

明 細 書

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

技術分野

[0001] 本発明の実施形態は、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に関する。

背景技術

[0002] 近年、情報処理装置のデータ秘匿、電子署名、機器認証等にハードウェアセキュリティモジュール（H S M : Hardware Security Module）に格納された暗号鍵を利用する機会が増えている。ここで、H S Mは、暗号処理および鍵管理機能を有し、国際規格（例えば、連邦情報処理規格（F I P S : Federal Information Processing Standard）、C C（Common Criteria）、P C I（Peripheral Component Interconnect）等）の認定を取得しているデバイスである。

[0003] 例えば、特許文献1では、H S Mに記憶された暗号鍵を所定時間経過後に消去し、データを暗号化して利用する場合のセキュリティを高める技術が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：日本国特許第4 9 4 6 5 6 2号公報

発明の概要

発明が解決しようとする課題

[0005] P K C S（Public-Key Cryptography Standards）# 1 1ベースのH S Mでは、特定の個人ではなく、ロールとして認証される。そのため、ユーザ（個人）を特定できないという問題がある。

[0006] この発明は、上記事情に着目してなされたもので、その目的とするところは、PKCS#11ベースのHSMにおいて、ユーザを特定した認証ができる技術を提供することにある。

課題を解決するための手段

[0007] 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、DB鍵をセキュアに記憶する記憶部と、前記暗号化済み認証情報に前記DB鍵を用いて復号し、前記復号された認証情報および前記認証情報を用いて認証する第1の認証部と、前記認証結果に基づいて、前記ユーザIDに紐付けられたチケットを生成し、前記チケットを含む事前認証応答を生成する生成部と、前記事前認証応答を出力する第1の出力部と、前記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、前記セッション情報に含まれる前記チケットに基づいて前記セッション情報を認証し、前記チケットに対応する暗号鍵を生成する第2の認証部と、前記第2の認証部による認証結果を出力する第2の出力部と、を備えるものである。

図面の簡単な説明

[0008] [図1]図1は、実施形態に係る鍵管理システムの構成例を概念的に示す図である。

[図2]図2は、実施形態に係る鍵管理システムにおけるホスト装置およびHSMの構成例を示すブロック図である。

[図3]図3は、実施形態に係る鍵管理システムにおけるアプリケーションサーバの構成例を示すブロック図である。

[図4]図4は、ホスト装置、HSM、およびアプリケーションサーバのソフトウェア構成の一例を示した図である。

[図5]図5は、実施形態に係るユーザ認証登録処理の一例を示したシーケンス図である。

[図6]図6は、図5を用いて説明した登録処理の概念図の一例を示した図である。

[図7]図7は、実施形態に係る認証処理の一例を示したシーケンス図である。

[図8]図8は、図7を用いて説明した登録処理の概念図の一例を示した図である。

[図9]図9は、図7を用いて説明した登録処理の概念図の一例を示した図である。

実施形態

[0009] 以下、図面を参照しながら鍵管理装置、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について詳細に説明する。なお、以下の実施形態では、同一の番号を付した部分については同様の動作を行うものとして、重ねての説明を省略する。例えば、複数の同一または類似の要素が存在する場合に、各要素を区別せずに説明するために共通の符号を用いることがあるし、各要素を区別して説明するために当該共通の符号に加えて枝番号を用いることもある。

[0010] (構成)

図1は、実施形態に係る鍵管理システム100の構成例を概念的に示す図である。図1に示すように、鍵管理システム100は、ホスト装置1と、HSM2と、アプリケーションサーバ3と、を備える。

[0011] ホスト装置1とHSM2は、例えば、事業者事務所10に配置される。ホスト装置1は、HSM2とアプリケーションサーバ3と接続される。ホスト装置1は、アプリケーションサーバ3からの署名生成要求等の依頼をHSM2に送信し、デジタル署名等をアプリケーションサーバ3に送信する。

[0012] 鍵管理装置としてのHSM2は、セキュアに鍵情報の生成、保護および管理を行う耐タンパ性を備えるハードウェアデバイスである。例えば、HSM2は、PCIEでホスト装置1に接続される、或いはLANを介してホスト装置と接続される。例えば、LANで接続される場合、HSM2は、ホスト装置1が配置されるラックと同じラック内に配置されて良い。HSM2は、暗号鍵を含む鍵情報を生成し、生成した暗号鍵をセキュアに保存する。また、HSM2は、保存した鍵情報を用いた暗号化プロセスを含む演算処理を実

行する。例えば、H S M 2 は、保存した鍵情報を用いたデータの暗号化および復号、電子署名、および電子証明書を作成などの演算処理を行う。

[0013] ホスト装置 1 は、H S M 2 と協働することで、アプリケーションサーバ 3 からの依頼に応じて H S M 2 によって生成する暗号鍵をアプリケーションサーバ 3 に提供する。例えば、ホスト装置 1 は、鍵生成機能として、アプリケーションサーバ 3 からの依頼に応じて H S M 2 により生成された鍵情報をアプリケーションサーバ 3 に提供する。例えば、ホスト装置 1 は、アプリケーションサーバ 3 からの依頼に応じて H S M 2 により公開鍵と秘密鍵との鍵ペアを含む鍵情報を生成するように指示して良い。

