(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-540802
(P2010-540802A)
(43)公表日　平成22年12月24日(2010.12.24)

(51)Int.Cl.		F I			テーマコード（参考）
E05B 49/00	***(2006.01)***	E05B	49/00	J	2E250
G06Q 50/00	***(2006.01)***	G06F	17/60	132	
G06Q 10/00	***(2006.01)***	G06F	17/60	512	

審査請求 未請求　予備審査請求 有　（全 25 頁）

(21)出願番号　特願2010-526330 (P2010-526330)
(86)(22)出願日　平成20年9月24日 (2008.9.24)
(85)翻訳文提出日　平成22年5月21日 (2010.5.21)
(86)国際出願番号　PCT/FI2008/050529
(87)国際公開番号　WO2009/040470
(87)国際公開日　平成21年4月2日 (2009.4.2)
(31)優先権主張番号　07117498.1
(32)優先日　平成19年9月28日 (2007.9.28)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　509234744
イロク　オサケ　ユキチュア
フィンランド国　エフアイ　－　９０５７０　オウル、エレクトロニーカティエ　９
(74)代理人　110000855
特許業務法人浅村特許事務所
(74)代理人　100066692
弁理士　浅村　皓
(74)代理人　100072040
弁理士　浅村　肇
(74)代理人　100091339
弁理士　清水　邦明
(74)代理人　100094673
弁理士　林　鉐三

最終頁に続く

(54)【発明の名称】錠管理システム

(57)【要約】
自己給電式錠の錠管理システムを提供する。錠管理システムは、インターネットに利用可能な状態で接続され、錠システムに関連する情報を格納するＡＳＰ（アプリケーション・サービス・プロバイダ）サーバと、暗号化および復号化のための共有機密の生成と、トークンを用いて錠アクセス・データ・パケットの生成と暗号化を行うことを制御し、公衆ネットワークを用いてデータ・パケットをＡＳＰサーバへ転送し、ＡＳＰサーバから暗号化された状態パケットを受信し、状態パケットの復号化を制御し、公衆ネットワークを用いて復号化された状態パケットに関する情報をＡＳＰサーバへ送信する少なくとも１つの顧客モジュールと、公衆ネットワークを介してＡＳＰサーバからデータ・パケットを受信し、データ・パケットを復号化し、暗号化された状態パケットをＡＳＰサーバへ送信する、少なくとも１つの錠を含む。

