

明 細 書

発明の名称：ＩＣカード、携帯可能電子装置及び発行装置

技術分野

[0001] 本発明の実施形態は、ＩＣカード、携帯可能電子装置及び発行装置に関する。

背景技術

[0002] 生体情報のテンプレートを格納する親ＩＣカードに紐付いた子ＩＣカードを発行する手法が提供されている。子ＩＣカードは、親ＩＣカードの機能又は一部の機能を実現する。

[0003] 従来、子ＩＣカードを発行する発行装置は、親ＩＣカードが格納する生体情報を用いて本人を認証するなど、親ＩＣカードから生体情報を取得する機構が必要となる。

先行技術文献

特許文献

[0004] 特許文献１：日本国特開２００９－２７７１８４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、効果的に発行処理を行うことができるＩＣカード、携帯可能電子装置及び発行装置を提供する。

課題を解決するための手段

[0006] 実施形態によれば、親ＩＣカードに紐付くＩＣカードは、センサと、第１の記憶部と、第２の記憶部と、通信部と、プロセッサと、を備える。センサは、生体情報を取得する。第１の記憶部は、前記生体情報と照合するためのテンプレートを格納する。第２の記憶部は、前記親ＩＣカードが格納する第１のデータに関連する第２のデータを格納する。通信部は、上位装置とデータを送受信する。プロセッサは、前記上位装置からのコマンドに従って前記生体情報と前記テンプレートとの照合結果に基づいてユーザを認証し、前記

ユーザの認証に成功すると、前記第2のデータの少なくとも一部を前記上位装置に送信する。

図面の簡単な説明

[0007] [図1]図1は、第1の実施形態に係る発行システムの構成例を示すブロック図である。

[図2]図2は、第1の実施形態に係る発行装置の構成例を示すブロック図である。

[図3]図3は、第1の実施形態に係る親ICカードの構成例を示すブロック図である。

[図4]図4は、第1の実施形態に係る子ICカードの構成例を示すブロック図である。

[図5]図5は、第1の実施形態に係る管理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の実施形態に係る発行システムの動作例を示すシーケンス図である。

[図7]図7は、第1の実施形態に係る発行システムの動作例を示すシーケンス図である。

[図8]図8は、第2の実施形態に係る発行システムの動作例を示すシーケンス図である。

[図9]図9は、第3の実施形態に係る発行システムの動作例を示すシーケンス図である。

[図10]図10は、第3の実施形態に係る第3の証明書情報の構成例を示す図である。

[図11]図11は、第4の実施形態に係る発行システムの動作例を示すシーケンス図である。

[図12]図12は、第5の実施形態に係る発行システムの動作例を示すシーケンス図である。

[図13]図13は、第6の実施形態に係る発行システムの構成例を示すブロッ

ク図である。

[図14]図14は、第6の実施形態に係る鍵サーバの構成例を示すブロック図である。

[図15]図15は、第6の実施形態に係る発行システムの動作例を示すシーケンス図である。

実施形態

[0008] 以下、実施形態について、図面を参照して説明する。

(第1の実施形態)

まず、第1の実施形態について説明する。

[0009] 実施形態に係る発行システムは、マイナンバーカードなどのICカードを親ICカードとして子ICカードを発行する。発行システムは、親ICカードが格納する情報に関連する情報を子ICカードに格納する。また、発行システムは、生体認証を行うことができる子ICカードを発行する。

[0010] 図1は、実施形態に係る発行システム1の構成例を示す。図1が示すように、発行システム1は、発行装置10、親ICカード20、子ICカード30及び管理サーバ40などを備える。発行装置10は、親ICカード20及び子ICカード30に接続する。また、発行装置10は、ネットワーク50を介して管理サーバ40に接続する。

[0011] なお、発行システム1は、図1が示すような構成の他に必要に応じた構成をさらに具備したり、発行システム1から特定の構成が除外されたりしてもよい。

[0012] 発行装置10（上位装置）は、親ICカードに紐付く子ICカードを発行する。発行装置10は、親ICカード20と接続した状態で子ICカード30を発行する。発行装置10は、管理サーバ40又は親ICカード20などから子ICカード30に格納するデータを取得する。発行装置10は、取得されたデータを子ICカード30に格納する。発行装置10については、後に詳述する。

[0013] 親ICカード20は、所定の認証処理を行うためのICカードである。親

ＩＣカード２０は、顔などの生体情報を格納する。親ＩＣカード２０は、パスワードあるいは生体情報を用いてユーザを認証する。親ＩＣカード２０は、外部装置に生体情報を出力する。外部装置は、カメラなどを用いてユーザの顔画像を撮影して、親ＩＣカード２０からの生体情報と照合してもよい。また、外部装置は、親ＩＣカード２０からの生体情報を表示してオペレータによる認証を受け付けるものであってもよい。

[0014] また、親ＩＣカード２０は、秘密鍵、および、公開鍵などから構成される証明書情報を格納する。また、親ＩＣカード２０は、秘密鍵と証明書情報とをそれぞれ複数格納する場合もある。親ＩＣカード２０については、後に詳述する。

[0015] 子ＩＣカード３０は、親ＩＣカード２０に紐づくＩＣカードである。子ＩＣカード３０は、親ＩＣカード２０に関連する機能を実現する。たとえば、子ＩＣカード３０は、親ＩＣカード２０の機能又は一部の機能を実現する。また、子ＩＣカード３０は、親ＩＣカード２０が用いる生体情報と異なる生体情報を用いてユーザを認証する。子ＩＣカード３０については、後に詳述する。

[0016] 管理サーバ４０（外部装置）は、子ＩＣカード３０に格納するデータを管理する。たとえば、管理サーバ４０は、親ＩＣカード２０に格納するデータを格納する。管理サーバ４０は、親ＩＣカード２０に格納するデータに基づいて子ＩＣカード３０に格納するデータを生成する。たとえば、管理サーバ４０は、子ＩＣカード３０に格納するデータとして、秘密鍵、および、公開鍵などから構成される証明書情報などを生成する。管理サーバ４０については、後に詳述する。

[0017] ネットワーク５０は、発行装置１０と管理サーバ４０との間の通信などを中継する。たとえば、ネットワーク５０は、インターネットなどである。また、ネットワーク５０は、ＬＡＮ（Local Area Network）などであってもよい。

[0018] 次に、発行装置１０について説明する。

図2は、実施形態に係る発行装置10の構成例を示す。図2は、発行装置10の構成例を示すブロック図である。図2が示すように、発行装置10は、プロセッサ11、ROM12、RAM13、NVM14、通信部15、操作部16、表示部17、第1のリーダライタ18及び第2のリーダライタ19などを備える。

[0019] プロセッサ11と、ROM12、RAM13、NVM14、通信部15、操作部16、表示部17、第1のリーダライタ18及び第2のリーダライタ19と、は、データバスなどを介して互いに接続する。

なお、発行装置10は、図2が示すような構成の他に必要に応じた構成を具備したり、発行装置10から特定の構成が除外されたりしてもよい。

[0020] プロセッサ11は、発行装置10全体の動作を制御する機能を有する。プロセッサ11は、内部キャッシュ及び各種のインターフェースなどを備えてもよい。プロセッサ11は、内部メモリ、ROM12又はNVM14が予め記憶するプログラムを実行することにより種々の処理を実現する。

[0021] なお、プロセッサ11がプログラムを実行することにより実現する各種の機能のうちの一部は、ハードウェア回路により実現されるものであってもよい。この場合、プロセッサ11は、ハードウェア回路により実行される機能を制御する。

[0022] ROM12は、制御プログラム及び制御データなどが予め記憶された不揮発性のメモリである。ROM12に記憶される制御プログラム及び制御データは、発行装置10の仕様に依じて予め組み込まれる。

[0023] RAM13は、揮発性のメモリである。RAM13は、プロセッサ11の処理中のデータなどを一時的に格納する。RAM13は、プロセッサ11からの命令に基づき種々のアプリケーションプログラムを格納する。また、RAM13は、アプリケーションプログラムの実行に必要なデータ及びアプリケーションプログラムの実行結果などを格納してもよい。

[0024] NVM14は、データの書き込み及び書き換えが可能な不揮発性のメモリである。NVM14は、たとえば、HDD (Hard Disk Drive)、SSD (So

lid State Drive) 又はフラッシュメモリなどから構成される。NVM 14は、発行装置10の運用用途に応じて制御プログラム、アプリケーション及び種々のデータなどを格納する。

[0025] 通信部15は、ネットワーク50と通信するためのインターフェースである。即ち、通信部15は、ネットワーク50を通じて管理サーバ40などとデータを送受信するためのインターフェースである。たとえば、通信部15は、有線又は無線のLAN接続をサポートするインターフェースである。

[0026] 操作部16は、オペレータから種々の操作の入力を受け付ける。操作部16は、入力された操作を示す信号をプロセッサ11へ送信する。操作部16は、タッチパネルから構成されてもよい。

[0027] 表示部17は、プロセッサ11からの画像データを表示する。たとえば、表示部17は、液晶モニタから構成される。操作部16がタッチパネルから構成される場合、表示部17は、操作部16と一体的に形成されてもよい。

