(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
2023年3月16日(16.03.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/037530 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)

(21) 国際出願番号： PCT/JP2021/033437

(22) 国際出願日： 2021年9月13日(13.09.2021)

(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：ＧＶＥ株式会社 (**GVE LTD.**) [JP/JP]；〒1030026 東京都中央区日本橋兜町１３番１号 Tokyo (JP).

(72) 発明者：高松　圭太 (**TAKAMATSU Keita**)；〒1030026 東京都中央区日本橋兜町１３番１号 ＧＶＥ株式会社内 Tokyo (JP). 房広治 (**FUSA Koji**)；〒1030026 東京都中央区日本橋兜町１３番１号 ＧＶＥ株式会社内 Tokyo (JP). 日下部 佑 (**KUSAKABE Yu**)；〒1030026 東京都中央区日本橋兜町１３番１号 ＧＶＥ株式会社内 Tokyo (JP).

(74) 代理人：蟹田昌之 (**KANIDA Masayuki**)；〒1006208 東京都千代田区丸の内１－１１－１ パシフィックセンチュリープレイス丸の内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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, MK, MT, NL, NO, PL, PT, RO, RS,

(54) **Title:** DATA MANAGEMENT SYSTEM

(54) 発明の名称： データ管理システム

	暗号鍵 AA	権限 BB
CC	クライアント装置の暗号鍵	電子署名の付与及び検証 DD
EE	データ管理装置の暗号鍵	電子署名の検証 GG
FF	データ保管装置の暗号鍵	電子署名の検証 GG

AA Encryption key
BB Authority
CC Encryption key for client device
DD Imparting and verification of electronic signature
EE Encryption key for data management device
FF Encryption key for data saving device
GG Verification of electronic signature

(57) **Abstract:** This data management system comprises a client device, a first electronic signature device, a data management device, a second electronic signature device, a data saving device, and a third electronic signature device. At least one of the first electronic signature device, the second electronic signature device, and the third electronic signature device stores encryption keys and authorities in association with each other, and can execute only processes according to the authorities, among processes using the encryption keys.

(57) 要約：クライアント装置と、第１電子署名装置と、データ管理装置と、第２電子署名装置と、データ保管装置と、第３電子署名装置と、を備えたデータ管理システムであって、前記第１電子署名装置、前記第２電子署名装置、及び前記第３電子署名のうちの少なくとも１つの電子署名装置は、暗号鍵と権限とを対応付けて記憶し、前記暗号鍵を用いた処理のうち、前記権限に応じた処理のみを実行することができる電子署名装置であるデータ管理システム。

WO 2023/037530 A1

［続葉有］

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)）

明　細　書

発明の名称 ： データ管理システム

技術分野

[0001]　本発明は、データの管理に関する。

背景技術

[0002]　公開鍵方式で電子署名を付与し検証するシステムが提案されている（特許文献１参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開２００８－１４０２９８号公報

発明の概要

発明が解決しようとする課題

[0004]　本発明の一実施形態では、秘密鍵方式で電子署名を付与し検証するデータ管理システムを提供することを目的とする。

課題を解決するための手段

[0005]　本発明は、次の一実施形態を含む。

[0006]　クライアント装置と、第１電子署名装置と、データ管理装置と、第２電子署名装置と、データ保管装置と、第３電子署名装置と、を備えたデータ管理システムであって、前記第１電子署名装置、前記第２電子署名装置、及び前記第３電子署名のうちの少なくとも１つの電子署名装置は、暗号鍵と権限とを対応付けて記憶し、前記暗号鍵を用いた処理のうち、前記権限に応じた処理のみを実行することができる電子署名装置であるデータ管理システム。

発明の効果

[0007]　本発明の一実施形態によれば、秘密鍵方式で電子署名を付与し検証するデータ管理システムを提供することができる。

図面の簡単な説明

[0008] [図1]実施形態１に係るデータ管理システムの構成例を示す図である。

[図2]実施形態１に係るデータ管理システムの動作例を示す図である。

[図3A]第１電子署名装置における鍵と権限の記憶例を示す図である。

[図3B]第２電子署名装置における鍵と権限の記憶例を示す図である。

[図3C]第３電子署名装置における鍵と権限の記憶例を示す図である。

[図4]実施形態２に係るデータ管理システムの構成例を示す図である

発明を実施するための形態

[0009] ［実施形態１に係るデータ管理システム］

図１は、実施形態１に係るデータ管理システムの構成例を示す図である。図１に示すように、実施形態１に係るデータ管理システムは、クライアント装置と、第１電子署名装置と、データ管理装置と、第２電子署名装置と、データ保管装置と、第３電子署名装置と、を備えたデータ管理システムである。以下、各装置について説明する。