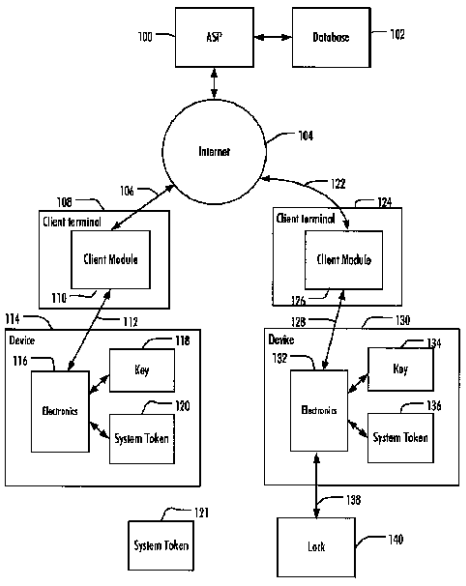


FIG. 1

【特許請求の範囲】
【請求項１】
自己給電式錠の錠管理システムであって：
インターネットに使用可能な状態で接続され、錠システムに関連する情報を格納するように構成された、１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバ；
暗号化および復号化のための共有機密の生成と、１つのトークンを用いて錠アクセス・データ・パケットの生成と暗号化を行うことを制御し；
前記データ・パケットを公衆ネットワークを用いてＡＳＰサーバに転送し；
暗号化された状態パケットをＡＳＰサーバから公衆ネットワークを用いて受信し、前記状態パケットの復号化を制御し、復号化された状態パケットに関する情報をＡＳＰサーバへ公衆ネットワークを用いて送信するように構成された、少なくとも１つの顧客モジュール；
データ・パケットを前記ＡＳＰサーバから公衆ネットワーク経由で受信；
前記データ・パケットを復号化し１つの暗号化された状態パケットを前記ＡＳＰサーバに公衆ネットワークを用いて送信するように構成された少なくとも１つの錠を含む、前記錠管理システム。
【請求項２】
請求項１記載の錠管理システムにおいて、顧客モジュールが錠が属している施錠システムに関する情報と前記錠のアクセス権に関する情報を含む、錠アクセス・データ・パケットを生成するように構成されている、前記錠管理システム。
【請求項３】
請求項１記載の錠管理システムにおいて、顧客モジュールが錠を初期状態に戻すための命令を含む、錠アクセス・データ・パケットを生成するように構成されている、前記錠管理システム。
【請求項４】
請求項１記載の錠管理システムにおいて、鍵、顧客モジュールと接続し、トークンと通信するように構成されている第１装置を含む、前記錠管理システム。
【請求項５】
請求項１記載の錠管理システムにおいて、錠と接続し、トークンと通信するように構成されている第２装置を含む、前記錠管理システム。
【請求項６】
請求項５記載の錠管理システムにおいて、前記ＡＳＰサーバと公衆回線で接続し、前記第２装置と有線または無線接続で接続するように構成された、第２顧客モジュールを含む、前記錠管理システム。
【請求項７】
請求項６記載の錠管理システムにおいて、前記第２顧客モジュールが錠アクセス・データ・パケットを前記ＡＳＰサーバから受信し、前記錠アクセス・データ・パケットを前記第２装置経由で錠に転送するように構成されている、前記錠管理システム。
【請求項８】
請求項６記載の錠管理システムにおいて、前記第２顧客モジュールが暗号化された状態パケットを錠から前記第２装置経由で受信し、前記状態パケットを前記ＡＳＰサーバに転送するように構成されている、前記錠管理システム。
【請求項９】
請求項６記載の錠管理システムにおいて、前記第２顧客モジュールと前記ＡＳＰサーバとの間の接続は少なくとも一部分が無線である、前記錠管理システム。
【請求項１０】
請求項６記載の錠管理システムにおいて、該錠管理システムが第２顧客モジュールを携帯端末の中に含む、前記錠管理システム。
【請求項１１】

請求項１記載の錠管理システムにおいて、顧客モジュールが暗号化および復号化のための共有機密を生成し、１つのトークンを用いて錠アクセス・データ・パケットを生成し暗号化するように構成され；
状態パケットの復号化を行う、前記錠管理システム。
【請求項１２】
請求項４記載の錠管理システムにおいて、前記第１装置が暗号化および復号化のための共有機密を生成し、１つのトークンを用いて錠アクセス・データ・パケットを生成し暗号化するように構成され；
状態パケットの復号化を行う、前記錠管理システム。
【請求項１３】
自己給電式錠用システムを管理するための方法であって：
１つの顧客モジュールによって暗号化および復号化用の共有機密の生成を制御し；
錠アクセス・データ・パケットを、セキュリティ・トークンを用いて生成し；
生成された錠アクセス・データ・パケットを、トークンを用いて暗号化し；
暗号化されたデータ・パケットをＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバに公衆ネットワークを用いて転送し；
暗号化されたデータ・パケットをＡＳＰサーバ内に格納し；
暗号化されたデータ・パケットを１つの錠によりサーバから公衆ネットワーク経由で読み取り；
前記データ・パケットを前記錠の中で復号化し；
前記錠の中で暗号化された状態パケットを生成し、前記データ・パケットをＡＳＰサーバへ転送し；
１つの状態パケットをＡＳＰサーバから読み取り、顧客モジュールによる状態パケットの復号化を制御し；
復号化された状態パケットに関する情報を顧客モジュールからＡＳＰサーバに転送する、ことを含む、前記錠管理方法。
【請求項１４】
請求項１３記載の方法が更に：
錠が属している施錠システムに関する情報と前記錠のアクセス権に関する情報を含む、錠アクセス・データ・パケットを生成することを含む、前記錠管理方法。
【請求項１５】
請求項１３記載の方法が更に：
顧客モジュール内で、錠命令「初期状態に復元」を含む錠アクセス・データ・パケットを生成することを含む、前記錠管理方法。
【請求項１６】
自己給電式錠用の錠管理システム内の１つの顧客モジュールであって、前記錠管理システムはインターネットに使用可能な状態で接続され、錠システムに関連する情報を格納するように構成された１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバを含む、前記顧客モジュールであって：
暗号化および復号化のための共有機密を生成し；
鍵データと共有機密から１つのトークンを用いて１つのユニークな鍵機密を生成し；
１つのセキュリティ・トークンを用いて錠アクセス・データ・パケットを生成して暗号化し；
ＡＳＰサーバと公衆ネットワークを用いて通信するように構成されている、前記顧客モジュール。
【請求項１７】
自己給電式錠用の錠管理システム内の錠であって、前記錠管理システムは、インターネットに使用可能な状態で接続され、錠システムに関連する情報を格納するように構成された１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバを含む、前記錠であって：