[0028] 第1のリーダライタ18は、親ICカード20とデータを送受信するためのインターフェース装置である。第1のリーダライタ18は、親ICカード20の通信方式に応じたインターフェースにより構成される。たとえば、親ICカード20が接触型のICカードである場合、第1のリーダライタ18は、親ICカード20のコンタクト部と物理的かつ電氣的に接続するための接触部などにより構成される。また、親ICカード20は、携帯可能電子装置であってもよい。たとえば、携帯可能電子装置は、USBインターフェースを備えたデバイスである場合、第1のリーダライタ18は、親ICカード20としての携帯可能電子装置のUSBコネクタ部と物理的かつ電氣的に接続するための接続部などにより構成される。すなわち、親ICカード20は、ICカードではなく、USBデバイスであってもよい。

[0029] また、親ICカード20が非接触型のICカードである場合、第1のリーダライタ18は、親ICカード20との無線通信を行うためのアンテナ及び通信制御部などにより構成される。第1のリーダライタ18は、親ICカード20に対する電源供給、クロック供給、リセット制御及びデータの送受信

などを行う。

[0030] このような機能によって第1のリーダライタ18は、プロセッサ11による制御に基づいて親ICカード20に対する電源供給、親ICカード20の活性化（起動）、クロック供給、リセット制御、種々のコマンドの送信及び送信したコマンドに対する応答（レスポンス）の受信などを行なう。

[0031] 第2のリーダライタ19は、子ICカード30とデータを送受信するためのインターフェース装置である。第2のリーダライタ19は、第1のリーダライタ18と同様の構成であるため詳細な説明を省略する。

[0032] 次に、親ICカード20について説明する。

親ICカード20は、発行装置10からのコマンドに従って動作する。親ICカード20は、コマンドに対するレスポンスを発行装置10に送信する。たとえば、親ICカード20は、マイナンバーカードである。

[0033] 図3は、親ICカード20の構成例を示す。図3が示すように、親ICカード20は、プラスチックなどで形成されたカード状の本体S aを有する。親ICカード20は、本体S a内にモジュールM aを内蔵する。モジュールM aは、ICチップC a、通信部25及びMPU26が接続された状態で一体的に形成され、親ICカード20の本体S a内に埋設される。

[0034] 親ICカード20は、モジュールM aなどを備える。モジュールM aは、ICチップC a、通信部25及びMPU26などを備える。ICチップC aは、プロセッサ21、ROM22、RAM23及びNVM24などを備える。プロセッサ21は、データバスなどを介してROM22、RAM23、NVM24、通信部25及びMPU26に接続する。

[0035] なお、親ICカード20は、図3が示すような構成の他に必要に応じた構成を具備したり、親ICカード20から特定の構成が除外されたりしてもよい。

[0036] プロセッサ21は、親ICカード20全体の制御を司る制御部として機能する。プロセッサ21は、ROM22又はNVM24に記憶される制御プログラム及び制御データに基づいて種々の処理を行う。たとえば、プロセッサ

２１は、ＲＯＭ２２に記憶されているプログラムを実行することにより、親ＩＣカード２０の動作制御又は親ＩＣカード２０の運用形態に応じた種々の処理を行う。

[0037] たとえば、プロセッサ２１は、プログラムを実行することにより、親ＩＣカード２０内の各部の制御及び情報処理を実現するプロセッサであればよい。

なお、プロセッサ２１がプログラムを実行することにより実現する各種の機能のうちの一部は、ハードウェア回路により実現されるものであっても良い。この場合、プロセッサ２１は、ハードウェア回路により実行される機能を制御する。

[0038] ＲＯＭ２２は、予め制御用のプログラム及び制御データなどを記憶する不揮発性のメモリである。ＲＯＭ２２は、製造段階で制御プログラム及び制御データなどを記憶した状態で親ＩＣカード２０に組み込まれる。即ち、ＲＯＭ２２に記憶される制御プログラム及び制御データは、予め親ＩＣカード２０の仕様などに応じて組み込まれる。

[0039] ＲＡＭ２３は、揮発性のメモリである。ＲＡＭ２３は、プロセッサ２１の処理中のデータなどを一時的に格納する。たとえば、ＲＡＭ２３は、計算用バッファ、受信用バッファ及び送信用バッファとして機能する。計算用バッファは、プロセッサ２１が実行する種々の演算処理の結果などを一時的に保持する。受信用バッファは、通信部２５を介して第１のリーダライタ１８から受信するコマンドデータなどを保持する。送信用バッファは、通信部２５を介して第１のリーダライタ１８へ送信するメッセージ（レスポンスデータ）などを保持する。

[0040] ＮＶＭ２４は、フラッシュＲＯＭなどのデータの書き込み及び書換えが可能な不揮発性のメモリにより構成される。ＮＶＭ２４は、親ＩＣカード２０の運用用途に応じて制御プログラム、アプリケーション及び種々のデータを格納する。例えば、ＮＶＭ２４では、プログラムファイル及びデータファイルなどが作成される。作成された各ファイルは、制御プログラム及び種々の

データなどが書き込まれる。

[0041] また、NVM24は、第1の秘密鍵と、第2の秘密鍵と、第1の公開鍵などから構成される第1の証明書情報と第2の公開鍵などから構成される第2の証明書情報とを格納する。第1の秘密鍵、第2の秘密鍵、第1の証明書情報及び第2の証明書情報については、後述する。

[0042] 通信部25は、第1のリーダライタ18とデータを送受信するためのインターフェースである。即ち、通信部25は、第1のリーダライタ18を通じて発行装置10とデータを送受信するためのインターフェースである。

[0043] 親ICカード20が接触型のICカードとして実現される場合、通信部25は、第1のリーダライタ18と物理的かつ電氣的に接触して信号の送受信を行うための通信制御部とコンタクト部とにより構成される。たとえば、親ICカード20は、コンタクト部を介して第1のリーダライタ18からの動作電源及び動作クロックの供給を受けて活性化される。

[0044] 親ICカード20が非接触型のICカードとしての実現される場合、通信部25は、第1のリーダライタ18との無線通信を行うための変復調回路などの通信制御部とアンテナとにより構成される。たとえば、親ICカード20は、アンテナ及び変復調回路などを介して第1のリーダライタ18からの電波を受信する。親ICカード20は、その電波から図示しない電源部により動作電源及び動作クロックを生成して活性化する。

[0045] MPU26 (Micro Processing Unit) は、第1の証明書情報又は第2の証明書情報を出力のためのパスワード照合を行う。

[0046] MPU26は、予めテンプレートを登録する。たとえば、テンプレートは、顔画像である。また、テンプレートは、顔画像から抽出された特徴量から構成されるものであってもよい。MPU26は、外部装置にテンプレートを出力する制御などを行う。すなわち、親ICカード20で生体認証を行う場合は、顔画像のような生体情報を外部装置に出力する必要がある。

[0047] 第1の証明書情報は、所定の桁数（たとえば、6桁）のパスワード照合で出力され、所定の処理に用いられる。たとえば、第1の証明書情報は、署名

用の電子証明書である。たとえば、第1の証明書情報は、電子申請又はオンライン取引の登録などに用いられる。

[0048] 第2の証明書情報は、第1の証明書情報よりもセキュリティレベルが低い証明書である。第2の証明書情報は、第1の証明書情報よりも小さな桁数（たとえば、4桁）のパスワード照合で出力され、所定の処理に用いられる。たとえば、第2の証明書情報は、利用者証明用の電子証明書である。たとえば、第2の証明書情報は、行政サイト（ポータルサイトなど）又は民間サイト（オンラインバンキングなど）へのログインに用いられる。

[0049] また、第2の証明書情報が第1の証明書情報よりもセキュリティレベルが低いケースとして、第2の証明書情報の認証に必要な鍵長が、第1の証明書情報の認証に必要な鍵長よりも桁数が低い場合もある。

[0050] 次に、子ICカード30について説明する。

子ICカード30は、発行装置10からのコマンドに従って動作する。子ICカード30は、コマンドに対するレスポンスを発行装置10に送信する。

[0051] 図4は、子ICカード30の構成例を示す。図4が示すように、子ICカード30は、プラスチックなどで形成されたカード状の本体Sbを有する。子ICカード30は、本体Sb内にモジュールMb及び指紋センサ37を内蔵する。モジュールMbは、ICチップCb、通信部35及びMPU36が接続された状態で一体的に形成され、子ICカード30の本体Sb内に埋設される。

[0052] 子ICカード30は、モジュールMb及び指紋センサ37などを備える。モジュールMbは、ICチップCb、通信部35及びMPU36などを備える。ICチップCbは、プロセッサ31、ROM32、RAM33及びNVM34（第1の記憶部および第2の記憶部）などを備える。プロセッサ31は、データバスなどを介してROM32、RAM33、NVM34、通信部35及びMPU36に接続する。MPU36は、データバスなどを介して指紋センサ37に接続する。なお、第1の記憶部、第2の記憶部は、物理的に

同じハードウェア内、例えば、1つのセキュアなNVM34内に実装しても良いし、物理的に異なる2つのセキュアなNVM34にそれぞれ実装してもよい。また、セキュアエレメントなどの別のハードウェアにて実装してもよい。

[0053] なお、子ICカード30は、図4が示すような構成の他に必要に応じた構成を具備したり、子ICカード30から特定の構成が除外されたりしてもよい。

[0054] プロセッサ31、ROM32、RAM33及びNVM34は、それぞれプロセッサ21、ROM22、RAM23及びNVM24と同様であるため説明を省略する。

