECTION
280...TEMPORARY KEY GENERATION SECTION
290...AUTHENTICATION DATA 1 CHECK SECTION
295...AUTHENTICATION DATA 2 GENERATION SECTION
240...ENCRYPTION PROCESSING SECTION
296...AUTHENTICATION PROCESSING SECTION
220...STORAGE SECTION
230...CONTROL SECTION
211...RECEPTION SECTION
212...TRANSMISSION SECTION
210...COMMUNICATION PROCESSING SECTION
100...COMMUNICATION DEVICE (AUTHENTICATOR DEVICE)
111...RECEPTION SECTION
112...TRANSMISSION SECTION
110...COMMUNICATION PROCESSING SECTION
120...STORAGE SECTION
130...CONTROL SECTION
160...SELECTION SECTION
140...ENCRYPTION PROCESSING SECTION
150...RANDOM NUMBER GENERATION SECTION
170...INDIVIDUAL KEY GENERATION SECTION
180...TEMPORARY KEY GENERATION SECTION
190...AUTHENTICATION DATA 1 GENERATION SECTION
195...AUTHENTICATION DATA 2 CHECK SECTION
196...AUTHENTICATION PROCESSING SECTION

(57) **Abstract:** An authenticatee device (200) includes: a storage section (220) for storing at least one algorithm identifier and at least one encryption key identifier; a transmission section (212) for transmitting the at least one algorithm identifier and the at least one encryption key identifier stored in the storage section (220) to an authenticator device (100); a reception section (211) for receiving a predetermined algorithm identifier and a predetermined encryption key identifier selected from the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticator device (100) by the transmission section (212); and an authentication processing section (296) for performing authentication processing together with the authenticator device (100) according to the predetermined algorithm identifier and the encryption key identifier received by the reception section (211).

(57) 要約: 被認証装置２００に、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する記憶部２２０と、上記記憶部２２０により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置１００に送信する送信部２１２と、上記認証装置１００から上記送信部２１２により送信された少なくとも１つのアルゴリズム識

[続葉有]

WO 2005/067199 A1

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) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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).

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。

別子と少なくとも１つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部２１１と、上記受信部２１１により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置１００との間で認証処理をおこなう認証処理部２９６とを備えた。