データ・パケットをＡＳＰサーバから受信し；
前記データ・パケットを復号化し、共有機密を前記データ・パケット情報を用いて生成し、前記共有機密を格納し、暗号化された状態パケットをＡＳＰサーバへ送信するように、構成されている前記錠。
【請求項１８】
請求項１７記載の錠において、前記錠が：
鍵と通信し；
鍵データと共有機密からユニークな鍵機密を生成し；
その生成された前記鍵機密が前記鍵内に格納されている鍵機密に対応する際に前記鍵を認証するように構成されている、前記錠。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は電子機械式錠用の錠管理システムに関するものである。特に本発明は自己給電式錠に関するものである。
【背景技術】
【０００２】
種々の型式の電子機械式錠が従来型機械式錠に置き換えられている。電子機械式錠は、外部供給電源、錠内部の電池、鍵内部の電池、またはその錠に自己電源を供給するための、錠内部で電力を発生するための手段を必要とする。電子錠は従来式錠に比較して多くの利点を提供する。これらはより良好なセキュリティを提供し、鍵の制御またはセキュリティ・トークンがより簡単になる。
【０００３】
加えて、ほとんどの電子機械式錠および／または鍵並びにトークンはプログラム可能である。その錠が異なる鍵を受け入れまたその他を拒絶するようにプログラムすることが可能である。
【０００４】
電子機械式および自己給電式錠に関連する１つの問題は、錠と鍵のプログラミングである。多くの知られている電子機械式錠システムにおいて、錠製造者は最終顧客に対して工場でプログラムされた錠を配送する。錠製造者は指定された施錠システムに属する錠の、所望されたプログラミングを実施してきた。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本発明の１つの特徴によれば、自己給電式錠の錠管理システムが提供されており、これは：インターネットに使用可能な状態で接続され、錠システムに関連する情報を格納するように構成された１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバ；暗号化および復号化のための共有機密の生成と、１つのトークンを用いて錠アクセス・データ・パケットの生成と暗号化を行うことを制御し、それらのデータ・パケットを公衆ネットワークを用いてＡＳＰサーバに転送し、暗号化された状態パケットをＡＳＰサーバから公衆ネットワークを用いて受信し、その状態パケットの復号化を制御し、そして復号化された状態パケットに関する情報をＡＳＰサーバへ公衆ネットワークを用いて送信するように構成された少なくとも１つの顧客モジュールと；データ・パケットをＡＳＰサーバから公衆ネットワーク経由で受信し、それらのデータ・パケットを復号化し１つの暗号化された状態パケットをＡＳＰサーバに公衆ネットワークを用いて送信するように構成された少なくとも１つの錠、を含む。
【０００６】
本発明の別の特徴によれば、自己給電式錠用システムを管理するための方法が提供されており、これは：１つの顧客モジュールによって暗号化および復号化用の共有機密の生成を制御し；錠アクセス・データ・パケットをセキュリティ・トークンを用いて生成し；生

成された錠アクセス・データ・パケットをトークンを用いて暗号化し；暗号化されたデータ・パケットをＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバに公衆ネットワークを用いて転送し；暗号化されたデータ・パケットをＡＳＰサーバ内に格納し；暗号化されたデータ・パケットを１つの錠によりサーバから公衆ネットワーク経由で読み取り；そのデータ・パケットをその錠の中で復号化し；その錠の中で暗号化された状態パケットを生成し、そのパケットをＡＳＰサーバへ転送し；１つの状態パケットをＡＳＰサーバから読み取り、顧客モジュールによる状態パケットの復号化を制御し；復号化された状態パケットに関する情報を顧客モジュールからＡＳＰサーバに転送する、ことを含む。