[0055] 通信部35は、第2のリーダライタ19とデータを送受信するためのインターフェースである。即ち、通信部35は、第2のリーダライタ19を通じて発行装置10とデータを送受信するためのインターフェースである。

通信部35は、通信部25と同様の構成であるため詳細な説明を省略する。

[0056] 指紋センサ37は、ユーザの指から指紋画像（生体情報）を取得する。指紋センサ37は、テンプレートを生成するため及びユーザを認証するための指紋画像を取得する。たとえば、指紋センサ37は、CCDセンサなどを備える。また、指紋センサ37は、電気容量の変化を検出するセンサなどを備えるものであってもよい。指紋センサ37は、指紋画像をMPU36に送信する。

[0057] MPU36は、指紋センサ37からの指紋画像を処理する。MPU36は、指紋画像に基づいてテンプレートを生成する。たとえば、テンプレートは、指紋画像である。また、テンプレートは、指紋画像から抽出された特徴量から構成されるものであってもよい。プロセッサ31は、生成されたテンプレートはNVM34に格納する。

[0058] また、MPU36は、指紋センサ37からの指紋画像とテンプレートとの照合処理を行う。MPU36は、所定のアルゴリズムに従って、指紋センサ

37からの指紋画像とテンプレートとの類似度を算出する。MPU36は、算出された類似度に基づいて、指紋画像とテンプレートとの照合の成否を判定する。たとえば、MPU36は、算出された類似度が所定の閾値を超えていると照合に成功したと判定する。子ICカード30は、指紋画像のような生体情報の子ICカード30の外部に出力することではなく、生体認証を行うことができる。

[0059] MPU36は、照合の成否をプロセッサ31に送信する。

[0060] なお、プロセッサ31が、MPU36の機能を包含する形で実装することもできる。同様にMPU36がプロセッサ31の機能を包含する形で実装しても良い。

[0061] 次に、管理サーバ40について説明する。

図5は、実施形態に係る管理サーバ40の構成例を示す。図5は、管理サーバ40の構成例を示すブロック図である。図5が示すように、管理サーバ40は、プロセッサ41、ROM42、RAM43、NVM44、通信部45、操作部46及び表示部47などを備える。

[0062] プロセッサ41と、ROM42、RAM43、NVM44、通信部45、操作部46及び表示部47と、は、データバスなどを介して互いに接続する。

なお、管理サーバ40は、図5が示すような構成の他に必要に応じた構成を具備したり、管理サーバ40から特定の構成が除外されたりしてもよい。

[0063] プロセッサ41は、管理サーバ40全体の動作を制御する機能を有する。プロセッサ41は、内部キャッシュ及び各種のインターフェースなどを備えてもよい。プロセッサ41は、内部メモリ、ROM42又はNVM44が予め記憶するプログラムを実行することにより種々の処理を実現する。

[0064] なお、プロセッサ41がプログラムを実行することにより実現する各種の機能のうちの一部は、ハードウェア回路により実現されるものであってもよい。この場合、プロセッサ41は、ハードウェア回路により実行される機能を制御する。

- [0065] ROM 4 2 は、制御プログラム及び制御データなどが予め記憶された不揮発性のメモリである。ROM 4 2 に記憶される制御プログラム及び制御データは、管理サーバ 4 0 の仕様に応じて予め組み込まれる。
- [0066] RAM 4 3 は、揮発性のメモリである。RAM 4 3 は、プロセッサ 4 1 の処理中のデータなどを一時的に格納する。RAM 4 3 は、プロセッサ 4 1 からの命令に基づき種々のアプリケーションプログラムを格納する。また、RAM 4 3 は、アプリケーションプログラムの実行に必要なデータ及びアプリケーションプログラムの実行結果などを格納してもよい。
- [0067] NVM 4 4 は、データの書き込み及び書き換えが可能な不揮発性のメモリである。NVM 4 4 は、たとえば、HDD、SSD又はフラッシュメモリなどから構成される。NVM 4 4 は、管理サーバ 4 0 の運用用途に応じて制御プログラム、アプリケーション及び種々のデータなどを格納する。
- [0068] 通信部 4 5 は、ネットワーク 5 0 と通信するためのインターフェースである。即ち、通信部 4 5 は、ネットワーク 5 0 を通じて発行装置 1 0 とデータを送受信するためのインターフェースである。たとえば、通信部 4 5 は、有線又は無線のLAN接続をサポートするインターフェースである。
- [0069] 操作部 4 6 は、オペレータから種々の操作の入力を受け付ける。操作部 4 6 は、入力された操作を示す信号をプロセッサ 4 1 へ送信する。操作部 4 6 は、タッチパネルから構成されてもよい。
- [0070] 表示部 4 7 は、プロセッサ 4 1 からの画像データを表示する。たとえば、表示部 4 7 は、液晶モニタから構成される。操作部 4 6 がタッチパネルから構成される場合、表示部 4 7 は、操作部 4 6 と一体的に形成されてもよい。
- たとえば、管理サーバ 4 0 は、デスクトップPCなどである。
- [0071] 次に、子ICカード 3 0 が実現する機能について説明する。子ICカード 3 0 が実現する機能は、プロセッサ 3 1 がROM 3 2 又はNVM 3 4 などに格納されるプログラムを実行することで実現される。
- [0072] まず、プロセッサ 3 1 は、指紋画像による認証を行うためのテンプレートを登録する機能を有する。

[0073] プロセッサ 31 は、通信部 35 を通じて、テンプレートの登録を指示するコマンド（登録コマンド）を発行装置 10 から受信する。当該登録コマンドを受信すると、プロセッサ 31 は、指紋センサ 37 に指紋画像を取得させる。たとえば、プロセッサ 31 は、MPU 36 などを通じて、指紋センサ 37 を起動する。

[0074] ここで、ユーザは、指紋センサ 37 に所定の指を置くものとする。

指紋センサ 37 は、ユーザの所定の指から指紋画像を取得する。指紋センサ 37 は、取得した指紋画像を MPU 36 に送信する。

[0075] MPU 36 は、指紋センサ 37 から指紋画像を取得する。指紋画像を取得すると、MPU 36 は、取得された指紋画像に基づいてテンプレートを生成する。たとえば、MPU 36 は、所定のアルゴリズムに従って指紋画像から特徴量を抽出する。特徴量を抽出すると、MPU 36 は、抽出された特徴量から構成されるテンプレートを生成する。また、MPU 36 は、取得された指紋画像をテンプレートとしてもよい。

MPU 36 がテンプレートを生成すると、プロセッサ 31 は、生成されたテンプレートを NVM 34 に格納する。

[0076] なお、MPU 36 は、複数の指紋画像に基づいてテンプレートを生成してもよい。また、MPU 36 は、複数の指からの指紋画像に基づいてテンプレートを生成してもよい。MPU 36 がテンプレートを生成する方法は、特定の方法に限定されるものではない。

[0077] テンプレートを格納すると、プロセッサ 31 は、通信部 35 を通じて、登録が完了したことを示すレスポンス（登録完了レスポンス）を発行装置 10 に送信する。

[0078] また、プロセッサ 31 は、親 IC カード 20 が格納するデータ（第 1 のデータ）に関連するデータ（第 2 のデータ）を NVM 34 に格納する機能を有する。

[0079] ここでは、第 1 のデータは、第 1 の秘密鍵と第 1 の証明書情報、又は第 2 の秘密鍵と第 2 の証明書情報である。第 1 の証明書情報は、第 1 の秘密鍵の

ペアとなる第 1 の公開鍵から生成される。同様に第 2 の証明書情報は、第 2 の秘密鍵のペアとなる第 2 の公開鍵から生成される。

また、第 2 のデータについては、後に詳述する。

[0080] プロセッサ 31 は、通信部 35 を通じて、第 2 のデータを格納することを指示する格納コマンドを発行装置 10 から受信する。ここでは、格納コマンドは、第 2 のデータを含む。

[0081] 格納コマンドを受信すると、プロセッサ 31 は、格納コマンドに従って第 2 のデータを NVM 34 に格納する。第 2 のデータを格納すると、プロセッサ 31 は、通信部 35 を通じて、格納が完了したことを示すレスポンス（格納完了レスポンス）を発行装置 10 に送信する。

[0082] なお、プロセッサ 31 は、複数の格納コマンドを受信してもよい。各格納コマンドは、分割された第 2 のデータを含む。プロセッサ 31 は、各格納コマンドに従って、第 2 のデータを NVM 34 に格納する。

[0083] また、プロセッサ 31 は、第 2 のデータを上位装置に送信する機能を有する。

プロセッサ 31 は、上位装置からのコマンドに従って、テンプレートを用いてユーザを認証する。プロセッサ 31 は、指紋センサ 37 に指紋画像を取得させる。プロセッサ 31 は、MPU 36 に、取得された指紋画像とテンプレートとを照合させる。プロセッサ 31 は、MPU 36 から照合結果を取得する。プロセッサ 31 は、照合結果に基づいてユーザを認証する。プロセッサ 31 は、照合が成功した場合、ユーザの認証に成功したものと判定する。また、プロセッサ 31 は、照合が失敗した場合、ユーザの認証に失敗したものと判定する。