[0014] また、ホスト装置 1 は、処理内容を示すログデータを保存する機能を有するものであっても良い。例えば、ホスト装置 1 は、H S M 2 が保存する秘密鍵を用いた電子署名などの暗号処理を実行した場合に暗号処理内容を示すログデータを生成し、生成したログデータに H S M 2 が電子署名したデータ（署名付きログデータ）を記憶装置に保存するようにしても良い。なお、処理内容を示すログデータを保存する機能は、H S M 2 が有する形態であってもよい。事業所事務所 10 に配置されていてもよい。

[0015] アプリケーションサーバ 3 は、ホスト装置 1 に電子署名などの処理の依頼を送信する。そして、アプリケーションサーバ 3 は、ホスト装置 1 から、H S M 2 が演算処理（電子署名または暗号化）したデータを取得する。なお、図 1 の例では、1 つのアプリケーションサーバ 3 を示しているが、複数のアプリケーションサーバ 3 がホスト装置 1 と接続されて良いのは勿論である。

また、アプリケーションサーバ 3 は、ホスト装置 1 と一体になっていてもよい、アプリケーションサーバ 3 は事業者事務所 10 に設置されていてもよい。

[0016] 図 2 は、実施形態に係る鍵管理システム 100 におけるホスト装置 1 および H S M 2 の構成例を示すブロック図である。

図 2 に示すように、ホスト装置 1 は、プロセッサ 11、R A M 12、R O M 13、通信部 14、入出力インタフェース 15、入力装置 16、および出

力装置 17 等を備える。プロセッサ 11 は、CPU (central processing unit)、MPU (micro processing unit)、またはDSP (digital signal processor) 等である。プロセッサ 11 は、システムバスを介してホスト装置 1 内の各部と接続され、各部との間でデータを送受信する。プロセッサ 11 は、RAM 12 およびROM 13 と協働してホスト装置 1 における制御およびデータ処理などの動作を実行する。

[0017] RAM (Read Access memory) 12 は、データを一時的に記憶する揮発性のメモリである。RAM 12 は、プロセッサ 11 がプログラムを実行する場合にワーキングメモリとして機能する。

[0018] ROM (Read Only memory) 13 は、ホスト装置 1 の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

[0019] 通信部 14 は、HSM 2 およびアプリケーションサーバ 3 と通信するためのインタフェースである。ここで、HSM 2 との通信において、HSM 2 とホスト装置 1 とがPCLeで接続される場合、通信部 14 を介さず、バスを介してHSM 2 と通信する。一方、HSM 2 とLANで接続される場合、ホスト装置 1 は、通信部 14 を介してHSMと通信する。また、アプリケーションサーバ 3 との通信では、通信部 14 は、有線または無線で通信を行うものであって良い。例えば、通信部 14 は、インターネットなどの広域のネットワークを介してアプリケーションサーバ 3 と接続する。或いは、通信部 14 は、LAN等で直接アプリケーションサーバ 3 と接続する。

[0020] 入出力インタフェース 15 は、入力装置 16 および出力装置 17 等と接続される。入出力インタフェース 15 は、入力装置 16 および出力装置 17 との間で情報の送受信を可能にするインタフェースである。入出力インタフェース 15 は、通信部 14 と一体であってもよい。例えば、ホスト装置 1 と入力装置 16 または出力装置 17 の少なくとも 1 つとは、近距離無線技術等を使用して無線接続されており、当該近距離無線技術を用いて情報の送受信を行ってもよい。

- [0021] 入力装置 16 は、例えば、ホスト装置 1 を管理する管理者がホスト装置 1 に対して各種情報を入力するためのキーボードやポインティングデバイス等を含んでも良い。また、入力装置 16 は、ROM 13 に格納するべきデータを、USB メモリ等のメモリ媒体から読み出すためのリーダや、そのようなデータをディスク媒体から読み出すためのディスク装置を含んでも良い。
- [0022] 出力装置 17 は、プロセッサ 11 で計算した結果、プロセッサ 11 が実行するアプリケーション等を表示するディスプレイ等を含む。また、出力装置 17 は、ディスプレイに表示された情報を印刷するプリンタ等を含む。
- [0023] さらに、図 2 に示すように、HSM 2 は、プロセッサ 21、RAM 22、ROM 23、通信部 24、コプロセッサ 25、セキュア ROM 26 等を備える。
- [0024] プロセッサ 21 は、CPU、MPU、または DSP 等である。プロセッサ 21 は、システムバスを介して HSM 2 内の各部と接続され、各部との間でデータを送受信する。プロセッサ 21 は、RAM 22 および ROM 23 と協働して HSM 2 における制御およびデータ処理などの動作を実行する。
- [0025] RAM 22 は、データを一時的に記憶する揮発性のメモリである。RAM 22 は、プロセッサ 21 がプログラムを実行する場合にワーキングメモリとして機能する。
- [0026] ROM 23 は、HSM 2 の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。
- [0027] 通信部 24 は、ホスト装置 1 と通信するためのインタフェースである。一方、ホスト装置 1 と LAN で接続される場合、HSM は、通信部 24 を介してホスト装置 1 と接続される。
- [0028] コプロセッサ 25 は、CPU、MPU、または DSP 等である。コプロセッサ 25 は、暗号処理やセキュアメッセージングの生成処理などの暗号演算処理を実行する。例えば、コプロセッサ 25 は、公開鍵暗号の暗号化処理および復号処理、共通鍵暗号の暗号化処理および復号処理、ハッシュ関数による演算、等を実行する。