【０００７】

本発明の別の特徴によれば、自己給電式錠用の錠管理システム内の１つの顧客モジュールが提供されており、このシステムはインターネットに使用可能な状態で接続され、錠システムに関連する情報を格納するように構成された１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバを含み、顧客モジュールは：暗号化および復号化のための共有機密を生成し、鍵データと共有機密から１つのトークンを用いて１つのユニークな（固有の）鍵機密を生成し；１つのセキュリティ・トークンを用いて錠アクセス・データ・パケットを生成して暗号化し；そしてＡＳＰサーバと公衆ネットワークを用いて通信するように構成されている。

【０００８】

本発明の更に別の特徴によれば、自己給電式錠用の錠管理システム内の錠が提供されており、このシステムは、インターネットに使用可能な状態で接続され、錠システムに関連する情報を格納するように構成された１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバを含み；錠は：データ・パケットをＡＳＰサーバから受信し；そのデータ・パケットを復号化し、共有機密をそのデータ・パケット情報を用いて生成し、その共有機密を格納し、そして暗号化された状態パケットをＡＳＰサーバへ送信するように、構成されている。

【課題を解決するための手段】

【０００９】

本発明はいくつかの特長を有する。提案された解決方法はフレキシブルな錠及び鍵のプログラミングを可能とする。錠製造者または卸業者は錠システムのデータベースを保存しているＡＳＰサーバの保守を行う。しかしながら、錠および鍵のプログラミングは最終顧客によって実行される。従って、錠製造者は錠を初期状態、即ちいずれの特定の施錠システムにも属していない状態で配達する。初期状態の錠は如何なるセキュリティ機密情報も格納していない。

【００１０】

提案された解決方法において、これらの錠はＡＳＰサーバへの専用有線接続を必要としない。暗号化された錠プログラミング・データはその錠に対して公衆ネットワーク経由で転送され、これは有線または無線接続で差し支えない。