[0010] （クライアント装置）

クライアント装置は、各種の要求電文を送信する装置である。クライアント装置の一例には、ラップトップコンピュータ、スマートフォン、タブレット型コンピュータなどが含まれる。要求電文の一例には、パケットや信号などの各種のデータが含まれる。後述する第１要求電文や第２要求電文は要求電文の一例である。第１要求電文はデータ保管装置に対して所定の処理を要求する電文であり、第２要求電文はデータ管理装置に対して所定の処理を要求する電文である。クライアント装置は、第１応答電文及び／又は第２応答電文に基づいて所定の処理を実行する。第１応答電文に基づく所定の処理の一例には取得データ表示やデータ登録結果の表示やこれを確認する処理が含まれる。第２応答電文に基づく所定の処理の一例には第１要求および第２要求処理拒否事由の表示やこれを確認する処理（処理をデータ管理装置またはデータ保管装置に拒否された場合のみ）や電文送受信履歴の保存が含まれる。

[0011] （データ管理装置）

データ管理装置は、クライアント装置から受信した第２要求電文に基づいて所定の処理を実行し、クライアント装置に対して第２応答電文を送信する装置である。データ管理装置が実行する所定の処理の一例にはデータ登録やデータ取得が含まれる。データ管理装置の一例には、サーバコンピュータなどが含まれる。第２応答電文の一例にはデータ登録応答やデータ取得応答が含まれる。

[0012]（データ保管装置）

データ保管装置は、クライアント装置からデータ管理装置を介して受信した第１要求電文に基づいて所定の処理を実行し、データ管理装置を介してクライアント装置に対し第２応答電文を送信する装置である。データ保管装置が実行する所定の処理の一例にはデータ暗号化分散書き込みや分散データ復号読み込みが含まれる。データ保管装置の一例には、分散ストレージサーバ（ＤＳＳ：Ｄｉｓｔｒｉｂｕｔｅ　Ｓｔｏｒａｇｅ　Ｓｅｒｖｅｒ）などが含まれる。第１応答電文の一例にはデータ暗号化分散書き込み応答や分散データ復号読み込み応答が含まれる。

[0013]（第１電子署名装置、第２電子署名装置、第３電子署名装置）

第１電子署名装置、第２電子署名装置、第３電子署名装置は、要求電文や応答電文などの電文に対する電子署名の付与、及びそれら電文に付与された電子署名の検証を行う装置である。第１電子署名装置、第２電子署名装置、第３電子署名装置には、例えば、ＨＳＭ（ハードウェア・セキュリティ・モジュール）などを用いることができる。第１電子署名装置は、クライアント装置に用いられる電子署名装置である。第２電子署名装置は、データ管理装置に用いられる電子署名装置である。第３電子署名装置は、データ保管装置に用いられる電子署名装置である。

[0014] 第１電子署名装置は、ネットワークを介してクライアント装置に接続されていてもよいし、ネットワークを介さずにクライアント装置に接続されていてもよいし、クライアント装置に内蔵されていてもよい。本実施形態では、第１電子署名装置は、ネットワークを介してクライアント装置に接続されて

いるものとする。

[0015] 第２電子署名装置は、ネットワークを介してデータ管理装置に接続されていてもよいし、ネットワークを介さずにデータ管理装置に接続されていてもよいし、データ管理装置に内蔵されていてもよい。本実施形態では、第２電子署名装置は、ネットワークを介さずにデータ管理装置に接続されているものとする。

[0016] 第３電子署名装置は、ネットワークを介してデータ保管装置に接続されていてもよいし、ネットワークを介さずにデータ保管装置に接続されていてもよいし、データ保管装置に内蔵されていてもよい。本実施形態では、第３電子署名装置は、ネットワークを介さずにデータ保管装置に接続されているものとする。

[0017] 図３Ａは第１電子署名装置における鍵と権限の記憶例を示す図である。図３Ｂは第２電子署名装置における鍵と権限の記憶例を示す図である。図３Ｃは第３電子署名装置における鍵と権限の記憶例を示す図である。図３Ａ、図３Ｂ、図３Ｃに示すように、第１電子署名装置、第２電子署名装置、及び第３電子署名装置のうちの少なくとも１つの電子署名装置（本実施形態ではすべての電子署名装置）は、暗号鍵と権限とを対応付けて記憶し、暗号鍵を用いた処理のうち、権限に応じた処理のみを実行することができる電子署名装置である。

