

明 細 書

発明の名称： リモート発行システムおよびデータ生成サーバ

技術分野

[0001] 本発明の実施形態は、リモート発行システムおよびデータ生成サーバに関する。

背景技術

[0002] 従来、携帯可能電子装置としてのＩＣカードは、クレジットカード等として運用するための情報を運用機関が書き込んで使用可能とする二次発行という手続きが必要である。また、ＩＣカードに対して、新たな機能を追加する場合も運用機関による所定の手続きが必要である。従来、ＩＣカードに対する二次発行や機能追加は、運用機関又は取扱い店舗の係員が公的な証明書などによってユーザの本人確認を行った後に、専用の発行機を用いて行っている。

[0003] 上述したような従来のＩＣカードに対する二次発行や機能追加などの発行処理の手続きでは、ユーザが運用機関又は店舗などの指定場所へ行ったり、指定場所の係員による人的な本人確認を行ったりする必要がある。また、近年では、指紋などの生体情報を用いて本人確認を行う機能を有するＩＣカードが開発されているが、このような生体認証機能を有するＩＣカードであっても、従来のＩＣカードと同様な手続きで二次発行や機能追加などの発行処理を行う必要があるという問題がある。

先行技術文献

特許文献

[0004] 特許文献１：日本国特開２０１６－１６７２０１号公報

発明の概要

発明が解決しようとする課題

[0005] 上記の課題を解決するために、本発明は、利便性が高い発行処理の手続きを実現できるリモート発行システムおよびデータ生成サーバを提供すること

を目的とする。

課題を解決するための手段

[0006] 実施形態によれば、リモート発行システムは、携帯可能電子装置とデータ生成サーバとを有する。携帯可能電子装置は、生体センサとメモリと通信インターフェースと第1プロセッサとを有する。生体センサは、生体情報を取得する。メモリは、ユーザの生体情報を記憶する記憶領域を含む。通信インターフェースは、ユーザ端末と接続されるリーダライタと通信する。第1プロセッサは、生体センサにより取得する生体情報とメモリに保存する生体情報との照合による生体認証が成功した場合に当該携帯可能電子装置において発行処理を行うための認証データを生成し、認証データを前記リーダライタへ出力し、リーダライタから供給される認証データに対応する発行データに基づいて発行処理を実行する。データ生成サーバは、通信部と第2プロセッサとを有する。通信部は、ユーザ端末と通信する。第2プロセッサは、ユーザ端末から携帯可能電子装置が生成した認証データと契約IDとを含む発行リクエストを受信した場合、契約IDに対応する申請データと認証データとに基づいて携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データをユーザ端末へ送信する。

図面の簡単な説明

[0007] [図1]図1は、第1実施形態に係るリモート発行システムとしてのICカード発行システムの構成例を概略的に示す図である。

[図2]図2は、第1実施形態に係るリモート発行システムとしてのICカード発行システムによって発行手続きがなされるICカードの構成例を示すブロック図である。

[図3]図3は、第1実施形態に係るリモート発行システムとしてのICカード発行システムにおける携帯端末の構成例を示すブロック図である。

[図4]図4は、第1実施形態に係るリモート発行システムとしてのICカード発行システムにおける契約管理サーバの構成例を示すブロック図である。

[図5]図5は、第1実施形態に係るリモート発行システムとしてのICカード

発行システムにおけるデータ生成サーバの構成例を示すブロック図である。

[図6]図6は、第1実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける申請手続きの動作例を説明するためのシーケンスである。

[図7]図7は、第1実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンスである。

[図8]図8は、第1実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンスである。

[図9]図9は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムの構成例を概略的に示す図である。

[図10]図10は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムによって発行手続きがなされるＩＣカードの構成例を示すブロック図である。

[図11]図11は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける携帯端末の構成例を示すブロック図である。

[図12]図12は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける契約管理サーバの構成例を示すブロック図である。

[図13]図13は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおけるデータ生成サーバの構成例を示すブロック図である。

[図14]図14は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける申請手続きの動作例を説明するためのシーケンスである。

[図15]図15は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンス

である。

[図16]図16は、第2実施形態に係るリモート発行システムとしてのＩＣカード発行システムにおける発行手続きの動作例を説明するためのシーケンスである。

実施形態

[0008] 以下、第1および第2実施形態について、図面を参照しつつ説明する。

(第1実施形態)

まず、第1実施形態に係るリモート発行システムとしてのＩＣカード発行システム1について説明する。

[0009] 図1は、第1実施形態に係るリモート発行システムとしてのＩＣカード発行システム1の構成例を模式的に示す図である。

図1に示す構成例において、ＩＣカード発行システム1は、ＩＣカード2、ユーザ端末3、データ管理システム4、および、発行制御システム5を有する。

[0010] ＩＣカード2は、生体認証を実行する機能を有する携帯可能電子装置の一例である。第1実施形態に係るＩＣカード2は、人物から取得する認証情報としての生体情報を取得するための生体センサ20を備える。例えば、ＩＣカード2が具備する生体センサ20は、生体情報の一例としての指紋を読み取る指紋センサである。生体センサとしての指紋センサ20を備えるＩＣカード2は、指紋センサが読み取る人物の指紋とＩＣカード2内のメモリに予め登録されている登録者（ユーザ、カードホルダ）の指紋とを照合することにより本人確認としての指紋認証（生体認証）を実行する。

[0011] 第1実施形態において、ＩＣカード2は、生体情報としての指紋を用いて生体認証を行う機能を有する指紋センサカードであるものとして説明するものとする。ただし、第1実施形態に係る携帯可能電子装置としてのＩＣカード2は、生体情報として指紋による指紋（生体）認証を行うものに限定されるものではない。例えば、ＩＣカード2で例示される携帯可能電子装置は、指紋以外の生体情報によって生体認証を行うものであっても良い。

- [0012] ユーザ端末3は、ユーザが所持する情報処理装置である。ユーザ端末3は、例えば、スマートフォン、タブレットPC、パソコンなどである。ユーザ端末3は、ユーザ自身が操作するものであって、ICカード2と通信するカードリーダーおよびインターネットなどのネットワークを介して各サーバ4A、5Aと通信する通信部とを備えるものであれば良い。また、ユーザ端末3は、ICカード2と通信するカードリーダーを備えるものに代えて、外部機器としてのカードリーダーに接続するためのインターフェースを備えるものであっても良い。
- [0013] データ管理システム4は、遠隔によってユーザが保持するICカードにおける発行処理（二次発行又は機能追加など）の申請を受け付けるシステムである。データ管理システム4は、契約管理サーバ4Aとデータストレージ4Bとを有する。契約管理サーバ4Aは、サーバ装置で構成される。データストレージ4Bは、契約管理サーバ4Aからアクセス可能な記憶装置を含む装置である。契約管理サーバ4Aは、データストレージ4Bにアクセスする機能、インターネットを介してユーザ端末3と通信する機能および発行制御システム5のデータ生成サーバ5Aと通信する機能を有する。
- [0014] 契約管理サーバ4Aは、ユーザが所持するユーザ端末3と通信し、ユーザ端末3からの当該ユーザが保持するICカードに対する発行処理（契約）に関する申請データを取得する。ここで、ICカードに対する発行処理とは、二次発行又は機能追加を含むものとする。ICカードの二次発行とは、発行業者からユーザ（カードホルダ）に渡したICカードに対して個人データなどを書き込む処理（パーソナライズ）を含む処理である。また、機能追加は、ICカードに対してアプリケーションなどを追加する処理である。例えば、機能追加としては、ジャバカード（Java（登録商標）Card）としてのICカードにアプレットを追加する処理などが含まれる。
- [0015] 契約管理サーバ4Aは、ユーザ端末3から申請データを取得した後、ユーザ端末3からの申請データに基づく申請内容の契約が可能であれば、契約IDを発行する。契約管理サーバ4Aは、契約IDを発行した場合、発行した

ユーザ端末3を通知し、契約IDに対応づけた申請データ等をデータストレージ4Bに記憶する。また、契約管理サーバ4Aは、発行制御システム5におけるデータ生成サーバ5Aからの契約IDに基づく申請データの問い合わせに応じて、データストレージ4Bに保存している契約IDに対応する申請データを提供する。

[0016] 発行制御システム5は、遠隔によるICカードに対して発行処理（二次発行又は機能追加）を実行させるためのシステムである。発行制御システム5は、データ生成サーバ5AとHSM（ハードウェアセキュリティモジュール：Hardware Security Module）5Bとを有する。データ生成サーバ5Aは、サーバ装置で構成される。HSM5Bは、セキュアに鍵情報に保存し、鍵情報を用いた暗号処理を行うデバイスである。データ生成サーバ5Aは、HSM5Bにアクセスする機能、インターネットを介してユーザ端末3と通信する機能およびデータ管理システム4の契約管理サーバ4Aと通信する機能を有する。

[0017] データ生成サーバ5Aは、HSM5Bに保存する鍵および暗号処理機能を用いてユーザ端末3を介したICカード2とのセキュアな通信を行う。データ生成サーバ5Aは、ユーザ端末3からICカード2が鍵情報を用いて生成するカード認証データと契約IDとを含む発行リクエストを取得する。

[0018] データ生成サーバ5Aは、ユーザ端末3からの発行リクエストに応じてデータ管理システム4の契約管理サーバ4Aが管理する申請データを取得する。データ生成サーバ5Aは、発行リクエストに応じて取得した申請データに基づいてユーザが所持するICカードに対する発行処理を行うための発行データをHSM5Bが保存する鍵情報を用いて生成し、生成した発行データをユーザ端末3へ供給する。

[0019] 次に、第1実施形態に係る携帯可能電子装置としてのICカード2における制御系の構成について説明する。

図2は、第1実施形態に係る携帯可能電子装置としてのICカード2の構成例を示すブロック図である。

ＩＣカード２は、外部装置から供給される電力により活性化する（動作可能な状態になる）携帯可能電子装置の一例である。ＩＣカード２は、スマートカードとも称される。図２に示すように、ＩＣカード２は、本体Ｃを有する。本体Ｃは、プラスチックなどによりカード状に形成される。ＩＣカード２の本体Ｃ内には、制御モジュールＭが埋設される。制御モジュールＭは、１つ又は複数のＩＣチップに通信インターフェースが接続された状態で一体的に形成される。

[0020] 図２に示す構成例において、制御モジュールＭは、プロセッサ２１、ＲＯＭ２２、ＲＡＭ２３、データメモリ２４および通信インターフェース２５を有する。また、ＩＣカード２の本体Ｃ内において、制御モジュールＭには、表示器２６および生体センサとしての指紋センサ２７が接続される。

[0021] プロセッサ２１は、種々の処理を実行する回路を含む。プロセッサ２１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。プロセッサ２１は、ＩＣカード２全体の制御を司る。プロセッサ２１は、ＲＯＭ２２あるいはデータメモリ２４に記憶されているプログラムを実行することにより、種々の処理機能を実現する。ただし、後述するプロセッサ２１が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0022] ＲＯＭ２２は、プログラムメモリとして機能する不揮発性のメモリである。ＲＯＭ２２は、予め制御用のプログラムおよび制御データなどが記憶される。ＲＯＭ２２は、製造段階で制御プログラムや制御データなどが記憶された状態でＩＣカード２内に組み込まれるものである。ＲＯＭ２２に記憶される制御プログラムや制御データは、予め当該ＩＣカード２の仕様に応じて組み込まれる。例えば、ＲＯＭ２２には、外部装置（カードリーダライタ）から受信するコマンドに応じた処理をプロセッサ２１が実行するためのプログラムが記憶される。

[0023] ＲＡＭ２３は、ワーキングメモリとして機能する揮発性のメモリである。また、ＲＡＭ２３は、プロセッサ２１が処理中のデータなどを一時保管する

バッファとしても機能する。例えば、RAM 23は、通信インターフェース 25を介して外部装置との間で送受信するデータを一時保管する通信バッファとして機能する。

[0024] データメモリ 24は、データの書き込みおよび書換えが可能な不揮発性のメモリである。データメモリ 24は、例えば、EEPROM（登録商標）（Electrically Erasable Programmable Read Only Memory）などで構成する。データメモリ 24には、当該ICカード2の運用用途に応じたプログラムや種々のデータが書き込まれる。データメモリ 24には、プログラムファイルあるいはデータファイルなどが定義され、それらのファイルに制御プログラムや種々のデータが書き込まれる。また、データメモリ 24は、一部又は全部の領域が耐タンパー性を有し、セキュアにデータが格納できる。