【００１１】

本発明のいくつかの実施例が、例としてのみ以下に添付図を参照して説明されている。

【図面の簡単な説明】

【００１２】

【図１】図１は１つの錠管理システムの構造の１例を図示する。

【図２】図２は鍵および錠を図示する。

【図３Ａ】図３Ａは施錠システムの共有機密が生成される実施例を図示する流れ図である。

【図３Ｂ】図３Ｂは追加のシステム・トークンがその施錠システムの中に生成される実施例を図示する流れ図である。

【図３Ｃ】図３Ｃは施錠システム共有機密が錠の中に転送される実施例を図示する流れ図である。

【図３Ｄ】図３Ｄは鍵共有機密が新しい鍵に設定される実施例を図示する流れ図である。
【図３Ｅ】図３Ｅは錠が新たな鍵を用いて解錠されることに関する実施例を図示する流れ図である。
【図４】図４は本発明の１つの実施例を図示する信号伝達図である。
【図５】図５は鍵および錠の別の例を図示する。
【発明を実施するための形態】
【００１３】
以下の実施例は典型例である。本明細書は様々な場所で「或る１つ（an）」、「１つの（one）」、「いくつかの（some）」実施例を参照しているが、これは必ずしも、各々のその様な参照が同一の１つまたは複数の実施例に対してなされるものであったり、またはその特徴が単一の実施例に対してのみ適用されることを意味するものでは無い。異なる複数の実施例の特徴はまた、別の実施例を提供するために組み合わされることもあり得る。
【実施例】
【００１４】
図１を参照すると、錠管理システムの構造の１つの例が説明されている。このシステムは、インターネット１０４に使用可能な状態で接続され、錠システムに関連する情報をデータベース１０２格納するように構成されたアプリケーション・サービス・プロバイダ（ASP：application service provider）サーバ１００を含む。データベース１０２は取り外し可能な大容量記憶装置または当該サーバ内の固定大容量記憶装置で実現したり、または別のコンピュータとすることが可能である。その他の実現方法もまた可能である。典型的に錠システム製造者または錠システム卸業者がＡＳＰサーバ１００を保守する。データベースは当該施錠システムに属する錠および鍵上のデータを保守する。このデータは、例えば錠および鍵識別子、鍵保持者、錠および鍵状態およびアクセス権に関する情報を含む。
【００１５】
このシステムは更に顧客モジュール１１０を含む。顧客モジュールは顧客構内の顧客端末１０８内で動作する顧客ソフトウェアである。典型的に顧客端末１０８は、有線または無線接続１０６を通してインターネット１０４に接続されたパーソナル・コンピュータまたは対応する処理ユニットである。
【００１６】
顧客モジュール１１０の実現は顧客端末設計に依存して変化するであろう。顧客モジュールはプログラム言語でコード化されたプログラム命令から成り、このプログラム言語は例えばＣ，Ｊａｖａ（登録商標）等の高レベルプログラム言語、または機械言語またはアセンブラの様な低レベルプログラム言語である。
【００１７】
顧客モジュール１１０は施錠システムに関する情報を管理するように構成されている。例えば、顧客モジュールは暗号化および復号化用の共有機密を生成し、１つのセキュリティ・トークンを用いて錠アクセス・データ・パケットの生成および暗号化を行う。
【００１８】
顧客モジュールは鍵１１８およびシステム・トークン１２０と接続するように構成された第１装置１１４に接続１１２されている。顧客モジュールと第１装置との間の接続１１２は、有線または無線接続で実現される。この接続はＵＳＢ，ブルートゥース、赤外線またはその他の既知の無線技術で実現される。
【００１９】
第１装置１１４は電子回路１１６および鍵１１８並びにトークン１２０用容器を含む。電子回路１１６はプロセッサとデータ格納用メモリ、およびプロセッサ用ソフトウェアを含む。電子回路は施錠データに関する計算を実行し、顧客モジュール、鍵およびシステム・トークン間で情報を転送するように構成される。第１装置１１４および顧客端末１０８は、顧客モジュール１１０と鍵１１８およびシステム・トークン１２０通信用のプラットフォームを提供する。顧客モジュール１１０とＡＳＰサーバ１００は、錠システムの共有

機密を格納し、錠アクセス・データ・パケットの暗号化および復号化を行い、そして錠システム内での使用者アクセスの認証を行うために、システム・トークン１２０と通信する。

【００２０】

錠管理システムは更に第２顧客モジュール１２６を含む。第２顧客モジュール１２６は顧客端末１２４内で動作する顧客ソフトウェアである。顧客端末１２４はパーソナル・コンピュータ、携帯情報端末（pda：personal data assistant）またはインターネット１０４に接続された携帯電話機１２２である。第２顧客モジュール１２６は顧客モジュール１１０と同様な方法で実現される。

【００２１】

第２顧客モジュール１２６は鍵１３４およびシステム・トークン１３６と接続するように構成された第２装置１３０に接続１２８されている。第２顧客モジュールと第２装置との間の接続１２８は、有線または無線接続で実現される。この接続はＵＳＢ、ブルートゥース（登録商標）、赤外線またはその他の既知の無線技術で実現される。加えて、第２装置は錠１４０への接続１３８を有する。接続は有線または無線である。例えば、有線接続は１線式バス接続で実現される。有線接続は自己給電式錠に電力を供給する。無線接続は既知の無線プロトコルで実現される。

【００２２】

第２装置１３０および顧客端末１２４は顧客モジュール１２６、鍵１３４、システム・トークン１３６および錠１４０に対して、施錠システムの共有機密を格納し、錠アクセス・データ・パケットの暗号化および復号化を行い、また錠システム内の使用者アクセスを認証するための、通信用のプラットフォームを提供する。

【００２３】

１つの実施例において、第１装置および第２装置はそれぞれ同一の装置である。

【００２４】

１つの実施例において、顧客モジュール１１０または１２６の使用者は、ＡＳＰサーバ１００にログインすることで顧客モジュールとＡＳＰサーバ１００との間のセッションを確立する。顧客モジュールはＡＳＰサーバに接触し利用可能モジュールの更新版が有るか否かをチェックする。もし有る場合には、更新版がダウンロードされ顧客端末にインストールされる。所望された施錠システム管理操作が開始されるかまたは実施されると、そのセッションはＡＳＰサーバからログアウトすることで終了される。

