明　細　書

発明の名称 ： 認証システムおよび認証プログラム

技術分野

[0001] 本発明は、認証連携のための技術に関するものである。

背景技術

[0002] ＰＫＩ認証によって複数の組織のサービスを利用する場合、各組織のユーザは、利用する端末の数だけクライアント証明書を発行してもらう必要がある。そのため、利便性に欠けていた。ＰＫＩはＰｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅの略称である。

[0003] 特許文献１は、複数のクライアント証明書を用いない方法を開示している。

この方法では、認証連携装置が、サービス提供装置に対して、証明書がインストールされている端末のユーザを提示する。これにより、ユーザは１つの個人認証情報で複数の端末を利用することが可能である。例えば、個人認証情報は、ＩＤ（ｉｄｅｎｔｉｆｉｅｒ）とパスワードとの組、または、秘密鍵と公開鍵との組である。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１１－２３８０８３号公報

発明の概要

発明が解決しようとする課題

[0005] 特許文献１に開示された方法では、ユーザ認証とは別に機器認証を行う必要がある。また、機器認証のために機器認証装置が必要である。さらに、機器認証のためにデバイス鍵または電子証明書などを機器と機器認証装置とに保存する必要がある。つまり、新たな機器を追加する場合には、デバイス鍵または電子証明書などを新たな機器に保存する作業が発生するため、手間がかかる。

[0006] 本発明は、機器認証のためにデバイス鍵または電子証明書などをユーザ端末（機器の一例）に保存しなくても、ユーザがユーザ端末から他組織のサービスにアクセスした場合にユーザの認証を行えるようにすることを目的とする。

課題を解決するための手段

[0007] 本発明の認証システムは、第１ユーザが属する第１組織の認証システムである。

前記認証システムは、

前記第１ユーザが前記第１組織のユーザ端末から他組織のサービスにアクセスした場合に他組織システムからハローメッセージを受信し、前記第１ユーザのクライアント秘密鍵を用いて前記ハローメッセージを暗号化し、暗号化されたハローメッセージを署名メッセージとして前記他組織システムに送信する代理証明部を備える。

発明の効果

[0008] 本発明によれば、機器認証のためにデバイス鍵または電子証明書などをユーザ端末（機器の一例）に保存しなくても、ユーザがユーザ端末から他組織のサービスにアクセスした場合にユーザの認証を行うことが可能になる。

図面の簡単な説明

[0009] [図1]実施の形態１における認証連携システム１００の構成図。

[図2]実施の形態１における組織システム１１０の構成図。

[図3]実施の形態１におけるユーザ端末１３０の構成図。

[図4]実施の形態１におけるサーバ装置１４０の構成図。

[図5]実施の形態１における認証システム１２０の構成図。

[図6]実施の形態１における管理装置２００の構成図。

[図7]実施の形態１における認証装置３００の構成図。

[図8]実施の形態１における認証局装置４００の構成図。

[図9]実施の形態１における登録処理のフローチャート。

[図10]実施の形態１におけるトランザクションデータ１２１を示す図。

[図11]実施の形態１における発行処理のフローチャート。

[図12]実施の形態１における発行処理のフローチャート。

[図13]実施の形態１におけるトランザクションデータ１２２を示す図。

[図14]実施の形態１における検証処理（Ｓ２１０）のフローチャート。

[図15]実施の形態１における代理証明処理のフローチャート。

[図16]実施の形態１における代理証明処理のフローチャート。

[図17]実施の形態１におけるログアウト処理のフローチャート。

[図18]実施の形態１におけるトランザクションデータ１２３を示す図。

[図19]実施の形態２における認証局装置４００の構成図。

[図20]実施の形態２における検証処理（Ｓ２１０）のフローチャート。

[図21]実施の形態３における認証連携システム１００の構成図。

[図22]各実施の形態における管理装置２００のハードウェア構成図。

[図23]各実施の形態における認証装置３００のハードウェア構成図。

[図24]各実施の形態における認証局装置４００のハードウェア構成図。

発明を実施するための形態

[0010] 実施の形態および図面において、同じ要素および対応する要素には同じ符号を付している。同じ符号が付された要素の説明は適宜に省略または簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。

[0011] 実施の形態１．

認証連携システム１００について、図１から図１８に基づいて説明する。

[0012] ＊＊＊構成の説明＊＊＊

図１に基づいて、認証連携システム１００の構成を説明する。

認証連携システム１００は、複数の組織システムを備える。

複数の組織システムは、インターネット１０１を介して互いに通信する。インターネット１０１は、ネットワークの一例である。

組織システムは、組織におけるコンピュータシステムである。

[0013] 実施の形態１において、認証連携システム１００は、第１組織システム１１０Ａと第２組織システム１１０Ｂと第３組織システム１１０Ｃとを備える

。

第１組織システム１１０Ａは、第１組織のコンピュータシステムである。

第２組織システム１１０Ｂは、第２組織のコンピュータシステムである。

第３組織システム１１０Ｃは、第３組織のコンピュータシステムである。

組織システムは、２つであってもよいし、４つ以上であってもよい。

[0014] 組織システムを特定しない場合、それぞれを組織システム１１０と称する。

[0015] 図２に基づいて、組織システム１１０の構成を説明する。

組織システム１１０は、認証システム１２０とユーザ端末群１３０Ｇとサーバ装置群１４０Ｇとゲートウェイ装置１１２とを備える。

認証システム１２０とユーザ端末群１３０Ｇとサーバ装置群１４０Ｇとゲートウェイ装置１１２とは、イントラネット１１１を介して互いに通信する。イントラネット１１１はネットワークの一例である。

認証システム１２０とユーザ端末群１３０Ｇとサーバ装置群１４０Ｇとは、イントラネット１１１とゲートウェイ装置１１２とインターネット１０１とを介して、他の組織システム１１０と通信する。

[0016] ユーザ端末群１３０Ｇは、１台以上のユーザ端末である。

ユーザ端末を特定しない場合、それぞれをユーザ端末１３０と称する。

[0017] サーバ装置群１４０Ｇは、１台以上のサーバ装置である。サーバ装置はサービスを提供する装置である。サーバ装置はアプリケーションサーバまたはサービス提供装置とも呼ばれる。

サーバ装置を特定しない場合、それぞれをサーバ装置１４０と称する。

[0018] 図３に基づいて、ユーザ端末１３０の構成を説明する。

ユーザ端末１３０は、プロセッサ１３１Ａとメモリ１３１Ｂと補助記憶装置１３１Ｃと通信装置１３１Ｄと入出力インタフェース１３１Ｅといったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0019] プロセッサ１３１Ａは、演算処理を行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃ

ｉｒｃｕｉｔ）であり、他のハードウェアを制御する。例えば、プロセッサ１３１Ａは、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）、またはＧＰＵ（Ｇｒａｐｈｉｃｓ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。プロセッサ１３１Ａはブラウザ部１３２の機能を実現する。

メモリ１３１Ｂは揮発性の記憶装置である。メモリ１３１Ｂは、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ１３１ＢはＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）である。メモリ１３１Ｂに記憶されたデータは必要に応じて補助記憶装置１３１Ｃに保存される。

補助記憶装置１３１Ｃは不揮発性の記憶装置である。例えば、補助記憶装置１３１Ｃは、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、またはフラッシュメモリである。補助記憶装置１３１Ｃに記憶されたデータは必要に応じてメモリ１３１Ｂにロードされる。

通信装置１３１Ｄはレシーバ及びトランスミッタである。例えば、通信装置１３１Ｄは通信チップまたはＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　認証局ｒｄ）である。

入出力インタフェース１３１Ｅは入力装置および出力装置が接続されるポートである。例えば、入出力インタフェース１３１ＥはＵＳＢ端子であり、入力装置はキーボードおよびマウスであり、出力装置はディスプレイである。ＵＳＢはＵｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓの略称である。

[0020] 図４に基づいて、サーバ装置１４０の構成を説明する。

サーバ装置１４０は、プロセッサ１４１Ａとメモリ１４１Ｂと補助記憶装置１４１Ｃと通信装置１４１Ｄといったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0021] プロセッサ１４１Ａは、演算処理を行うＩＣであり、他のハードウェアを制御する。例えば、プロセッサ１４１Ａは、ＣＰＵ、ＤＳＰ、またはＧＰＵである。プロセッサ１４１Ａはアプリケーション部１４２の機能を実現する

。

メモリ１４１Ｂは揮発性の記憶装置である。メモリ１４１Ｂは、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ１４１ＢはＲＡＭである。メモリ１４１Ｂに記憶されたデータは必要に応じて補助記憶装置１４１Ｃに保存される。

