(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 2005/067200 A1

(51) 国際特許分類[7]: H04L 9/32, 9/14

(21) 国際出願番号: PCT/JP2004/005879

(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 2003-432447
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).

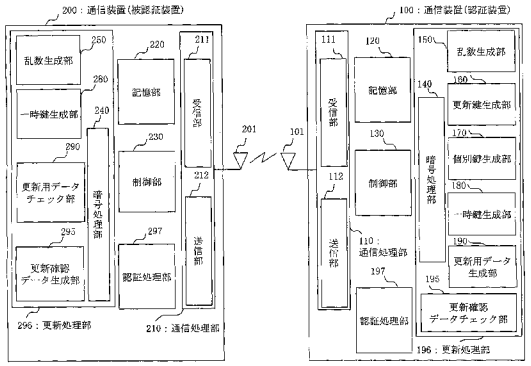
(74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (JP).

(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,

[続葉有]

(54) Title: AUTHENTICATION DEVICE, DEVICE TO BE AUTHENTICATED, AND KEY UPDATE METHOD

(54) 発明の名称: 認証装置及び被認証装置及び鍵更新方法



200...COMMUNICATION DEVICE (DEVICE TO BE AUTHENTICATED)
250...RANDOM NUMBER GENERATION SECTION
280...TEMPORARY KEY GENERATION SECTION
290...UPDATE DATA CHECK SECTION
295...UPDATE CONFIRAMATION DATA GENERATION SECTION
240...ENCRYPTION PROCESSING SECTION
296...UPDATE PROCESSING SECTION
220...STORAGE SECTION
230...CONTROL SECTION
297...AUTHENTICATION PROCESSING SECTION
211...RECEPTION SECTION
212...TRANSMISSION SECTION
210...COMMUNICATION PROCESSING SECTION
100...COMMUNICATION DEVICE (AUTHENTICATION DEVICE)
111...RECEPTION SECTION
112...TRANSMISSION SECTION
120...STORAGE SECTION
130...CONTROL SECTION
110...COMMUNICATION PROCESSING SECTION
197...AUTHENTICATION PROCESSING SECTION
140...ENCRYPTION PROCESING SECTION
150...RANDOM NUMBER GENERATION SECTION
160...UPDATE KEY GENERATION SECTION
170...INDIVIDUAL KEY GENERATION SECTION
180...TEMPORARY KEY GENERATION SECTION
190...UPDATE DATA GENERATION SECTION
195...UPDATE CONFIRMATION DATA CHECK SECTION
196...UPDATE PROCESSING SECTION

(57) Abstract: An authentication device (100) includes: an authentication processing section (197) for performing authentication of a communication device (200) by using an authentication key; and an update key generation key section (160)for generating a new authentication key when the communication device (200) does not have an authentication key to be used for the authentication processing by the authentication processing section (197) and generating a new authentication key for updating the authentication key when the communication device (200) has an authentication key but authentication of the communication device (200) by the authentication processing section (197) has failed. By using the new authentication key generated by the update key generation section (160), the authentication processing section (197) again performs authentication of the communication device (200).

(57) 要約: 認証装置１００に、認証用鍵を用いて通信装置２００との間で認証処理をおこなう認証処理部１９７と、上記認証処理部１９７による認証処理に用いる認証用鍵を通信装置２００が保持していない場合に新たな認証用鍵を生成し、上記通信装置２００が保持している場合で上記認証処理部１９７による通信装置２００との間での認証処理が失敗した場合に上記認証用鍵の更新のために新たな認証用鍵を生成する更新鍵生成部１６０とを備え、上記認証処理部１９７は、上記更新鍵生成部１６０によ

[続葉有]

WO 2005/067200 A1

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) 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。

り生成された新たな認証用鍵を用いて通信装置２００との間での認証処理を再度おこなうことを特徴とする。