[0018] 電子署名装置としては、公開鍵方式に基づいて電子署名の作成・検証を行うものが知られている。

[0019] しかし、公開鍵方式の場合は、公開鍵と秘密鍵があり、公開鍵は非常に長いものとなる（例：２０４８ビット）。

[0020] 他方、秘密鍵方式の場合、秘密鍵（例：２５６ビット）で暗号と検証を行う。このため、秘密鍵方式の場合は、長い公開鍵を使わずに済むため、電子署名の作成・付与や検証の時間を短縮できる。ただし、秘密鍵方式を採用する場合は、複数の電子署名装置の間で暗号鍵（秘密鍵）を共有しなければならない。このため、ある暗号鍵で作成された電子署名の検証だけしか行なわ

ない電子署名装置であっても、その暗号鍵を用いて電子署名の作成までできてしまうことになり、セキュリティ上の問題がある。例えば、上記の例でいうと、第１電子署名装置は、クライアント装置の暗号鍵に加えて、データ管理装置やデータ保管装置の暗号鍵も所有することになる。しかし、第１電子署名装置において、データ管理装置やデータ保管装置の暗号鍵は、電子署名の検証に用いられるに過ぎない。にもかかわらず、第１電子署名装置は、データ管理装置やデータ保管装置の暗号鍵を用いて、電子署名を作成できてしまう。換言すると、クライアント装置は、第１電子署名装置を用いて、データ管理装置やデータ保管装置になりすますことができてしまう。

[0021] そこで、本実施形態では、第１電子署名装置、第２電子署名装置、及び第３電子署名装置が秘密鍵方式を採用し、暗号鍵（秘密鍵）がこれら電子署名装置の間で共有されるものとする。ただし、本実施形態では、セキュリティ上の問題が生じないように、共有される複数の暗号鍵（秘密鍵）に権限が付与されるものとし、第１電子署名装置、第２電子署名装置、及び第３電子署名装置は、複数の暗号鍵（秘密鍵）それぞれをその権限に応じた処理でしか使用できないものとする。このようにすれば、セキュリティを確保ししつつ、電子署名の作成・付与や検証の時間を短縮できる。例えば、第１電子署名装置であれば、図３Ａに示すように、クライアント装置の暗号鍵だけでなく、データ管理装置やデータ保管装置の暗号鍵を有している。しかし、クライアント装置の暗号鍵に対しては付与及び検証の権限が与えられており、その他の装置の暗号鍵に対しては検証の権限のみが与えられているものとする。このようにすれば、第１電子署名装置は、クライアント装置の暗号鍵を用いては、電子署名の付与及び検証の双方を実行できるが、他の装置の暗号鍵を用いては、電子署名の検証しか実行できない。

[0022] 本実施形態では、セキュリティを十分に確保すべく、第１電子署名装置、第２電子署名装置、及び第３電子署名装置が、いずれも、暗号鍵と権限とを対応付けて記憶し、暗号鍵を用いた処理のうち、権限に応じた処理のみを実行することができる電子署名装置であるものとする。

[0023] 暗号鍵のビット数は例えば１２８や２５６である。暗号鍵は電子署名の付与と検証の双方に用いられる。電子署名の付与や検証にはＡＥＳ方式やその他の方式を用いることができる。

[0024] 権限の一例には、「電子署名の付与及び検証を行うことができる」、「電子署名の検証のみ行うことができる」などが含まれるが、その他、「電子署名の付与を所定の場合にのみ行うことができる」、「電子署名の検証を所定の場合にのみ行うことができる」、「電子署名の検証は何時でも行うことができるが、電子署名の付与は所定の場合にのみ行うことができる」などが含まれる。

[0025] （動作例）

図２は、実施形態１に係るデータ管理システムの動作例を示す図である。以下、図２を参照しつつ、実施形態１に係るデータ管理システムの動作例を説明する。なお、本明細書では、電子署名を「付与する」ことを、電子署名を「付す」ということがある。