補助記憶装置１４１Ｃは不揮発性の記憶装置である。例えば、補助記憶装置１４１Ｃは、ＲＯＭ、ＨＤＤ、またはフラッシュメモリである。補助記憶装置１４１Ｃに記憶されたデータは必要に応じてメモリ１４１Ｂにロードされる。

通信装置１４１Ｄはレシーバ及びトランスミッタである。例えば、通信装置１４１Ｄは通信チップまたはＮＩＣである。

[0022] 図５に基づいて、認証システム１２０の構成を説明する。

認証システム１２０は、管理装置２００と認証装置３００と認証局装置４００とを備える。

認証装置３００は、イントラネット１１１を介して、管理装置２００と認証局装置４００と通信する。

[0023] 図６に基づいて、管理装置２００の構成を説明する。

管理装置２００は、プロセッサ２０１とメモリ２０２と補助記憶装置２０３と通信装置２０４といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0024] プロセッサ２０１は、演算処理を行うＩＣであり、他のハードウェアを制御する。例えば、プロセッサ２０１は、ＣＰＵ、ＤＳＰ、またはＧＰＵである。

メモリ２０２は揮発性の記憶装置である。メモリ２０２は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ２０２はＲＡＭである。メモリ２０２に記憶されたデータは必要に応じて補助記憶装置２０３に保存される。

補助記憶装置２０３は不揮発性の記憶装置である。例えば、補助記憶装置

２０３は、ＲＯＭ、ＨＤＤ、またはフラッシュメモリである。補助記憶装置２０３に記憶されたデータは必要に応じてメモリ２０２にロードされる。

通信装置２０４はレシーバ及びトランスミッタである。例えば、通信装置２０４は通信チップまたはＮＩＣである。

[0025] 管理装置２００は、トランザクション発行部２１１とトランザクション受付部２１２と証明書検証部２１３とブロックチェーン管理部２１４とトランザクション検証部２１５といった要素を備える。これらの要素はソフトウェアで実現される。

[0026] 補助記憶装置２０３には、トランザクション発行部２１１とトランザクション受付部２１２と証明書検証部２１３とブロックチェーン管理部２１４とトランザクション検証部２１５としてコンピュータを機能させるためのプログラムが記憶されている。プログラムは、メモリ２０２にロードされて、プロセッサ２０１によって実行される。

さらに、補助記憶装置２０３にはＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）が記憶されている。ＯＳの少なくとも一部は、メモリ２０２にロードされて、プロセッサ２０１によって実行される。

つまり、プロセッサ２０１は、ＯＳを実行しながら、プログラムを実行する。

プログラムを実行して得られるデータは、メモリ２０２、補助記憶装置２０３、プロセッサ２０１内のレジスタまたはプロセッサ２０１内のキャッシュメモリといった記憶装置に記憶される。

[0027] メモリ２０２はブロックチェーン記憶部２９０として機能する。但し、他の記憶装置が、メモリ２０２の代わりに、又は、メモリ２０２と共に、ブロックチェーン記憶部２９０として機能してもよい。

[0028] 管理装置２００は、プロセッサ２０１を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ２０１の役割を分担する。

[0029] プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータで読み取り可能に記録（格納）することができる。

[0030] 図７に基づいて、認証装置３００の構成を説明する。

認証装置３００は、プロセッサ３０１とメモリ３０２と補助記憶装置３０３と通信装置３０４といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0031] プロセッサ３０１は、演算処理を行うＩＣであり、他のハードウェアを制御する。例えば、プロセッサ３０１はＣＰＵ、ＤＳＰまたはＧＰＵである。

メモリ３０２は揮発性の記憶装置である。メモリ３０２は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ３０２はＲＡＭである。メモリ３０２に記憶されたデータは必要に応じて補助記憶装置３０３に保存される。

補助記憶装置３０３は不揮発性の記憶装置である。例えば、補助記憶装置３０３は、ＲＯＭ、ＨＤＤまたはフラッシュメモリである。補助記憶装置３０３に記憶されたデータは必要に応じてメモリ３０２にロードされる。

通信装置３０４はレシーバ及びトランスミッタである。例えば、通信装置３０４は通信チップまたはＮＩＣである。

[0032] 認証装置３００は、認証部３１１と代理証明部３１２とログアウト受付部３１３といった要素を備える。これらの要素はソフトウェアで実現される。

[0033] 補助記憶装置３０３には、認証部３１１と代理証明部３１２とログアウト受付部３１３としてコンピュータを機能させるためのプログラムが記憶されている。プログラムは、メモリ３０２にロードされて、プロセッサ３０１によって実行される。

さらに、補助記憶装置３０３にはＯＳが記憶されている。ＯＳの少なくとも一部は、メモリ３０２にロードされて、プロセッサ３０１によって実行される。

つまり、プロセッサ３０１は、ＯＳを実行しながら、プログラムを実行する。

プログラムを実行して得られるデータは、メモリ３０２、補助記憶装置３０３、プロセッサ３０１内のレジスタまたはプロセッサ３０１内のキャッシ

ュメモリといった記憶装置に記憶される。

[0034] メモリ３０２は認証情報記憶部３９１とクライアント秘密鍵記憶部３９２として機能する。但し、他の記憶装置が、メモリ３０２の代わりに、又は、メモリ３０２と共に、認証情報記憶部３９１とクライアント秘密鍵記憶部３９２として機能してもよい。

[0035] 認証装置３００は、プロセッサ３０１を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ３０１の役割を分担する。

[0036] プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータで読み取り可能に記録（格納）することができる。

[0037] 図８に基づいて、認証局装置４００の構成を説明する。

認証局装置４００は、プロセッサ４０１とメモリ４０２と補助記憶装置４０３と通信装置４０４といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0038] プロセッサ４０１は、演算処理を行うＩＣであり、他のハードウェアを制御する。例えば、プロセッサ４０１はＣＰＵ、ＤＳＰまたはＧＰＵである。

メモリ４０２は揮発性の記憶装置である。メモリ４０２は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ４０２はＲＡＭである。メモリ４０２に記憶されたデータは必要に応じて補助記憶装置４０３に保存される。

補助記憶装置４０３は不揮発性の記憶装置である。例えば、補助記憶装置４０３は、ＲＯＭ、ＨＤＤまたはフラッシュメモリである。補助記憶装置４０３に記憶されたデータは必要に応じてメモリ４０２にロードされる。

通信装置４０４はレシーバ及びトランスミッタである。例えば、通信装置４０４は通信チップまたはＮＩＣである。

[0039] 認証局装置４００は、秘密鍵生成部４１１と証明書生成部４１２といった要素を備える。これらの要素はソフトウェアで実現される。

[0040] 補助記憶装置４０３には、秘密鍵生成部４１１と証明書生成部４１２としてコンピュータを機能させるためのプログラムが記憶されている。プログラ

ムは、メモリ４０２にロードされて、プロセッサ４０１によって実行される。

さらに、補助記憶装置４０３にはＯＳが記憶されている。ＯＳの少なくとも一部は、メモリ４０２にロードされて、プロセッサ４０１によって実行される。

つまり、プロセッサ４０１は、ＯＳを実行しながら、プログラムを実行する。

プログラムを実行して得られるデータは、メモリ４０２、補助記憶装置４０３、プロセッサ４０１内のレジスタまたはプロセッサ４０１内のキャッシュメモリといった記憶装置に記憶される。

[0041] メモリ４０２は認証局秘密鍵記憶部４９０として機能する。但し、他の記憶装置が、メモリ４０２の代わりに、又は、メモリ４０２と共に、認証局秘密鍵記憶部４９０として機能してもよい。

[0042] 認証局装置４００は、プロセッサ４０１を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ４０１の役割を分担する。

[0043] プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータで読み取り可能に記録（格納）することができる。

[0044] ＊＊＊動作の説明＊＊＊

認証連携システム１００の動作は認証連携方法に相当する。

認証システム１２０の動作は認証方法に相当する。また、認証方法の手順は認証プログラムの手順に相当する。

認証プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータで読み取り可能に記録（格納）することができる。

[0045] 認証連携方法および認証方法について、以下の事項を説明する。

（１）ブロックチェーンの構築

（２）ブロックチェーンへの参加

（３）認証局証明書の登録

（４）クライアント証明書の発行

（５）ユーザの代理証明

（６）ユーザのログアウト

[0046] 実施の形態において、ＢＣはブロックチェーンを意味し、ＣＡは認証局を意味し、ＣＬはクライアントを意味する。また、署名は電子署名を意味する。

[0047] まず、（１）ブロックチェーンの構築について説明する。

認証連携システム１００において、認証局証明書ブロックチェーン、クライアント証明書ブロックチェーンおよび失効リストブロックチェーンが構築される。

認証局証明書ブロックチェーンは、認証局証明書用のブロックチェーンである。

クライアント証明書ブロックチェーンは、クライアント証明書用のブロックチェーンである。

失効リストブロックチェーンは、失効リスト用のブロックチェーンである。失効リストは、失効されたクライアント証明書のリストである。

[0048] それぞれの認証システム１２０において、ブロックチェーン秘密鍵とブロックチェーン証明書との組が用意される。ブロックチェーン秘密鍵とブロックチェーン証明書との組は、認証局証明書ブロックチェーンとクライアント証明書ブロックチェーンと失効リストブロックチェーンとに共通で使用される。