[0084] ユーザの認証に成功すると、プロセッサ 31 は、通信部 35 を通じて、上位装置からのコマンドに従って、第 2 のデータの少なくとも一部を上位装置に送信する。たとえば、プロセッサ 31 は、通信部 35 を通じて、第 1 の証明書情報又は第 2 の証明書情報を含むレスポンスを上位装置に送信する。また、プロセッサ 31 は、第 2 のデータの少なくとも一部、例えば、第 1 の秘

密鍵あるいは第2の秘密鍵を使って暗号化した乱数を上位装置に送信することもできる。

[0085] また、プロセッサ31は、テンプレートを削除する機能を有する。

プロセッサ31は、通信部35を通じて、テンプレートを削除することを指示する削除コマンドを発行装置10から受信する。

[0086] 削除コマンドを受信すると、プロセッサ31は、MPU36からテンプレートを削除する。テンプレートを削除すると、プロセッサ31は、通信部35を通じて、削除が完了したことを示すレスポンス（削除完了レスポンス）を発行装置10に送信する。

[0087] 次に、発行装置10が実現する機能について説明する。発行装置10が実現する機能は、プロセッサ11がROM12又はNVM14などに格納されるプログラムを実行することで実現される。

[0088] まず、プロセッサ11は、子ICカード30にテンプレートを登録させる機能を有する。

[0089] ここでは、プロセッサ11は、第1のリーダライタ18を通じて親ICカード20と接続しているものとする。また、プロセッサ11は、第2のリーダライタ19を通じて子ICカード30と接続しているものとする。

[0090] 親ICカード20との接続及び子ICカード30との接続を確認すると、プロセッサ11は、第2のリーダライタ19を通じて、登録コマンドを子ICカード30に送信する。

[0091] 子ICカード30が登録を完了すると、プロセッサ11は、第2のリーダライタ19を通じて、登録完了レスポンスを子ICカード30から受信する。

[0092] また、プロセッサ11は、親ICカード20の真正を判定する機能を有する。

ここでは、プロセッサ11は、親ICカード20を所持するユーザを認証する。

[0093] プロセッサ11は、操作部16を通じてパスワードの入力を受け付ける。

ここで、ユーザは、操作部にパスワードを入力するものとする。

[0094] パスワードの入力を受け付けると、プロセッサ 11 は、通信部 15 を通じて、ユーザを認証する認証リクエストを管理サーバ 40 に送信する。認証リクエストは、親 IC カード 20 の ID（たとえば、マイナンバー）及び入力されたパスワードを含む。

[0095] プロセッサ 11 は、通信部 15 を通じて、認証結果を示すレスポンスを管理サーバ 40 から受信する。プロセッサ 11 は、レスポンスが認証に成功したことを示す場合、親 IC カード 20 が真正であると判定する。また、プロセッサ 11 は、レスポンスが認証に失敗したことを示す場合、親 IC カード 20 が真正でないと判定する。

[0096] また、プロセッサ 11 は、第 2 のデータを子 IC カード 30 に格納する機能を有する。親 IC カード 20 が真正であると判定すると、プロセッサ 11 は、通信部 15 を通じて、第 2 のデータを要求するリクエスト（データリクエスト）を管理サーバ 40 に送信する。

[0097] データリクエストを送信すると、プロセッサ 11 は、通信部 15 を通じて、第 2 のデータを含むレスポンス（データレスポンス）を管理サーバ 40 から受信する。データレスポンスを受信すると、プロセッサ 11 は、第 2 のリーダーライタ 19 を通じて、データレスポンスが含む第 2 のデータの格納を指示する格納コマンドを子 IC カード 30 に送信する。

[0098] また、プロセッサ 11 は、親 IC カード 20 が真正であると判定すると、親 IC カード 20 から第 2 のデータを取得し、子 IC カード 30 に格納を指示する格納コマンドを子 IC カード 30 に送信してもよい。

[0099] 子 IC カード 30 が格納を完了すると、プロセッサ 11 は、第 2 のリーダーライタ 19 を通じて、格納完了レスポンスを子 IC カード 30 から受信する。

[0100] また、プロセッサ 11 は、子 IC カード 30 からテンプレートを削除する機能を有する。

親 IC カード 20 が真正でないと判定すると、プロセッサ 11 は、第 2 の

リーダーライタ 19 を通じて、削除コマンドを子 I C カード 30 に送信する。

[0101] 子 I C カード 30 が削除を完了すると、プロセッサ 11 は、第 2 のリーダーライタ 19 を通じて、削除完了レスポンスを子 I C カード 30 から受信する。

[0102] 次に、管理サーバ 40 が実現する機能について説明する。管理サーバ 40 が実現する機能は、プロセッサ 41 が R O M 42 又は N V M 44 などに格納されるプログラムを実行することで実現される。

[0103] まず、プロセッサ 41 は、親 I C カード 20 のユーザを認証する機能を有する。

[0104] ここでは、N V M 44 は、親 I C カード 20 の I D とパスワードとを対応付けて予め格納しているものとする。

[0105] プロセッサ 41 は、通信部 45 を通じて、発行装置 10 から認証リクエストを受信する。認証リクエストを受信すると、プロセッサ 41 は、N V M 44 を参照して、認証リクエストが格納するパスワードと予め格納されているパスワードとを照合する。

[0106] 両者が一致すると、プロセッサ 41 は、通信部 45 を通じて、認証に成功したことを示すレスポンスを発行装置 10 に送信する。

両者が一致しないと、プロセッサ 41 は、通信部 45 を通じて、認証に失敗したことを示すレスポンスを発行装置 10 に送信する。

[0107] また、プロセッサ 41 は、第 2 のデータを発行装置 10 に送信する機能を有する。

プロセッサ 41 は、通信部 45 を通じて、データリクエストを発行装置 10 から受信する。データリクエストを受信すると、プロセッサ 41 は、第 2 のデータを取得する。

[0108] 前述の通り、第 2 のデータは、第 1 のデータに関連する。即ち、第 2 のデータは、第 1 の秘密鍵、第 2 の秘密鍵、第 1 の証明書情報及び第 2 の証明書情報に関連する。また、N V M 44 は、第 1 のデータを予め格納しているものとする。

- [0109] ここでは、第2のデータは、第1のデータと同様に、第1の秘密鍵、第2の秘密鍵、第1の証明書情報及び第2の証明書情報から構成される。
- [0110] 第2のデータを取得すると、プロセッサ41は、通信部45を通じて、第2のデータを含むデータレスポンスを発行装置10に送信する。
- [0111] 次に、発行システム1の動作例について説明する。
- 図6は、発行システム1の動作例について説明するためのシーケンス図である。
- [0112] ここでは、親ICカード20は、第1のリーダライタ18にセットされているものとする。また、子ICカード30は、第2のリーダライタ19にセットされているものとする。
- [0113] まず、発行装置10のプロセッサ11は、第1のリーダライタ18を通じて、親ICカード20との通信を確立する(S11)。親ICカード20との通信を確立すると、プロセッサ11は、第2のリーダライタ19を通じて、子ICカード30との通信を確立する(S12)。
- [0114] 親ICカード20及び子ICカード30との通信を確認すると(S13)、プロセッサ11は、第2のリーダライタ19を通じて登録コマンドを子ICカード30に送信する(S14)。
- [0115] 子ICカード30のプロセッサ31は、通信部35を通じて登録コマンドを受信する。登録コマンドを受信すると、プロセッサ31は、指紋のテンプレートを登録する(S15)。指紋のテンプレートを登録すると、プロセッサ31は、通信部35を通じて、登録完了レスポンスを発行装置10に送信する(S16)。
- [0116] 発行装置10のプロセッサ11は、第2のリーダライタ19を通じて登録完了レスポンスを子ICカード30から受信する。登録完了レスポンスを受信すると、プロセッサ11は、親ICカード20の真正を判定する(S17)。親ICカード20の真正方法としては、例えば、親ICカード20に格納された第1の秘密鍵を使って暗号化された乱数と暗号化前の乱数を管理サーバに送信し、管理サーバにて第1の秘密鍵に対応する第1の公開鍵で暗号

化された乱数を復号した結果が、送られた乱数と一致することを確認することにより、正しい秘密鍵が格納されていること、すなわち、真正の親ＩＣカード２０であると判定する。ここでは、プロセッサ１１は、親ＩＣカード２０が真正であると判定したものとする。

[0117] 親ＩＣカード２０が真正であると判定すると、プロセッサ１１は、通信部１５を通じてデータリクエストを管理サーバ４０に送信する（Ｓ１８）。

[0118] 管理サーバ４０のプロセッサ４１は、通信部４５を通じてデータリクエストを受信する。データリクエストを受信すると、プロセッサ４１は、第２のデータとして第１の秘密鍵、第２の秘密鍵、第１の証明書情報及び第２の証明書情報を含むデータレスポンスを発行装置１０に送信する（Ｓ１９）。

[0119] 発行装置１０のプロセッサ１１は、通信部１５を通じてデータレスポンスを受信する。データレスポンスを受信すると、プロセッサ１１は、第２のリーダーライタ１９を通じて、第２のデータとして第１の秘密鍵、第２の秘密鍵、第１の証明書情報及び第２の証明書情報を格納することを指示する格納コマンドを子ＩＣカード３０に送信する（Ｓ２０）。