[0029] セキュアROM 26は、耐タンパ性を有するROMである。セキュアROMは、コプロセッサ25が処理を実行する際に使用する暗号鍵等を記憶する不揮発性のメモリである。ここで、耐タンパ性は、HSM2全体として有していても良いし、セキュアROMのみが有していても良い。

[0030] 図3は、実施形態に係る鍵管理システム100におけるアプリケーションサーバ3の構成例を示すブロック図である。

図3に示すように、アプリケーションサーバ3は、プロセッサ31、RAM32、ROM33、通信部34、入出力インタフェース35、入力装置36、出力装置37等を備える

プロセッサ31は、CPU、MPU、またはDSP等である。プロセッサ31は、システムバスを介してアプリケーションサーバ3内の各部と接続され、各部との間でデータを送受信する。プロセッサ31は、RAM32およびROM33と協働してアプリケーションサーバ3における制御およびデータ処理などの動作を実行する。

[0031] RAM32は、データを一時的に記憶する揮発性のメモリである。RAM32は、プロセッサ31がプログラムを実行する場合にワーキングメモリとして機能する。

[0032] ROM33は、アプリケーションサーバ3の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

[0033] 通信部34は、ホスト装置1と通信するためのインタフェースである。通信部34は、有線または無線で通信を行うものであって良い。例えば、通信部34は、インターネットなどの広域のネットワークを介してホスト装置1と接続する。或いは、通信部34は、LAN等で直接ホスト装置1と接続する。

[0034] 入出力インタフェース35は、入力装置36および出力装置37等と接続される。入出力インタフェース35は、入力装置36および出力装置37との間で情報の送受信を可能にするインタフェースである。入出力インタフェース35は、通信部34と一体であってもよい。例えば、アプリケーション

サーバ3と入力装置36または出力装置37の少なくとも1つとは、近距離無線技術等を使用して無線接続されており、当該近距離無線技術を用いて情報の送受信を行ってもよい。

[0035] 入力装置36は、例えば、アプリケーションサーバ3を管理するユーザがホスト装置1に対して各種情報を入力するためのキーボードやポインティングデバイス等を含んでも良い。また、入力装置36は、ROM33に格納すべきデータを、USBメモリ等のメモリ媒体から読み出すためのリーダや、そのようなデータをディスク媒体から読み出すためのディスク装置を含んでも良い。

[0036] 出力装置37は、プロセッサ31で計算した結果、プロセッサ31が実行するアプリケーション等を表示するディスプレイ等を含む。また、出力装置37は、ディスプレイに表示された情報を印刷するプリンタ等を含む。

[0037] 図4は、ホスト装置1、HSM2、およびアプリケーションサーバ3のソフトウェア構成の一例を示した図である。

ホスト装置1は、HSM設定アプリケーション101（図4ではHSM設定アプリと表示）と、独自API102、鍵管理API103、およびユーザデータベース104（図4ではユーザDBと表示）を備える。HSM2は、認証認可機能部201、スロット202、鍵管理エンジン203を備える。また、アプリケーションサーバ3は、ユーザアプリケーション301を備える。

[0038] HSM設定アプリケーション101は、ホストPCの管理者がアプリケーションサーバ3を利用するユーザの登録を行うためのアプリケーションである。HSM設定アプリケーション101は、例えば、HSMを製作する事業者が提供するアプリケーションである。HSM設定アプリケーション101は、プロセッサ11の制御の下、動作可能である。

[0039] 独自API102は、HSMを製作する事業者が提供するAPIであり、HSM2の後述する認証認可機能部201と接続することが可能なAPIである。独自API102は、プロセッサ11の制御の下、動作可能である。

- [0040] 鍵管理API103は、PKCS#11を準拠したAPIであり、例えば、HSM2の鍵管理エンジン203と接続することが可能である。鍵管理API103は、プロセッサ11の制御の下、動作可能である。
- [0041] ユーザデータベース104は、例えば、ユーザアプリケーション301を利用するユーザのユーザIDと暗号化済み認証情報等を記憶するデータベースである。なお、暗号化済み認証情報は、後述する。例えば、ユーザデータベース104は、ROM13の一部を利用する記憶部である。
- [0042] 認証認可機能部201は、プロセッサ21により制御され、後述するスロット202に記憶されたDB鍵等を用いて認証動作を行う。例えば、認証認可機能部201は、コプロセッサ25の制御の下、動作可能である。
- [0043] スロット202は、例えば、スロット0、・・・スロットXを備え、各スロット202は、図4等では示していないが、対応するトークンを備える。通常、各スロットとトークンは、アプリケーションサーバ3ごと（すなわち顧客ごと）に1つのスロットとトークンを割り当てられる。そのため、従来の方法では、ユーザアプリケーション301を利用するユーザのうちどのユーザが利用したかまでは分からない。なお、本実施形態におけるアプリケーションサーバ3は、スロットXを用いる例を説明するが、任意のスロットに割り当てられるのは勿論である。また、スロット202は、例えば、事前にDB（Data Base）鍵、ログ鍵、チケットを生成するための乱数の生成方法等を記憶する。これらの情報は、例えば、セキュアROM26に記憶される。
- [0044] 鍵管理エンジン203は、ホスト装置1とPKCS#11準拠の暗号通信を行うためのAPIである。鍵管理エンジン203は、プログラム21の制御の下、動作可能である。鍵管理エンジン203は、標準規格対応したAPIであれば良いため、ここでの詳細な説明を省略する。
- [0045] ユーザアプリケーション301は、アプリケーションサーバ3の各ユーザが利用するアプリケーションであり、プロセッサ31の制御の下、動作する。なお、ユーザアプリケーション301から独自API102又は鍵管理対応API103への通信は、ユーザアプリケーション301が独自API1

