

(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
2025年1月30日(30.01.2025)



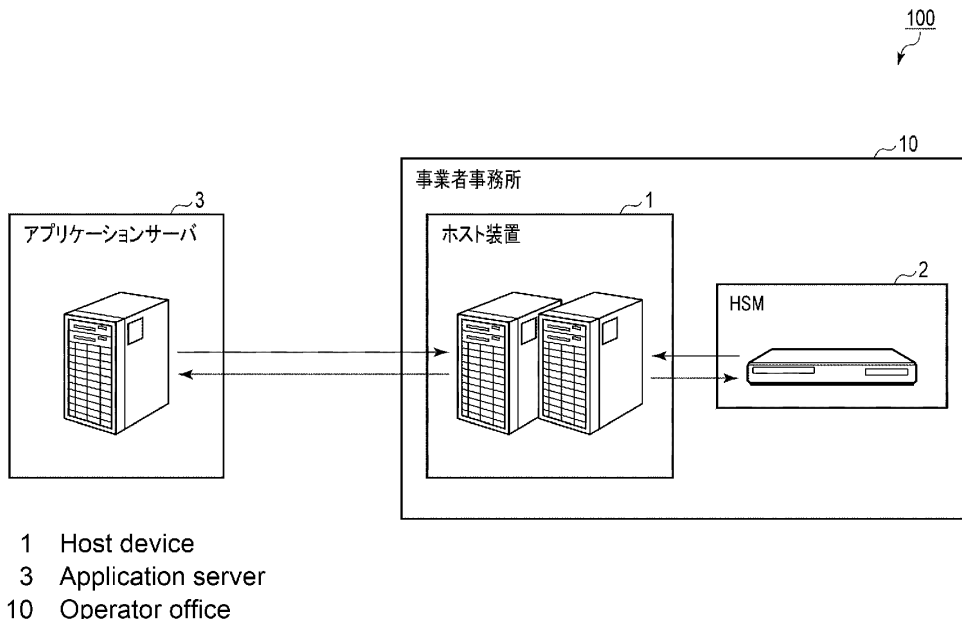
(10) 国際公開番号

WO 2025/022911 A1

- (51) 国際特許分類:
H04L 9/10 (2006.01) H04L 9/32 (2006.01) CORPORATION) [JP/JP]; 〒2120013 神奈川県
川崎市幸区堀川町 7 2 番地 3 4 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP2024/023017 (72) 発明者: 三澤 裕人(MISAWA, Yuto); 〒2120013
神奈川県川崎市幸区堀川町 7 2 番地 3 4 東芝イン
フラシステムズ株式会社内 Kanagawa (JP).
- (22) 国際出願日: 2024年6月25日(25.06.2024)
- (25) 国際出願の言語: 日本語 (74) 代理人: 弁理士法人 鈴 榮 特 許 綜 合 事 務 所
(SUZUYE & SUZUYE); 〒1050014 東京都港区
芝三丁目 2 3 番 1 号 セレスティン芝三井
ビルディング 1 1 階 Tokyo (JP).
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2023-121905 2023年7月26日(26.07.2023) JP
- (71) 出願人: 株式会社 東芝(KABUSHIKI KAISHA
TOSHIBA) [JP/JP]; 〒1050023 東京都港区芝
浦一丁目 1 番 1 号 Tokyo (JP). 東芝イン
フラシステムズ株式会社(TOSHIBA
INFRASTRUCTURE SYSTEMS & SOLUTIONS
- (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC,
EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,

(54) Title: KEY MANAGEMENT DEVICE, KEY MANAGEMENT SYSTEM, KEY MANAGEMENT METHOD, KEY MANAGEMENT PROGRAM, AND COMPUTER-READABLE STORAGE MEDIUM

(54) 発明の名称: 鍵管理装置、鍵管理システム、鍵管理方法、鍵管理プログラム、およびコンピュータ可読記憶媒体



- 1 Host device
3 Application server
10 Operator office

(57) Abstract: The purpose of the present invention is to specify a user using a PKCS#11-based HSM. A key management device according to an embodiment comprises: a first acquisition unit that acquires pre-authentication information including a user ID, authentication information, and encrypted authentication information; a storage unit that securely stores a

[続葉有]

HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告 (条約第21条(3))

DB key; a first authentication unit that decrypts the encrypted authentication information using the DB key and performs authentication using the decrypted authentication information and the authentication information; a generation unit that generates a ticket associated with the user ID on the basis of an authentication result, and generates a pre-authentication response including the ticket; a first output unit that outputs the pre-authentication response; a second acquisition unit that acquires session information including the ticket; a second authentication unit that authenticates the session information on the basis of the ticket included in the session information and generates a cipher key corresponding to the ticket; and a second output unit that outputs an authentication result from the second authentication unit.

(57) 要約: P K C S # 1 1 ベースの H S M を用いてユーザを特定すること。実施形態に係る鍵管理装置は、ユーザ ID、認証情報、暗号化済み認証情報を含む事前認証情報を取得する第 1 の取得部と、D B 鍵をセキュアに記憶する記憶部と、暗号化済み認証情報に D B 鍵を用いて復号し、復号された認証情報および認証情報を用いて認証する第 1 の認証部と認証結果に基づいて、ユーザ ID に紐付けられたチケットを生成し、チケットを含む事前認証応答を生成する生成部と、事前認証応答を出力する第 1 の出力部と、チケットを含むセッション情報を取得する第 2 の取得部と、セッション情報に含まれるチケットに基づいてセッション情報を認証し、チケットに対応する暗号鍵を生成する第 2 の認証部と、第 2 の認証部による認証結果を出力する第 2 の出力部と、を備える。