ブロックチェーン秘密鍵とブロックチェーン証明書との組はブロックチェーン記憶部２９０に記憶される。つまり、第１組織の認証システム１２０において、第１組織用のブロックチェーン秘密鍵と第１組織用のブロックチェーン証明書との組がブロックチェーン記憶部２９０に記憶される。第２組織の認証システム１２０において、第２組織用のブロックチェーン秘密鍵と第２組織用のブロックチェーン証明書との組がブロックチェーン記憶部２９０に記憶される。第３組織の認証システム１２０において、第３組織用のブロックチェーン秘密鍵と第３組織用のブロックチェーン証明書との組がブロッ

クチェーン記憶部２９０に記憶される。

ブロックチェーン秘密鍵とブロックチェーン証明書との組の生成方法は、ブロックチェーンの実装方式によって異なる。例えば、認証システム１２０がブロックチェーン秘密鍵とブロックチェーン証明書との組を自ら生成する。または、代表の認証局がそれぞれの認証システム１２０に対してブロックチェーン秘密鍵とブロックチェーン証明書との組を生成する。

以下では、ブロックチェーン秘密鍵とブロックチェーン証明書との組が認証局証明書ブロックチェーンとクライアント証明書ブロックチェーンと失効リストブロックチェーンとに共通で使用されるものとして説明する。しかし、認証局証明書ブロックチェーンとクライアント証明書ブロックチェーンと失効リストブロックチェーンとのそれぞれで、ブロックチェーン秘密鍵とブロックチェーン証明書との組が異なってもよい。

[0049] 次に、（２）ブロックチェーンへの参加について説明する。

ブロックチェーンへの参加とは、起動済みのブロックチェーンに対してデータ登録の権利またはデータ参照の権利を得るための処理である。認証システム１２０がブロックチェーンへの参加によってデータ登録の権利を得た場合、認証システム１２０は、ブロックチェーンにデータを登録することができる。認証システム１２０がブロックチェーンへの参加によってデータ参照の権利を得た場合、認証システム１２０は、ブロックチェーンに登録されているデータを参照することができる。

それぞれの認証システム１２０は、認証局証明書ブロックチェーンとクライアント証明書ブロックチェーンと失効リストブロックチェーンとのそれぞれに参加する。

ブロックチェーンへの参加のためには、ブロックチェーン起動処理およびブロックチェーン参加処理が必要である。

ブロックチェーン起動処理では、ブロックチェーン起動機能が利用される。ブロックチェーン起動機能は、ブロックチェーンを起動するための処理を実行する機能である。例えば、ブロックチェーンを起動するために提供され

たプログラムが実行される。

ブロックチェーン参加処理では、ブロックチェーン参加機能が利用される。ブロックチェーン参加機能は、ブロックチェーンに参加するための処理を実行する機能である。例えば、ブロックチェーンに参加するために提供されたプログラムの実行によって、ブロックチェーンサーバへのアクセスが行われる。また、ブロックチェーンの通信仕様に従って、参加メッセージがやり取りされる。

ブロックチェーンへの参加の方法は、ブロックチェーンによって異なる。例えば、第１組織の認証システム１２０がブロックチェーンを起動し、第２組織と第３組織とのそれぞれの認証システム１２０がブロックチェーンに参加する。

[0050] それぞれの認証システム１２０において、認証局秘密鍵と認証局証明書との組が用意される。

認証局秘密鍵は秘密鍵生成部４１１によって生成され、認証局秘密鍵記憶部４９０に記憶される。つまり、第１組織の認証システム１２０において、第１組織用の認証局秘密鍵が認証局秘密鍵記憶部４９０に記憶される。第２組織の認証システム１２０において、第２組織用の認証局秘密鍵が認証局秘密鍵記憶部４９０に記憶される。第３組織の認証システム１２０において、第３組織用の認証局秘密鍵が認証局秘密鍵記憶部４９０に記憶される。

認証局証明書は証明書生成部４１２に生成される。例えば、認証局証明書は、Ｘ．５０９の規格に従って生成される。ブロックチェーン証明書およびクライアント証明書も、例えば、Ｘ．５０９の規格に従って生成される。

認証局証明書には認証局秘密鍵と対を成す認証局公開鍵が含まれる。また、ブロックチェーン証明書にはブロックチェーン秘密鍵と対を成すブロックチェーン公開鍵が含まれ、クライアント証明書にはクライアント秘密鍵と対を成すクライアント公開鍵が含まれる。

認証局秘密鍵と認証局公開鍵との組は、ＲＳＡ暗号または楕円曲線暗号などのアルゴリズムによって生成される。ブロックチェーン秘密鍵とブロック

チェーン公開鍵との組およびクライアント秘密鍵とクライアント公開鍵との組も、ＲＳＡ暗号または楕円曲線暗号などのアルゴリズムによって生成される。ＲＳＡはＲｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ ｃｒｙｐｔｏｓｙｓｔｅｍの略称である。

[0051] 次に、（３）認証局証明書の登録について説明する。

それぞれの認証システム１２０は、認証局証明書を認証局証明書ブロックチェーンに登録する。

[0052] 図９に基づいて、第１組織の認証局証明書が認証局証明書ブロックチェーンに登録される場合を例にして、登録処理を説明する。

この登録処理は、（３）認証局証明書の登録のための処理である。

[0053] ステップＳ１０１において、第１組織の認証局証明書用の登録トランザクションが発行される。

認証局証明書用の登録トランザクションは、認証局証明書を認証局証明書ブロックチェーンに登録するためのトランザクションである。

[0054] ステップＳ１０１の処理は以下の通りである。

第１組織の認証システム１２０において、トランザクション発行部２１１は、第１組織の認証局証明書用の登録トランザクションを発行する。具体的には、トランザクション発行部２１１は、トランザクションデータ１２１を生成し、トランザクションデータ１２１をそれぞれの他の認証システム１２０に送信する。トランザクションデータ１２１は、ブロックチェーンの機能により送信される。他の認証システム１２０は、第２組織の認証システム１２０および第３組織の認証システム１２０である。

それぞれの他の認証システム１２０において、トランザクション受付部２１２は、第１組織の認証局証明書用の登録トランザクションを受け付ける。具体的には、トランザクション受付部２１２は、トランザクションデータ１２１を受信する。

[0055] 図１０に基づいて、トランザクションデータ１２１を説明する。

トランザクションデータ１２１は、基本情報１２１Ａと所有者情報１２１

Ｂと認証局証明書１２１Ｃとその他情報１２１Ｄとを有する。

基本情報１２１Ａは、例えば、トランザクションＩＤ（ｉｄｅｎｔｉｆｉｅｒ）と、発行元のブロックチェーン証明書と、発行元の署名と、発行時のタイムスタンプとを含む。発行元は、第１組織の認証システム１２０である。発行元の署名は、発行元のブロックチェーン秘密鍵を用いて生成される。

所有者情報１２１Ｂは、認証局証明書の所有者を示す。所有者は、第１組織の認証システム１２０である。

認証局証明書１２１Ｃは、第１組織の認証局証明書である。

[0056] 図９に戻り、ステップＳ１０２から説明を続ける。

ステップＳ１０２において、第１組織の認証局証明書が検証される。つまり、トランザクションデータ１２１に含まれる認証局証明書１２１Ｃが検証される。

[0057] ステップＳ１０２の処理は以下の通りである。

それぞれの他の認証システム１２０において、証明書検証部２１３は、第１組織の認証局証明書を検証する。具体的には、証明書検証部２１３は、トランザクションデータ１２１から認証局証明書１２１Ｃを取得し、認証局証明書１２１Ｃを検証する。

[0058] 例えば、証明書検証部２１３は、以下に示す方法の少なくともいずれかによって、認証局証明書１２１Ｃを検証する。複数の方法で検証を行うことにより、認証局証明書１２１Ｃの真偽をより正しく確かめることができる。

証明書検証部２１３は、認証局証明書１２１Ｃの形式を確かめる。具体的には、証明書検証部２１３は、認証局証明書１２１Ｃの形式が認証局証明書の規定の形式と一致することを確かめる。