02又は鍵管理対応API103の機能を直接呼び出しても良いし、ホスト装置1がユーザアプリケーション301からの通信を中継するアプリケーションを有していてもよい。

[0046] (動作)

(登録動作)

最初に、実施形態に係るHSM2へのユーザ認証登録処理について説明する。

図5は、実施形態に係るユーザ認証登録処理の一例を示したシーケンス図である。このシーケンスの各動作は、ホスト装置1のプロセッサ11およびHSM2のプロセッサ21およびコプロセッサ25がプロセッサ11の内部メモリ、RAM12またはROM13、およびプロセッサ21の内部メモリ、RAM22、ROM、またはセキュアROM26に格納されたプログラムを読み出して実行することにより、実現される。

[0047] ここで、以下で説明する処理において、ホスト装置1の管理者は、一般的な方法を用いてホスト装置1に登録済みであるとする。そのため、ユーザデータベースには、管理者ユーザIDに紐付けられた暗号化済み管理者認証情報が記憶されているものとする。また、アプリケーションサーバ3は、スロットXを利用するものとする。そのため、アプリケーションサーバ3のユーザは、HSM2のスロットXに対して登録を実施することになる。

[0048] ステップST101で、ホスト装置1のプロセッサ11は、事前登録要求をHSM2に送信する。最初に、プロセッサ11は、ユーザ登録をしたいという管理者からの入力に応じて、HSMを作成した事業者が提供するアプリケーションを立ち上げ、出力装置17にアプリケーションを表示させるように制御する。そして、取得部として動作するプロセッサ11は、入力装置16から管理者ユーザIDおよび管理者認証情報を取得する。さらに、取得部として動作するプロセッサ11は、ユーザデータベースに記憶された管理者ユーザIDに紐付けられた暗号化済み管理者認証情報を取得する。そして、送信部と動作するプロセッサ11は、独自API102を介して、取得した

管理者ユーザID、管理者認証情報、暗号化済み管理者認証情報をHSM2に送信する。

[0049] ステップST102で、HSM2のプロセッサ21およびコプロセッサ25は、認証処理を実施する。出力部として動作するプロセッサ21は、事前登録要求に含まれる管理者ユーザIDに基づいてスロットXを用いて認証処理を実施する指示と共にコプロセッサ25に暗号化済み管理者認証情報を出力する。復号部としてコプロセッサ25は、DB鍵を用いて、暗号化済み管理者認証情報を復号する。そして、認証部として動作するプロセッサ21は、復号された管理者認証情報および管理者認証情報に基づいて認証処理を実施する。例えば、復号された管理者認証情報および管理者認証情報が一致すれば認証され、不一致の場合、認証されない。認証できたことを確認したコプロセッサ25は、乱数を用いたチケットを発行するとともに当該チケットの有効期限を設定する。そして、出力部として動作するコプロセッサ25は、チケットおよび当該チケットの有効期限プロセッサ21に出力する。

[0050] ステップST103で、プロセッサ21は、認証認可機能部201を介して、当該チケットおよび有効期限を含む事前登録応答をホスト装置1に送信する。

[0051] ステップST104で、プロセッサ11は、ユーザ登録要求をHSM2に送信する。事前登録応答を受信したプロセッサ11は、HSM設定アプリケーション101を用いて、チケットを取得したことおよび当該チケットの有効期限を管理者に知らせる。管理者は、登録したいユーザ（例えば、アプリケーションサーバ3のユーザ）のユーザIDを入力する。ユーザIDは、ユーザを一意に特定することが可能な情報であれば良く、例えば、メールアドレス、アプリケーションサーバ3に登録されたユーザ登録番号等であって良い。プロセッサ11は、独自APIを介して、ユーザID、チケット、および管理者ユーザIDを含むユーザ登録要求を送信する。

[0052] ステップST105で、プロセッサ21およびコプロセッサ25は、仮認証情報を発行する。プロセッサ21は、事前登録要求に含まれる管理者ユー

ザIDに基づいてスロットXを用いて認証処理を実施する指示と共にコプロセッサ25にユーザIDを出力する。生成部として動作するコプロセッサ25は、乱数を用いて仮認証情報を生成し、ユーザIDと紐付ける。さらにコプロセッサ25は、仮認証情報にDB鍵を用いて暗号化する。そして、コプロセッサ25は、仮認証情報をおよび暗号化済み仮認証情報をプロセッサ21に出力する。

[0053] ステップST106で、プロセッサ21は、認証認可機能部201を介して、仮認証情報および暗号化済み仮認証情報をホスト装置1に送信する。プロセッサ11は、ユーザIDと紐付けて暗号化済み仮認証情報をユーザデータベースに記憶させる。