[0026] （ステップ１）

まず、クライアント装置が、第１要求電文を作成する。

[0027] （ステップ２）

次に、クライアント装置が、第１電子署名装置に対し、第１要求電文を送信する。

[0028] （ステップ３）

次に、第１電子署名装置は、第１要求電文にクライアント装置の暗号鍵を用いて電子署名を付し、クライアント装置に対し、電子署名が付された第１要求電文を送信する。

[0029] （ステップ４）

次に、クライアント装置は、電子署名が付された第１要求電文を含む第２要求電文を作成する。

[0030] （ステップ５）

次に、クライアント装置は、第１電子署名装置に対し、第２要求電文を送

信する。

[0031]（ステップ６）

次に、第１電子署名装置は、第２要求電文にクライアント装置の暗号鍵を用いて電子署名を付し、クライアント装置に対し、電子署名が付された第２要求電文を送信する。

[0032]（ステップ７）

次に、クライアント装置は、データ管理装置に対し、電子署名が付された第２要求電文を送信する。

[0033]（ステップ８）

次に、データ管理装置は、第２電子署名装置に対し、電子署名が付された第２要求電文を送信する。

[0034]（ステップ９）

次に、第２電子署名装置は、第２要求電文に付されている電子署名をクライアント装置の暗号鍵を用いて検証し、データ管理装置に対し、検証の結果を送信する。

[0035]（ステップ１０）

次に、データ管理装置は、第２電子署名装置による検証の結果に基づいて、データ保管装置に対し、電子署名が付された第１要求電文を送信する。

[0036]（ステップ１１）

次に、データ保管装置は、第３電子署名装置に対し、電子署名が付された第１要求電文を送信する。

[0037]（ステップ１２）

次に、第３電子署名装置は、第１要求電文に付されている電子署名をクライアント装置の暗号鍵を用いて検証し、データ保管装置に対し、検証の結果を送信する。

[0038]（ステップ１３）

次に、データ保管装置は、第３電子署名装置による検証の結果に基づいて、第１要求電文に応じた処理を実行する。

[0039] （ステップ１４）

次に、データ保管装置は、第１応答電文を作成する。

[0040] （ステップ１５）

次に、データ保管装置は、第３電子署名装置に対して、第１応答電文を送信する。

[0041] （ステップ１６）

次に、第３電子署名装置は、第１応答電文にデータ保管装置の暗号鍵を用いて電子署名を付し、データ保管装置に対して、電子署名が付された第１応答電文を送信する。

[0042] （ステップ１７）

次に、データ保管装置は、データ管理装置に対して、電子署名が付された第１応答電文を送信する。

[0043] （ステップ１８）

次に、データ管理装置は、第２要求電文に応じた処理を実行する。

[0044] （ステップ１９）

次に、データ管理装置は、電子署名が付された第１応答電文を含む第２応答電文を作成する。

[0045] （ステップ２０）

次に、データ管理装置は、第２電子署名装置に対して、第２応答電文を送信する。

[0046] （ステップ２１）

次に、第２電子署名装置は、第２応答電文にデータ管理装置の暗号鍵を用いて電子署名を付し、データ管理装置に対し、電子署名が付された第２応答電文を送信する。

[0047] （ステップ２２）

次に、データ管理装置は、クライアント装置に対し、電子署名が付された第２応答電文を送信する。

[0048] （ステップ２３）

次に、クライアント装置は、第１電子署名装置に対し、電子署名が付された第２応答電文を送信する。

[0049]（ステップ２４）

次に、第１電子署名装置は、第２応答電文に付されている電子署名をデータ管理装置の暗号鍵を用いて検証し、クライアント装置に対して、その検証の結果を送信する。

[0050]（ステップ２５）

次に、クライアント装置は、第１電子署名装置に対し、電子署名が付された第１応答電文を送信する。

[0051]（ステップ２６）

次に、第１電子署名装置は、第１応答電文に付されている電子署名をデータ保管装置の暗号鍵を用いて検証し、クライアント装置に対して、その検証の結果を送信する。

[0052]（ステップ２７）

次に、クライアント装置は、検証の結果に基づいて、所定の処理を実行する。

[0053] 以上説明した実施形態１によれば、秘密鍵方式（複数の電子署名装置の間で暗号鍵が共有される方式）で電子署名を付与し検証するデータ管理システムを提供することができる。また、実施形態１によれば、複数の電子署名装置の間で暗号鍵が共有されるにもかかわらず、ある装置（例：クライアント装置）が他の装置（例：データ管理装置やデータ保管装置）になりすることが防止されたセキュリティの高いデータ管理システムを提供することができる。また、暗号鍵に対応付ける権限として様々な条件を設定することにより、クライアント装置やデータ管理装置やデータ保管装置は、データ管理システム上で許容された電子署名の付与や検証のみを利用するものとなり、秘密鍵方式（複数の電子署名装置の間で暗号鍵が共有される方式）でありながらも、厳格に管理された電子署名の運用が可能となる。