[0025] データメモリ 24は、鍵情報を記憶する第1の記録領域 24aおよび生体情報を格納する第2の記憶領域 24bを有する。第1の記憶領域 24aは、セキュアにデータを記憶できる耐タンパー性を有するメモリである。第1の記憶領域 24aには、当該ICカード2を使用可能な状態とする処理（一次発行）において鍵情報が書き込まれる。本ICカード発行システム1においては、一次発行済みのICカード2における第1の記憶領域 24aに書き込んだ鍵情報に対応する鍵情報が発行制御システム5におけるHSM 5Bに保存されるものとする。

[0026] また、第2の記憶領域 24bは、当該ICカード2の所有者であるユーザの生体情報を記憶する。例えば、ICカード2は、生体情報として指紋を用いた生体情報を行う指紋センサカードであることを想定する。ICカード2が指紋センサカードである場合、ICカード2の第2の記憶領域 24bには所有者であるユーザの生体情報としての指紋情報が書き込まれる。なお、以下に説明する第1実施形態では、ICカード2は、二次発行又は機能追加を実行する前に、第2の記憶領域にユーザの生体情報としての指紋情報が書き込まれた状態でユーザが所持しているものであることを前提とする。

- [0027] 通信インターフェース25は、通信制御部とインターフェース部とを有し、通信部を構成する。通信インターフェース25は、ユーザ端末3が備えるカードリーダーライタ（RW）又はユーザ端末3とインターフェースを介して接続されるカードリーダーライタと通信接続するためのインターフェースである。通信インターフェース25は、カードRWのインターフェースに対応した通信方式による通信機能を実現する。また、通信インターフェース25は、複数の通信方式（例えば、接触通信と非接触通信）をサポートするものとして構成しても良い。
- [0028] 当該ICカード2が非接触型のICカードとして実現される場合、通信インターフェース25は、ユーザ端末3が備えるカードRW又はユーザ端末3とインターフェースを介して接続されるカードRWと非接触（無線）で通信する通信部を構成する。この場合、通信インターフェース25は、電波の送受信を行うアンテナを備え、アンテナから送信する電波を生成するための変調回路およびアンテナが受信した電波から信号を生成するための復調回路などにより構成される。
- [0029] また、当該ICカード2が接触型のICカードとして実現される場合、通信インターフェース25は、ユーザ端末3が備えるカードRW又はユーザ端末3とインターフェースを介して接続されるカードRWと接触して通信する通信部を構成する。この場合、通信インターフェース25は、カードRWに設けられたコンタクト部と物理的かつ電氣的に接触するコンタクト部を備え、コンタクト部を介した信号の送受信を制御する通信制御回路などにより構成される。
- [0030] 生体センサ20は、認証情報を取得する認証情報取得部の一例である。生体センサ20は、認証処理に用いる認証情報として人物の生体情報を取得するセンサである。第1実施形態において、生体センサ20は、利用者の指紋情報（指紋画像）を読み取る指紋センサであるものとする。生体センサ20としての指紋センサは、指紋を読み取るセンサがカード本体Cの表面に露出するように設けられ、露出したセンサ部分に翳された人物の指の指紋を読み

取る。生体センサ20が読み取る指紋情報が、データメモリ24の第2の記憶領域24bに記憶されている指紋情報と照合されるにで指紋認証が実行される。

[0031] なお、生体センサ20は、指紋センサに限定されるものではなく、指紋以外の生体情報（例えば、掌紋、静脈、虹彩等）を取得するセンサであっても良い。指紋以外の生体情報を取得するセンサを備える場合、ICカード2は、センサが取得する生体情報に対応した生体認証を行う機能（例えば、掌紋照合、静脈照合、虹彩照合等を実行するICチップ）を備えるようにすれば良い。

[0032] 次に、第1実施形態に係るICカード発行システム1におけるユーザ端末3の構成について説明する。

図3は、第1実施形態に係るICカード発行システム1におけるユーザ端末3の構成例を示すブロック図である。

ユーザ端末3は、オペレーティングシステム（OS）上で種々のアプリケーションプログラムが実行される電子装置である。ユーザ端末3は、ICカード2を所持するカードホルダとしてのユーザが使用する電子装置であれば良い。例えば、ユーザ端末3は、スマートフォン、タブレット端末、携帯電話などのカードRWを備える携帯端末又はカードRWを接続するインターフェースを備える携帯端末である。また、ユーザ端末3は、カードRWを備えるパーソナルコンピュータ（PC）又はカードRWを接続するインターフェースを備えるPCであっても良い。

[0033] 図3に示す構成例において、ユーザ端末3は、プロセッサ31、ROM32、RAM33、データメモリ34、ネットワーク（NW）通信部35、カードリーダーライタ（RW）36、表示部37、および、入力部38などを有する。

[0034] プロセッサ31は、プログラムを実行することにより各種の処理を実行する。プロセッサ31は、例えば、CPU（Central Processing Unit）である。プロセッサ31は、システムバスを介してユー

ザ端末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、ROM32およびRAM33と協働してユーザ端末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。例えば、プロセッサ31は、ROM32あるいはデータメモリ34に記憶されているアプリケーションプログラムを実行することにより種々の処理機能を実現する。ただし、後述するプロセッサ31が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0035] ROM (Read Only Memory) 32は、ユーザ端末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。例えば、ROM32は、オペレーティングシステム(OS)などの基本動作を司るプログラムを記憶する。また、ROM32は、ユーザ端末3が具備する機能を実現するためのアプリケーションプログラムなどを記憶しても良い。ROM32は、書き換え可能な不揮発性のメモリで構成しても良い。例えば、書き換え可能なROM32としては、EEPROM (Electrically Erasable Programmable ROM) 又はフラッシュROMなどで実現される。

[0036] RAM (Random Access Memory) 33は、データを一時的に記憶する揮発性のメモリである。RAM33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。

[0037] データメモリ34は、各種のデータを記憶する記憶部である。データメモリ34は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ34は、フラッシュROM、SSD (Solid State Drive) などの半導体素子メモリ、あるいは、HDD (Hard Disc Drive) などの記憶装置が用いられる。データメモリ34は、アプリケーションプログラム、動作設定値、個人情報などを記憶する。また、データメモリ34は、OSプログラムを記憶するようにしても良い。

[0038] NW通信部35は、外部装置と通信するための通信インターフェースである。NW通信部35は、無線で通信を行うものであって良いし、有線で通信

を行うものであっても良い。ＩＣカード発行システム１において、ＮＷ通信部３５は、インターフェースを介して、契約管理サーバ４Ａおよびデータ生成サーバ５Ａと通信するものであれば良い。

[0039] カードリーダライタ３６は、ＩＣカード２と通信する機能を有する。カードリーダライタ３６は、ＩＣカード２に対して、電源供給、クロック供給、リセット制御、データの送受信を行う。カードリーダライタ３６は、ＩＣカード２を活性化（起動）させた後、プロセッサ３１による制御に基づいて種々のコマンドを送信したり送信したコマンドに対する応答を受信したりする。なお、ユーザ端末３は、外部機器としてのカードリーダライタに接続するためのインターフェースを備える構成としても良い。

[0040] カードリーダライタ３６は、ＩＣカード２が備える通信方式に対応する構成を備える。例えば、ＩＣカード２が非接触型のＩＣカードとして実現される場合、カードリーダライタ３６は、非接触型のＩＣカードの通信方式に準拠する通信プロトコルで、非接触（無線）でＩＣカード２と通信する。また、ＩＣカード２が接触型のＩＣカードとして実現される場合、カードリーダライタ３６は、ＩＣカード２のコンタクト部（インターフェース）と物理的かつ電氣的に接触するコンタクト部を有し、コンタクト部を介してデータの送受信を行う。

[0041] 表示部３７は、液晶パネル等の表示デバイスである。入力部３８は、ユーザ端末３に対して操作指示を入力する操作デバイスである。入力部３８は、例えば、タッチパネルを含む。表示部３７と入力部３８とは、タッチパネル付き表示装置（以下、タッチスクリーンと称する）で構成しても良い。また、入力部３８は、ボタンスイッチで構成する操作キー、静電容量の変化に基づいて操作者の手指が触れたことを検出するタッチセンサなどを含むものであっても良い。

[0042] 次に、第１実施形態に係るＩＣカード発行システム１における契約管理サーバ４Ａの構成について説明する。

図４は、第１実施形態に係るＩＣカード発行システム１における契約管理

サーバ4 Aの構成例を示すブロック図である。

図4に示すように、契約管理サーバ4 Aは、プロセッサ4 1、ROM4 2、RAM4 3、データメモリ4 4、インターフェース4 5、ネットワーク（NW）通信部4 6、および、通信部4 7を有する。

[0043] プロセッサ4 1は、プログラムを実行することにより各種の処理を実行する。プロセッサ4 1は、例えば、CPU（Central Processing Unit）である。プロセッサ4 1は、システムバスを介してサーバ4 A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4 1は、ROM4 2およびRAM4 3と協働して契約管理サーバ4 Aにおける制御およびデータ処理などの動作を実行する。

[0044] ROM（Read Only Memory）4 2は、契約管理サーバ4 A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。

RAM（Random Access Memory）4 3は、データを一時的に記憶する揮発性のメモリである。RAM4 3は、プロセッサ4 1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。

データメモリ4 4は、各種のデータを記憶する記憶部である。データメモリ4 4は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ4 4は、OSプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0045] インターフェース4 5は、データストレージ4 Bにアクセスするためのインターフェースである。データストレージ4 Bが外部デバイスとしての記憶装置である場合、インターフェース4 5は、データストレージ4 Bとしての記憶装置が備えるインターフェース規格に対応したものであれば良い。また、データストレージ4 Bがデータサーバ等である場合、インターフェースは、データストレージ4 Bとしてのサーバと通信するための通信インターフェースで構成すれば良い。

[0046] ネットワーク（NW）通信部4 6は、外部装置と通信するための通信イン

ターフェースである。NW通信部46は、無線で通信を行うものであって良いし、有線で通信を行うものであって良い。第1実施形態に係るICカード発行システム1において、NW通信部46は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末3と通信するものであれば良い。

[0047] 通信部47は、データ生成サーバと通信するための通信インターフェースである。通信部47は、無線で通信を行うものであって良いし、有線で通信を行うものであって良い。第1実施形態に係るICカード発行システム1において、通信部47は、データ生成サーバ5Aとの通信がセキュアに行えるものであれば良い。

なお、NW通信部46および通信部47は、1つの通信インターフェースで実現する構成しても良い。さらに、インターフェース45についても、NW通信部46又は通信部47と共通化した通信インターフェースとする構成としても良い。

[0048] 次に、第1実施形態に係るICカード発行システム1におけるデータ生成サーバ5Aの構成について説明する。

図5は、第1実施形態に係るICカード発行システム1におけるデータ生成サーバ5Aの構成例を示すブロック図である。

図5に示すように、データ生成サーバ5Aは、プロセッサ51、ROM52、RAM53、データメモリ54、インターフェース55、ネットワーク(NW)通信部56、および、通信部57を有する。

[0049] プロセッサ51は、プログラムを実行することにより各種の処理を実行する。プロセッサ51は、例えば、CPU(Central Processing Unit)である。プロセッサ51は、システムバスを介してサーバ5A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51は、ROM52およびRAM53と協働してデータ生成サーバ5Aにおける制御およびデータ処理などの動作を実行する。

[0050] ROM(Read Only Memory)52は、データ生成サーバ

5 A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。

RAM (Random Access Memory) 53は、データを一時的に記憶する揮発性のメモリである。RAM 53は、プロセッサ51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。

データメモリ54は、各種のデータを記憶する記憶部である。データメモリ54は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ54は、OSプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0051] インターフェース55は、HSM 5Bにアクセスするためのインターフェースである。インターフェース55は、HSM 5Bが備えるインターフェース規格に対応したものであれば良い。

ネットワーク (NW) 通信部56は、外部装置と通信するための通信インターフェースである。NW通信部56は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第1実施形態に係るICカード発行システム1において、NW通信部56は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末3と通信するものであれば良い。

[0052] 通信部57は、契約管理サーバ4Aと通信するための通信インターフェースである。通信部57は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第1実施形態に係るICカード発行システム1において、通信部57は、契約管理サーバ4Aとの通信がセキュアに行えるものであれば良い。