【００２５】

図２は鍵１１８と錠１４０を図示する。錠１４０は鍵１１８からアクセス・データを読み取り、そのデータを予め定められた判定基準に対して整合を取るように構成されている。鍵１１８はアクセス・データを格納し、暗号化および復号化に関する計算を実施するように構成されている。この電子回路は例えばMaxim Integrated Products 社製iButton（登録商標）（www.ibutton.com）であり、その様な電子回路は1-Wire（登録商標）プロトコルで読まれる。この電子回路は、例えば鍵またはトークンの中に設置されるが、これはまたその他の適切な機器または物体の中に配置することも可能である。唯一必要なことは、錠がデータをこの電子回路から読み取れることである。鍵から錠１４０へのデータ転送は任意の好適な有線または無線通信技術により実行できる。自己給電式錠において、生成されたエネルギー量が使用される技術を制約する。磁気ストライプ技術またはスマートカード技術もまた鍵の中で使用される。無線技術は例えば、ＲＦＩＤ（無線周波数識別：Radio-frequency identification）技術、または携帯電話技術を含む。鍵はトランスポンダ、ＲＦタグ、またはデータを格納することの出来る任意のその他の好適なメモリ型式を含む。

【００２６】

鍵から読み取られたデータは、そのデータを予め定められた判定基準に照らし合わせて整合をとることで認証のために使用される。この認証は国家安全保障局（NSA：National Security Agency）で設計されたＳＨＡ－１（セキュア・ハッシュ・アルゴリズム：Secur

e Hash Algorithm）関数で実行される。ＳＨＡ－１において、圧縮されたデジタル表現（メッセージ・ダイジェストとして知られている）が与えられた入力データ・シーケンス（メッセージとして知られている）から計算される。このメッセージ・ダイジェストはそのメッセージに対して高い確率でユニークである。ＳＨＡ－１は「安全」と呼ばれるが、それは指定されたアルゴリズムに関して、与えられたメッセージ・ダイジェストに対応するメッセージを探し出すこと、または同一メッセージ・ダイジェストを生成する２つの異なるメッセージを見つけることが計算上実行不能であるからである。メッセージに対する全ての変更は、非常に高い確率で、結果として異なるメッセージ・ダイジェストとなる。安全性を増す必要が有る場合には、ＳＨＡ群内の別のハッシュ関数（ＳＨＡ－２２４，ＳＨＡ－２５６，ＳＨＡ－３８４およびＳＨＡ－５１２）、各々より長い桁数の、纏めてＳＨＡ－２として知られているものが使用できる。当然、外部情報源から読み取られたデータの認証を行うために、任意の好適な認証技術が使用出来る。認証技術の選択は錠１４０に所望される安全レベルと、またおそらくは認証（特に、使用者給電式の電子機械式錠における認証）のために使用することが許される電力消費量に依存する。

【００２７】

図３Ａは施錠システム共有機密（ＳＳ：shared secret）が生成され、第１システム・トークンが施錠システムの中に作成される、１つの実施例を図示する流れ図である。この施錠システム共有機密は錠アクセス・データの暗号化および復号化で用いられる。システム・トークンは先に説明した電子回路を含み、これは第１装置１１４内で施錠システム共有機密を生成し格納するために使用される。このシステム・トークンは特別なトークンであって、それは鍵として使用されるのではなく、施錠システムの鍵および錠をプログラムするために使用されるものである。典型的にシステム・トークンの作成は新規施錠システム用の錠および鍵をプログラムする際の第１ステップである。１つの施錠システムは複数のシステム・トークンを持つであろうが、それらは全て同一の施錠システム共有機密を格納している。

【００２８】

顧客モジュール１１０は施錠システム共有機密とシステム・トークンの生成を制御する責任がある。顧客モジュールは顧客端末内に存在するので、この処理はその顧客モジュールがインターネット接続されており、装置１１４が顧客端末１０８に接続されているという条件で、顧客の施設内で実施される。１つの実施例において、顧客モジュール１１０は、以下においてそれらが顧客モジュールに割り当てられている仕事のいくつかまたは全てを、装置１１４を制御して実行する。錠製造者または卸業者はＡＳＰサーバ１００の保守以外にこの処理手順において何の役割も担わない。

