

(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
2014 年 4 月 3 日(03.04.2014)



(10) 国際公開番号
WO 2014/049749 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) **G06F 21/20** (2006.01)
- (21) 国際出願番号: PCT/JP2012/074781
- (22) 国際出願日: 2012 年 9 月 26 日(26.09.2012)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人: 株式会社 東芝(KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 Tokyo (JP). 東芝ソリューション株式会社 (TOSHIBA SOLUTIONS CORPORATION) [JP/JP]; 〒1056691 東京都港区芝浦一丁目 1 番 1 号 Tokyo (JP).
- (72) 発明者: 池田 竜朗(IKEDA, Tatsuro); 〒1056691 東京都港区芝浦一丁目 1 番 1 号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 山田 朝彦(YAMADA, Asahiko); 〒1056691 東京都港区芝浦一丁目 1 番 1 号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 岡田 光司(OKADA, Koji); 〒1056691 東京都港区芝浦一丁目 1 番 1 号 東

芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP).

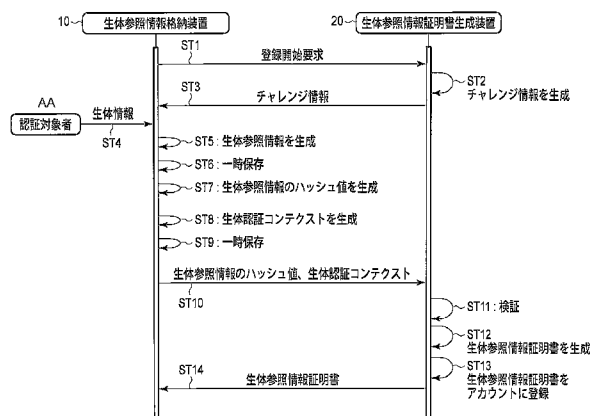
- (74) 代理人: 蔵田 昌俊, 外(KURATA, Masatoshi et al.); 〒1050001 東京都港区虎ノ門一丁目三番二号 勸銀不二屋ビル六階 鈴榮特許総合事務所内 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT,

[続葉有]

(54) Title: BIOMETRIC REFERENCE INFORMATION REGISTRATION SYSTEM, DEVICE, AND PROGRAM

(54) 発明の名称: 生体参照情報登録システム、装置及びプログラム

[図9]



- 10 Biometric reference information storage device
20 Biometric reference information certificate generation device
ST1 Request to start registration
ST2 Challenge information generated
ST3 Challenge information
ST4 Biometric information
ST5 Biometric reference information generated
ST6 Temporarily saved
ST7 Hash value for Biometric reference information generated
ST8 Biometric verification context generated
ST9 Temporarily saved
ST10 Biometric reference information hash value, Biometric verification context
ST11 Verification
ST12 Biometric reference information certificate created
ST13 Biometric reference information certificate registered in account
ST14 Biometric reference information certificate
AA Verification subject

(57) Abstract: In an embodiment of the present invention a biometric reference information storage device receives challenge information from a biometric reference information certificate generation device. The biometric reference information storage device generates biometric reference information on the basis of biometric information obtained from a verification subject. The biometric reference information storage device transmits to the biometric reference information certificate generation device a biometric verification context containing the challenge information, a hash value for the biometric reference information, and a first digital signature. The biometric reference information certificate generation device verifies the challenge information. The biometric reference information certificate generation device verifies the first digital signature on the basis of a first public key. The biometric reference information certificate generation device transmits a biometric reference information certificate to the biometric reference information storage device. The biometric reference information storage device writes the biometric reference information and the biometric reference information certificate in a storage means.

(57) 要約:

[続葉有]



NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI 添付公開書類:
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, — 国際調査報告 (条約第 21 条(3))
NE, SN, TD, TG).

実施形態において、生体参照情報格納装置は生体参照情報証明書生成装置からチャレンジ情報を受信する。前記生体参照情報格納装置は、前記認証対象者から採取した生体情報に基づいて生体参照情報を生成する。前記生体参照情報格納装置は、前記チャレンジ情報、前記生体参照情報のハッシュ値、及び第1デジタル署名を含む生体認証コンテキストを前記生体参照情報証明書生成装置に送信する。前記生体参照情報証明書生成装置は前記チャレンジ情報を検証する。前記生体参照情報証明書生成装置は、前記第1デジタル署名を第1公開鍵に基づいて検証する。前記生体参照情報証明書生成装置は生体参照情報証明書を前記生体参照情報格納装置に送信する。前記生体参照情報格納装置は、前記生体参照情報及び前記生体参照情報証明書を格納手段に書込む。