なお、NW通信部56および通信部57は、1つの通信インターフェースで実現する構成しても良い。

[0053] 次に、第1実施形態に係るICカード発行システム1におけるICカード2に対する発行処理の申請手続きおよび発行手続きについて説明する。

以下に説明する動作の前提条件として、ICカード2は、一次発行 (カー

ド製造と初期化)の処理がなされた後にユーザ(カードホルダ)に渡されるものとする。また、ユーザに渡されるＩＣカード２には、一次発行においてカード認証データの生成に関する鍵(鍵情報)が書き込まれているものとする。ＩＣカード２に書き込まれた鍵情報は、発行制御システム５におけるＨＳＭ５Ｂに保存されている。さらに、ユーザ(カードホルダ)が所持するＩＣカード２には、当該ユーザの本人認証が行われた上で当該ユーザ(本人)の指紋情報が書き込まれているものとする。

[0054] まず、第１実施形態に係るＩＣカード発行システム１におけるＩＣカード２に対する発行処理の申請手続きについて説明する。

図６は、ＩＣカード発行システム１におけるＩＣカード２に対する発行処理の申請手続きの動作例を説明するためのシーケンスである。

カードホルダは、ユーザ端末３のプロセッサ３１は、カードホルダとしてのユーザの操作に応じて入力部３８による申請データの入力を受け付ける(ＳＴ２１)。申請データとしては、例えば、発行処理(二次発行又は機能追加)に必要な情報、カードホルダであるユーザ自身の個人情報、および、カードホルダ(ユーザ)が所持するＩＣカード２に関する情報などが含まれることが想定される。

[0055] また、ユーザ端末３は、申請用のプログラムにより申請データが入力されるようにしても良いし、インターネット上に提供される申請データの入力用のＷｅｂサイトで申請データが入力されるようにしても良い。前者の場合、ユーザ端末３は、データメモリ３４に申請用のプログラムをインストールしておく。ユーザ端末３のプロセッサ３１は、ユーザの操作に応じて申請用のプログラムを起動し、申請用のプログラムで提示される申請データの入力フォーマットに従って申請データを入力する。また、後者の場合、ユーザ端末３のプロセッサ３１は、ＮＷ通信部３５によりインターネット上で提供される申請データの入力用のサイトにアクセスし、入力用のサイトで提示される申請データの入力フォーマットに沿って申請データを入力する。

[0056] また、ユーザ端末３は、カードホルダ(ユーザ)が所持するＩＣカード２

に関する情報を当該ＩＣカード２から読み取るようにしても良い。当該ＩＣカード２に関する情報（カードデータ）は、例えば、当該ＩＣカード２を識別するための固有な識別情報（ＩＤ）などを含む。また、カードホルダであるユーザ自身の個人情報がＩＣカード２に保存されている場合、ユーザ端末３は、ユーザの個人情報をＩＣカード２から読み取るようにしても良い。図６に示す動作例において、ＩＣカード２は、ユーザ端末３のカードリーダー３６からの要求に応じて、生体（指紋）認証で本人確認が成功した後にカードデータを出力するものとする。

[0057] すなわち、ユーザ端末３のプロセッサ３１は、カードＲＷ３６により生体認証としての指紋認証の要求とカードデータの要求とをＩＣカード２へ送信する（ＳＴ２２）。ＩＣカード２のプロセッサ２１は、ユーザ端末３からの要求に応じてデータメモリ２４に記憶されている指紋データを用いて指紋認証を実行する（ＳＴ１１）。ＩＣカード２のプロセッサ２１は、指紋認証による本人確認が成功した後に当該ＩＣカード２の情報をユーザ端末３へ出力する（ＳＴ１２）。

[0058] 申請データの入力完了すると、ユーザ端末３のプロセッサ３１は、入力された申請データによる発行処理（契約）に関する審査を要求する審査リクエストを作成する（ＳＴ２３）。審査リクエストは、申請データとして入力された申請内容によって、カードホルダが所持するＩＣカード２に対する発行処理（二次発行又は機能追加）を実行すること（契約）が可能であるか否かの審査を要求するものである。

[0059] 審査リクエストを作成すると、ユーザ端末３のプロセッサ３１は、データ管理システム４の契約管理サーバ４Ａへ審査リクエストを送信する（ＳＴ２４）。プロセッサ３１は、ＮＷ通信部３５によりインターネットを介して契約管理サーバ４Ａにアクセスし、審査リクエストを契約管理サーバ４Ａへ送信する。

[0060] 契約管理サーバ４Ａは、ＮＷ通信部４６によりユーザ端末３からの審査リクエストを受け付ける（ＳＴ３１）。ユーザ端末３からの審査リクエストを

受信すると、契約管理サーバ4 Aのプロセッサ4 1は、受信した審査リクエストに応じて申請された発行処理を許可するか否かを審査する。例えば、契約管理サーバ4 Aは、申請データが示す申請内容に問題がないか、および、申請者であるカードホルダに関して発行処理を行うための契約上の問題がないかを審査する。審査の内容および手続きは、運用形態に準じたものであれば特定の形態に限定されるものではない。審査リクエストに応じた審査結果が契約管理サーバ4 Aに入力されるものであれば良い。

[0061] 審査リクエストに対する審査結果が契約不可（発行処理が不可）であった場合、契約管理サーバ4 Aのプロセッサ4 1は、審査結果として契約不可となった旨を審査リクエストの送信元であるユーザ端末3へ通知する（ST 34）。また、プロセッサ4 1は、申請データでカードホルダが指定した連絡先に審査結果を通知するようにしても良い。

[0062] ユーザ端末3のプロセッサ3 1は、契約管理サーバ4 Aから審査リクエストに対する審査結果が契約不可である旨の通知を受けると、審査結果が契約不可であった旨を表示部3 7に表示することによりカードホルダに報知する（ST 25）。

[0063] 審査リクエストに対する審査結果が契約可（発行処理が可）であった場合、契約管理サーバ4 Aのプロセッサ4 1は、契約IDを発行する（ST 32）。契約IDを発行すると、プロセッサ4 1は、審査結果が契約可となった審査リクエストに含まれる申請データを発行した契約IDに対応づけてデータストレージ4 Bに登録する（ST 33）。データストレージ4 Bは、契約管理サーバ4 Aからの申請データと契約IDとを契約情報として保存する（ST 41）。

[0064] 申請データと契約IDとをデータストレージ4 Bに登録すると、契約管理サーバ4 Aのプロセッサ4 1は、審査結果および契約IDを審査リクエストの送信元であるユーザ端末3へ通知する（ST 34）。

[0065] ユーザ端末3のプロセッサ3 1は、契約管理サーバ4 Aから審査リクエストに対する審査結果が契約可である旨の通知を受けると、審査結果として契

約可であった旨の案内とともに、契約IDを表示部37に表示する（ST25）。また、審査結果が可であった場合、ユーザ端末3のプロセッサ31は、表示部37に発行処理の手続きに関する案内などを表示するようにしても良い。

[0066] 以上のような申請手続きによって、契約管理サーバは、ユーザ端末からの審査リクエストが契約可となった場合、当該審査リクエストを行ったカードホルダからの申請データと契約IDと対応づけてデータストレージに保存することができる。この結果、カードホルダが所持するICカード2は、後述するような動作によるリモートでの発行処理が可能な状態となる。これにより、カードホルダは、発行処理が可能な状態となった後、つまり、契約IDの通知を受けた後、ユーザ端末3を用いてICカード2に対してリモートで発行処理を行うための後述するような発行手続きを実行する。

[0067] 次に、第1実施形態に係るICカード発行システム1におけるICカード2に対する発行処理を行うための発行手続きについて説明する。

図7および図8は、ICカード発行システム1におけるICカード2に対する発行処理を行うための発行手続きの動作例を説明するためのシーケンスである。

カードホルダとしてのユーザは、ユーザ端末3においてICカード2に対する発行処理用のアプリケーションプログラム（以下、発行アプリと称する）を起動させる。発行アプリは、予めデータメモリ24に記憶しておくようにしても良いし、契約管理サーバ4A又はデータ生成サーバ5Aからダウンロードするようにしても良い。

[0068] ユーザ端末3のプロセッサ31は、カードホルダが入力部38に入力する発行アプリの起動指示に応じて発行アプリを起動させる（ST120）。発行アプリが起動すると、プロセッサ31は、カードホルダに対して契約IDの入力を要求する（ST121）。カードホルダは、申請データに対する審査結果と共に取得した契約IDを入力部38により入力する。プロセッサ31は、入力部38に契約IDが入力されると、カードRW36によりICカ

ード2にアクセスし、本人確認のための生体認証としての指紋認証をICカード2に要求する(ST122)。

[0069] ICカード2は、カードRW36から供給される電力により起動する。ICカード2が起動すると、プロセッサ21は、カードRW36から供給される指紋認証の要求に応じて指紋認証処理を実行する(ST111)。プロセッサ21は、指紋センサ20によりユーザの指紋を取得する。プロセッサ21は、指紋センサ20が取得した指紋情報とデータメモリ24に記憶している指紋データとを比較することにより指紋認証を行う。

[0070] 指紋センサ20が取得した指紋情報とデータメモリ24に記憶している指紋データとが同一人物の指紋であると判定された場合、プロセッサ21は、指紋認証が成功したものとする。指紋センサ20が取得した指紋情報とデータメモリ24に記憶している指紋データとが同一人物の指紋であると判定できなかった場合、プロセッサ21は、指紋認証が失敗したものとする。

[0071] ICカード2における指紋認証が失敗した場合、プロセッサ21は、指紋認証が失敗したことをカードRW36へ通知する。カードRW36によりICカード2から指紋認証が失敗した旨の通知を受けた場合、ユーザ端末3のプロセッサ31は、ICカード2に対する発行処理を実行するための発行手続きを中止する。この場合、プロセッサ31は、表示部37に本人確認が失敗したためにICカード2に対する発行処理で不可となった旨を表示することによりユーザに発行手続きの中止を報知する。

[0072] ICカード2における指紋認証が成功した場合、プロセッサ21は、指紋認証が成功したことをカードRW36へ通知する。カードRW36によりICカード2から指紋認証が成功した旨の通知を受けた場合、ユーザ端末3のプロセッサ31は、カードRW36を介してICカード2に発行処理を実行するためのカード認証データを要求する。これに対して、ICカード2のプロセッサ21は、カード認証データを生成し、生成したカード認証データをカードRW36へ供給する。

[0073] すなわち、ICカード2のプロセッサ21は、指紋認証が成功した場合、

カード認証データ（認証データ）を生成する（ST112）。カード認証データは、当該ICカード2における生体認証が成功した場合に生成される認証データであり、当該ICカード2に機能追加（例えば、アプレットの追加）あるいは二次発行などの発行処理を実施するための情報を含む。

[0074] カード認証データは、セキュアメモリであるデータメモリ24の記憶領域24aに記憶されている鍵情報を用いて生成される。また、カード認証データには、発行処理を実施するための情報として、例えば、CPLC（当該ICカードのプロダクトサイクルを示す情報）、INITIALIZE UPD DATEコマンドおよびレスポンスデータなどが含まれる。

[0075] 指紋認証が成功した後にカード認証データを生成すると、ICカード2のプロセッサ21は、生成したカード認証データをユーザ端末3のカードRW36へ出力する（ST113）。カード認証データを出力した後、ICカード2のプロセッサ21は、当該カード認証データに対応してデータ生成サーバ5Aが生成する発行データに基づく発行処理が実行可能な状態とする。

[0076] ユーザ端末3のプロセッサ31は、カードRW36により指紋認証が成功したICカード2からカード認証データを取得すると、ICカード2に対する発行処理を要求する発行リクエストを生成し、生成した発行リクエストをデータ生成サーバ5Aへ送信する（ST124）。

[0077] 例えば、プロセッサ31は、カード認証データおよび契約IDを含む発行リクエストを生成する。発行リクエストを生成すると、プロセッサ31は、NW通信部35によりインターネットを介して発行制御システム5におけるデータ生成サーバ5Aにアクセスする。データ生成サーバ5Aにアクセスすると、プロセッサ31は、カード認証データおよび契約IDを含む発行リクエストをデータ生成サーバ5Aへ送信する。

[0078] データ生成サーバ5Aは、NW通信部56によりユーザ端末3からの発行リクエストを受信する。発行リクエストを受信した場合、データ生成サーバ5Aのプロセッサ51は、発行リクエストに含まれる契約IDを抽出する。発行リクエストに含まれる契約IDを抽出すると、プロセッサ51は、通信