[0054] ステップST107で、送信部として動作するプロセッサ11は、ユーザ本認証情報をHSM2に送信する。プロセッサ11は、HSM設定アプリケーション101を用いて、仮認証情報を管理者に示す。そして、管理者は、ユーザID、仮認証情報、および本認証情報をホスト装置1に入力する。ここで、本認証情報は、ユーザが使用するパスワードであり、ユーザにより設定される情報であって良い。そのため、ホスト装置1は、アプリケーションサーバ3のユーザから本認証情報を事前に取得しておいて良い。プロセッサ11は、ユーザIDに紐付けられた暗号化済み仮認証情報をユーザデータベースから取得する。そして、プロセッサ11は、独自APIを介して、ユーザID、仮認証情報、暗号化済み仮認証情報、および本認証情報をHSM2に送信する。

[0055] ステップST108で、プロセッサ21およびコプロセッサ25は、認証処理および暗号化を実施する。プロセッサ21は、コプロセッサ25に、ユーザIDに基づいてスロットXを用いて認証処理を実施する指示と共にユーザ本認証情報に含まれる暗号化済み仮認証情報、仮認証情報、および本認証情報を出力する。認証部として動作するコプロセッサ25は、暗号化済み仮認証情報を復号し、復号された仮認証情報と仮認証情報が一致するかどうかを判定する。一致する場合、認証され、不一致の場合、認証されない。認証

された場合、コプロセッサ 25 は、DB 鍵を用いて本認証情報を暗号化する。そして、暗号化済み本認証情報をプロセッサ 21 に出力する。

[0056] ステップ ST109 で、プロセッサ 21 は、認証認可機能部 201 を介して、暗号化済み本認証情報をホスト装置 1 に送信する。

[0057] ステップ ST110 で、プロセッサ 11 は、ユーザ ID と紐付けて暗号化済み本認証情報をユーザデータベースに記憶させる。

[0058] 図 6 は、図 5 を用いて説明した登録処理の概念図の一例を示した図である。

図 6 に示したステップ ST は、図 5 で示したステップ ST に対応する。図 6 に示すように、最初に、HSM 設定アプリケーション 101 から管理者ユーザ ID および管理者認証情報を用いて HSM 2 に管理者の認証を実施させる。その後、登録させたいユーザのユーザ ID およびチケットを含むユーザ登録要求を HSM 2 に出力させ、仮認証情報を発行させる。そして、ユーザ ID、仮認証情報および本認証情報を HSM 2 に出力することにより、ユーザ ID に紐づけた本認証情報を登録させる。

[0059] (認証処理)

次に、HSM 2 を用いた認証処理の一例について説明する。

図 7 は、実施形態に係る認証処理の一例を示したシーケンス図である。

このシーケンスの各動作は、ホスト装置 1 のプロセッサ 11、HSM 2 のプロセッサ 21 およびコプロセッサ 25、およびアプリサーバ 3 のプロセッサ 31 がプロセッサ 11 の内部メモリ、RAM 12、または ROM 13、プロセッサ 21 の内部メモリ、RAM 22、または ROM 23、またはセキュア ROM 26、およびプロセッサ 31 の内部メモリ、RAM 32、または ROM 33 に格納されたプログラムを読み出して実行することにより、実現される。

[0060] ここで、以下の説明におけるアプリケーションサーバ 3 のユーザは、上述した登録動作により登録されたユーザであるとする。以下において、上述した本認証情報は、単に認証情報と記載する。

- [0061] ステップST201で、プロセッサ31は、事前認証情報をホスト装置1に送信する。送信部として動作するプロセッサ31は、ユーザアプリケーション301等を用いてユーザに対してユーザIDおよび認証情報を要求する。プロセッサ31は、ユーザがユーザアプリケーション301に入力したユーザIDおよび認証情報を取得する。プロセッサ31は、取得したユーザIDおよび認証情報を含む事前認証情報を送信する。
- [0062] ステップST202で、送信部として動作するプロセッサ11は、事前認証要求をHSM2に送信する。プロセッサ11は、ユーザIDに対応する暗号化済み認証情報をユーザデータベース104から取得する。そして、プロセッサ11は、独自API102を介して、ユーザID、認証情報、および暗号化済み認証情報を含む事前認証要求をHSM2に送信する。
- [0063] ステップST203で、プロセッサ21およびコプロセッサ25は、認証処理を実施する。プロセッサ21は、事前認証要求に含まれるユーザIDに基づいてスロットXを用いて認証処理を実施する指示と共に、認証情報および暗号化済み認証情報をコプロセッサ25に出力する。認証部として動作するコプロセッサ25は、暗号化済み認証情報を復号する。そして、復号された認証情報と認証情報が一致するかどうか判定する。一致する場合、認証され、不一致の場合、認証されない。認証された場合、生成部として動作するコプロセッサ25は、乱数を用いてチケットを発行するとともに、当該チケットに対する有効期限を設定する。有効期限は、任意の時間を設定して良い。
- [0064] ステップST204で、プロセッサ21は、認証応答をホスト装置1に送信する。コプロセッサ25は、チケットおよび当該チケットの有効期限をプロセッサ21に出力する。プロセッサ21は、認証認可機能部201を介して、チケットおよびチケットの有効期限を含む事前認証応答をホスト装置1に送信する。
- [0065] ステップST205で、プロセッサ11は、事前認証応答をアプリケーションサーバ3に送信する。これにより、アプリケーションサーバ3のユーザ