[0120] 子ＩＣカード３０のプロセッサ３１は、通信部３５を通じて格納コマンドを発行装置１０から受信する。格納コマンドを受信すると、プロセッサ３１は、格納コマンドに従ってＮＶＭ３４に第２のデータを格納する（Ｓ２１）。

[0121] 第２のデータを格納すると、プロセッサ３１は、通信部３５を通じて格納完了レスポンスを発行装置１０に送信する（Ｓ２２）。

[0122] 発行装置１０のプロセッサ１１は、第２のリーダーライタ１９を通じて格納完了レスポンスを受信する。プロセッサ１１が格納完了レスポンスを受信すると、発行システム１は、動作を終了する。

[0123] 次に、親ＩＣカード２０が真正でない場合における発行システム１の動作例について説明する。

図７は、親ＩＣカード２０が真正でない場合における発行システム１の動作例について説明するためのシーケンス図である。

- [0124] S 1 1 乃至 S 1 7 については、前述の通りであるため説明を省略する。
- [0125] ここでは、発行装置 1 0 のプロセッサ 1 1 は、親 I C カード 2 0 が真正でないと判定したものとする。
- [0126] 親 I C カード 2 0 が真正でないと判定すると、プロセッサ 1 1 は、第 2 のリーダライタ 1 9 を通じて、削除コマンドを子 I C カード 3 0 に送信する（S 2 3）。
- [0127] 子 I C カード 3 0 のプロセッサ 3 1 は、通信部 3 5 を通じて削除コマンドを発行装置 1 0 から受信する。削除コマンドを受信すると、プロセッサ 3 1 は、削除コマンドに従ってテンプレートを削除する（S 2 4）。
- [0128] テンプレートを削除すると、プロセッサ 3 1 は、通信部 3 5 を通じて削除完了レスポンスを発行装置 1 0 に送信する（S 2 5）。
- [0129] 発行装置 1 0 のプロセッサ 1 1 は、第 2 のリーダライタ 1 9 を通じて削除完了レスポンスを受信する。プロセッサ 1 1 が削除完了レスポンスを受信すると、発行システム 1 は、動作を終了する。
- [0130] なお、発行装置 1 0 のプロセッサ 1 1 は、親 I C カード 2 0 が真正でない場合以外であっても、子 I C カード 3 0 の発行に失敗した場合、削除コマンドを子 I C カード 3 0 に送信してもよい。たとえば、プロセッサ 1 1 は、子 I C カード 3 0 に第 2 のデータを格納することに失敗した場合、削除コマンドを子 I C カード 3 0 に送信してもよい。また、プロセッサ 1 1 は、管理サーバ 4 0 から第 2 のデータの取得に失敗した場合、削除コマンドを子 I C カード 3 0 に送信してもよい。
- [0131] また、発行システム 1 は、親 I C カード 2 0 に紐付く携帯可能電子装置を発行するものであってもよい。たとえば、携帯可能電子装置は、U S B 接続などをサポートするデバイスなどであってもよい。
- [0132] 以上のように構成された発行システムは、子 I C カードに生体情報に基づくテンプレートを登録する。発行システムは、親 I C カードが格納するデータに関連するデータを子 I C カードに格納する。その結果、発行システムは、親 I C カードに格納されている生体情報のテンプレートを用いることなく

子 I C カードを発行することができる。

(第 2 の実施形態)

次に、第 2 の実施形態について説明する。

第 2 の実施形態に係る発行システム 1 は、第 2 のデータとして子 I D など
を子 I C カード 3 0 に格納する点で第 1 の実施形態に係るそれと異なる。従
って、その他の点については、同一の符号を付して詳細な説明を省略する。

[0133] 発行システム 1 の構成は、第 1 の実施形態に係るそれと同様であるため説
明を省略する。

[0134] 次に、管理サーバ 4 0 が実現する機能について説明する。管理サーバ 4 0
が実現する機能は、プロセッサ 4 1 が R O M 4 2 又は N V M 4 4 などに格納
されるプログラムを実行することで実現される。

[0135] プロセッサ 4 1 は、第 2 のデータとして子 I D などを発行装置 1 0 に送信
する機能を有する。

プロセッサ 4 1 は、第 1 のデータに関連する子 I D を発行する。たとえば
、プロセッサ 4 1 は、第 1 の証明書情報又は第 2 の証明書情報に基づいて子
I D を発行する。たとえば、子 I D は、マイキー I D である。

[0136] また、プロセッサ 4 1 は、子 I D に対応するパスワードを発行する。たと
えば、パスワードは、子 I D が用いられる際にユーザを認証するために用い
られる。

[0137] プロセッサ 4 1 は、通信部 4 5 を通じてデータリクエストを発行装置 1 0
から受信する。データリクエストを受信すると、プロセッサ 4 1 は、第 2 の
データとして、子 I D 、パスワード、第 1 の証明書情報及び第 2 の証明書情
報を含むデータレスポンスを発行装置 1 0 に送信する。

[0138] 次に、発行システム 1 の動作例について説明する。

図 8 は、発行システム 1 の動作例について説明するためのシーケンス図で
ある。

[0139] ここでは、親 I C カード 2 0 は、真正であるものとする。

S 1 1 乃至 S 1 8 については、前述の通りであるため説明を省略する。

[0140] 管理サーバ40のプロセッサ41は、通信部45を通じてデータリクエストを受信する。データリクエストを受信すると、プロセッサ41は、第2のデータとして、子ID、パスワード、第1の秘密鍵、第2の秘密鍵、第1の証明書情報及び第2の証明書情報を含むデータレスポンスを発行装置10に送信する(S31)。

[0141] 発行装置10のプロセッサ11は、通信部15を通じてデータレスポンスを受信する。データレスポンスを受信すると、プロセッサ11は、第2のリーダーライタ19を通じて、第2のデータとして、子ID、パスワード、第1の秘密鍵、第2の秘密鍵、第1の証明書情報及び第2の証明書情報を格納することを指示する格納コマンドを子ICカード30に送信する(S32)。

[0142] 子ICカード30のプロセッサ31は、通信部35を通じて格納コマンドを発行装置10から受信する。格納コマンドを受信すると、プロセッサ31は、格納コマンドに従ってNVM34に第2のデータを格納する(S33)。

[0143] 第2のデータを格納すると、プロセッサ31は、通信部35を通じて格納完了レスポンスを発行装置10に送信する(S34)。

[0144] 発行装置10のプロセッサ11は、第2のリーダーライタ19を通じて格納完了レスポンスを受信する。プロセッサ11が格納完了レスポンスを受信すると、発行システム1は、動作を終了する。

[0145] なお、別の発行方法として、発行装置10が、親ICカード20から取得した第1のデータから第2のデータを生成し、子ICカード30に第2のデータを格納する方法をとることもできる。

[0146] 以上のように構成された発行システムは、子ICカードに子IDを格納することができる。その結果、子ICカードは、親ICカードと異なるIDによって利用されることができる。

(第3の実施形態)

次に、第3の実施形態について説明する。

第3の実施形態に係る発行システム1は、第2のデータとしてセキュリテ

ィレベルが低い証明書情報を子ICカード30に格納する点で第1の実施形態に係るそれと異なる。従って、その他の点については、同一の符号を付して詳細な説明を省略する。

[0147] 発行システム1の構成は、第1の実施形態に係るそれと同様であるため説明を省略する。

[0148] 次に、管理サーバ40が実現する機能について説明する。管理サーバ40が実現する機能は、プロセッサ41がROM42又はNVM44などに格納されるプログラムを実行することで実現される。

[0149] プロセッサ11は、第2のデータとしてセキュリティレベルが低い証明書情報と当該証明書情報に対応する秘密鍵とを発行装置10に送信する機能を有する。

発行装置10からデータリクエストを受信すると、プロセッサ11は、第1の証明書情報と第2の証明書情報とからセキュリティレベルが低い証明書情報を選択する。前述の通り、第2の証明書情報のセキュリティレベルは、第1の証明書情報のそれよりも低い。

[0150] 従って、プロセッサ11は、セキュリティレベルが低い証明書情報として第2の証明書情報を選択する。

[0151] セキュリティレベルが低い証明書情報を選択すると、プロセッサ11は、通信部15を通じて、選択された証明書情報と選択された証明書情報に対応する秘密鍵（ここでは、第2の秘密鍵）を含むデータレスポンスを発行装置10に送信する。

[0152] 次に、発行システム1の動作例について説明する。

図9は、発行システム1の動作例について説明するためのシーケンス図である。

[0153] ここでは、親ICカード20は、真正であるものとする。

S11乃至S18については、前述の通りであるため説明を省略する。

[0154] 管理サーバ40のプロセッサ41は、通信部45を通じてデータリクエストを受信する。データリクエストを受信すると、プロセッサ41は、第2の

データとして、セキュリティレベルが低い証明書情報（ここでは、第2の証明書情報）及び当該証明書情報に対応する秘密鍵（ここでは、第2の秘密鍵）を含むデータレスポンスを発行装置10に送信する（S41）。