[0054]［実施形態２に係るデータ管理システム］

図４は、実施形態２に係るデータ管理システムの構成例を示す図である。図４に示すように、実施形態２に係るデータ管理システムは、鍵管理装置が第１電子署名装置、第２電子署名装置、及び第３電子署名装置に接続されている点で、実施形態１に係るデータ管理システムと相違する。上記のとおり、第１電子署名装置、第２電子署名装置、及び第３電子署名装置においては、クライアント装置、データ管理装置、及びデータ保管装置の暗号鍵が共有されている。鍵管理装置は、これら共有される暗号鍵に異なる権限を対応付けて各電子署名装置に対して設定する装置である。このようにすれば例えば一つの装置が新規に署名鍵を追加した際に、他の装置にその署名鍵から作成された署名を検証するための適切な権限を持つ鍵を配布することができる。鍵管理装置は、ネットワークを介して第１電子署名装置、第２電子署名装置、及び第３電子署名装置に接続されていてもよいし、ネットワークを介さずに第１電子署名装置、第２電子署名装置、及び第３電子署名装置に接続されていてもよい。本実施形態では、鍵管理装置が、ネットワークを介さずに第１電子署名装置、第２電子署名装置、及び第３電子署名装置に接続されているものとする。

[0055] 以下、実施形態１、２を用いたデータ管理システムの一例を説明する。

実施例 1

[0056] 実施形態１、２に係るデータ管理システムは、例えば、ワクチンの接種証明書（例：ワクチンパスポート）の管理に用いることができる。この場合、例えば、クライアント装置の一例には、病院、ワクチンを接種した者、空港の税関、遊園地、飲食店などにより使用される装置が含まれる。病院は、病院が管理する装置を用いて、データ保管装置にワクチンの接種証明書を保管する。また、ワクチンを接種した者、空港の税関、遊園地、飲食店などは、それぞれの者が管理する装置を用いて、データ保管装置に保管されているワクチンの接種証明証をクライアント装置の画面に表示したり印刷したりできる。

実施例 2

[0057] 実施形態１、２に係るデータ管理システムは、例えば、不動産登記に用いることができる。この場合、例えば、クライアント装置の一例には、登記局、法人、個人、金融機関などにより使用される装置が含まれる。登記局は、自己の装置を用いて、不動産登記に関するデータをデータ保管装置に保管する。また、法人、個人、金融機関などは、それぞれの者が管理する装置を用いて、データ保管装置に保管されている不動産登記に関するデータをクライアント装置の画面に表示したり印刷したりできる。

実施例 3

[0058] 実施形態１、２に係るデータ管理システムは、例えば、会社登記に用いることができる。この場合、例えば、クライアント装置は、登記局、法人、個人、金融機関などに用いられる。登記局は、クライアント装置を用いて、会社登記に関するデータをデータ保管装置に保管する。また、法人、個人、金融機関などは、クライアント装置を用いて、データ保管装置に保管されている会社登記に関するデータをクライアント装置の画面に表示したり印刷したりできる。

[0059] 以上、実施例について説明したが、実施形態１、２に係るデータ保管システムは、その他様々なデータの保管に用いることができる。

[0060] 以上、実施形態について説明したが、これらの説明によって本発明は何ら限定されるものではない。

請求の範囲

[請求項1] クライアント装置と、第１電子署名装置と、データ管理装置と、第２電子署名装置と、データ保管装置と、第３電子署名装置と、を備えたデータ管理システムであって、

前記クライアント装置は、第１要求電文を作成し、

前記クライアント装置は、前記第１電子署名装置に対し、前記第１要求電文を送信し、

前記第１電子署名装置は、前記第１要求電文に前記クライアント装置の暗号鍵を用いて電子署名を付し、前記クライアント装置に対し、前記電子署名が付された前記第１要求電文を送信し、

前記クライアント装置は、前記電子署名が付された前記第１要求電文を含む第２要求電文を作成し、

前記クライアント装置は、前記第１電子署名装置に対し、前記第２要求電文を送信し、

前記第１電子署名装置は、前記第２要求電文に前記クライアント装置の暗号鍵を用いて電子署名を付し、前記クライアント装置に対し、前記電子署名が付された前記第２要求電文を送信し、