は、認証される。そして、ユーザは、H S M 2 から送信されたチケットに基づいて各種処理を実施することになる。

[0066] ステップS T 2 0 6で、プロセッサ3 1は、初期化指示をホスト装置1に送信する。プロセッサ3 1は、ユーザアプリケーション3 0 1を介して所定の処理に基づいて、H S M 2の利用時認証を必要とすると判定する。そしてプロセッサ3 1は、プロセスにおけるH S M 2への接続を初期化するための初期化指示を生成し、当該初期化指示をホスト装置1に送信する。

[0067] ステップS T 2 0 7で、プロセッサ1 1は、鍵管理A P I 1 0 3を介して、初期化指示をH S M 2に送信する。さらに、初期化指示を受信したプロセッサ1 1は、H S M 2で利用可能な初期化指示に変換し、変換した初期化指示を鍵管理A P I 1 0 3を介して、H S M 2に送信する。H S M 2のプロセッサ2 1またはコプロセッサ2 5は、初期化指示に従って、例えばC _ I n i t i a l i z eを用いて、アプリケーションサーバ3のH S M 2への接続を初期化する。

[0068] ステップS T 2 0 8で、プロセッサ3 1は、スロット番号をホスト装置1に送信する。次に、プロセッサ3 1は、ユーザアプリケーション3 0 1を介して、ユーザが利用するスロット番号（例えば、本実施形態ではスロットX）をホスト装置1に送信する。

[0069] ステップS T 2 0 9で、プロセッサ1 1は、スロット番号をH S M 2に送信する。スロット番号を受信したプロセッサ1 1は、スロット番号をH S M 2で利用可能なスロット番号に変換し、鍵管理A P I 1 0 3を介して、セッション開放指示をH S M 2に送信する。セッション開放指示を受信したコプロセッサ2 5は、例えばC _ O p e n S e s s i o nを用いて、スロット番号（スロットX）に対応するトークンとユーザアプリケーション3 0 1との間にセッションを確立させ、確立されたセッションを識別するセッションハンドルを取得する。

[0070] ステップS T 2 1 0で、プロセッサ2 1は、鍵管理エンジン2 0 3を介して、ホスト装置1にセッションハンドルであるセッションを送信する。

- [0071] ステップST211で、プロセッサ11は、通信部14を用いて、セッションをアプリケーションサーバ3に送信する。
- [0072] ステップST212で、プロセッサ31は、セッション情報をホスト装置1に送信する。セッションを受信したプロセッサ31は、セッションハンドル、ロール、およびチケットを含むセッション情報を生成し、生成したセッション情報をホスト装置1に送信する。
- [0073] ここで、一般には、セッション情報は、セッションハンドル、ロール、PINを含むが、本実施形態では、事前認証応答に含まれるチケットをセッション情報に含むように生成する。
- [0074] ステップST213で、プロセッサ11は、セッション情報をHSM2に送信する。セッション情報を受信したプロセッサ11は、セッション情報をHSM2で利用可能なセッション情報に変換し、鍵管理API103を介して、セッション情報をHSM2に送信する。
- [0075] ステップST214で、プロセッサ21およびコプロセッサ25は、認証処理を実施する。認証部として動作するコプロセッサ25は、例えば、C_Loginを用いて、セッション情報を認証する。例えば、コプロセッサ25は、セッション情報に含まれるロールの認証を行う。認証の結果、コプロセッサ25は、例えば、チケットに対応する暗号鍵を生成する。暗号鍵は、例えば、セキュアROM26に記憶される。この際、セッション情報に含まれるチケットに対応するユーザIDを識別することが可能である。出力部として動作するコプロセッサ25は、認証結果をプロセッサ21に出力する。
- [0076] ステップST215で、プロセッサ21は、鍵管理エンジン203を介して、認証結果をホスト装置1に送信する。
- [0077] ステップST216で、プロセッサ11は、通信部14を用いて、認証結果をアプリケーションサーバ3に送信する。
- [0078] ステップST217で、プロセッサ31は、暗号演算依頼をホスト装置1に送信する。プロセッサ31は、例えば、C_Encrypt等の暗号演算を必要とすると、当該暗号演算を実施する依頼である暗号演算依頼をホスト

装置 1 に送信する。

- [0079] ステップ S T 2 1 8 で、プロセッサ 1 1 は、PKCS # 1 1 対応 API 1 0 2 3 を通じて、暗号演算依頼を HSM 2 に送信する。
- [0080] ステップ S T 2 1 9 で、プロセッサ 2 1 およびコプロセッサ 2 5 は、暗号演算を実施する。コプロセッサ 2 5 は、暗号演算依頼による暗号演算をステップ S T 2 1 4 で生成されたチケットに対応する暗号鍵を用いて実施する。そして、コプロセッサ 2 5 は、暗号演算による処理結果、暗号演算のログ、チケット、メッセージ認証コード (MAC : Message Authentication Code) を含む暗号演算結果を生成する。プロセッサ 2 1 は、演算結果を ROM 2 3 に記憶して良い。メッセージ認証コードは、生成されたログ及び取得されたチケットに対して生成される。ホスト装置 1、HSM 2、及びユーザアプリケーションサーバ 3 は、必要に応じて、メッセージ認証コードに基づいてログ又はチケットの改ざんを検知することができ、ユーザの否認防止を確実にすることができる。
- [0081] ステップ S T 2 2 0 で、プロセッサ 2 1 は、演算結果をホスト装置 1 に送信する。
- [0082] ステップ S T 2 2 1 で、プロセッサ 1 1 は、演算結果を記憶させる。例えば、プロセッサ 1 1 は、演算結果のチケットとユーザ ID を紐付け、演算結果 (ログおよび MAC) をユーザデータベースに記憶させる。
- [0083] ステップ S T 2 2 2 で、プロセッサ 1 1 は、暗号演算処理による処理結果をアプリケーションサーバ 3 に送信する。
- [0084] 図 8 および図 9 は、図 7 を用いて説明した登録処理の概念図の一例を示した図である。