部57を介して契約管理サーバ4Aにアクセスする。契約管理サーバ4Aにアクセスすると、プロセッサ51は、発行リクエストに含まれる契約IDに対応する申請データの要求（リクエスト）を契約管理サーバ4Aへ送信する（ST131）。

[0079] 契約管理サーバ4Aは、通信部47を介してデータ生成サーバ5Aと通信する。契約管理サーバ4Aのプロセッサ41は、データ生成サーバ5Aから契約IDに対応する申請データを要求するリクエストを受信した場合、データストレージ4Bにおいて当該契約IDに対応する申請データを検索する（ST141）。データ生成サーバ5Aから要求された契約IDに対応する申請データを検出すると、プロセッサ41は、通信部47を介して当該契約IDに対応する申請データをデータ生成サーバ5Aへ送信する（ST142）。

[0080] 発行リクエストに含まれる契約IDに対応する申請データを契約管理サーバ4Aから受信すると、データ生成サーバ5Aのプロセッサ51は、ICカード2において申請データに基づく発行処理を実行するための発行データを生成する（ST132）。発行データは、申請データに基づく一連の発行処理においてICカード2に実行させるべきコマンドと一連の発行処理においてICカード2に書き込むべきデータとを含む。

[0081] 例えば、発行処理としてICカード2にアプレットを追加する場合、発行データには、ICカード2に実行させるべきコマンドとしてインストール（INSTALL）コマンドが含まれる。また、あるクレジットカードの規格でアプレットを追加する場合、発行データには、ICカード2に実行させるべきコマンドとして外部認証（EXTERNAL AUTHENTICATE）コマンド、および、ストアデータ（STORE DATA）コマンドが含まれる。

[0082] また、プロセッサ51は、発行データをセキュアにICカード2に供給するためにHSM5Bが保管する鍵情報を用いて発行データを処理する（ST133）。ここで、HSM5Bには、ICカード2内に保持する鍵情報に対

応する鍵情報が保存されている。これにより、H S M 5 Bを用いた暗号化によって安全に発行データをI Cカード2へ供給できる。例えば、プロセッサ5 1は、H S M 5 Bにおいて当該I Cカード2内の保存される鍵情報と共有する鍵情報を用いて発行データに含まれるデータを暗号化する。

[0083] 発行データをH S M 5 Bが保存する鍵情報で暗号化処理した後、プロセッサ5 1は、発行リクエストの送信元であるユーザ端末3へH S M 5 Bで暗号化処理した発行データを送信する（S T 1 3 4）。

[0084] ユーザ端末3は、データ生成サーバ5 Aへ発行リクエストを送信した後、発行リクエストに対する応答としての発行データの受信待ちとなる。この状態において、ユーザ端末3は、NW通信部3 5 4によりデータ生成サーバ5 Aから送信される発行データを受信する（S T 1 2 5）。発行データを受信した場合、ユーザ端末3のプロセッサ3 1は、カードR W 3 6によりI Cカード2に対して発行データを出力する（S T 1 2 6）。

[0085] I Cカード2のプロセッサ2 1は、生体認証が成功した後に生成したカード認証データに対応する発行データをユーザ端末3のカードR W 3 6から取得する。発行データを取得すると、プロセッサ2 1は、取得した発行データに従って発行処理を実行する（S T 1 1 3）。

[0086] 例えば、プロセッサ2 1は、発行データに含まれるコマンドを実行することにより発行処理として書き込むべきデータをデータメモリ2 4に書き込む。また、プロセッサ2 1は、発行処理において供給される発行データに含まれる暗号化データをデータメモリ2 4におけるセキュアメモリである第1の記憶領域2 4 aに記憶している鍵情報を用いて復号化する。

[0087] I Cカード2のプロセッサ2 1は、供給された発行データに基づく発行処理が完了すると、発行処理の完了をユーザ端末3のカードR W 3 6へ通知する（S T 1 1 4）。

ユーザ端末3は、カードR W 3 6によりI Cカード2へ発行データを出力した後にI Cカード2から発行処理が完了した旨の通知を受信する。ユーザ端末3のプロセッサ3 1は、カードR W 3 6によりI Cカード2から発行処

理の完了通知を受けると、ＩＣカード２における発行処理（機能追加あるいは二次発行）が完了した旨の案内を表示部３７に表示する（ＳＴ１２７）。

[0088] また、発行データに基づくＩＣカード２における発行処理が完了した旨の通知を受けると、プロセッサ３１は、ＮＷ通信部３５により発行データの送信元であるデータ生成サーバ５Ａへ発行処理の完了を通知する（ＳＴ１２８）。

データ生成サーバ５Ａのプロセッサ５１は、ユーザ端末３からのＩＣカード２における発行処理の完了通知をＮＷ通信部５６により受信すると、通信部５７によりＩＣカード２における発行処理の完了通知を契約管理サーバ４Ａへ転送（送信）する。

[0089] 契約管理サーバ４Ａは、通信部４７によりデータ生成サーバ５Ａを介してＩＣカード２における発行処理の完了通知を受信する。契約管理サーバ４Ａのプロセッサ４１は、データ生成サーバ５Ａを経由してＩＣカード２における発行処理の完了通知を受信すると、データストレージ４Ｂにおいて申請データに対応して発行処理の完了を記録する（ＳＴ１４３）。

[0090] 以上のような発行手続きによって、第１実施形態に係るＩＣカード発行システムは、生体センサとしての指紋センサを有するＩＣカード２において生体認証による本人認証が成功した後に、セキュアにリモートでＩＣカードに対して機能追加あるいは二次発行などの発行処理を行うことができる。

[0091] （第２実施形態）

以下、第２実施形態について、図面を参照しつつ説明する。

まず、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システム２０１について説明する。

[0092] 図９は、第２実施形態に係るリモート発行システムとしてのＩＣカード発行システム２０１の構成例を模式的に示す図である。

図９に示す構成例において、ＩＣカード発行システム２０１は、ＩＣカード２０２、ユーザ端末２０３、データ管理システム２０４、および、発行制御システム２０５を有する。

[0093] ICカード202は、生体認証を実行する機能を有する携帯可能電子装置の一例である。第2実施形態に係るICカード202は、人物から取得する認証情報としての生体情報を取得するための生体センサ220を備える。例えば、ICカード202が具備する生体センサ220は、生体情報の一例としての指紋を読み取る指紋センサである。生体センサとしての指紋センサ220を備えるICカード202は、指紋センサが読み取る人物の指紋とICカード202内のメモリに予め登録されている登録者（ユーザ、カードホルダ）の指紋とを照合することにより本人確認としての指紋認証（生体認証）を実行する。

[0094] また、本実施形態に係る携帯可能電子装置としてのICカード202は、固有な個体機別情報としてPUF（Physically Uncloable Function：物理複製困難関数）データを出力する機能を有する。PUFは、例えば、半導体チップのシリコン結晶パターンのばらつきなど、物体の物理的な特徴のばらつきからその物体に固有な情報（ID）を示すものである。PUFデータは、ICチップなどのICカード202に含まれる電子回路から得られるものとする。PUFは、電子回路を構成する個々のデバイスのばらつきによるものであるため、たとえ回路パターンが不正に複製されたとしても、PUF自体は、複製困難である。PUFデータは、個々のICカード202ごとに固有な情報となる。

[0095] 第2実施形態において、ICカード202は、生体情報としての指紋を用いて生体認証を行う機能を有する指紋センサカードであるものとして説明するものとする。ただし、第2実施形態に係る携帯可能電子装置としてのICカード202は、生体情報として指紋による指紋（生体）認証を行うものに限定されるものではない。例えば、ICカード202で例示される携帯可能電子装置は、指紋以外の生体情報によって生体認証を行うものであっても良い。

[0096] ユーザ端末203は、ユーザが所持する情報処理装置である。ユーザ端末203は、例えば、スマートフォン、タブレットPC、パソコンなどである。

。ユーザ端末203は、ユーザ自身が操作するものであって、ICカード202と通信するカードリーダーおよびインターネットなどのネットワークを介して各サーバ4A、5Aと通信する通信部とを備えるものであれば良い。また、ユーザ端末203は、ICカード202と通信するカードリーダーを備えるものに代えて、外部機器としてのカードリーダーに接続するためのインターフェースを備えるものであっても良い。

[0097] データ管理システム204は、遠隔によってユーザが保持するICカードにおける発行処理（二次発行又は機能追加など）の申請を受け付けるシステムである。データ管理システム204は、契約管理サーバ204Aとデータストレージ204Bとを有する。契約管理サーバ204Aは、サーバ装置で構成される。データストレージ204Bは、契約管理サーバ204Aからアクセス可能な記憶装置を含む装置である。契約管理サーバ204Aは、データストレージ204Bにアクセスする機能、インターネットを介してユーザ端末203と通信する機能および発行制御システム205のデータ生成サーバ205Aと通信する機能を有する。

[0098] 契約管理サーバ204Aは、ユーザが所持するユーザ端末203と通信し、ユーザ端末203からの当該ユーザが保持するICカードに対する発行処理（契約）に関する申請データを取得する。ここで、ICカードに対する発行処理とは、二次発行又は機能追加を含むものとする。ICカードの二次発行とは、発行業者からユーザ（カードホルダ）に渡したICカードに対して個人データなどを書き込む処理（パーソナライズ）を含む処理である。また、機能追加は、ICカードに対してアプリケーションなどを追加する処理である。例えば、機能追加としては、ジャバカード（Java Card）（登録商標）としてのICカードにアプレットを追加する処理などが含まれる。

[0099] 契約管理サーバ204Aは、ユーザ端末203から申請データを取得した後、ユーザ端末203からの申請データに基づく申請内容の契約が可能であれば、契約IDを発行する。契約管理サーバ204Aは、契約IDを発行し

た場合、発行したユーザ端末203を通知し、契約IDに対応づけた申請データとカードホルダが所持するICカード202のPUFデータとをデータストレージ204Bに記憶する。また、契約管理サーバ204Aは、発行制御システム205におけるデータ生成サーバ205Aからの契約IDに基づく申請データの問い合わせに応じて、データストレージ204Bに保存している契約IDに対応する申請データとPUFデータとを提供する。

[0100] 発行制御システム205は、遠隔によるICカードに対して発行処理（二次発行又は機能追加）を実行させるためのシステムである。発行制御システム205は、データ生成サーバ205AとHSM（ハードウェアセキュリティモジュール：Hardware Security Module）205BとPUFストレージ205Cとを有する。

[0101] データ生成サーバ205Aは、サーバ装置で構成される。HSM205Bは、セキュアに鍵情報に保存し、鍵情報を用いた暗号処理を行うデバイスである。HSM205Bには、本ICカード発行システム201においてリモートでの発行処理を実行可能とするICカード202が保持する鍵情報に対応する鍵情報を保存する。また、PUFストレージ205Cは、本ICカード発行システム201においてリモートでの発行処理を実行可能とするICカードのPUFデータを保持する記憶装置である。PUFストレージ205Cには、例えば、ICカード発行システム201での発行処理に実行対象となるICカードの正規の製造者が発行（製造）したICカード202のPUFデータが登録される。

[0102] データ生成サーバ205Aは、HSM205Bにアクセスする機能、PUFストレージ205Cにアクセスする機能、インターネットを介してユーザ端末203と通信する機能およびデータ管理システム204の契約管理サーバ204Aと通信する機能を有する。

[0103] データ生成サーバ205Aは、HSM205Bに保存する鍵および暗号処理機能を用いてユーザ端末203を介したICカード202とのセキュアな通信を行う。データ生成サーバ205Aは、ユーザ端末203からICカー

ド 202 が鍵情報を用いて生成するカード認証データと契約 ID とを含む発行リクエストを取得する。

[0104] データ生成サーバ 205 A は、ユーザ端末 203 からの発行リクエストに応じてデータ管理システム 204 の契約管理サーバ 204 A が管理する申請データと PUF データとを取得する。データ生成サーバ 205 A は、発行リクエストに含まれる PUF データが PUF ストレージに登録されているか、および、発行リクエストに含まれる PUF データが契約管理サーバ 204 A から申請データとともに取得する PUF データと一致するかをチェックする。

[0105] データ生成サーバ 205 A は、発行リクエストに含まれる PUF データが PUF ストレージに登録され、かつ、申請時に取得した PUF データと一致することを確認した後、申請データに基づいて IC カードに対する発行処理を行うための発行データを生成する。データ生成サーバは、申請データに基づく発行データを HSM 205 B が保存する鍵情報を用いて処理した後にユーザ端末 203 へ供給する。