証明書検証部２１３は、認証局証明書１２１Ｃに含まれる認証局公開鍵を用いて、基本情報１２１Ａの中の発行元の署名を検証する。

証明書検証部２１３は、認証局証明書１２１Ｃの正しさを確かめる。具体的には、証明書検証部２１３は、発行元の認証システム１２０と通信することによって、認証局証明書１２１Ｃの内容を確認する。

[0059] ステップＳ１０３において、他の認証システム群によって、検証結果の合意形成が図られる。他の認証システム群は１つ以上の他の認証システム１２０である。具体的には、他の認証システム群は、第１組織の認証システム１２０以外の全ての認証システム１２０である。つまり、他の認証システム群は、第２組織の認証システム１２０および第３組織の認証システム１２０である。

[0060] ステップＳ１０３の処理は以下の通りである。

他の認証システム群において、１つ以上の証明書検証部２１３は、合意形成機能によって、検証結果の合意形成を図る。

合意形成機能は、コンセンサスアルゴリズムと呼ばれる。

コンセンサスアルゴリズムは、ブロックチェーンの種類によって異なる。有名なコンセンサスアルゴリズムとして、Ｐｒｏｏｆ ｏｆ Ｗｏｒｋ（ＰｏＷ）およびＰｒａｃｔｉｃａｌ Ｂｙｚａｎｔｉｎｅ Ｆａｕｌｔ Ｔｏｌｅｒａｎｃｅ（ＰＢＦＴ）などが挙げられる。

[0061] 認証局証明書は、認証システム１２０の認証局装置４００を証明するものである。そのため、認証局証明書には、高いセキュリティが求められる。

例えば、全ての他の認証システム１２０において、認証局証明書が正しいと判定された場合にだけ、認証局証明書が正しいという合意が得られる。

[0062] 合意形成の結果によって、処理は分岐する。

第１組織の認証局証明書が正しいという結果が得られた場合、処理はステップＳ１０４に進む。

第１組織の認証局証明書が正しくないという結果が得られた場合、第１組織の認証局証明書が認証局証明書ブロックチェーンに登録されず、処理はステップＳ１０５に進む。

[0063] ステップＳ１０４において、第１組織の認証局証明書が認証局証明書ブロックチェーンに登録される。

[0064] ステップＳ１０４の処理は以下の通りである。

それぞれの他の認証システム１２０において、ブロックチェーン管理部２

１４は、第１組織の認証局証明書を認証局証明書ブロックチェーンに登録する。具体的には、ブロックチェーン管理部２１４は、認証局証明書１２１Ｃを認証局証明書ブロックチェーンの一部としてブロックチェーン記憶部２９０に記憶する。

[0065] ステップＳ１０５において、登録トランザクションの結果が通知される。

[0066] ステップＳ１０５の処理は以下の通りである。

それぞれの他の認証システム１２０において、トランザクション受付部２１２は、登録結果通知を第１組織の認証システム１２０に送信する。登録結果通知は、第１組織の認証局証明書が認証局証明書ブロックチェーンに登録されたか否かを示す。

第１組織の認証システム１２０において、トランザクション発行部２１１は、登録結果通知を受信する。

[0067] 次に、（４）クライアント証明書の発行について説明する。

それぞれの認証システム１２０は、組織内のユーザのためにクライアント証明書を発行する。クライアント証明書の発行は、クライアント証明書ブロックチェーンへのクライアント証明書の登録を意味する。

[0068] 図１１および図１２に基づいて、第１組織に属する第１ユーザのためにクライアント証明書が発行される場合を例にして、発行処理を説明する。

この発行処理は、（４）クライアント証明書の発行のための処理である。

[0069] ステップＳ２０１において、第１ユーザの認証情報が第１組織の認証システム１２０に送信される。

認証情報は、ユーザを認証するための情報である。例えば、認証情報は、ユーザＩＤとパスワードとの組、または、生体情報である。

[0070] ステップＳ２０１の処理は以下の通りである。

第１組織システム１１０Ａにおいて、第１ユーザは、認証情報をユーザ端末１３０に入力する。

ユーザ端末１３０のブラウザ部１３２は、第１組織の認証システム１２０に認証情報を送信する。

第１組織の認証システム１２０において、認証部３１１は認証情報を受信する。

[0071] ステップＳ２０２において、第１ユーザの認証情報が検証される。

[0072] ステップＳ２０２の処理は以下の通りである。

第１組織の認証システム１２０において、認証情報記憶部３９１には、第１組織のそれぞれのユーザの認証情報が予め登録されている。

認証部３１１は、受信した認証情報が認証情報記憶部３９１に登録されているいずれかの認証情報と一致するか判定する。

受信した認証情報が認証情報記憶部３９１に登録されているいずれかの認証情報と一致する場合、ユーザの認証情報は正しい。

[0073] ユーザの認証情報が正しい場合、処理はステップＳ２０３に進む。

ユーザの認証情報が正しくない場合、認証部３１１は、エラーメッセージをユーザ端末１３０に送信する。ユーザ端末１３０のブラウザ部１３２は、エラーメッセージを受信し、エラーメッセージをディスプレイに表示する。そして、処理はステップＳ２０１に進む。

[0074] ステップＳ２０３において、第１ユーザのクライアント秘密鍵が生成される。

[0075] ステップＳ２０３の処理は以下の通りである。

第１組織の認証システム１２０において、認証部３１１は、第１ユーザのクライアント秘密鍵と第１ユーザのクライアント証明書とを発行するための発行要求を送信する。秘密鍵生成部４１１は、発行要求を受信し、第１ユーザのクライアント秘密鍵を生成する。

[0076] ステップＳ２０４において、第１ユーザのクライアント証明書が生成される。

[0077] ステップＳ２０４の処理は以下の通りである。

第１組織の認証システム１２０において、証明書生成部４１２は、第１組織の認証局秘密鍵を用いて署名を生成し、第１ユーザのクライアント証明書を生成する。

第１ユーザのクライアント証明書は、第１組織の認証局秘密鍵を用いて生成された署名を含む。

[0078] ステップＳ２０５において、第１ユーザのクライアント証明書用の登録トランザクションが発行される。

クライアント証明書用の登録トランザクションは、クライアント証明書をクライアント証明書ブロックチェーンに登録するためのトランザクションである。

[0079] ステップＳ２０５の処理は以下の通りである。

第１組織の認証システム１２０において、証明書生成部４１２はクライアント秘密鍵とクライアント証明書との組を送信し、認証部３１１はクライアント秘密鍵とクライアント証明書との組を受信する。認証部３１１はクライアント証明書を送信し、トランザクション発行部２１１はクライアント証明書を受信する。そして、トランザクション発行部２１１は、第１ユーザのクライアント証明書用の登録トランザクションを発行する。具体的には、トランザクション発行部２１１は、トランザクションデータ１２２を生成し、トランザクションデータ１２２をそれぞれの他の認証システム１２０に送信する。他の認証システム１２０は、第２組織の認証システム１２０および第３組織の認証システム１２０である。

それぞれの他の認証システム１２０において、トランザクション受付部２１２は、第１ユーザのクライアント証明書用の登録トランザクションを受け付ける。具体的には、トランザクション受付部２１２は、トランザクションデータ１２２を受信する。

[0080] 図１３に基づいて、トランザクションデータ１２２を説明する。

トランザクションデータ１２２は、基本情報１２２Ａと所有者情報１２２Ｂとクライアント証明書１２２Ｃとその他情報１２２Ｄとを有する。

基本情報１２２Ａは、例えば、トランザクションＩＤと、発行元情報と、発行元のブロックチェーン証明書と、発行元の署名と、発行時のタイムスタンプとを含む。発行元情報は、トランザクションデータ１２２の発行元を示

す。発行元は、第１組織の認証システム１２０である。発行元の署名は、発行元のブロックチェーン秘密鍵を用いて生成される。

所有者情報１２２Ｂは、クライアント証明書の所有者を示す。所有者は第１ユーザである。

クライアント証明書１２２Ｃは、第１ユーザのクライアント証明書である。

[0081] 図１１に戻り、ステップＳ２１０から説明を続ける。

ステップＳ２１０において、第１ユーザのクライアント証明書が検証される。つまり、トランザクションデータ１２２に含まれるクライアント証明書１２２Ｃが検証される。

[0082] ステップＳ２１０の処理は以下の通りである。

それぞれの他の認証システム１２０において、証明書検証部２１３は、第１ユーザのクライアント証明書を検証する。具体的には、証明書検証部２１３は、トランザクションデータ１２２からクライアント証明書１２２Ｃを取得し、クライアント証明書１２２Ｃを検証する。