[0155] 発行装置10のプロセッサ11は、通信部15を通じてデータレスポンスを受信する。データレスポンスを受信すると、プロセッサ11は、第2のリーダーライタ19を通じて、第2のデータとして、セキュリティレベルが低い証明書情報及び第2の秘密鍵を格納することを指示する格納コマンドを子ICカード30に送信する（S42）。

[0156] 子ICカード30のプロセッサ31は、通信部35を通じて格納コマンドを発行装置10から受信する。格納コマンドを受信すると、プロセッサ31は、格納コマンドに従ってNVM34に第2のデータを格納する（S43）。

[0157] 第2のデータを格納すると、プロセッサ31は、通信部35を通じて格納完了レスポンスを発行装置10に送信する（S44）。

[0158] 発行装置10のプロセッサ11は、第2のリーダーライタ19を通じて格納完了レスポンスを受信する。プロセッサ11が格納完了レスポンスを受信すると、発行システム1は、動作を終了する。

[0159] なお、別の発行方法として、発行装置10が、親ICカード20から取得したセキュリティレベルの低い秘密鍵及び証明書情報を、子ICカード30に格納する方法をとることもできる。

[0160] 以上のように構成された発行システムは、セキュリティレベルが低い証明書情報を子ICカードに格納する。その結果、発行システムは、親ICカードより機能を限定してより安全に子ICカードを発行することができる。

（第4の実施形態）

次に、第4の実施形態について説明する。

第4の実施形態に係る発行システム1は、第2のデータとして第1の証明書情報及び第2の証明書情報に基づく第3の証明書情報などを子ICカード30に格納する点で第1の実施形態に係るそれと異なる。従って、その他の

点については、同一の符号を付して詳細な説明を省略する。

[0161] 発行システム 1 の構成は、第 1 の実施形態に係るそれと同様であるため説明を省略する。

[0162] 次に、管理サーバ 40 が実現する機能について説明する。管理サーバ 40 が実現する機能は、プロセッサ 41 が ROM 42 又は NVM 44 などに格納されるプログラムを実行することで実現される。

[0163] プロセッサ 11 は、第 2 のデータとして第 1 の証明書情報、第 2 の証明書情報及び第 3 の証明書情報を発行装置 10 に送信する機能を有する。

発行装置 10 からデータリクエストを受信すると、プロセッサ 11 は、第 1 の証明書情報及び第 2 の証明書情報に基づいて第 3 の証明書情報を生成する。

[0164] 図 10 は、第 3 の証明書情報の構成例を示す。

図 10 が示すように、第 3 の証明書情報は、第 1 のハッシュ値、第 2 のハッシュ値、第 3 の公開鍵及び第 3 の電子署名などから構成される。

[0165] なお、第 3 の証明書情報は、図 10 が示すような構成の他に必要に応じた構成を具備したり、第 3 の証明書情報から特定の構成が除外されたりしてもよい。

[0166] 第 1 のハッシュ値は、第 1 の証明書情報から所定のハッシュ関数によって算出されるハッシュ値である。

[0167] 第 2 のハッシュ値は、第 2 の証明書情報から所定のハッシュ関数によって算出されるハッシュ値である。

[0168] 第 3 の公開鍵は、第 1 の公開鍵及び第 2 の公開鍵と異なる公開鍵である。たとえば、管理サーバ 40 のプロセッサ 41 は、所定のアルゴリズムに従って第 3 の公開鍵を生成する。また、第 3 の公開鍵に対応する第 3 の秘密鍵は、NVM 44 などに格納されてもよい。

[0169] 第 3 の電子署名は、第 3 の公開鍵によって生成される電子署名である。たとえば、プロセッサ 41 は、第 1 のハッシュ値及び第 2 のハッシュ値を第 3 の公開鍵で暗号化して第 3 の電子署名を生成する。

なお、第3の証明書情報は、特定の構成に限定されるものではない。

[0170] 第3の証明書情報を生成すると、プロセッサ11は、通信部15を通じて、第2のデータとして第1の秘密鍵と第1の証明書情報と第2の秘密鍵と第2の証明書情報と第3の秘密鍵と第3の証明書情報とを含むデータレスポンスを発行装置10に送信する。

[0171] 次に、発行システム1の動作例について説明する。

図11は、発行システム1の動作例について説明するためのシーケンス図である。

[0172] ここでは、親ICカード20は、真正であるものとする。

S11乃至S18については、前述の通りであるため説明を省略する。

[0173] 管理サーバ40のプロセッサ41は、通信部45を通じてデータリクエストを受信する。データリクエストを受信すると、プロセッサ41は、第3の秘密鍵と第3の証明書情報を生成する(S51)。

[0174] 第3の秘密鍵と第3の証明書情報を生成すると、プロセッサ41は、第2のデータとして、第1の秘密鍵と第1の証明書情報と第2の秘密鍵と第2の証明書情報と第3の秘密鍵と第3の証明書情報とを含むデータレスポンスを発行装置10に送信する(S52)。

[0175] 発行装置10のプロセッサ11は、通信部15を通じてデータレスポンスを受信する。データレスポンスを受信すると、プロセッサ11は、第2のリーダーライタ19を通じて、第2のデータとして、第1の秘密鍵と第1の証明書情報と第2の秘密鍵と第2の証明書情報と第3の秘密鍵と第3の証明書情報とを格納することを指示する格納コマンドを子ICカード30に送信する(S53)。

[0176] 子ICカード30のプロセッサ31は、通信部35を通じて格納コマンドを発行装置10から受信する。格納コマンドを受信すると、プロセッサ31は、格納コマンドに従ってNVM34に第2のデータを格納する(S54)。

[0177] 第2のデータを格納すると、プロセッサ31は、通信部35を通じて格納

完了レスポンスを発行装置 10 に送信する (S 55)。

[0178] 発行装置 10 のプロセッサ 11 は、第 2 のリーダライタ 19 を通じて格納完了レスポンスを受信する。プロセッサ 11 が格納完了レスポンスを受信すると、発行システム 1 は、動作を終了する。

[0179] 子 IC カード 30 が第 3 の証明書情報を格納することで以下のような利点が生じる。

子 IC カード 30 を用いて所定の処理を行う際に管理サーバ 40 のプロセッサ 41 は、リーダライタを用いて第 1 の証明書情報、第 2 の証明書情報及び第 3 の証明書情報を取得する。

[0180] プロセッサ 41 は、取得された第 1 の証明書情報及び第 2 の証明書情報からそれぞれハッシュ値を算出する。ハッシュ値を算出すると、プロセッサ 41 は、算出されたハッシュ値を、第 3 の証明書情報が格納する第 1 のハッシュ値及び第 2 のハッシュ値とそれぞれ一致することを確認する。

[0181] また、プロセッサ 41 は、第 3 の秘密鍵を用いて第 3 の電子署名を検証し、第 3 の証明書情報が格納する第 1 のハッシュ値及び第 2 のハッシュ値が改ざんされていないことを検証する。

[0182] プロセッサ 41 は、上記の処理によって、第 1 の証明書情報及び第 2 の証明書情報が改ざんされていないことを検証することができる。

[0183] 以上のように構成された発行システムは、第 3 の証明書情報を子 IC カードに格納する。その結果、発行システムは、子 IC カードが格納する第 1 の証明書情報及び第 2 の証明書情報を検証可能なものにすることができる。

(第 5 の実施形態)

次に、第 5 の実施形態について説明する。

第 5 の実施形態に係る発行システム 1 は、第 2 のデータとして第 1 の秘密鍵及び第 1 の証明書情報と第 2 の秘密鍵及び第 2 の証明書情報とに対応する第 4 の秘密鍵及び第 4 の証明書情報などを子 IC カード 30 に格納する点で第 1 の実施形態に係るそれと異なる。従って、その他の点については、同一の符号を付して詳細な説明を省略する。

[0184] 発行システム 1 の構成は、第 1 の実施形態に係るそれと同様であるため説明を省略する。

[0185] 次に、管理サーバ 40 が実現する機能について説明する。管理サーバ 40 が実現する機能は、プロセッサ 41 が ROM 42 又は NVM 44 などに格納されるプログラムを実行することで実現される。

[0186] プロセッサ 11 は、第 2 のデータとして第 1 の秘密鍵及び第 1 の証明書情報と第 2 の秘密鍵及び第 2 の証明書情報とに対応する第 4 の秘密鍵及び第 4 の証明書情報などを発行装置 10 に送信する機能を有する。

発行装置 10 からデータリクエストを受信すると、プロセッサ 11 は、所定のアルゴリズムに従って第 4 の公開鍵及び第 4 の秘密鍵を生成する。第 4 の公開鍵及び第 4 の秘密鍵を生成すると、プロセッサ 11 は、第 4 の秘密鍵を第 1 の秘密鍵及び第 2 の秘密鍵と対応付けて NVM 44 に格納する。

[0187] 第 4 の秘密鍵を格納すると、プロセッサ 11 は、第 4 の公開鍵から構成される第 4 の証明書情報を生成する。第 4 の証明書情報を生成すると、プロセッサ 11 は、子 ID 及びパスワードを生成する。子 ID 及びパスワードは、前述の通りである。

[0188] 子 ID 及びパスワードを生成すると、プロセッサ 11 は、通信部 15 を通じて、第 2 のデータとして第 4 の秘密鍵、第 4 の証明書情報、子 ID 及びパスワードを含むデータレスポンスを発行装置 10 に送信する。