[0106] 次に、第 2 実施形態に係る携帯可能電子装置としての IC カード 202 における制御系の構成について説明する。

図 10 は、第 2 実施形態に係る携帯可能電子装置としての IC カード 202 の構成例を示すブロック図である。

IC カード 202 は、外部装置から供給される電力により活性化する（動作可能な状態になる）携帯可能電子装置の一例である。IC カード 202 は、スマートカードとも称される。図 10 に示すように、IC カード 202 は、本体 C を有する。本体 C は、プラスチックなどによりカード状に形成される。IC カード 202 の本体 C 内には、制御モジュール M が埋設される。制御モジュール M は、1 つ又は複数の IC チップに通信インターフェースが接続された状態で一体的に形成される。

[0107] 図 10 に示す構成例において、制御モジュール M は、プロセッサ 221、ROM 222、RAM 223、データメモリ 224 および通信インターフェ

ース225を有する。また、ICカード202の本体C内において、制御モジュールMには、表示器26および生体センサとしての指紋センサ220が接続される。

[0108] プロセッサ221は、種々の処理を実行する回路を含む。プロセッサ221は、例えば、CPU (Central Processing Unit) である。プロセッサ221は、ICカード202全体の制御を司る。プロセッサ221は、ROM222あるいはデータメモリ224に記憶されているプログラムを実行することにより、種々の処理機能を実現する。ただし、後述するプロセッサ221が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0109] ROM222は、プログラムメモリとして機能する不揮発性のメモリである。ROM222は、予め制御用のプログラムおよび制御データなどが記憶される。ROM222は、製造段階で制御プログラムや制御データなどが記憶された状態でICカード202内に組み込まれるものである。ROM222に記憶される制御プログラムや制御データは、予め当該ICカード202の仕様に応じて組み込まれる。例えば、ROM222には、外部装置（カードリーダーライタ）から受信するコマンドに応じた処理をプロセッサ221が実行するためのプログラムが記憶される。

[0110] RAM223は、ワーキングメモリとして機能する揮発性のメモリである。また、RAM223は、プロセッサ221が処理中のデータなどを一時保管するバッファとしても機能する。例えば、RAM223は、通信インターフェース225を介して外部装置との間で送受信するデータを一時保管する通信バッファとして機能する。

[0111] データメモリ224は、データの書き込みおよび書換えが可能な不揮発性のメモリである。データメモリ224は、例えば、EEPROM（登録商標）(Electrically Erasable Programmable Read Only Memory) などで構成する。データメモリ224には、当該ICカード202の運用用途に応じたプログラムや種々の

データが書き込まれる。データメモリ 224 には、プログラムファイルあるいはデータファイルなどが定義され、それらのファイルに制御プログラムや種々のデータが書き込まれる。また、データメモリ 224 は、一部又は全部の領域が耐タンパー性を有し、セキュアにデータが格納できる。

[0112] データメモリ 224 は、鍵情報を記憶する第 1 の記憶領域 224 a、生体情報を記憶する第 2 の記憶領域 224 b、および、PUF データを保持する第 3 の記憶領域 224 c を有する。第 1 の記憶領域 224 a は、セキュアにデータを記憶できる耐タンパー性を有するメモリである。第 1 の記憶領域 224 a には、当該 IC カード 202 を使用可能な状態とする処理（一次発行）において鍵情報が書き込まれる。本 IC カード発行システム 201 においては、一次発行済みの IC カード 202 における第 1 の記憶領域 224 a に書き込んだ鍵情報に対応する鍵情報が発行制御システム 205 における HSM 205 B に保存されるものとする。

[0113] また、第 2 の記憶領域 224 b は、当該 IC カード 202 の所有者であるユーザの生体情報を記憶する。例えば、IC カード 202 は、生体情報として指紋を用いた生体情報を行う指紋センサカードであることを想定する。IC カード 202 が指紋センサカードである場合、IC カード 202 の第 2 の記憶領域 224 b には所有者であるユーザの生体情報としての指紋情報が書き込まれる。なお、以下に説明する第 2 実施形態では、IC カード 202 は、二次発行又は機能追加を実行する前に、第 2 の記憶領域にユーザの生体情報としての指紋情報が書き込まれた状態でユーザが所持しているものであることを前提とする。

[0114] 第 3 の記憶領域 224 c は、PUF データが記憶される。第 3 の記憶領域 224 c に記憶される PUF データは、当該 IC カード 202 に固有な識別情報の一例である。第 3 の記憶領域 224 c に記憶される PUF データは、当該 IC カード 202 内に存在する電子回路（IC チップなど）から得られる情報である。例えば、PUF データは、当該 IC カード 202 の製造時などに第 3 の記憶領域に記憶されるものとする。

- [0115] なお、PUFデータは、データメモリ224に予め記憶しておくものに限定されず、申請手続きおよび発行手続きにおいてプロセッサ221が取得できるようにすれば良い。例えば、ICカード202は、データメモリ224にPUFデータを記憶するのに代えて、PUFデータを出力するハードウェアとしてのPUF回路を設けても良い。この場合、プロセッサ221は、PUF回路からPUFデータを取得するようにすれば良い。
- [0116] 通信インターフェース225は、通信制御部とインターフェース部とを有し、通信部を構成する。通信インターフェース225は、ユーザ端末203が備えるカードリーダーライター（RW）又はユーザ端末203とインターフェースを介して接続されるカードリーダーライターと通信接続するためのインターフェースである。通信インターフェース225は、カードRWのインターフェースに対応した通信方式による通信機能を実現する。また、通信インターフェース225は、複数の通信方式（例えば、接触通信と非接触通信）をサポートするものとして構成しても良い。
- [0117] 当該ICカード202が非接触型のICカードとして実現される場合、通信インターフェース225は、ユーザ端末203が備えるカードRW又はユーザ端末203とインターフェースを介して接続されるカードRWと非接触（無線）で通信する通信部を構成する。この場合、通信インターフェース225は、電波の送受信を行うアンテナを備え、アンテナから送信する電波を生成するための変調回路およびアンテナが受信した電波から信号を生成するための復調回路などにより構成される。
- [0118] また、当該ICカード202が接触型のICカードとして実現される場合、通信インターフェース225は、ユーザ端末203が備えるカードRW又はユーザ端末203とインターフェースを介して接続されるカードRWと接触して通信する通信部を構成する。この場合、通信インターフェース225は、カードRWに設けられたコンタクト部と物理的かつ電氣的に接触するコンタクト部を備え、コンタクト部を介した信号の送受信を制御する通信制御回路などにより構成される。

[0119] 生体センサ２２０は、認証情報を取得する認証情報取得部の一例である。
生体センサ２２０は、認証処理に用いる認証情報として人物の生体情報を取得するセンサである。第２実施形態において、生体センサ２２０は、利用者の指紋情報（指紋画像）を読み取る指紋センサであるものとする。生体センサ２２０としての指紋センサは、指紋を読み取るセンサがカード本体Ｃの表面に露出するように設けられ、露出したセンサ部分に翳された人物の指の指紋を読み取る。生体センサ２２０が読み取る指紋情報が、データメモリ２２４の第２の記憶領域２２４ｂに記憶されている指紋情報と照合されることで指紋認証が実行される。

[0120] なお、生体センサ２２０は、指紋センサに限定されるものではなく、指紋以外の生体情報（例えば、掌紋、静脈、虹彩等）を取得するセンサであっても良い。指紋以外の生体情報を取得するセンサを備える場合、ＩＣカード２０２は、センサが取得する生体情報に対応した生体認証を行う機能（例えば、掌紋照合、静脈照合、虹彩照合等を実行するＩＣチップ）を備えるようにすれば良い。

[0121] 次に、第２実施形態に係るＩＣカード発行システム２０１におけるユーザ端末２０３の構成について説明する。

図１１は、第２実施形態に係るＩＣカード発行システム２０１におけるユーザ端末２０３の構成例を示すブロック図である。

ユーザ端末２０３は、オペレーティングシステム（ＯＳ）上で種々のアプリケーションプログラムが実行される電子装置である。ユーザ端末２０３は、ＩＣカード２０２を所持するカードホルダとしてのユーザが使用する電子装置であれば良い。例えば、ユーザ端末２０３は、スマートフォン、タブレット端末、携帯電話などのカードＲＷを備える携帯端末又はカードＲＷを接続するインターフェースを備える携帯端末である。また、ユーザ端末２０３は、カードＲＷを備えるパーソナルコンピュータ（ＰＣ）又はカードＲＷを接続するインターフェースを備えるＰＣであっても良い。

[0122] 図１１に示す構成例において、ユーザ端末２０３は、プロセッサ２３１、

ROM 232、RAM 233、データメモリ 234、ネットワーク (NW) 通信部 235、カードリーダーライタ (RW) 236、表示部 237、および、入力部 238などを有する。

[0123] プロセッサ 231は、プログラムを実行することにより各種の処理を実行する。プロセッサ 231は、例えば、CPU (Central Processing Unit) である。プロセッサ 231は、システムバスを介してユーザ端末 203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 231は、ROM 232およびRAM 233と協働してユーザ端末 203における制御およびデータ処理などの動作を実行する。例えば、プロセッサ 231は、ROM 232あるいはデータメモリ 234に記憶されているアプリケーションプログラムを実行することにより種々の処理機能を実現する。ただし、後述するプロセッサ 231が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0124] ROM (Read Only Memory) 232は、ユーザ端末 203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。例えば、ROM 232は、オペレーティングシステム (OS) などの基本動作を司るプログラムを記憶する。また、ROM 232は、ユーザ端末 203が具備する機能を実現するためのアプリケーションプログラムなどを記憶しても良い。ROM 232は、書き換え可能な不揮発性のメモリで構成しても良い。例えば、書き換え可能なROM 232としては、EEPROM (Electrically Erasable Programmable ROM) 又はフラッシュROMなどで実現される。

[0125] RAM (Random Access Memory) 233は、データを一時的に記憶する揮発性のメモリである。RAM 233は、プロセッサ 231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。

[0126] データメモリ 234は、各種のデータを記憶する記憶部である。データメモリ 234は、データの書き換えが可能な不揮発性のメモリで構成される。

例えば、データメモリ234は、フラッシュROM、SSD（Solid State Drive）などの半導体素子メモリ、あるいは、HDD（Hard Disc Drive）などの記憶装置が用いられる。データメモリ234は、アプリケーションプログラム、動作設定値、個人情報などを記憶する。また、データメモリ234は、OSプログラムを記憶するようにしても良い。

[0127] NW通信部235は、外部装置と通信するための通信インターフェースである。NW通信部235は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。ICカード発行システム201において、NW通信部235は、インターフェースを介して、契約管理サーバ204Aおよびデータ生成サーバ205Aと通信するものであれば良い。

[0128] カードリーダーライター236は、ICカード202と通信する機能を有する。カードリーダーライター236は、ICカード202に対して、電源供給、クロック供給、リセット制御、データの送受信を行う。カードリーダーライター236は、ICカード202を活性化（起動）させた後、プロセッサ231による制御に基づいて種々のコマンドを送信したり送信したコマンドに対する応答を受信したりする。なお、ユーザ端末203は、外部機器としてのカードリーダーライターに接続するためのインターフェースを備える構成としても良い。

[0129] カードリーダーライター236は、ICカード202が備える通信方式に対応する構成を備える。例えば、ICカード202が非接触型のICカードとして実現される場合、カードリーダーライター236は、非接触型のICカードの通信方式に準拠する通信プロトコルで、非接触（無線）でICカード202と通信する。また、ICカード202が接触型のICカードとして実現される場合、カードリーダーライター236は、ICカード202のコンタクト部（インターフェース）と物理的かつ電氣的に接触するコンタクト部を有し、コンタクト部を介してデータの送受信を行う。

[0130] 表示部237は、液晶パネル等の表示デバイスである。入力部238は、

ユーザ端末203に対して操作指示を入力する操作デバイスである。入力部238は、例えば、タッチパネルを含む。表示部237と入力部238とは、タッチパネル付き表示装置（以下、タッチスクリーンと称する）で構成しても良い。また、入力部238は、ボタンスイッチで構成する操作キー、静電容量の変化に基づいて操作者の手指が触れたことを検出するタッチセンサなどを含むものであっても良い。