[0083] 図１４に基づいて、ステップＳ２１０における検証処理を説明する。

ステップＳ２１１において、証明書検証部２１３は、トランザクションデータ１２２の形式を検証する。

例えば、証明書検証部２１３は、トランザクションデータ１２２の形式がクライアント証明書用の登録トランザクションの規定の形式と一致するか、および、クライアント証明書１２２Ｃの有効期限が切れていないか等を検証する。

トランザクションデータ１２２の形式が正しい場合、処理はステップＳ２１２に進む。

トランザクションデータ１２２の形式が正しくない場合、証明書検証部２１３はクライアント証明書１２２Ｃが正しくないと判定し、処理は終了する。

[0084] ステップＳ２１２において、証明書検証部２１３は、トランザクションデ

ータ１２２の基本情報１２２Ａから発行元情報を取得する。

そして、証明書検証部２１３は、発行元情報に基づいて、発行元の認証局証明書をブロックチェーン記憶部２９０から取得する。

[0085] ステップＳ２１３において、証明書検証部２１３は、発行元の認証局証明書から認証局公開鍵を取得する。

また、証明書検証部２１３は、トランザクションデータ１２２からクライアント証明書１２２Ｃを取得する。

そして、証明書検証部２１３は、認証局公開鍵を用いて、クライアント証明書１２２Ｃの中の署名を検証する。つまり、証明書検証部２１３は、クライアント証明書１２２Ｃの署名が本物であるか検証する。

[0086] ステップＳ２１４において、証明書検証部２１３は、クライアント証明書１２２Ｃの署名についての検証結果を判定する。

クライアント証明書１２２Ｃの署名が正しい場合、証明書検証部２１３はクライアント証明書１２２Ｃが正しいと判定し、処理は終了する。

クライアント証明書１２２Ｃの署名が正しくない場合、証明書検証部２１３はクライアント証明書１２２Ｃが正しくないと判定し、処理は終了する。

[0087] 図１１に戻り、ステップＳ２２０から説明を続ける。

ステップＳ２２１において、他の認証システム群によって、検証結果の合意形成が図られる。他の認証システム群は１つ以上の他の認証システム１２０である。具体的には、他の認証システム群は、第１組織の認証システム１２０以外の全ての認証システム１２０である。つまり、他の認証システム群は、第２組織の認証システム１２０および第３組織の認証システム１２０である。

[0088] ステップＳ２２０の処理は以下の通りである。

他の認証システム群において、１つ以上の証明書検証部２１３は、合意形成機能によって、検証結果の合意形成を図る。

合意形成機能は、コンセンサスアルゴリズムと呼ばれる。

例えば、多数決によって、検証結果が決定される。つまり、クライアント

証明書が正しいという検証結果の数がクライアント証明書が正しくないという検証結果の数よりも多い場合、クライアント証明書が正しいという合意が得られる。

[0089] 合意形成の結果によって、処理は分岐する。

第１ユーザのクライアント証明書が正しいという結果が得られた場合、処理はステップＳ２３１に進む。

第１ユーザのクライアント証明書が正しくないという結果が得られた場合、処理はステップＳ２４１に進む。

[0090] ステップＳ２３１において、第１ユーザのクライアント証明書がクライアント証明書ブロックチェーンに登録される。

[0091] ステップＳ２３１の処理は以下の通りである。

それぞれの他の認証システム１２０において、ブロックチェーン管理部２１４は、第１ユーザのクライアント証明書をクライアント証明書ブロックチェーンに登録する。つまり、ブロックチェーン管理部２１４は、クライアント証明書１２２Ｃをクライアント証明書ブロックチェーンの一部としてブロックチェーン記憶部２９０に記憶する。

[0092] ステップＳ２３２において、第１ユーザのクライアント秘密鍵が保存される。

[0093] ステップＳ２３２の処理は以下の通りである。

それぞれの他の認証システム１２０において、トランザクション受付部２１２は、登録完了通知を第１組織の認証システム１２０に送信する。登録完了通知は、第１ユーザのクライアント証明書がクライアント証明書ブロックチェーンに登録されたことを示す。

第１組織の認証システム１２０において、トランザクション発行部２１１は、登録完了通知を受信する。トランザクション発行部２１１は登録完了通知を送信し、認証部３１１は登録完了通知を受信する。そして、認証部３１１は、第１ユーザのクライアント秘密鍵をクライアント秘密鍵記憶部３９２に保存する。

[0094] ステップＳ２３２の後、処理はステップＳ２５０に進む。

[0095] ステップＳ２４１において、登録トランザクションの棄却が第１組織の認証システム１２０に通知される。

[0096] ステップＳ２４１の処理は以下の通りである。

それぞれの他の認証システム１２０において、トランザクション受付部２１２は、棄却通知を第１組織の認証システム１２０に送信する。棄却通知は、第１ユーザのクライアント証明書用の登録トランザクションが棄却されたことを示す。つまり、棄却通知は、第１ユーザのクライアント証明書がクライアント証明書ブロックチェーンに登録されなかったことを示す。例えば、棄却通知は、棄却理由情報を含む。棄却理由情報は、棄却理由を区別する情報である。例えば、棄却理由情報は、コードまたは文字列などによって棄却理由を示す。

第１組織の認証システム１２０において、トランザクション発行部２１１は、棄却通知を受信する。

[0097] ステップＳ２４２において、第１ユーザのクライアント秘密鍵が削除される。

[0098] ステップＳ２４２の処理は以下の通りである。

第１組織の認証システム１２０において、トランザクション発行部２１１は棄却通知を送信し、認証部３１１は棄却通知を受信する。そして、認証部３１１は、第１ユーザのクライアント秘密鍵を削除する。

[0099] ステップＳ２４２の後、処理はステップＳ２５０に進む。

[0100] ステップＳ２５０において、クライアント証明書の発行結果がユーザ端末１３０に通知される。

[0101] ステップＳ２５０の処理は以下の通りである。

第１組織の認証システム１２０において、認証部３１１は、発行結果通知をユーザ端末１３０に送信する。発行結果通知は、第１ユーザのクライアント証明書が発行されたか否かを示す。

第１組織システム１１０Ａにおいて、ユーザ端末１３０のブラウザ部１３

２は発行結果通知を受信し、発行結果をディスプレイに表示する。例えば、第１ユーザのクライアント証明書が発行されなかった場合、ブラウザ部１３２は、棄却理由をディスプレイに表示する。

[0102] 次に、（５）ユーザの代理証明について説明する。

ユーザが他組織のサーバ装置１４０にアクセスする場合、つまり、ユーザが他組織のサービスにアクセスする場合、ユーザが属する組織の認証システム１２０が、他組織の認証システム１２０の代わりにユーザを認証する。

[0103] 図１５および図１６に基づいて、第１組織の第１ユーザが第２組織のサービスにアクセスする場合を例にして、代理証明処理を説明する。

この代理証明処理は、（５）ユーザの代理証明のための処理である。

[0104] ステップＳ３０１において、第１ユーザのクライアント証明書が発行される。つまり、第１ユーザのクライアント証明書がクライアント証明書ブロックチェーンに登録される。

ステップＳ３０１の処理は、図１１および図１２で説明した発行処理に相当する。

[0105] ステップＳ３０２において、アクセス要求が第２組織のサーバ装置１４０に送信される。

[0106] ステップＳ３０２の処理は以下の通りである。

第１組織システム１１０Ａにおいて、第１ユーザは、第２組織のサービスに対するアクセス要求をユーザ端末１３０に入力する。

アクセス情報は、第１組織と第１ユーザとアクセス内容とを示す。

ユーザ端末１３０のブラウザ部１３２は、アクセス要求を第２組織のサーバ装置１４０に送信する。

第２組織システム１１０Ｂにおいて、サーバ装置１４０はアクセス要求を受信する。

[0107] ステップＳ３０３において、第１ユーザの認証要求が第２組織の認証システム１２０に送信される。

[0108] ステップＳ３０３の処理は以下の通りである。

第２組織システム１１０Ｂにおいて、サーバ装置１４０は、第１ユーザの認証要求を送信する。この認証要求は、第１組織と第１ユーザとを示す。

第２組織の認証システム１２０において、認証部３１１は、第１ユーザの認証要求を受信する。

[0109] ステップＳ３０４において、第１ユーザのクライアント証明書が第２組織のクライアント証明書ブロックチェーンから取得される。

[0110] ステップＳ３０４の処理は以下の通りである。

第２組織の認証システム１２０において、認証部３１１は第１ユーザ識別子を送信し、ブロックチェーン管理部２１４は第１ユーザ識別子を受信する。ブロックチェーン管理部２１４は、第１ユーザ識別子に基づいて、第１ユーザのクライアント証明書をクライアント証明書ブロックチェーンから取得する。つまり、ブロックチェーン管理部２１４は、第１ユーザのクライアント証明書をブロックチェーン記憶部２９０から取得する。