前記クライアント装置は、前記データ管理装置に対し、前記電子署名が付された前記第２要求電文を送信し、

前記データ管理装置は、前記第２電子署名装置に対し、前記電子署名が付された前記第２要求電文を送信し、

前記第２電子署名装置は、前記第２要求電文に付されている電子署名を前記クライアント装置の暗号鍵を用いて検証し、前記データ管理装置に対し、前記検証の結果を送信し、

前記データ管理装置は、前記第２電子署名装置による検証の結果に基づいて、前記データ保管装置に対し、前記電子署名が付された前記第１要求電文を送信し、

前記データ保管装置は、前記第３電子署名装置に対し、前記電子署

名が付された前記第１要求電文を送信し、

前記第３電子署名装置は、前記第１要求電文に付されている電子署名を前記クライアント装置の暗号鍵を用いて検証し、前記データ保管装置に対し、前記検証の結果を送信し、

前記データ保管装置は、前記第３電子署名装置による検証の結果に基づいて、前記第１要求電文に応じた処理を実行し、第１応答電文を作成し、前記第３電子署名装置に対して、前記第１応答電文を送信し、

前記第３電子署名装置は、前記第１応答電文に前記データ保管装置の暗号鍵を用いて電子署名を付し、前記データ保管装置に対して、前記電子署名が付された前記第１応答電文を送信し、

前記データ保管装置は、前記データ管理装置に対して、前記電子署名が付された前記第１応答電文を送信し、

前記データ管理装置は、前記第２要求電文に応じた処理を実行し、前記電子署名が付された前記第１応答電文を含む第２応答電文を作成し、前記第２電子署名装置に対して、前記第２応答電文を送信し、

前記第２電子署名装置は、前記第２応答電文に前記データ管理装置の暗号鍵を用いて電子署名を付し、前記データ管理装置に対し、前記電子署名が付された前記第２応答電文を送信し、

前記データ管理装置は、前記クライアント装置に対し、前記電子署名が付された前記第２応答電文を送信し、

前記クライアント装置は、前記第１電子署名装置に対し、前記電子署名が付された前記第２応答電文を送信し、

前記第１電子署名装置は、前記第２応答電文に付されている電子署名を前記データ管理装置の暗号鍵を用いて検証し、前記クライアント装置に対して、その検証の結果を送信し、

前記クライアント装置は、前記第１電子署名装置に対し、前記電子署名が付された前記第１応答電文を送信し、

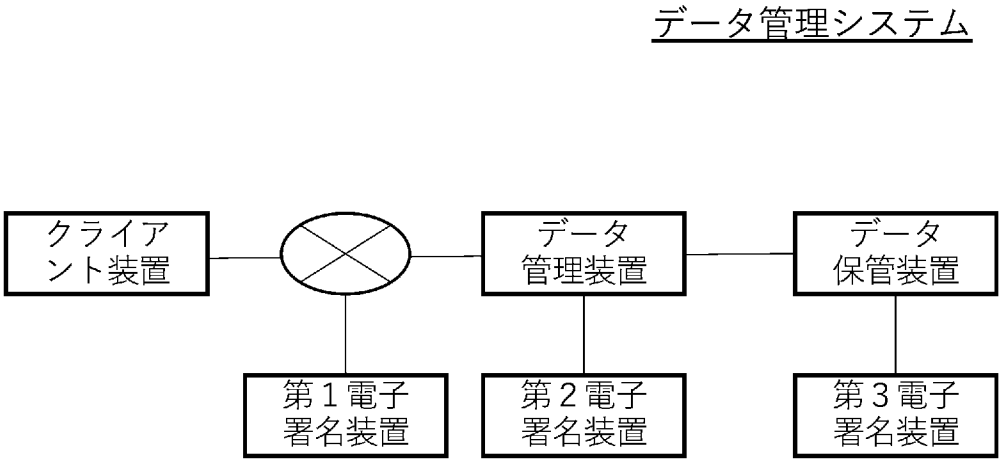
前記第１電子署名装置は、前記第１応答電文に付されている電子署名を前記データ保管装置の暗号鍵を用いて検証し、前記クライアント装置に対して、その検証の結果を送信し、