[0189] 次に、発行システム 1 の動作例について説明する。

図 11 は、発行システム 1 の動作例について説明するためのシーケンス図である。

[0190] ここでは、親 IC カード 20 は、真正であるものとする。

S11 乃至 S18 については、前述の通りであるため説明を省略する。

[0191] 管理サーバ 40 のプロセッサ 41 は、通信部 45 を通じてデータリクエストを受信する。データリクエストを受信すると、プロセッサ 41 は、第 4 の公開鍵及び第 4 の秘密鍵を生成する (S61)。

[0192] 第 4 の公開鍵及び第 4 の秘密鍵を生成すると、プロセッサ 41 は、第 4 の

秘密鍵を第1の秘密鍵及び第2の秘密鍵と対応付けてNVM44に格納する(S62)。第4の秘密鍵を格納すると、プロセッサ41は、第2のデータとして、第4の秘密鍵、第4の証明書情報、子ID及びパスワードを含むデータレスポンスを発行装置10に送信する(S63)。

[0193] 発行装置10のプロセッサ11は、通信部15を通じてデータレスポンスを受信する。データレスポンスを受信すると、プロセッサ11は、第2のリーダーライタ19を通じて、第2のデータとして、第4の秘密鍵、第4の証明書情報、子ID及びパスワードを格納することを指示する格納コマンドを子ICカード30に送信する(S64)。

[0194] 子ICカード30のプロセッサ31は、通信部35を通じて格納コマンドを発行装置10から受信する。格納コマンドを受信すると、プロセッサ31は、格納コマンドに従ってNVM34に第2のデータを格納する(S65)。

[0195] 第2のデータを格納すると、プロセッサ31は、通信部35を通じて格納完了レスポンスを発行装置10に送信する(S66)。

[0196] 発行装置10のプロセッサ11は、第2のリーダーライタ19を通じて格納完了レスポンスを受信する。プロセッサ11が格納完了レスポンスを受信すると、発行システム1は、動作を終了する。

[0197] なお、発行システム1は、第1の秘密鍵及び第1の証明書情報に対応する第4aの秘密鍵及び第4aの証明書情報と、第2の秘密鍵及び第2の証明書情報に対応する第4bの秘密鍵及び第4bの証明書情報とを生成し、第4aの秘密鍵、第4aの証明書情報、第4bの秘密鍵及び第4bの証明書情報を第2のデータとして子ICカード30に格納することもできる。以下では、第4aの秘密鍵と第4bの秘密鍵のように複数の秘密鍵の場合であっても第4の秘密鍵と簡略化して表記し、第4aの証明書情報と第4bの証明書情報のように複数の証明書情報の場合であっても第4の証明書情報と簡略化して表記する。

[0198] 以上のように構成された発行システムは、親ICカードが格納する証明書情報に対応付けられた第4の秘密鍵と第4の証明書情報とを子ICカードに

格納する。その結果、子ＩＣカードが格納する第４の秘密鍵、あるいは、第４の証明書情報が流出した場合であっても、親ＩＣカードが格納する証明書情報は、影響を受けない。そのため、子ＩＣカードが発行されても、親ＩＣカードのセキュリティは、低下しにくい。

(第６の実施形態)

次に、第６の実施形態について説明する。

第６の実施形態に係る発行システムは、鍵サーバが第４の秘密鍵及び第４の証明書情報を発行する点で第５の実施形態に係るそれと異なる。従って、その他の点については、同一の符号を付して詳細な説明を省略する。

[0199] 図１３は、第６の実施形態に係る発行システム１’の構成例を示す。図１３が示すように、発行システム１’は、発行装置１０、親ＩＣカード２０、子ＩＣカード３０、管理サーバ４０及び鍵サーバ６０などを備える。鍵サーバ６０は、ネットワーク５０を介して発行装置１０に接続する。

[0200] なお、発行システム１’は、図１３が示すような構成の他に必要に応じた構成をさらに具備したり、発行システム１’から特定の構成が除外されたりしてもよい。

[0201] 発行装置１０、親ＩＣカード２０、子ＩＣカード３０及び管理サーバ４０は、第１の実施形態に係るそれらと同様であるため説明を省略する。

[0202] 鍵サーバ６０（外部装置）は、第１の秘密鍵及び第１の証明書情報と第２の秘密鍵及び第２の証明書情報とに対応する第４の秘密鍵及び第４の証明書情報を発行する。

[0203] 図１６は、鍵サーバ６０の構成例を示す。図１６は、鍵サーバ６０の構成例を示すブロック図である。図１６が示すように、鍵サーバ６０は、プロセッサ６１、ＲＯＭ６２、ＲＡＭ６３、ＮＶＭ６４、通信部６５、操作部６６及び表示部６７などを備える。

[0204] プロセッサ６１と、ＲＯＭ６２、ＲＡＭ６３、ＮＶＭ６４、通信部６５、操作部６６及び表示部６７と、は、データバスなどを介して互いに接続する。

なお、鍵サーバ60は、図16が示すような構成の他に必要に応じた構成を具備したり、鍵サーバ60から特定の構成が除外されたりしてもよい。

[0205] プロセッサ61は、鍵サーバ60全体の動作を制御する機能を有する。プロセッサ61は、内部キャッシュ及び各種のインターフェースなどを備えてもよい。プロセッサ61は、内部メモリ、ROM62又はNVM64が予め記憶するプログラムを実行することにより種々の処理を実現する。

[0206] なお、プロセッサ61がプログラムを実行することにより実現する各種の機能のうちの一部は、ハードウェア回路により実現されるものであってもよい。この場合、プロセッサ61は、ハードウェア回路により実行される機能を制御する。

[0207] ROM62は、制御プログラム及び制御データなどが予め記憶された不揮発性のメモリである。ROM62に記憶される制御プログラム及び制御データは、鍵サーバ60の仕様に依拠して予め組み込まれる。

[0208] RAM63は、揮発性のメモリである。RAM63は、プロセッサ61の処理中のデータなどを一時的に格納する。RAM63は、プロセッサ61からの命令に基づき種々のアプリケーションプログラムを格納する。また、RAM63は、アプリケーションプログラムの実行に必要なデータ及びアプリケーションプログラムの実行結果などを格納してもよい。

[0209] NVM64は、データの書き込み及び書き換えが可能な不揮発性のメモリである。NVM64は、たとえば、HDD、SSD又はフラッシュメモリなどから構成される。NVM64は、鍵サーバ60の運用用途に依拠して制御プログラム、アプリケーション及び種々のデータなどを格納する。

[0210] 通信部65は、ネットワーク50と通信するためのインターフェースである。即ち、通信部65は、ネットワーク50を通じて発行装置10などに接続するためのインターフェースである。たとえば、通信部65は、有線又は無線のLAN接続をサポートするインターフェースである。

[0211] 操作部66は、オペレータから種々の操作の入力を受け付ける。操作部66は、入力された操作を示す信号をプロセッサ61へ送信する。操作部66

は、タッチパネルから構成されてもよい。

[0212] 表示部 67 は、プロセッサ 61 からの画像データを表示する。たとえば、表示部 67 は、液晶モニタから構成される。操作部 66 がタッチパネルから構成される場合、表示部 67 は、操作部 66 と一体的に形成されてもよい。

たとえば、鍵サーバ 60 は、デスクトップ PC などである。

[0213] 次に、発行装置 10 が実現する機能について説明する。発行装置 10 が実現する機能は、プロセッサ 11 が ROM 12 又は NVM 14 などに格納されるプログラムを実行することで実現される。

[0214] まず、プロセッサ 11 は、子 ID 及びパスワードを管理サーバ 40 から取得する機能を有する。

[0215] 親 IC カード 20 が真正であると判定すると、プロセッサ 11 は、通信部 15 を通じて、子 ID 及びパスワードを要求するリクエスト（ID リクエスト）を管理サーバ 40 に送信する。

子 ID 及びパスワードは、前述の通りである。

[0216] ID リクエストを送信すると、プロセッサ 11 は、通信部 15 を通じて、子 ID 及びパスワードを含むレスポンス（ID レスポンス）を管理サーバ 40 から受信する。

[0217] また、プロセッサ 11 は、第 4 の秘密鍵及び第 4 の証明書情報を鍵サーバ 60 から取得する機能を有する。

[0218] プロセッサ 11 は、通信部 15 を通じて、第 4 の秘密鍵及び第 4 の証明書情報を要求するリクエスト（鍵リクエスト）を管理サーバ 40 に送信する。ここでは、鍵リクエストは、子 ID 及びパスワードを含む。

[0219] 鍵リクエストを送信すると、プロセッサ 11 は、通信部 15 を通じて、第 4 の秘密鍵及び第 4 の証明書情報を含むレスポンス（鍵レスポンス）を管理サーバ 40 から受信する。

[0220] また、プロセッサ 11 は、第 2 のデータとして第 4 の秘密鍵及び第 4 の証明書情報、子 ID 及びパスワードを子 IC カード 30 に格納する機能を有する。