[0111] ステップＳ３０５において、第１ユーザのクライアント証明書が検証される。

[0112] ステップＳ３０５の処理は以下の通りである。

第２組織の認証システム１２０において、証明書検証部２１３は、第１ユーザのクライアント証明書から有効期限を取得し、有効期限を現在時刻と比較する。

有効期限が切れている場合、証明書検証部２１３は、第１ユーザのクライアント証明書が正しくないと判定する。

有効期限が切れていない場合、証明書検証部２１３は、第１ユーザのクライアント証明書が失効リストブロックチェーンに登録されているか判定する。つまり、証明書検証部２１３は、第１ユーザのクライアント証明書が失効リストブロックチェーンの一部としてブロックチェーン記憶部２９０に記憶されているか判定する。証明書検証部２１３は次のように判定を行う。まず、証明書検証部２１３は、第１ユーザのクライアント証明書から発行者とシリアル番号との組を取得する。そして、証明書検証部２１３は、取得した組

と同じ組が失効リストブロックチェーンに登録されているか判定する。

第１ユーザのクライアント証明書が失効リストブロックチェーンに登録されている場合、証明書検証部２１３は、第１ユーザのクライアント証明書が正しくないと判定する。

第１ユーザのクライアント証明書が失効リストブロックチェーンに登録されていない場合、証明書検証部２１３は、第１ユーザのクライアント証明書が正しいと判定する。

[0113] ステップＳ３０６において、第１ユーザのクライアント証明書についての検証結果が判定される。

[0114] ステップＳ３０６の処理は以下の通りである。

第２組織の認証システム１２０において、証明書検証部２１３は検証結果通知を送信し、認証部３１１は検証結果通知を受信する。検証結果通知は、第１ユーザのクライアント証明書が正しいか否かを示す。そして、認証部３１１は、検証結果通知に基づいて、第１ユーザのクライアント証明書について検証結果を判定する。

第１ユーザのクライアント証明書が正しい場合、処理はステップＳ３１１に進む。

第１ユーザのクライアント証明書が正しくない場合、処理はステップＳ３０７に進む。

[0115] ステップＳ３０７において、認証失敗がユーザ端末１３０に通知される。

[0116] ステップＳ３０７の処理は以下の通りである。

第２組織の認証システム１２０において、認証部３１１は認証失敗通知を送信する。

第２組織システム１１０Ｂにおいて、サーバ装置１４０は認証失敗通知を受信し、認証失敗通知を送信する。ユーザ端末１３０は認証失敗通知を受信し、認証失敗をディスプレイに表示する。

[0117] ステップＳ３０７の後、処理は終了する。この場合、第１ユーザは、第２組織のサービスにアクセスすることができない。

[0118] ステップＳ３１１において、ハローメッセージが第１組織の認証システム１２０に送信される。

[0119] ステップＳ３１１の処理は以下の通りである。

第２組織の認証システム１２０において、認証部３１１は、ハローメッセージを生成し、ハローメッセージと第１ユーザ識別子とを第１組織の認証システム１２０に送信する。ハローメッセージは乱数を含む。

第１組織の認証システム１２０において、代理証明部３１２は、ハローメッセージと第１ユーザ識別子とを受信する。

[0120] ステップＳ３１２において、署名メッセージが第２組織の認証システム１２０に返信される。

[0121] ステップＳ３１２の処理は以下の通りである。

第１組織の認証システム１２０において、代理証明部３１２は、第１ユーザ識別子に基づいて、第１ユーザのクライアント秘密鍵をクライアント秘密鍵記憶部３９２から取得する。代理証明部３１２は、第１ユーザのクライアント秘密鍵を用いてハローメッセージを暗号化する。暗号されたハローメッセージが署名メッセージである。代理証明部３１２は、署名メッセージを第２組織の認証システム１２０に送信する。

第２組織の認証システム１２０において、認証部３１１は署名メッセージを受信する。

[0122] ステップＳ３１３において、署名メッセージが検証される。

[0123] ステップＳ３１３の処理は以下の通りである。

第２組織の認証システム１２０において、認証部３１１は、第１ユーザのクライアント証明書から第１ユーザのクライアント公開鍵を取得する。認証部３１１は、第１ユーザのクライアント公開鍵を用いて、署名メッセージを復号する。そして、認証部３１１は、復号後の署名メッセージがハローメッセージと一致するか判定する。

復号後の署名メッセージがハローメッセージと一致する場合、署名メッセージは正しい。

[0124] ステップＳ３１４において、署名メッセージの検証結果が判定される。

[0125] ステップＳ３１４の処理は以下の通りである。

第２組織の認証システム１２０において、認証部３１１は、署名メッセージの検証結果を判定する。

[0126] 署名メッセージが正しい場合、認証部３１１は第１ユーザが正当なユーザであると判定し、処理はステップＳ３１５に進む。

署名メッセージが正しくない場合、認証部３１１は第１ユーザが不当なユーザであると判定し、処理はステップＳ３１６に進む。

[0127] ステップＳ３１５において、認証成功がユーザ端末１３０に通知される。

[0128] ステップＳ３１５の処理は以下の通りである。

第２組織の認証システム１２０において、認証部３１１は認証成功通知を送信する。

第２組織システム１１０Ｂにおいて、サーバ装置１４０は認証成功通知を受信し、認証成功通知を送信する。ユーザ端末１３０は認証成功通知を受信し、認証成功をディスプレイに表示する。

[0129] ステップＳ３１５の後、処理は終了する。この場合、第１ユーザは、第２組織のサービスにアクセスすることができる。

[0130] ステップＳ３１６において、認証失敗がユーザ端末１３０に通知される。

[0131] ステップＳ３１６の処理は以下の通りである。

第２組織の認証システム１２０において、認証部３１１は認証失敗通知を送信する。

第２組織システム１１０Ｂにおいて、サーバ装置１４０は認証失敗通知を受信し、認証失敗通知を送信する。ユーザ端末１３０は認証失敗通知を受信し、認証失敗をディスプレイに表示する。

[0132] ステップＳ３１６の後、処理は終了する。この場合、第１ユーザは、第２組織のサービスにアクセスすることができない。

[0133] 次に、（６）ユーザのログアウトについて説明する。

それぞれの他の認証システム１２０において、ユーザのクライアント証明

書が失効リストブロックチェーンに登録される。

[0134] 図１７に基づいて、第１組織の第１ユーザがログアウトする場合を例にして、ログアウト処理を説明する。

このログアウト処理は、（６）ユーザのログアウトのための処理である。

[0135] ステップＳ４０１において、ログアウト要求が第１組織の認証システム１２０に送信される。

[0136] ステップＳ４０１の処理は以下の通りである。

第１組織システム１１０Ａにおいて、第１ユーザは、ログアウト要求をユーザ端末１３０に入力する。

ログアウト要求は、第１組織と第１ユーザとを示す。

ユーザ端末１３０のブラウザ部１３２は、ロウアウト要求を第１組織の認証システム１２０に送信する。

第１組織の認証システム１２０において、ログアウト受付部３１３はログアウト要求を受信する。

[0137] ステップＳ４０２において、第１ユーザのクライアント証明書用の失効トランザクションが発行される。

クライアント証明書用の失効トランザクションは、クライアント証明書を失効リストブロックチェーンに登録するためのトランザクションである。

[0138] ステップＳ４０２の処理は以下の通りである。

第１組織の認証システム１２０において、ログアウト受付部３１３は第１ユーザ識別子をトランザクション発行部２１１に送信する。トランザクション発行部２１１は、第１ユーザ識別子に基づいて、第１ユーザのクライアント証明書を第１組織のクライアント証明書ブロックチェーンから取得する。そして、トランザクション発行部２１１は、第１ユーザのクライアント証明書用の失効トランザクションを発行する。具体的には、トランザクション発行部２１１は、トランザクションデータ１２３を生成し、トランザクションデータ１２３をそれぞれの他の認証システム１２０に送信する。他の認証システム１２０は、第２組織の認証システム１２０および第３組織の認証シス

テム１２０である。

それぞれの他の認証システム１２０において、トランザクション受付部２１２は、トランザクションデータ１２３を受信する。

[0139] 図１８に基づいて、トランザクションデータ１２３を説明する。

トランザクションデータ１２３は、基本情報１２３Ａとクライアント証明書情報１２３Ｂとその他情報１２３Ｃとを有する。

基本情報１２３Ａは、例えば、トランザクションＩＤと、発行元情報と、発行元のブロックチェーン証明書と、発行元の署名と、発行時のタイムスタンプとを含む。発行元情報は、トランザクションデータ１２３の発行元を示す。発行元は、第１組織の認証システム１２０である。発行元の署名は、発行元のブロックチェーン秘密鍵を用いて生成される。