【００２９】

この処理は、使用者が空のトークン１２０を第１装置１１４の中に設定した時に、ステップ３００で開始される。

【００３０】

ステップ３０２において、顧客モジュール１１０は使用者にシード１（seed 1）をタイプ入力するように要求する。シード１は典型的に、１０－２０文字の英数字列である。シード１はシステム内に格納されない。使用者は覚えておかなければならない。

【００３１】

ステップ３０４において、顧客モジュール１１０は乱数発生器を用いてシード２を生成する。シード２は典型的に１０から２０バイト長の数字のリストである。各々のバイトは０から２５５の間の任意の値を持ちうる。

【００３２】

ステップ３０６において、顧客モジュール１１０は乱数発生器を用いてシード３を生成する。シード３は典型的に１０から２０バイト長である。各々のバイトは０から２５５の間の任意の値を持ちうる。

【００３３】

ステップ３０８において、顧客モジュール１１０はシード１－３をトークン１２０へ送

信する。トークンはこれらのシードを受信し、施錠システム共有機密で使用される１つのＳＨＡ－１ハッシュを生成する。トークン１２０は共有機密をその隠し書き込み専用メモリの中に格納する。この共有機密は顧客モジュールに返送されることも、使用者に明かされることも無い。

【００３４】

このハッシュは当業者は良く知っているように、何らかの別の暗号化ハッシュ関数を用いて生成することも可能である。ＳＨＡ－１は本明細書の中で単に１例として用いられている。

【００３５】

１つの実施例において、顧客モジュール１１０は共有機密として使用されるハッシュを計算し、そのハッシュを、ハッシュを格納するトークン１２０に送信するように構成されている。

【００３６】

ステップ３１０において、顧客モジュール１１０はシード３をトークン１２０の中に格納する。

【００３７】

ステップ３１２において、顧客モジュール１１０はシード２をＡＳＰサーバで保守されている施錠システム・データベース１０２に転送する。この転送は、例えばＳＳＬ（安全ソケット・レイヤ：Secure Sockets Layer）で暗号化されている。

【００３８】

ステップ３１４において、顧客モジュール１１０はそのトークン１２０をシステム・トークンとして施錠システム・データベース１０２の中に登録する。各々のトークンはユニークなシリアル番号を有してデータベース１０２の中に格納されている。この格納は、例えばＳＳＬ（安全ソケット・レイヤ：Secure Sockets Layer）で暗号化されている。

【００３９】

この処理手順は３１６で終了する。

【００４０】

図３Ｂは追加のシステム・トークンが施錠システムの中に作成される、１つの実施例を図示する流れ図である。この施錠システムは、図３Ａで説明された手順を用いて作成された、少なくとも１つのシステム・トークンを既に有している。顧客モジュール１１０は追加システム・トークンの生成を制御する責任を有する。顧客モジュールは顧客端末の中に存在するので、この顧客モジュールがインターネット接続を有し、装置１１４が顧客端末１０８に接続されているという条件で、顧客の施設内で実施される。１つの実施例において、顧客モジュール１１０は、以下においてそれらが顧客モジュールに割り当てられている仕事のいくつかまたは全てを、装置１１４を制御して実行する。錠製造者または卸業者はＡＳＰサーバ１００の保守以外にこの処理手順において何の役割も担わない。

【００４１】

この処理手順は使用者が、装置１１４内にインストールされた既存のシステム・トークン１２０の１つを有する場合に開始される。

【００４２】

ステップ３２２において、顧客モジュール１１０は使用者にシード１をタイプ入力するように要求する。シード１は第１システム・トークン１２０を生成する際にタイプ入力されたものとまさしく同一のものでなければならない。

【００４３】

ステップ３２４において、顧客モジュール１１０錠システム・データベース１０２にインターネット経由で接触し、データベース１０２からシード２を読み取る。

【００４４】

ステップ３２６において、顧客モジュール１１０はシード３を装置１１４内にインストールされた既存のシステム・トークン１２０から読み取る。

【００４５】

ステップ３２８において、顧客モジュール１１０はシード１から３を使用して１つのＳＨＡ－１ハッシュを生成する。

【００４６】

ステップ３３０において、顧客モジュール１１０はそのハッシュを既存のシステム・トークン１２０を使用して検証する。

【００４７】

ステップ３３２において、その検証結果が分析される。検証に失敗した場合、おそらく使用者が正しく無いシード１をタイプ入力したためであり、その処理手続きは取り消されるかまたはステップ３２２から再開される。