- [0221] プロセッサ 11 は、第 2 のリーダライタ 19 を通じて、第 4 の秘密鍵及び第 4 の証明書情報、子 ID 及びパスワードの格納を指示する格納コマンドを子 IC カード 30 に送信する。
- [0222] 子 IC カード 30 が格納を完了すると、プロセッサ 11 は、第 2 のリーダライタ 19 を通じて、格納完了レスポンスを子 IC カード 30 から受信する。
- [0223] 次に、管理サーバ 40 が実現する機能について説明する。管理サーバ 40 が実現する機能は、プロセッサ 41 が ROM 42 又は NVM 44 などに格納されるプログラムを実行することで実現される。
- [0224] プロセッサ 41 は、子 ID 及びパスワードを発行装置 10 に送信する機能を有する。
- プロセッサ 41 は、子 ID 及びパスワードを発行する。
- プロセッサ 41 は、通信部 45 を通じて ID リクエストを発行装置 10 から受信する。ID リクエストを受信すると、プロセッサ 41 は、子 ID 及びパスワードを含む ID レスポンスを発行装置 10 に送信する。
- [0225] 次に、鍵サーバ 60 が実現する機能について説明する。鍵サーバ 60 が実現する機能は、プロセッサ 61 が ROM 62 又は NVM 64 などに格納されるプログラムを実行することで実現される。
- [0226] プロセッサ 61 は、第 1 の秘密鍵及び第 1 の証明書情報と第 2 の秘密鍵及び第 2 の証明書情報とに対応する第 4 の秘密鍵及び第 4 の証明書情報などを発行装置 10 に送信する機能を有する。
- プロセッサ 61 は、通信部 65 を通じて、鍵リクエストを発行装置 10 から受信する。鍵リクエストを受信すると、プロセッサ 61 は、所定のアルゴリズムに従って第 4 の公開鍵及び第 4 の秘密鍵を生成する。
- [0227] 第 4 の公開鍵及び第 4 の秘密鍵を生成すると、プロセッサ 61 は、第 4 の公開鍵から構成される第 4 の証明書情報を生成する。第 4 の証明書情報を生成すると、プロセッサ 61 は、通信部 65 を通じて、第 4 の秘密鍵及び第 4 の証明書情報を含む鍵レスポンスを発行装置 10 に送信する。

- [0228] 鍵レスポンスを送信すると、プロセッサ61は、第4の秘密鍵及び第4の証明書情報を鍵リクエストが含む子ID及びパスワードと対応付けてNVM64に格納する。
- [0229] 次に、発行システム1'の動作例について説明する。
- 図15は、発行システム1'の動作例について説明するためのシーケンス図である。
- [0230] ここでは、親ICカード20は、真正であるものとする。
- S11乃至S17については、前述の通りであるため説明を省略する。
- [0231] 親ICカード20が真正であると判定すると、プロセッサ11は、通信部15を通じてIDリクエストを管理サーバ40に送信する(S71)。
- [0232] 管理サーバ40のプロセッサ41は、通信部45を通じてIDリクエストを受信する。データリクエストを受信すると、プロセッサ41は、子ID及びパスワードを含むIDレスポンスを発行装置10に送信する(S72)。
- [0233] 発行装置10のプロセッサ11は、通信部15を通じてIDレスポンスを受信する。IDレスポンスを受信すると、プロセッサ11は、通信部15を通じて鍵リクエストを鍵サーバ60に送信する(S73)。
- [0234] 鍵サーバ60のプロセッサ61は、通信部65を通じて鍵リクエストを受信する。鍵リクエストを受信すると、プロセッサ61は、第4の公開鍵及び第4の秘密鍵を生成する(S74)。
- [0235] 第4の公開鍵及び第4の秘密鍵を生成すると、プロセッサ61は、第4の秘密鍵及び第4の証明書情報を含む鍵レスポンスを発行装置10に送信する(S75)。鍵レスポンスを送信すると、プロセッサ61は、第4の秘密鍵及び第4の証明書情報を鍵リクエストが含む子ID及びパスワードと対応付けてNVM64に格納する(S76)。
- [0236] 発行装置10のプロセッサ11は、通信部15を通じて鍵レスポンスを受信する。鍵レスポンスを受信すると、プロセッサ11は、第2のリーダライタ19を通じて、第2のデータとして、第4の秘密鍵及び第4の証明書情報、子ID及びパスワードを格納することを指示する格納コマンドを子ICカ

ード３０に送信する（Ｓ７７）。

[0237] 子ＩＣカード３０のプロセッサ３１は、通信部３５を通じて格納コマンドを発行装置１０から受信する。格納コマンドを受信すると、プロセッサ３１は、格納コマンドに従ってＮＶＭ３４に第２のデータを格納する（Ｓ７８）。

[0238] 第２のデータを格納すると、プロセッサ３１は、通信部３５を通じて格納完了レスポンスを発行装置１０に送信する（Ｓ７９）。

[0239] 発行装置１０のプロセッサ１１は、第２のリーダライタ１９を通じて格納完了レスポンスを受信する。プロセッサ１１が格納完了レスポンスを受信すると、発行システム１'は、動作を終了する。

[0240] 以上のように構成された発行システムは、鍵サーバを用いて第４の公開鍵及び第４の秘密鍵を管理する。その結果、発行システムは、既存の管理サーバを変更することなく、第４の証明書情報を子ＩＣカードに格納することができる。

[0241] 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] 親ＩＣカードに紐づくＩＣカードであって、
生体情報を取得するセンサと、
前記生体情報と照合するためのテンプレートを格納する第１の記憶部と、
前記親ＩＣカードが格納する第１のデータに関連する第２のデータを格納する第２の記憶部と、
上位装置とデータを送受信する通信部と、
前記上位装置からのコマンドに従って前記生体情報と前記テンプレートとの照合結果に基づいてユーザを認証し、
前記ユーザの認証に成功すると、前記第２のデータの少なくとも一部を前記上位装置に送信する、
プロセッサと、
を備えるＩＣカード。
- [請求項2] 前記第１のデータは、第１の秘密鍵と第１の公開鍵から構成される第１の証明書情報と第２の秘密鍵と第２の公開鍵から構成される第２の証明書情報とを含む、
請求項１に記載のＩＣカード。
- [請求項3] 前記第２のデータは、前記第１の秘密鍵と前記第１の証明書情報と前記第２の秘密鍵と前記第２の証明書情報とを含む、
請求項２に記載のＩＣカード。
- [請求項4] 前記第２のデータは、子ＩＤをさらに含む、
請求項３に記載のＩＣカード。
- [請求項5] 前記第２のデータは、前記子ＩＤに対応するパスワードをさらに含む、
請求項４に記載のＩＣカード。
- [請求項6] 前記第２のデータは、前記第１の証明書情報と前記第２の証明書情報とに基づく第３の証明書情報をさらに含む、

請求項 3 に記載の IC カード。

[請求項 7] 前記第 3 の証明書情報は、前記第 1 の証明書情報から生成される第 1 のハッシュ値と前記第 2 の証明書情報から生成される第 2 のハッシュ値とを含む、

請求項 6 に記載の IC カード。

[請求項 8] 前記第 2 のデータは、前記第 1 の証明書情報又は前記第 2 の証明書情報のいずれかセキュリティレベルが低い証明書情報を含む、

請求項 2 に記載の IC カード。

[請求項 9] 前記第 2 のデータは、前記第 1 の秘密鍵と前記第 2 の秘密鍵とに対応する第 4 の秘密鍵を含む、

請求項 2 に記載の IC カード。

[請求項 10] 前記生体情報は、指紋画像である、

請求項 1 乃至 9 の何れか 1 項に記載の IC カード。

[請求項 11] 親 IC カードに紐付く IC カードであって、

生体情報を取得するセンサと、前記生体情報と照合するためのテンプレートを格納する第 1 の記憶部と、前記親 IC カードが格納する第 1 のデータに関連する第 2 のデータを格納する第 2 の記憶部と、上位装置とデータを送受信する通信部と、前記上位装置からのコマンドに従って前記生体情報と前記テンプレートとの照合結果に基づいてユーザを認証し、前記ユーザの認証に成功すると、前記第 2 のデータの少なくとも一部を前記上位装置に送信する、プロセッサと、を備えるモジュールと、

前記モジュールを内蔵した本体と、

を備える IC カード。

[請求項 12] 親 IC カードに紐付く携帯可能電子装置であって、

生体情報を取得するセンサと、

前記生体情報と照合するためのテンプレートを格納する第 1 の記憶部と、

前記親ＩＣカードが格納する第１のデータに関連する第２のデータを格納する第２の記憶部と、

上位装置とデータを送受信する通信部と、

前記上位装置からのコマンドに従って前記生体情報と前記テンプレートとの照合結果に基づいてユーザを認証し、

前記ユーザの認証に成功すると、前記第２のデータの少なくとも一部を前記上位装置に送信する、

プロセッサと、

を備える携帯可能電子装置。

[請求項13]

親ＩＣカードに紐づくＩＣカードを発行する発行装置であって、

前記ＩＣカードとデータを送受信するリーダライタと、

外部装置とデータを送受信する通信部と、

前記リーダライタを通じて、生体情報のテンプレートを登録することを指示する登録コマンドを前記ＩＣカードに送信し、

前記通信部を通じて、前記親ＩＣカードが格納する第１のデータに関連する第２のデータを前記外部装置から取得し、

前記リーダライタを通じて、前記第２のデータを格納することを指示する格納コマンドを前記ＩＣカードに送信する、

プロセッサと、

を備える発行装置。