[0131] 次に、第2実施形態に係るICカード発行システム201における契約管理サーバ204Aの構成について説明する。

図12は、第2実施形態に係るICカード発行システム201における契約管理サーバ204Aの構成例を示すブロック図である。

図12に示すように、契約管理サーバ204Aは、プロセッサ241、ROM242、RAM243、データメモリ244、インターフェース245、ネットワーク（NW）通信部246、および、通信部247を有する。

[0132] プロセッサ241は、プログラムを実行することにより各種の処理を実行する。プロセッサ241は、例えば、CPU（Central Processing Unit）である。プロセッサ241は、システムバスを介してサーバ4A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241は、ROM242およびRAM243と協働して契約管理サーバ204Aにおける制御およびデータ処理などの動作を実行する。

[0133] ROM（Read Only Memory）242は、契約管理サーバ204A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。

RAM（Random Access Memory）243は、データを一時的に記憶する揮発性のメモリである。RAM243は、プロセッサ241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。

データメモリ244は、各種のデータを記憶する記憶部である。データメモリ244は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ244は、OSプログラム、アプリケーションプログ

ラム、動作設定情報などを記憶する。

[0134] インターフェース245は、データストレージ204Bにアクセスするためのインターフェースである。データストレージ204Bが外部デバイスとしての記憶装置である場合、インターフェース245は、データストレージ204Bとしての記憶装置が備えるインターフェース規格に対応したものであれば良い。また、データストレージ204Bがデータサーバ等である場合、インターフェースは、データストレージ204Bとしてのサーバと通信するための通信インターフェースで構成すれば良い。

[0135] ネットワーク（NW）通信部246は、外部装置と通信するための通信インターフェースである。NW通信部246は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第2実施形態に係るICカード発行システム201において、NW通信部246は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末203と通信するものであれば良い。

[0136] 通信部247は、データ生成サーバ205Aと通信するための通信インターフェースである。通信部247は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第2実施形態に係るICカード発行システム201において、通信部247は、データ生成サーバ205Aとの通信がセキュアに行えるものであれば良い。

なお、NW通信部246および通信部247は、1つの通信インターフェースで実現する構成しても良い。さらに、インターフェース245についても、NW通信部246又は通信部247と共通化した通信インターフェースとする構成としても良い。

[0137] 次に、第2実施形態に係るICカード発行システム201におけるデータ生成サーバ205Aの構成について説明する。

図13は、第2実施形態に係るICカード発行システム201におけるデータ生成サーバ205Aの構成例を示すブロック図である。

図13に示すように、データ生成サーバ205Aは、プロセッサ251、

ROM 252、RAM 253、データメモリ 254、インターフェース 255、ネットワーク（NW）通信部 256、通信部 257、および、インターフェース 258を有する。

[0138] プロセッサ 251は、プログラムを実行することにより各種の処理を実行する。プロセッサ 251は、例えば、CPU（Central Processing Unit）である。プロセッサ 251は、システムバスを介してサーバ 205 A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 251は、ROM 252およびRAM 253と協働してデータ生成サーバ 205 Aにおける制御およびデータ処理などの動作を実行する。

[0139] ROM（Read Only Memory）252は、データ生成サーバ 205 A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。

RAM（Random Access Memory）253は、データを一時的に記憶する揮発性のメモリである。RAM 253は、プロセッサ 251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。

データメモリ 254は、各種のデータを記憶する記憶部である。データメモリ 254は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ 254は、OSプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0140] インターフェース 255は、HSM 205 Bにアクセスするためのインターフェースである。インターフェース 255は、HSM 205 Bが備えるインターフェース規格に対応したものであれば良い。

ネットワーク（NW）通信部 256は、外部装置と通信するための通信インターフェースである。NW通信部 256は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第2実施形態に係るICカード発行システム 201において、NW通信部 256は、インターネットなどの広域のネットワークを介してユーザが使用するユーザ端末 203と通信するものであれば良い。

[0141] 通信部 257 は、契約管理サーバ 204A と通信するための通信インターフェースである。通信部 257 は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。第 2 実施形態に係る IC カード発行システム 201 において、通信部 257 は、契約管理サーバ 204A との通信がセキュアに行えるものであれば良い。

なお、NW 通信部 256 および通信部 257 は、1 つの通信インターフェースで実現する構成しても良い。

[0142] インターフェース 258 は、PUF ストレージ 205C にアクセスするためのインターフェースである。インターフェース 258 は、PUF ストレージ 205C が備えるインターフェース規格に対応したものであれば良い。プロセッサ 251 は、インターフェース 258 を介して PUF ストレージ 205C に登録されている PUF データを確認する。

[0143] 次に、第 2 実施形態に係る IC カード発行システム 201 における IC カード 202 に対する発行処理の申請手続きおよび発行手続きについて説明する。

以下に説明する動作の前提条件として、IC カード 202 は、一次発行（カード製造と初期化）の処理がなされた後にユーザ（カードホルダ）に渡されるものとする。また、ユーザに渡される IC カード 202 には、一次発行においてカード認証データの生成に関する鍵（鍵情報）が書き込まれているものとする。IC カード 202 に書き込まれた鍵情報は、発行制御システム 205 における HSM 205B に保存されている。さらに、ユーザ（カードホルダ）が所持する IC カード 202 には、当該ユーザの本人認証が行われた上で当該ユーザ（本人）の指紋情報が書き込まれているものとする。

[0144] まず、第 2 実施形態に係る IC カード発行システム 201 における IC カード 202 に対する発行処理の申請手続きについて説明する。

図 14 は、IC カード発行システム 201 における IC カード 202 に対する発行処理の申請手続きの動作例を説明するためのシーケンスである。

カードホルダは、ユーザ端末 203 のプロセッサ 231 は、カードホルダ

としてのユーザの操作に応じて入力部238による申請データの入力を受け付ける(ST221)。申請データとしては、例えば、発行処理(二次発行又は機能追加)に必要な情報、カードホルダであるユーザ自身の個人情報、および、カードホルダ(ユーザ)が所持するICカード202に関する情報などが含まれることが想定される。

[0145] また、ユーザ端末203は、申請用のプログラムにより申請データが入力されるようにしても良いし、インターネット上に提供される申請データの入力用のWebサイトで申請データが入力されるようにしても良い。前者の場合、ユーザ端末203は、データメモリ234に申請用のプログラムをインストールしておく。ユーザ端末203のプロセッサ231は、ユーザの操作に応じて申請用のプログラムを起動し、申請用のプログラムで提示される申請データの入力フォーマットに従って申請データを入力する。また、後者の場合、ユーザ端末203のプロセッサ231は、NW通信部235によりインターネット上で提供される申請データの入力用のサイトにアクセスし、入力用のサイトで提示される申請データの入力フォーマットに沿って申請データを入力する。

[0146] また、ユーザ端末203のプロセッサ231は、入力部238で入力される申請データの情報に加えて、カードホルダ(ユーザ)が所持するICカード202に関する情報を当該ICカード202から読み取る。ここでは、当該ICカード202に関する情報には、当該ICカード202を識別するための固有な識別情報(ID)としてPUFデータが含まれるものとする。

[0147] また、カードホルダであるユーザ自身の個人情報がICカード202に保存されている場合、ユーザ端末203のプロセッサ231は、ユーザの個人情報をICカード202から読み取るようにしても良い。

[0148] 図14に示す動作例において、ICカード202は、ユーザ端末203のカードRW236からの要求に応じて、生体認証で本人確認が成功した後にPUFデータを含むICカードに関する情報を出力するものとする。

[0149] この場合、ユーザ端末203のプロセッサ231は、カードRW236に

より生体認証としての指紋認証の要求とPUFデータの出力要求とICカード202へ送信する(ST222)。ICカード202のプロセッサ221は、ユーザ端末203からの要求に応じてデータメモリ224に記憶されている指紋データを用いて指紋認証を実行する(ST211)。ICカード202のプロセッサ221は、指紋認証による本人確認が成功した後に当該ICカード202のPUFデータを含むカードデータをユーザ端末203へ出力する(ST212)。

[0150] 申請データの入力およびPUFデータの取得が完了すると、ユーザ端末203のプロセッサ231は、入力された申請データによる発行処理(契約)に関する審査を要求する審査リクエストを作成する(ST223)。審査リクエストは、申請データとして入力された申請内容によって、カードホルダが所持するICカード202に対する発行処理(二次発行又は機能追加)を実行すること(契約)が可能であるか否かの審査を要求するものである。また、審査リクエストには、ICカード202から取得したPUFデータも含まれるものとする。

[0151] 申請データとPUFデータとを含む審査リクエストを作成すると、ユーザ端末203のプロセッサ231は、データ管理システム204の契約管理サーバ204Aへ審査リクエストを送信する(ST224)。プロセッサ231は、NW通信部235によりインターネットを介して契約管理サーバ204Aにアクセスし、審査リクエストを契約管理サーバ204Aへ送信する。

[0152] 契約管理サーバ204Aは、NW通信部246によりユーザ端末203からの審査リクエストを受け付ける(ST231)。ユーザ端末203からの審査リクエストを受信すると、契約管理サーバ204Aのプロセッサ241は、受信した審査リクエストに応じて申請された発行処理を許可するか否かを審査する。

[0153] 例えば、契約管理サーバ204Aは、申請データが示す申請内容に問題がないか、および、申請者であるカードホルダに関して発行処理を行うための契約上の問題がないかを審査する。審査の内容および手続きは、運用形態に

準じたものであれば良く、特定の形態に限定されるものではない。つまり、審査手続きは、契約管理サーバ204Aに審査リクエストに対する審査結果が入力されるものであれば良い。

[0154] 審査リクエストに対する審査結果が契約不可（発行処理が不可）であった場合、契約管理サーバ204Aのプロセッサ241は、審査結果として契約不可となった旨を審査リクエストの送信元であるユーザ端末203へ通知する（ST234）。また、プロセッサ241は、申請データでカードホルダが指定した連絡先に審査結果を通知するようにしても良い。

[0155] ユーザ端末203のプロセッサ231は、契約管理サーバ204Aから審査リクエストに対する審査結果が契約不可である旨の通知を受けると、審査結果が契約不可であった旨を表示部237に表示することによりカードホルダに報知する（ST225）。

[0156] 審査リクエストに対する審査結果が契約可（発行処理が可）であった場合、契約管理サーバ204Aのプロセッサ241は、契約IDを発行する（ST232）。契約IDを発行すると、プロセッサ241は、審査結果が契約可となった審査リクエストに含まれる申請データとPUFデータとを発行した契約IDに対応づけてデータストレージ204Bに登録する（ST233）。これにより、データストレージ204Bは、契約管理サーバ204Aからの申請データとPUFデータと契約IDとを対応づけた情報を保存する（ST241）。

[0157] 申請データとPUFデータと契約IDとをデータストレージ204Bに登録すると、契約管理サーバ204Aのプロセッサ241は、審査結果とともに契約IDを審査リクエストの送信元であるユーザ端末203へ通知する（ST234）。

[0158] ユーザ端末203のプロセッサ231は、契約管理サーバ204Aから審査リクエストに対する審査結果が契約可である旨の通知を受けると、審査結果として契約可であった旨の案内とともに、契約IDを表示部237に表示する（ST225）。ここで、審査結果が可であった場合、ユーザ端末20

3のプロセッサ231は、表示部237に発行処理の手続きに関する案内などを表示するようにしても良い。なお、契約IDは、審査結果が契約可であった場合にカードホルダとなるユーザに報知されるものであれば良い。例えば、契約管理サーバ204Aは、申請データに含まるカードホルダの連絡先（例えば、メールアドレス）に契約IDを通知するようにしても良い。

[0159] 以上のような申請手続きによって、契約管理サーバは、ユーザ端末からの審査リクエストが契約可となった場合、当該審査リクエストを行ったカードホルダからの申請データと発行処理の対象とするICカードのPUFデータと契約IDとをデータストレージに保存することができる。この結果、カードホルダが所持するICカード202は、後述するような動作によるリモートでの発行処理が可能な状態となる。つまり、カードホルダは、発行処理が可能な状態となった後、ユーザ端末203を用いてICカード202に対してリモートで発行処理を行うための後述するような発行手続きを実行する。