クライアント証明書情報１２３Ｂは、第１ユーザのクライアント証明書を識別する。例えば、クライアント証明書情報１２３Ｂは、第１ユーザのクライアント証明書について発行元ＩＤとシリアル番号とを示す。

[0140] 図１７に戻り、ステップＳ４０３から説明を続ける。

ステップＳ４０３において、第１ユーザのクライアント証明書用の失効トランザクションが検証される。

[0141] ステップＳ４０３の処理は以下の通りである。

それぞれの他の認証システム１２０において、トランザクション検証部２１５は、第１ユーザのクライアント証明書用の失効トランザクションを検証する。具体的には、トランザクション検証部２１５は、トランザクションデータ１２３を次のように検証する。

トランザクション検証部２１５は、トランザクションデータ１２３の形式が正しいか判定する。トランザクションデータ１２３の形式が失効トランザクションの規定の形式と一致する場合、トランザクションデータ１２３の形式は正しい。

トランザクションデータ１２３の形式が正しい場合、トランザクション検証部２１５は、トランザクションデータ１２３の中の発行元のブロックチェ

ーン証明書からブロックチェーン公開鍵を取得する。そして、トランザクション検証部２１５は、ブロックチェーン公開鍵を用いて、トランザクションデータ１２３の中の発行元の署名を検証する。

発行元の署名が正しい場合、トランザクション検証部２１５は、トランザクションデータ１２３から発行元情報とクライアント証明書情報１２３Ｂとを取得する。そして、トランザクション検証部２１５は、トランザクションデータ１２３の発行元が第１ユーザのクライアント証明書の発行元と一致するか判定する。トランザクションデータ１２３の発行元が第１ユーザのクライアント証明書の発行元と一致する場合、発行元情報は正しい。

発行元情報が正しい場合、トランザクション検証部２１５は、失効トランザクションが正しいと判定する。

トランザクションデータ１２３の形式が正しくない場合、トランザクション検証部２１５は、失効トランザクションが正しくないと判定する。

発行元の署名が正しくない場合、トランザクション検証部２１５は、失効トランザクションが正しくないと判定する。

発行元情報が正しくない場合、トランザクション検証部２１５は、失効トランザクションが正しくないと判定する。

[0142] ステップＳ４０４において、他の認証システム群によって、検証結果の合意形成が図られる。他の認証システム群は１つ以上の他の認証システム１２０である。具体的には、他の認証システム群は、第１組織の認証システム１２０以外の全ての認証システム１２０である。つまり、他の認証システム群は、第２組織の認証システム１２０および第３組織の認証システム１２０である。

[0143] ステップＳ４０４の処理は以下の通りである。

他の認証システム群において、１つ以上のトランザクション検証部２１５は、合意形成機能によって、検証結果の合意形成を図る。

合意形成機能は、コンセンサスアルゴリズムと呼ばれる。

例えば、多数決によって、検証結果が決定される。つまり、失効トランザ

クションが正しいという検証結果の数が失効トランザクションデータが正しくないという検証結果の数よりも多い場合、失効トランザクションが正しいという合意が得られる。

[0144] 合意形成の結果によって、処理は分岐する。

失効トランザクションが正しいという結果が得られた場合、処理はステップＳ４１１に進む。

失効トランザクションが正しくないという結果が得られた場合、処理はステップＳ４２１に進む。

[0145] ステップＳ４１１において、第１ユーザのクライアント証明書が失効リストブロックチェーンに登録される。

[0146] ステップＳ４１１の処理は以下の通りである。

それぞれの他の認証システム１２０において、ブロックチェーン管理部２１４は、第１ユーザのクライアント証明書を失効リストブロックチェーンに登録する。つまり、ブロックチェーン管理部２１４は、第１ユーザのクライアント証明書の情報を失効リストブロックチェーンの一部としてブロックチェーン記憶部２９０に記憶する。

[0147] ステップＳ４１２において、第１ユーザのクライアント秘密鍵が削除される。

[0148] ステップＳ４１２の処理は以下の通りである。

少なくともいずれかの他の認証システム１２０において、トランザクション受付部２１２は、合意形成の結果を第１組織の認証システム１２０に送信する。

第１組織の認証システム１２０において、トランザクション発行部２１１は、合意形成の結果を受信する。トランザクション発行部２１１は合意形成の結果を送信し、ログアウト受付部３１３は合意形成の結果を受信する。そして、ログアウト受付部３１３は、第１ユーザのクライアント秘密鍵をクライアント秘密鍵記憶部３９２から削除する。

[0149] ステップＳ４１３において、ログアウトの成功がユーザ端末１３０に通知

される。

[0150] ステップＳ４１３の処理は以下の通りである。

第１組織の認証システム１２０において、ログアウト受付部３１３は、ログアウト成功通知を送信する。

第１組織システム１１０Ａにおいて、ユーザ端末１３０はログアウト成功通知を受信し、ログアウトの成功をディスプレイに表示する。

[0151] ステップＳ４１３の後、処理は終了する。この場合、ユーザのログアウトは完了する。

[0152] ステップＳ４２１において、ログアウトの失敗がユーザ端末１３０に通知される。

[0153] ステップＳ４２１の処理は以下の通りである。

少なくともいずれかの他の認証システム１２０において、トランザクション受付部２１２は、合意形成の結果を第１組織の認証システム１２０に送信する。

第１組織の認証システム１２０において、トランザクション発行部２１１は、合意形成の結果を受信する。トランザクション発行部２１１は合意形成の結果を送信し、ログアウト受付部３１３は合意形成の結果を受信する。そして、ログアウト受付部３１３は、ログアウト失敗通知を送信する。

第１組織システム１１０Ａにおいて、ユーザ端末１３０はログアウト失敗通知を受信し、ログアウトの失敗をディスプレイに表示する。

[0154] ステップＳ４２１の後、処理は終了する。この場合、ユーザのログアウトは完了しない。ユーザのログアウトを完了させるためには、ログアウト処理が再度実行される必要がある。

[0155] ＊＊＊実施の形態１の効果＊＊＊

ユーザは必ず同じ認証装置３００によって認証される。具体的には、ユーザはユーザが属する組織の認証装置３００によって認証される。そのため、ユーザがユーザ端末群１３０Ｇのそれぞれのユーザ端末１３０を使用する場合であっても、認証装置３００に記憶された認証情報を用いてユーザを認証

することができる。

それぞれの組織の認証システム１２０は、ブロックチェーンを用いて連携することによって、クライアント証明書を共有することができる。

代理証明部３１２は代理証明を実施する。これにより、ユーザは、認証情報を１度入力するだけで、各組織のサービスにアクセスすることができる。

ブロックチェーンが利用されるため、複数の組織の複数の認証システム１２０において認証情報を安全に共有することが可能となる。そして、ユーザが所属する組織及びサービスを提供する組織で認証連携システム１００を運用することができる。

[0156] 各組織は同じ認証システム１２０を有する。そのため、ブロックチェーンの運用において、各組織の負担および各組織の責任が同程度になるような調整が可能である。つまり、認証連携システム１００において、各組織が負担と責任とを公平に受け持つことが可能である。

[0157] 実施の形態２.

認証局証明書ブロックチェーンを用いない形態について、主に実施の形態１と異なる点を図１９および図２０に基づいて説明する。

[0158] ＊＊＊構成の説明＊＊＊

認証連携システム１００の構成は、実施の形態１における構成と同じである（図１参照）。

組織システム１１０の構成は、実施の形態１における構成と同じである（図２参照）。

ユーザ端末１３０の構成は、実施の形態１における構成と同じである（図３参照）。

サーバ装置１４０の構成は、実施の形態１における構成と同じである（図４参照）。

認証システム１２０の構成は、実施の形態１における構成と同じである（図５参照）。

管理装置２００の構成は、実施の形態１における構成と同じである（図６

参照）。

認証装置３００の構成は、実施の形態１における構成と同じである（図７参照）。

[0159] 図１９に基づいて、認証局装置４００の構成を説明する。

認証局装置４００において、メモリ４０２は認証局秘密鍵記憶部４９０を有さない。

その他の構成は、実施の形態１における構成と同じである（図８参照）。

[0160] ＊＊＊動作の説明＊＊＊

実施の形態３において、認証局秘密鍵と認証局証明書との組は不要である。つまり、認証局証明書ブロックチェーンは不要である。そのため、登録処理（図９参照）は不要である。