図 8 および図 9 に示したステップ S T は、図 7 で示したステップ S T に対応する。図 8 に示すように、最初に、事前認証情報に基づいて認証を実施させ、チケットを払い出す。そして、少なくともチケットを含むセッション情報に基づいて認証を実施させ、チケットに対応する暗号鍵を生成させる。当該チケットは、ユーザ ID と紐付けされており、ユーザアプリケーション 3

01を扱っているユーザを特定することが可能である。そのため、チケットに対応する暗号鍵を用いた暗号演算のログがどのユーザの処理であるかを認識することが可能である。

[0085] 上述したように実施することにより、ユーザ個人の認否防止および責任追及性がサポートされる。すなわち、ユーザアプリケーション301を利用するユーザのうち誰が作ったのか、誰が使ったのか、誰が廃棄したのか等をログから特定することが可能となる。すなわち上記により、暗号演算に使用されスロットごとに生成、利用、及び削除される暗号鍵のライフサイクル全体の保証ができるようになる。

[0086] (実施形態の作用効果)

以上説明した実施形態によれば、PKCS#11を準拠しつつ、ユーザアプリケーション301を利用するユーザを特定した認証をすることができる。また、ユーザが利用したログを取ることで、ユーザによる不正利用に対する責任追跡性を有することができる。

[0087] (変形例)

上述した実施形態は、HSM2を用いてチケットを発行し、当該チケットをアプリケーションサーバ3に送信する例を示したが、ホスト装置1がチケットを発行し、アプリケーションサーバ3に送信しても良い。すなわち、チケット発行処理の際の認証および生成機能をホスト装置1が実施しても良い。

[0088] 本実施形態に係るプログラムは、ホスト装置1、HSM2、またはアプリケーションサーバ3としての電子機器（コンピュータ）に記憶された状態で譲渡されてよいし、電子機器に記憶されていない状態で譲渡されてもよい。後者の場合は、プログラムは、ネットワークを介して譲渡されてよいし、記憶媒体に記憶された状態で譲渡されてもよい。記憶媒体は、非一時的な有形の媒体である。記憶媒体は、ホスト装置1、HSM2、またはアプリケーションサーバ3としてのコンピュータが読み取り可能な媒体（コンピュータ可読媒体）である。記憶媒体は、光ディスク（例えば、CD-ROM）、磁気

ディスク、半導体メモリ（例えば、メモリカード）などのプログラムを記憶可能かつコンピュータで読取可能な媒体であればよく、その形態は問わない。

[0089] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

- [請求項1] 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、
DB鍵をセキュアに記憶する記憶部と、
前記暗号化済み認証情報に前記DB鍵を用いて復号し、前記復号された認証情報および前記認証情報を用いて認証する第1の認証部と、
前記認証結果に基づいて、前記ユーザIDに紐付けられたチケットを生成し、前記チケットを含む事前認証応答を生成する生成部と、
前記事前認証応答を出力する第1の出力部と、
前記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、
前記セッション情報に含まれる前記チケットに基づいて前記セッション情報を認証し、前記チケットに対応する暗号鍵を生成する第2の認証部と、
前記第2の認証部による認証結果を出力する第2の出力部と、
を備える鍵管理装置。
- [請求項2] 認証された前記セッション情報を含む暗号演算依頼を取得する第3の取得部と、
前記チケットに対応して生成された前記暗号鍵を用いて暗号演算を実施する暗号演算部と、
前記チケット、前記暗号演算によるログ、メッセージ認証コード（MAC）を含む演算結果を出力する第3の出力部と、
をさらに備える、
請求項1に記載の鍵管理装置。
- [請求項3] 認証された前記セッション情報を含む暗号演算依頼を取得する第3の取得部と、
前記チケットに対応して生成された前記暗号鍵を用いて暗号演算を実施する暗号演算部と、
前記チケット、前記暗号演算によるログ、メッセージ認証コード（

MAC)を含む演算結果を記憶する第2の記憶部と、

をさらに備える、

請求項1に記載の鍵管理装置。

[請求項4]

前記記憶部は、耐タンパ性を備える、

請求項1に記載の鍵管理装置。

[請求項5]

前記第1の取得部は、管理者ユーザID、管理者認証情報、暗号化済み管理者認証情報を含む事前登録要求を取得し、

前記第1の認証部は、前記暗号化済み管理者認証情報に前記DB鍵を用いて復号し、前記復号された前記管理者認証情報および前記管理者認証情報を用いて認証し、

前記生成部は、前記管理者認証情報の認証結果に基づいて前記管理者ユーザIDに紐付けられた第2のチケットを生成し、前記第2のチケットおよび前記第2のチケットの有効期限を含む事前登録応答を生成し、