[0160] 次に、第2実施形態に係るICカード発行システム201におけるICカード202に対する発行処理を行うための発行手続きについて説明する。

図15および図16は、ICカード発行システム201におけるICカード202に対する発行処理を行うための発行手続きの動作例を説明するためのシーケンスである。

カードホルダとしてのユーザは、ユーザ端末203においてICカード202に対する発行処理用のアプリケーションプログラム（以下、発行アプリと称する）を起動させる。発行アプリは、予めデータメモリ224に記憶しておくようにしても良いし、契約管理サーバ204A又はデータ生成サーバ205Aからダウンロードするようにしても良い。

[0161] ユーザ端末203のプロセッサ231は、カードホルダが入力部238に入力する発行アプリの起動指示に応じて発行アプリを起動させる（ST320）。発行アプリが起動すると、プロセッサ231は、カードホルダに対して契約IDの入力を要求する（ST321）。カードホルダは、申請データに対する審査結果と共に取得した契約IDを入力部238により入力する。

プロセッサ231は、入力部238に契約IDが入力されると、カードRW236によりICカード202にアクセスし、本人確認のための生体認証としての指紋認証をICカード202に要求する(ST322)。

[0162] ICカード202は、カードRW236から供給される電力により起動する。ICカード202が起動すると、プロセッサ221は、カードRW236から供給される生体(指紋)認証の要求に応じて指紋認証処理を実行する(ST311)。指紋認証を実行する場合、プロセッサ221は、指紋センサ220によってユーザ(カードホルダ)の指紋を取得する。プロセッサ221は、指紋センサ220が取得した指紋情報とデータメモリ224の第2の記憶領域224bに記憶している指紋データとを比較することにより指紋認証を行う。

[0163] 指紋センサ220が取得した指紋情報とデータメモリ224の第2の記憶領域224bに記憶している指紋データとが同一人物の指紋であると判定された場合、プロセッサ221は、指紋認証が成功したものとする。指紋センサ220が取得した指紋情報と第2の記憶領域224bに記憶している指紋データとが同一人物の指紋であると判定できなかった場合、プロセッサ221は、指紋認証が失敗したものとする。

[0164] ICカード202における指紋認証が失敗した場合、プロセッサ221は、指紋認証が失敗したことをカードRW236へ通知する。カードRW236によりICカード202から指紋認証が失敗した旨の通知を受けた場合、ユーザ端末203のプロセッサ231は、ICカード202に対する発行処理を実行するための発行手続きを中止する。この場合、プロセッサ231は、表示部237に本人確認が失敗したためにICカード202に対する発行処理で不可となった旨を表示することによりユーザに発行手続きの中止を報知する。

[0165] ICカード202における指紋認証が成功した場合、プロセッサ221は、指紋認証が成功したことをカードRW236へ通知する。カードRW236によりICカード202から指紋認証が成功した旨の通知を受けた場合、

ユーザ端末203のプロセッサ231は、カードRW236を介してICカード202に発行処理を実行するためのカード認証データとPUFデータとを要求する。これに対して、ICカード202のプロセッサ221は、カード認証データを生成するとともにPUFデータを取得し、生成したカード認証データとPUFデータとをカードRW236へ供給する。

[0166] すなわち、ICカード202のプロセッサ221は、指紋認証が成功した場合、カード認証データ（認証データ）を生成する（ST312）。カード認証データは、当該ICカード202における生体認証が成功した場合に生成される認証データであり、当該ICカード202に機能追加（例えば、アプリレットの追加）あるいは二次発行などの発行処理を実施するための情報を含む。

[0167] カード認証データは、セキュアメモリであるデータメモリ224の記憶領域224aに記憶されている鍵情報を用いて生成される。また、カード認証データには、発行処理を実施するための情報として、例えば、CPLC（当該ICカードのプロダクトサイクルを示す情報）、INITIALIZEUPDATEコマンドおよびレスポンスデータなどが含まれる。

[0168] また、ICカード202のプロセッサ221は、指紋認証が成功した場合、当該ICカード202に固有な情報であるPUFデータを取得する。図10に示すようにPUFデータがデータメモリ224の第3の記憶領域224cに保持される場合、プロセッサ221は、データメモリ224における第3の記憶領域からPUFデータを取得する。ただし、ICカード202がPUFデータを出力するデバイスとしてのPUF回路を備える構成である場合、プロセッサ221は、PUF回路からPUFデータを取得するようにすれば良い。

[0169] 指紋認証が成功した後にカード認証データを生成し、PUFデータを取得すると、ICカード202のプロセッサ221は、生成したカード認証データとPUFデータとをユーザ端末203のカードRW236へ出力する（ST313）。カード認証データとPUFデータとを出力した後、ICカード

202のプロセッサ221は、当該カード認証データに対応してデータ生成サーバ205Aが生成する発行データに基づく発行処理が実行可能な状態とする。

[0170] ユーザ端末203のプロセッサ231は、カードRW236により指紋認証が成功したICカード202からカード認証データとPUFデータとを取得すると、ICカード202に対する発行処理を要求する発行リクエストを生成し、生成した発行リクエストをデータ生成サーバ205Aへ送信する(ST324)。

[0171] 例えば、プロセッサ231は、ICカード202から取得するカード認証データとPUFデータとに加えて入力部238で入力された契約IDを含む発行リクエストを生成する。カード認証データとPUFデータと契約IDとを含む発行リクエストを生成すると、プロセッサ231は、NW通信部235によりインターネットを介して発行制御システム205におけるデータ生成サーバ205Aにアクセスする。データ生成サーバ205Aにアクセスすると、プロセッサ231は、カード認証データ、PUFデータおよび契約IDを含む発行リクエストをデータ生成サーバ205Aへ送信する。

[0172] データ生成サーバ205Aは、NW通信部256によりユーザ端末203からの発行リクエストを受信する。発行リクエストを受信した場合、データ生成サーバ205Aのプロセッサ251は、発行リクエストに含まれる契約IDを抽出する。発行リクエストに含まれる契約IDを抽出すると、プロセッサ251は、通信部257を介して契約管理サーバ204Aにアクセスする。契約管理サーバ204Aにアクセスすると、プロセッサ251は、発行リクエストに含まれる契約IDに対応する申請データの要求(リクエスト)を契約管理サーバ204Aへ送信する(ST331)。

[0173] 契約管理サーバ204Aは、通信部247を介してデータ生成サーバ205Aと通信する。契約管理サーバ204Aのプロセッサ241は、データ生成サーバ205Aから契約IDに対応する申請データを要求するリクエストを受信した場合、データストレージ204Bにおいて当該契約IDに対応す

る申請データを検索する（ST341）。データ生成サーバ205Aから要求された契約IDに対応する申請データを検出すると、プロセッサ241は、通信部247を介して当該契約IDに対応する申請データとPUFデータとをデータ生成サーバ205Aへ送信する（ST342）。

[0174] 契約管理サーバ204Aから契約IDに対応する申請データとPUFデータとを受信すると、データ生成サーバ205Aのプロセッサ251は、ユーザ端末203からの発行リクエストに含まれるPUFデータが、PUFストレージ205Cに登録され、かつ、申請データに対応するPUFデータと一致するかを確認する（ST332）。

[0175] 例えば、プロセッサ251は、発行リクエストに含まれるPUFデータがPUFストレージ205Cに登録されているかを確認する。つまり、プロセッサ251は、発行リクエストに含まれるPUFデータ（発行処理を要求するICカードのPUFデータ）がPUFストレージ205Cに登録されているか正規品のICカードのPUFデータであるかを確認（真偽判定）する。これにより、プロセッサ251は、発行処理を要求するICカードが正規品であることを確認できる。

[0176] 発行リクエストに含まれるPUFデータがPUFストレージ205Cに登録されている場合、プロセッサ251は、さらに、発行リクエストに含まれるPUFデータが契約管理サーバ204Aから取得したPUFデータと一致するかを確認する。つまり、プロセッサ251は、発行リクエストに含まれるPUFデータ（発行処理を要求するICカードのPUFデータ）が発行処理の申請を行ったICカードのPUFデータと一致するかを確認する。これにより、プロセッサ251は、発行処理を要求するICカードが発行処理の申請を行ったICカードと同一であることを確認できる。

なお、データ生成サーバ205Aのプロセッサ251は、ユーザ端末203から発行リクエストを受けた場合に、発行リクエストに含まれるPUFデータがPUFストレージに登録されているかをチェックするようにしても良い。すなわち、プロセッサ251は、発行リクエストに含まれるPUFデー

タがPUFストレージに登録されていることを確認した後に、契約管理サーバ204Aから申請データとPUFデータとを取得するようにしても良い。

[0177] PUFデータのチェックにより発行処理の対象とするICカード202が正規品で、かつ、申請を行ったICカードと一致することを確認した場合、データ生成サーバ205Aのプロセッサ251は、ICカード202において申請データに基づく発行処理を実行するための発行データを生成する(ST333)。発行データは、申請データに基づく一連の発行処理においてICカード202に実行させるべきコマンドと一連の発行処理においてICカード202に書き込むべきデータとを含む。

[0178] 例えば、発行処理としてICカード202にアプレットを追加する場合、発行データには、ICカード202に実行させるべきコマンドとしてインストール(INSTALL)コマンドが含まれる。また、あるクレジットカードの規格でアプレットを追加する場合、発行データには、ICカード202に実行させるべきコマンドとして外部認証(EXTERNAL AUTHENTICATE)コマンド、および、ストアデータ(STORE DATA)コマンドが含まれる。

[0179] また、プロセッサ251は、発行データをセキュアにICカード202に供給するためにHSM205Bが保管する鍵情報を用いて発行データを処理する(ST334)。ここで、HSM205Bには、ICカード202内に保持する鍵情報に対応する鍵情報が保存されている。これにより、HSM205Bを用いた暗号化によって安全に発行データをICカード202へ供給できる。例えば、プロセッサ251は、HSM205Bにおいて当該ICカード202内の保存される鍵情報と共有する鍵情報を用いて発行データに含まれるデータを暗号化する。

[0180] 発行データをHSM205Bが保管する鍵情報で暗号化処理した後、プロセッサ251は、発行リクエストの送信元であるユーザ端末203へHSM205Bで暗号化処理した発行データを送信する(ST335)。

[0181] ユーザ端末203は、データ生成サーバ205Aへ発行リクエストを送信

した後、発行リクエストに対する応答としての発行データの受信待ちとなる。この状態において、ユーザ端末203は、NW通信部2354によりデータ生成サーバ205Aから送信される発行データを受信する(ST325)。発行データを受信した場合、ユーザ端末203のプロセッサ231は、カードRW236によりICカード202に対して発行データを出力する(ST326)。

[0182] これにより、ICカード202のプロセッサ221は、生体認証が成功した後に生成したカード認証データに対応する発行データをユーザ端末203のカードRW236から取得することとなる。発行データを取得すると、プロセッサ221は、取得した発行データに従って発行処理を実行する(ST314)。

[0183] 例えば、プロセッサ221は、発行データに含まれるコマンドを実行することにより発行処理として書き込むべきデータをデータメモリ224に書き込む。また、プロセッサ221は、発行処理において供給される発行データに含まれる暗号化データをデータメモリ224におけるセキュアメモリである第1の記憶領域224aに記憶している鍵情報を用いて復号化する。

[0184] ICカード202のプロセッサ221は、供給された発行データに基づく発行処理が完了すると、発行処理の完了をユーザ端末203のカードRW236へ通知する(ST315)。

ユーザ端末203は、カードRW236によりICカード202へ発行データを出力した後にICカード202から発行処理が完了した旨の通知を受信する。ユーザ端末203のプロセッサ231は、カードRW236によりICカード202から発行処理の完了通知を受けると、ICカード202における発行処理（機能追加あるいは二次発行）が完了した旨の案内を表示部237に表示する(ST327)。

[0185] また、発行データに基づくICカード202における発行処理が完了した旨の通知を受けると、プロセッサ231は、NW通信部235により発行データの送信元であるデータ生成サーバ205Aへ発行処理の完了を通知する

(ST328)。

データ生成サーバ205Aのプロセッサ251は、ユーザ端末203からのICカード202における発行処理の完了通知をNW通信部256により受信すると、通信部257によりICカード202における発行処理の完了通知を契約管理サーバ204Aへ転送(送信)する。

[0186] 契約管理サーバ204Aは、通信部247によりデータ生成サーバ205Aを介してICカード202における発行処理の完了通知を受信する。契約管理サーバ204Aのプロセッサ241は、データ生成サーバ205Aを経由してICカード202における発行処理の完了通知を受信すると、データストレージ204Bにおいて申請データに対応して発行処理の完了を記録する(ST343)。

