(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12 月22 日 (22.12.2005)

PCT

(10) 国際公開番号
WO 2005/122468 A1

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

(21) 国際出願番号: PCT/JP2005/009862

(22) 国際出願日: 2005 年5 月30 日 (30.05.2005)

(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2004-170153 2004 年6 月8 日 (08.06.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１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): 窪田 知記 (KUBOTA, Tomoki) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 平塚 誠一 (HIRATSUKA, Seiichi) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

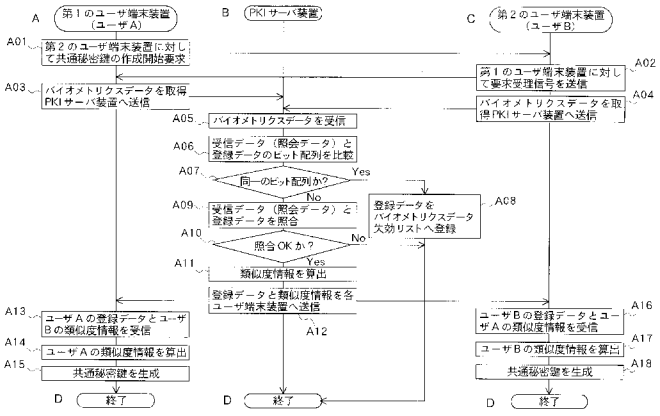
(74) 代理人: 宮崎 昭夫, 外(MIYAZAKI, Teruo et al.); 〒1070052 東京都港区赤坂１丁目９番２０号 第１６興和ビル８階 Tokyo (JP).

(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, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU,

[続葉有]

(54) Title: DATA COMMUNICATION METHOD AND SYSTEM

(54) 発明の名称: データ通信方法及びシステム



A... FIRST USER TERMINAL DEVICE (USER A)
B... PKI SERVER DEVICE
C... SECOND USER TERMINAL DEVICE (USER B)
A01... REQUEST THE SECOND USER TERMINAL DEVICE TO START CREATION OF A COMMON SECRET KEY
A03... ACQUIRE BIOMETRICS DATA AND TRANSMIT IT TO PKI SERVER DEVICE
A13... RECEIVE REGISTERED DATA ON USER A AND SIMILARITY INFORMATION ON USER B
A14... CALCULATE USER A SIMILARITY INFORMATION
A15... GENERATE COMMON SECRET KEY
D... END
A05... RECEIVE BIOMETRIC DATA
A06... COMPARE RECEIVED DATA (CORRELATION DATA) TO BIT ARRANGEMENT OF THE REGISTERED DATA
A07... SAME BIT ARRANGEMENT?
A09... CORRELATE RECEIVED DATA (CORRELATION DATA) WITH REGISTERED DATA
A08... REGISTER REGISTERED DATA IN BIOMETRICS DATA INVALIDATION LIST
A10... CORRELATION SUCCESSFUL?
A11... CALCULATE SIMILARITY INFORMATION
A12... TRANSMIT REGISTERED DATA AND SIMILARITY INFORMATION TO RESPECTIVE USER TERMINAL DEVICES
A02... TRANSMIT REQUEST RECEPTION SIGNAL TO THE FIRST USER TERMINAL DEVICE
A04... ACQUIRE BIOMETRICS DATA AND TRANSMIT IT TO PKI SERVER DEVICE
A16... RECEIVE REGISTERED DATA ON USER B AND SIMILARITY INFORMATION ON USER A
A17... CALCULATE SIMILARITY INFORMATION ON USER B
A18... GENERATE A COMMON SECRET KEY

(57) Abstract: Biological information on a user is digitalized into biometric data which is transmitted from a terminal to a server. In the server, the user is authenticated by using the biometric data. The server transmits registered data on its user and similarity information on the communication partner to the terminal. The terminal generates a secret key to be shared by the communication partner from the user similarity information calculated from the registered data and the similarity information on the communication partner. By using the secret key, an encrypted communication is performed.

(57) 要約:

ユーザの生体情報を数値化したバイオメトリクスデータを端末からサーバに送信し、サーバにおいて、そのバイオメトリクスデータを用いてユーザを認証する。サーバは自ユーザの登録データと通信相手の類似度情報を端末に送信し、端末は登録データから算出した自ユーザの類似度情報と通信相手の類似度情報とから通信相手と共通の秘密鍵を生成し、その秘密鍵を用いて暗号通信を行う。

WO 2005/122468 A1

ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, NA, 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, IS, IT, LT, 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。