前記第1の出力部は、前記事前登録応答を出力する、

請求項1に記載の鍵管理装置。

[請求項6]

前記第1の取得部は、前記事前登録応答の出力に応じて、前記第2のチケット、ユーザIDを含むユーザ登録要求をさらに取得し、

前記生成部は、乱数を用いて仮認証情報および暗号化済み仮認証情報を生成し、

前記第1の出力部は、前記仮認証情報および前記暗号化済み仮認証情報を出力する、

請求項5に記載の鍵管理装置。

[請求項7]

前記第1の取得部は、前記仮認証情報の出力に応じて前記ユーザID、前記仮認証情報、前記暗号化済み仮認証情報、および本認証情報を含むユーザ本認証情報を取得し、

前記第1の認証部は、前記暗号化済み仮認証情報に前記DB鍵を用いて復号化し、前記復号された仮認証情報および前記仮認証情報を用

いて認証し、前記認証に応じて、前記本認証情報に前記ＤＢ鍵を用いて暗号化する、

請求項６に記載の鍵管理装置。

[請求項８] 前記事前認証応答は、前記チケットの有効期限を含む、
請求項１に記載の鍵管理装置。

[請求項９] 鍵管理装置と、
前記鍵管理装置と接続されるホスト装置と、
を備える鍵管理システムであって、
前記ホスト装置は、
アプリケーションサーバから、ユーザＩＤ、認証情報を含む事前
認証情報を取得する取得部と、
前記認証情報を暗号化した暗号化済み認証情報を記憶する記憶部
と、
前記ユーザＩＤ、認証情報、前記暗号化済み仮認証情報を含む事
前認証要求を前記鍵管理装置に出力する第１の出力部と、
前記事前認証要求に応じてチケットを含む事前認証応答を取得し
、前記アプリケーションサーバに送信する送信部と、
前記チケットを含むセッション情報受信する受信部と、
前記セッション情報を出力する第２の出力部と、
を備え、
前記鍵管理装置は、
ＤＢ鍵をセキュアに記憶する記憶部と、
前記ＤＢ鍵を用いて前記事前認証要求に含まれる暗号化済み認証
情報を復号し、前記復号された認証情報および前記認証情報を用いて
認証する第１の認証部と、
前記認証結果に基づいて、前記ユーザＩＤに紐付けられたチケッ
トを生成し、前記チケットを含む事前認証応答を生成する生成部と、
前記事前認証応答を出力する第１の出力部と、

前記セッション情報に含まれる前記チケットに基づいて前記セッション情報を認証し、前記チケットに対応する暗号鍵を生成する第2の認証部と、

前記第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、鍵管理システム。

[請求項10] 鍵管理装置のプロセッサが実行する鍵管理方法であって、
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
取得することと、

DB鍵をセキュアに記憶することと、
前記暗号化済み認証情報に前記DB鍵を用いて復号することと、
前記復号された認証情報および前記認証情報を用いて認証すること
と

前記認証結果に基づいて、前記ユーザIDに紐付けられたチケット
を生成することと、 前記チケットを含む事前認証応答を生成すること
とと、

前記事前認証応答を出力することと、
前記チケットを含むセッション情報を取得することと、
前記セッション情報に含まれる前記チケットに基づいて前記セッション
情報を認証し、前記チケットに対応する暗号鍵を生成することと
、

前記セッション情報の認証結果を出力することと、
を備える、鍵管理方法。

[請求項11] 鍵管理装置のプロセッサによって実行させるための命令を備える鍵
管理プログラムであって、

前記命令は、
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
取得することと、

DB鍵をセキュアに記憶することと、

前記暗号化済み認証情報に前記ＤＢ鍵を用いて復号することと、
前記復号された認証情報および前記認証情報を用いて認証することと、
前記認証結果に基づいて、前記ユーザＩＤに紐付けられたチケットを生成することと、前記チケットを含む事前認証応答を生成することと、
前記事前認証応答を出力することと、
前記チケットを含むセッション情報を取得することと、
前記セッション情報に含まれる前記チケットに基づいて前記セッション情報を認証し、前記チケットに対応する暗号鍵を生成することと、
前記セッション情報の認証結果を出力することと、
を備える、鍵管理プログラム。

[請求項12] プロセッサによって実行されるプログラムを記憶した非一時的なコンピュータ可読記憶媒体であって、
前記プログラムは、前記プロセッサに、
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ことと、
ＤＢ鍵をセキュアに記憶することと、
前記暗号化済み認証情報に前記ＤＢ鍵を用いて復号することと、
前記復号された認証情報および前記認証情報を用いて認証することと
前記認証結果に基づいて、前記ユーザＩＤに紐付けられたチケットを生成することと、前記チケットを含む事前認証応答を生成することと、
前記事前認証応答を出力することと、
前記チケットを含むセッション情報を取得することと、
前記セッション情報に含まれる前記チケットに基づいて前記セッション

セッション情報を認証し、前記チケットに対応する暗号鍵を生成することと
、
前記セッション情報の認証結果を出力することと、
を実行させる、コンピュータ可読記憶媒体。