[0187] 以上のような発行手続きによって、第2実施形態に係るICカード発行システムは、生体センサとしての指紋センサを有するICカードにおける生体認証による本人認証が成功した後、当該ICカードが正規品で、かつ、申請時のICカードと一致するかについてPUFデータを用いて確認できる。この結果、第2実施形態に係るICカード発行システムは、正規品で、かつ、申請時と一致するICカードに対してリモートで機能追加あるいは二次発行などの発行処理を行うことができる。

[0188] 第2実施形態に係るICカード発行システムは、PUFデータを用いたが、これにより、従来のようにICカードを生成する際に人為的に個々のLSIに対する固有のデータを生成し、それをLSIに書き込むという作業が不要となる。PUFは、電子回路や半導体の結晶パターンなどの物理的な固有のばらつきを利用して、特定のアルゴリズムにより、自動的に生成させることができるからである。

[0189] また、ICカードに個別に付される識別符号のような固有データが必要となる場合、過去に発行してきたデータと必ず異なるデータとなることが必要となる。その点、PUFは、必ず固有のデータとなり、重複することがないため、IDとして、この第2実施形態に係る発明に好適となる。

- [0190] さらに、ＬＳＩに固有のデータを作成するには、ＬＳＩベンダーによって、作成する様式又は形式が異なるのが一般的である。その点、第２実施形態に係る発明によれば、ＰＵＦを使用することで、固有のデータの生成や形式を統一することができる。
- [0191] 上述の各実施形態で説明した機能は、ハードウェアを用いて構成するに留まらず、ソフトウェアを用いて各機能を記載したプログラムをコンピュータに読み込ませて実現することもできる。また、各機能は、適宜ソフトウェア、ハードウェアのいずれかを選択して構成するものであっても良い。
- [0192] 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] 携帯可能電子装置とデータ生成サーバとを有するリモート発行システムであって、
- 前記携帯可能電子装置は、
- 生体情報を取得する生体センサと、
- ユーザの生体情報を記憶する記憶領域を含むメモリと、
- ユーザ端末と接続されるリーダライタと通信する通信インターフェースと、
- 前記生体センサにより取得する生体情報と前記メモリに保存する生体情報との照合による生体認証が成功した場合に当該携帯可能電子装置において発行処理を行うための認証データを生成し、前記認証データを前記リーダライタへ出力し、前記リーダライタから供給される前記認証データに対応する発行データに基づいて発行処理を実行する第1プロセッサと、を有し、
- 前記データ生成サーバは、
- 前記ユーザ端末と通信する通信部と、
- 前記ユーザ端末から前記携帯可能電子装置が生成した前記認証データと契約IDとを含む発行リクエストを受信した場合、前記契約IDに対応する申請データと前記認証データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信する第2プロセッサと、を有する、
- リモート発行システム。
- [請求項2] 前記携帯可能電子装置は、前記生体センサ、前記メモリ、前記第1プロセッサ、および、前記通信インターフェースを有するモジュールと、前記モジュールを格納する本体と、を備えるICカードである、
- 請求項1に記載のリモート発行システム。
- [請求項3] 前記生体センサは、指紋情報を取得する指紋センサである、
- 請求項1又は2のいずれか1項に記載のリモート発行システム。

[請求項4]

前記携帯可能電子装置は、
前記メモリは、さらに、鍵情報を記憶するセキュアメモリを含み、
前記第1プロセッサは、前記セキュアメモリに記憶する鍵情報を用いて前記認証データを生成し、
前記データ生成サーバは、
さらに、前記携帯可能電子装置が備える前記セキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウェアセキュリティモジュールに接続するインターフェースを有し、
前記第2プロセッサは、前記ハードウェアセキュリティモジュールが保存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、
請求項1に記載のリモート発行システム。

[請求項5]

契約管理サーバとデータ生成サーバとを有するリモート発行システムであって、
前記契約管理サーバは、
ユーザ端末と通信する第1通信部と、
前記第1通信部によりユーザ端末から携帯可能電子装置に対する発行処理を申請する申請データを含む審査リクエストを受信し、前記審査リクエストに応じた審査で前記申請データで申請される発行処理が許可された場合に契約IDを発行する第1プロセッサと、前記契約IDと前記申請データとを対応づけて保存するデータストレージにアクセスするためのインターフェースと、と有し、
前記データ生成サーバは、
前記ユーザ端末と通信する第2通信部と、
携帯可能電子装置における生体認証が成功した場合に当該携帯可能電子装置が生成する認証データと前記契約管理サーバが発行した前記契約IDとを含む発行リクエストを前記ユーザ端末から受信し、
前記発行リクエストに含まれる契約IDに対応する申請データを

前記契約管理サーバから取得し、

前記契約管理サーバから取得した申請データに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記携帯可能電子装置と通信するリーダライタを備える前記ユーザ端末へ送信する、第2プロセッサと、を有する、

リモート発行システム。

[請求項6]

前記データ生成サーバは、

さらに、前記携帯可能電子装置が備えるセキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウェアセキュリティモジュールに接続するインターフェースを有し、

前記第2プロセッサは、前記ハードウェアセキュリティモジュールが保存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、

請求項5に記載のリモート発行システム。

[請求項7]

生体認証を行う機能を備える携帯可能電子装置と通信するリーダライタを接続するユーザ端末と通信する通信部と、

前記携帯可能電子装置における生体認証が成功した場合に当該携帯可能電子装置が生成する認証データと契約IDとを含む発行リクエストを前記ユーザ端末から受信し、

前記発行リクエストに含まれる前記認証データと前記契約IDに対応する申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信するプロセッサと、

を有するデータ生成サーバ。

[請求項8]

さらに、前記携帯可能電子装置が備えるセキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウェアセキュリティモジュールと接続するインターフェースを有し、

前記プロセッサは、前記ハードウェアセキュリティモジュールが保

存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、

請求項7に記載のデータ生成サーバ。

[請求項9]

携帯可能電子装置とデータ生成サーバとを有するリモート発行システムであって、

前記携帯可能電子装置は、

生体情報を取得する生体センサと、

ユーザの生体情報を記憶する記憶領域を含むメモリと、

リーダライタと通信する通信インターフェースと、

前記生体センサにより取得する生体情報と前記メモリに保存する生体情報との照合による生体認証が成功した場合に当該携帯可能電子装置において発行処理を行うための認証データを生成し、前記認証データと当該携帯可能電子装置に固有なPUFデータとを前記リーダライタへ出力し、前記リーダライタから供給される前記認証データに対応する発行データに基づいて発行処理を実行する第1プロセッサと、を有し、

前記データ生成サーバは、

発行処理が可能な携帯可能電子装置のPUFデータを保存するPUFストレージに接続するインターフェースと、

前記携帯可能電子装置が生成した認証データとPUFデータとを含む発行リクエストが入力された場合、前記発行リクエストに含まれるPUFデータが前記PUFストレージに登録されていれば、前記携帯可能電子装置に対する発行処理に関する申請データと前記認証データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成する第2プロセッサと、を有する、

リモート発行システム。

[請求項10]

前記携帯可能電子装置の前記メモリは、さらに、当該携帯可能電子装置に固有なPUFデータを記憶し、

前記携帯可能電子装置の前記第1プロセッサは、生体認証が成功した場合に前記メモリに記憶された前記PUFデータを取得する、
請求項9に記載のリモート発行システム。

- [請求項11] 前記携帯可能電子装置は、さらに、固有なPUFデータを出力するPUF回路を有し、前記携帯可能電子装置の前記第1プロセッサは、生体認証が成功した場合に前記PUF回路が出力するPUFデータを取得する、
請求項9に記載のリモート発行システム。

- [請求項12] 前記携帯可能電子装置は、前記生体センサ、前記メモリ、前記第1プロセッサおよび前記通信インターフェースを有するモジュールと、前記モジュールを格納する本体と、を備えるICカードである、
請求項9乃至11のいずれか1項に記載のリモート発行システム。

- [請求項13] 前記生体センサは、指紋情報を取得する指紋センサである、
請求項9乃至12のいずれか1項に記載のリモート発行システム。

- [請求項14] 前記携帯可能電子装置の前記通信インターフェースは、ユーザ端末と接続されるリーダライタと通信し、
前記データ生成サーバは、
さらに、前記ユーザ端末と通信する通信部を有し、
前記データ生成サーバの前記第2プロセッサは、前記ユーザ端末から前記携帯可能電子装置が生成した認証データとPUFデータとを含む発行リクエストを受信した場合、前記発行リクエストに含まれるPUFデータが前記PUFストレージに登録されていれば、前記携帯可能電子装置に対する発行処理に関する申請データと前記認証データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信する、
請求項9乃至13のいずれか1項に記載のリモート発行システム。

- [請求項15] 前記携帯可能電子装置の前記メモリは、さらに、鍵情報を記憶するセキュアメモリを含み、

前記携帯可能電子装置の前記第 1 プロセッサは、前記セキュアメモリに記憶する鍵情報を用いて前記認証データを生成し、

前記データ生成サーバは、

さらに、前記携帯可能電子装置が備える前記セキュアメモリに記憶される鍵情報に対応する鍵情報を保存するハードウェアセキュリティモジュールに接続する第 2 のインターフェースを有し、

前記データ生成サーバの前記第 2 プロセッサは、前記ハードウェアセキュリティモジュールが保存する鍵情報を用いて処理された前記認証データおよび前記申請データに基づく前記発行データを前記ユーザ端末へ送信する、

請求項 14 に記載のリモート発行システム。

[請求項16]

契約管理サーバとデータ生成サーバとを有するリモート発行システムであって、

前記契約管理サーバは、

ユーザ端末と通信する第 1 通信部と、

前記第 1 通信部によりユーザ端末から携帯可能電子装置に対する発行処理を申請する申請データを含む審査リクエストを受信し、前記審査リクエストに応じた審査で前記申請データで申請される発行処理が許可された場合に契約 ID を発行する第 1 プロセッサと、前記契約 ID と前記申請データとを対応づけて保存するデータストレージにアクセスするための第 1 インターフェースと、と有し、

前記データ生成サーバは、

前記ユーザ端末と通信する第 2 通信部と、

発行処理が可能な携帯可能電子装置の PUF データを保存する PUF ストレージに接続する第 2 インターフェースと、

生体認証が成功した携帯可能電子装置が生成する認証データと当該携帯可能電子装置の PUF データと契約 ID とを含む発行リクエストを前記ユーザ端末から受信した場合、前記発行リクエストに含まれ

る P U F データが前記 P U F ストレージに登録されていれば、前記発行リクエストに含まれる契約 I D に対応する申請データを前記契約管理サーバから取得し、

前記発行リクエストに含まれる認証データと前記契約管理サーバから取得した申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記携帯可能電子装置と通信するリーダライタを備える前記ユーザ端末へ送信する、第 2 プロセッサと、を有する、

リモート発行システム。

[請求項 17]

前記契約管理サーバは、

前記第 1 プロセッサは、前記第 1 通信部によりユーザ端末から携帯可能電子装置に対する発行処理を申請する申請データと P U F データとを含む審査リクエストを受信し、

前記データストレージには、前記契約 I D と前記申請データと前記 P U F データとを対応づけて保存し、

前記第 2 プロセッサは、

前記発行リクエストに含まれる P U F データが前記 P U F ストレージに登録されていれば、前記発行リクエストに含まれる契約 I D に対応する申請データと P U F データとを前記契約管理サーバから取得し、

前記発行リクエストに含まれる認証データと前記契約管理サーバから取得した P U F データと一致すれば、前記発行リクエストに含まれる認証データと前記契約管理サーバから取得した申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成する、

請求項 1 6 に記載のリモート発行システム。

[請求項 18]

生体認証を行う機能を備える携帯可能電子装置と通信するリーダライタを接続するユーザ端末と通信する通信部と、

発行処理が可能な携帯可能電子装置のPUFデータを保存するPUFストレージに接続するインターフェースと、

生体認証が成功した携帯可能電子装置が生成する認証データとPUFデータと契約IDとを含む発行リクエストを前記ユーザ端末から受信した場合、前記発行リクエストに含まれるPUFデータが前記PUFストレージに登録されていれば、前記発行リクエストに含まれる前記認証データと前記契約IDに対応する申請データとに基づいて前記携帯可能電子装置に発行処理を実行させる発行データを生成し、生成した発行データを前記ユーザ端末へ送信するプロセッサと、

を有するデータ生成サーバ。