[0161] 実施の形態３では、認証局証明書ブロックチェーンの代わりに、アドレスリストが使用される。

アドレスリストは、それぞれの認証システム１２０のアドレスを示す。例えば、アドレスリストは、それぞれの管理装置２００のＩＰアドレスを示す。ＩＰはＩｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌの略称である。

アドレスリストは、それぞれの認証システム１２０に記憶される。具体的には、アドレスリストは、それぞれの管理装置２００に記憶される。

[0162] 以下に、アドレスリストの使用方法について説明する。

図１１および図１２に基づいて、発行処理を説明する。

ステップＳ２０１からステップＳ２０３は、実施の形態１で説明した通りである。

[0163] ステップＳ２０４において、第１ユーザのクライアント証明書が生成される。

但し、第１ユーザのクライアント証明書は、第１組織の認証局秘密鍵を用いずに生成される。つまり、第１ユーザのクライアント証明書は、第１組織の認証局秘密鍵を用いて生成される署名を含まない。

[0164] ステップＳ２０５は、実施の形態１で説明した通りである。

[0165] ステップＳ２１０において、第１ユーザのクライアント証明書が検証される。

[0166] 図２０に基づいて、検証処理（Ｓ２１０）を説明する。

ステップＳ２１１は、実施の形態１で説明した通りである（図１４参照）。

トランザクションデータ１２２の形式が正しい場合、処理はステップＳ２１５に進む。

[0167] ステップＳ２１５において、証明書検証部２１３は、トランザクションデータ１２２の送信元アドレスを検証する。トランザクションデータ１２２の送信元アドレスは、クライアント証明書用の登録トランザクションの発行元のアドレスを意味する。

具体的には、証明書検証部２１３は、トランザクションデータ１２２の送信元アドレスがアドレスリストに登録されているか判定する。トランザクションデータ１２２の送信元アドレスがアドレスリストに登録されている場合、トランザクションデータ１２２の送信元アドレスは正しい。

トランザクションデータ１２２の送信元アドレスが正しい場合、証明書検証部２１３はクライアント証明書１２２Ｃが正しいと判定し、処理は終了する。

トランザクションデータ１２２の送信元アドレスが正しくない場合、証明書検証部２１３はクライアント証明書１２２Ｃが正しくないと判定し、処理は終了する。

[0168] ＊＊＊実施の形態２の効果＊＊＊

認証局証明書ブロックチェーンを用いることなく、実施の形態１と同様の機能を有する認証連携システム１００を実現することができる。

[0169] 実施の形態３．

仮想化技術を利用する形態について、主に実施の形態１および実施の形態２と異なる点を図２１に基づいて説明する。

[0170] ＊＊＊構成の説明＊＊＊

図２１に基づいて、認証連携システム１００の構成を説明する。

認証連携システム１００の構成は、実施の形態１における構成と同じである（図１参照）。

但し、それぞれの認証連携システム１００は、１台以上の物理計算機を備える。

物理計算機は、仮想化技術により、ユーザ端末１３０とサーバ装置１４０と管理装置２００と認証装置３００と認証局装置４００との少なくともいずれかを実装する。具体的な仮想化技術は、仮想マシンまたはコンテナ技術である。

例えば、それぞれの組織システム１１０において、管理装置２００、認証装置３００および認証局装置４００は、仮想化技術によって、１台の物理計算機に実装される。この場合、それぞれの組織システム１１０において、認証システム１２０が仮想化技術によって１台の物理計算機に実装される。

[0171] ＊＊＊動作の説明＊＊＊

認証連携システム１００の動作は、実施の形態１または実施の形態２における動作と同じである。

[0172] ＊＊＊実施の形態３の効果＊＊＊

実施の形態１と同等の機能を持つ認証連携システム１００を少ない物理計算機で実現できる。

[0173] ＊＊＊実施の形態の補足＊＊＊

図２２に基づいて、管理装置２００のハードウェア構成を説明する。

管理装置２００は処理回路２０９を備える。

処理回路２０９は、トランザクション発行部２１１とトランザクション受付部２１２と証明書検証部２１３とブロックチェーン管理部２１４とトランザクション検証部２１５とブロックチェーン記憶部２９０とを実現するハードウェアである。

処理回路２０９は、専用のハードウェアであってもよいし、メモリ２０２に格納されるプログラムを実行するプロセッサ２０１であってもよい。

[0174] 処理回路２０９が専用のハードウェアである場合、処理回路２０９は、例えば、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ、ＦＰＧＡまたはこれらの組み合わせである。

ＡＳＩＣはＡｐｐｌｉ認証局ｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔの略称であり、ＦＰＧＡはＦｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙの略称である。

管理装置２００は、処理回路２０９を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路２０９の役割を分担する。

[0175] 処理回路２０９において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0176] このように、処理回路２０９はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0177] 図２３に基づいて、認証装置３００のハードウェア構成を説明する。

認証装置３００は処理回路３０９を備える。

処理回路３０９は、認証部３１１と代理証明部３１２とログアウト受付部３１３と認証情報記憶部３９１とクライアント秘密鍵記憶部３９２とを実現するハードウェアである。

処理回路３０９は、専用のハードウェアであってもよいし、メモリ３０２に格納されるプログラムを実行するプロセッサ３０１であってもよい。

[0178] 処理回路３０９が専用のハードウェアである場合、処理回路３０９は、例えば、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ、ＦＰＧＡまたはこれらの組み合わせである。

認証装置３００は、処理回路３０９を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路３０９の役割を分担する。

[0179] 処理回路３０９において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0180] このように、処理回路３０９はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0181] 図２４に基づいて、認証局装置４００のハードウェア構成を説明する。

認証局装置４００は処理回路４０９を備える。

処理回路４０９は、秘密鍵生成部４１１と証明書生成部４１２とを実現するハードウェアである。

処理回路４０９は、専用のハードウェアであってもよいし、メモリ４０２に格納されるプログラムを実行するプロセッサ４０１であってもよい。

[0182] 処理回路４０９が専用のハードウェアである場合、処理回路４０９は、例えば、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ、ＦＰＧＡまたはこれらの組み合わせである。

認証局装置４００は、処理回路４０９を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路４０９の役割を分担する。

[0183] 処理回路４０９において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0184] このように、処理回路４０９はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0185] 実施の形態は、好ましい形態の例示であり、本発明の技術的範囲を制限することを意図するものではない。実施の形態は、部分的に実施してもよいし、他の形態と組み合わせて実施してもよい。フローチャート等を用いて説明した手順は、適宜に変更してもよい。

符号の説明

[0186] １００　認証連携システム、１０１　インターネット、１１０　組織システム、１１０Ａ　第１組織システム、１１０Ｂ　第２組織システム、１１０Ｃ　第３組織システム、１１１　イントラネット、１１２　ゲートウェイ装置、１２０　認証システム、１２１　トランザクションデータ、１２１Ａ　基本情報、１２１Ｂ　所有者情報、１２１Ｃ　認証局証明書、１２１Ｄ　その他情報、１２２　トランザクションデータ、１２２Ａ　基本情報、１２２Ｂ　所有者情報、１２２Ｃ　クライアント証明書、１２２Ｄ　その他情報、１２３　トランザクションデータ、１２３Ａ　基本情報、１２３Ｂ　クライ

アント証明書情報、１２３Ｃ　その他情報、１３０　ユーザ端末、１３０Ｇ　ユーザ端末群、１３１Ａ　プロセッサ、１３１Ｂ　メモリ、１３１Ｃ　補助記憶装置、１３１Ｄ　通信装置、１３１Ｅ　入出力インタフェース、１３２　ブラウザ部、１３３　鍵管理部、１４０　サーバ装置、１４０Ｇ　サーバ装置群、１４１Ａ　プロセッサ、１４１Ｂ　メモリ、１４１Ｃ　補助記憶装置、１４１Ｄ　通信装置、１４２　アプリケーション部、２００　管理装置、２０１　プロセッサ、２０２　メモリ、２０３　補助記憶装置、２０４　通信装置、２０９　処理回路、２１１　トランザクション発行部、２１２　トランザクション受付部、２１３　証明書検証部、２１４　ブロックチェーン管理部、２１５　トランザクション検証部、２９０　ブロックチェーン記憶部、３００　認証装置、３０１　プロセッサ、３０２　メモリ、３０３　補助記憶装置、３０４　通信装置、３０９　処理回路、３１１　認証部、３１２　代理証明部、３１３　ログアウト受付部、３９１　認証情報記憶部、３９２　クライアント秘密鍵記憶部、４００　認証局装置、４０１　プロセッサ、４０２　メモリ、４０３　補助記憶装置、４０４　通信装置、４０９　処理回路、４１１　秘密鍵生成部、４１２　証明書生成部、４９０　認証局秘密鍵記憶部。