前記クライアント装置は、前記第１電子署名装置による検証の結果に基づいて、所定の処理を実行するデータ管理システム。

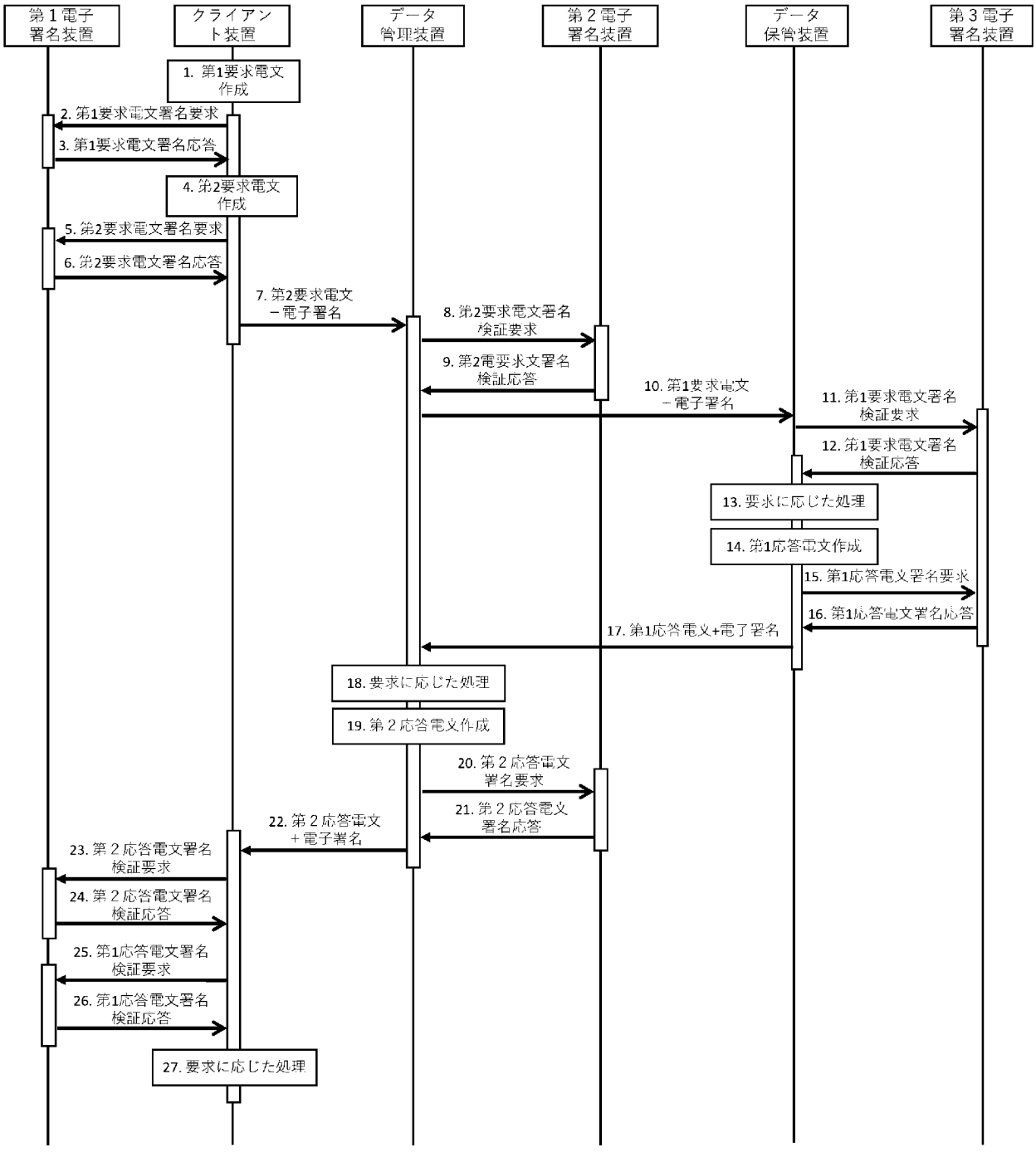
[請求項2] 請求項１に記載のデータ管理システムであって、

前記第１電子署名装置、前記第２電子署名装置、及び前記第３電子署名のうちの少なくとも１つの電子署名装置は、暗号鍵と権限とを対応付けて記憶し、前記暗号鍵を用いた処理のうち、前記権限に応じた処理のみを実行することができる電子署名装置であるデータ管理システム。

[図1]


データ管理システム
クライアント装置
データ管理装置
データ保管装置
第１電子署名装置
第２電子署名装置
第３電子署名装置

[図2]


第１電子署名装置
クライアント装置
データ管理装置
第２電子署名装置
データ保管装置
第３電子署名装置
1. 第1要求電文作成
2. 第1要求電文署名要求
3. 第1要求電文署名応答
4. 第2要求電文作成
5. 第2要求電文署名要求
6. 第2要求電文署名応答
7. 第2要求電文－電子署名
8. 第2要求電文署名検証要求
9. 第2電要求文署名検証応答
10. 第1要求電文－電子署名
11. 第1要求電文署名検証要求
12. 第1要求電文署名検証応答
13. 要求に応じた処理
14. 第1応答電文作成
15. 第1応答電文署名要求
16. 第1応答電文署名応答
17. 第1応答電文+電了署名
18. 要求に応じた処理
19. 第２応答電文作成
20. 第２応答電文署名要求
21. 第２応答電文署名応答
22. 第２応答電文＋電子署名
23. 第２応答電文署名検証要求
24. 第２応答電文署名検証応答
25. 第1応答電文署名検証要求
26. 第1応答電文署名検証応答
27. 要求に応じた処理

[図3A]

暗号鍵	権限
クライアント装置の暗号鍵	電子署名の付与及び検証
データ管理装置の暗号鍵	電子署名の検証
データ保管装置の暗号鍵	電子署名の検証

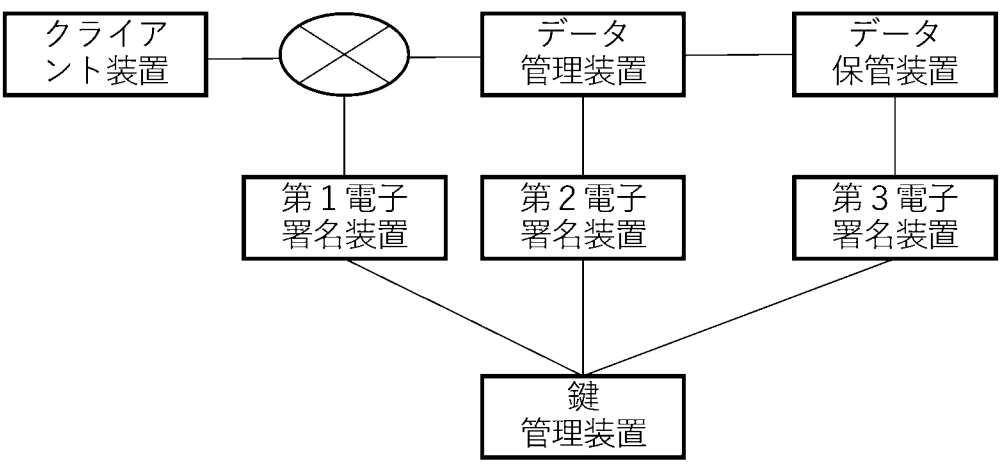
[図3B]

暗号鍵	権限
クライアント装置の暗号鍵	電子署名の検証
データ管理装置の暗号鍵	電子署名の付与及び検証
データ保管装置の暗号鍵	電子署名の検証

[図3C]

暗号鍵	権限
クライアント装置の暗号鍵	電子署名の検証
データ管理装置の暗号鍵	電子署名の検証
データ保管装置の暗号鍵	電子署名の付与及び検証

[図4]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/033437

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i
FI: H04L9/32 200A

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2021
Registered utility model specifications of Japan 1996-2021
Published registered utility model applications of Japan 1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2019-500799 A (SONY CORP.) 10 January 2019 (2019-01-10) paragraphs [0030]-[0058], fig. 1-4	1-2
A	JP 2002-247031 A (FUJITSU LTD.) 30 August 2002 (2002-08-30) paragraph [0020]	2

☐ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 November 2021	**07 December 2021**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/033437

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2019-500799 A	10 January 2019	US 2019/0020661 A1 paragraphs [0046]-[0066], fig. 1-4 WO 2017/107976 A1 EP 3396576 A1 CN 106911641 A CA 3009567 A1 KR 10-2018-0095896 A CN 108541318 A	
JP 2002-247031 A	30 August 2002	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2021/033437

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/32(2006.01)i
FI: H04L9/32 200A

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2019-500799 A (ソニー株式会社) 10.01.2019 (2019-01-10) 段落[0030]-[0058], 図1-4	1-2
A	JP 2002-247031 A (富士通株式会社) 30.08.2002 (2002-08-30) 段落[0020]	2

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
“O” 口頭による開示、使用、展示等に言及する文献
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
26.11.2021	07.12.2021

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
田名網　忠雄 5S 6306
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2021/033437

引用文献	公表日	パテントファミリー文献	公表日
JP 2019-500799 A	10.01.2019	US 2019/0020661 A1 段落[0046]-[0066], 図1-4 WO 2017/107976 A1 EP 3396576 A1 CN 106911641 A CA 3009567 A1 KR 10-2018-0095896 A CN 108541318 A	
JP 2002-247031 A	30.08.2002	（ファミリーなし）	