【００４８】

そうでなければ、処理はステップ３３４で継続し、此処で顧客モジュールは使用者に対して既存のシステム・トークン１２０を装置１１４から除去し１つの空のトークン１２１を装置１１４の中に設定するように要求する。

【００４９】

ステップ３３６において、顧客モジュール１１０はシード３を新たなトークン１２１の中に格納する。

【００５０】

ステップ３３８において、顧客モジュール１１０はシード１および２をトークン１２０に送信する。このトークンはこれらのシードを受信し、シード１から３を用いて１つのＳＨＡ－１ハッシュを生成する。この生成されたハッシュは施錠システム共有機密であり、第１システム・トークン１２０の中に格納されたものと同一である。トークンはこのハッシュを共有機密としてその隠し書き込み専用メモリ内に格納する。

【００５１】

ステップ３４０において、顧客モジュール１１０は新たなシステム・トークン１２１を錠システム・データベース１０２の中に登録する。この転送は、例えばＳＳＬ（安全ソケット・レイヤ：Secure Sockets Layer）で暗号化されている。

【００５２】

この処理手順は３４２で終了する。

【００５３】

図３Ｃは、施錠システム共有機密が１つの錠の中に転送される１つの実施例を図示する流れ図である。

【００５４】

この処理手順は、使用者が装置１１４の中にインストールされた既存のシステム・トークン１２０を有する場合にステップ３５０で開始される。此処でも顧客モジュール１１０は初期ステップに対して責任を有する。顧客モジュール１１０は顧客端末１０８内に存在するので、この処理はその顧客モジュール１１０がインターネット接続されており、装置１１４が顧客端末１０８に接続されているという条件で、顧客の施設内で実施される。初期ステップ３５０から３６６はその錠が置かれている場所以外の現場で実施されるはずである。錠製造者または卸業者はこの処理手順の中でＡＳＰサーバ１００の保守以外の役は負わない。１つの実施例において、顧客モジュール１１０は、以下においてそれらが顧客モジュールに割り当てられている仕事のいくつかまたは全てを、装置１１４を制御して実行する。

【００５５】

ステップ３５２において、顧客モジュール１１０は使用者に対して、シード１をタイプ入力するように要求する。シード１は第１システム・トークン１２０を生成する際にタイプ入力されたものとまさしく同一のものでなければならない。

【００５６】

ステップ３５４において、顧客モジュール１１０は錠システム・データベース１０２にインターネット経由で接触しシード２をデータベース１０２から読み取る。

【００５７】

ステップ３５６において、顧客モジュール１１０は、装置１１４内にインストールされたシステム・トークン１２０からシード３を読み取る。

【００５８】

ステップ３５８において、顧客モジュール１１０はシード１から３を使用して、１つのＳＨＡ－１ハッシュを生成する。このハッシュは施錠システムの共有機密に相当する。

【００５９】

ステップ３６０において、顧客モジュール１１０はそのハッシュを、装置１１４内にインストールされたシステム・トークン１２０の中に格納されている共有機密に対して検証する。

【００６０】

ステップ３６２において、その検証結果が分析される。その検証が失敗した場合、おそらく使用者が正しくないシード１をタイプ入力したためであり、この処理手順は取り消されるかまたはステップ３３２から再開される。

【００６１】

そうでない場合は、この処理手順はステップ３６４で継続され、此処でシード１から３は暗号化され、錠に対するプログラミング・ジョブ（programming job）としてシステム・トークンの中に格納される。

【００６２】

ステップ３６６において、システム・トークン１２０は、顧客モジュール１１０に接続された装置１１４から除去される。

【００６３】

この処理手順の残りのステップは、その錠が設置されている現場で実施される。顧客端末１２４は第２顧客モジュール１２６を含む。顧客端末はパーソナル・コンピュータ、携帯情報端末（ｐｄａ）、高機能電話機（smart phone）または相当する装置で構わない。第２装置１３０は顧客端末と第２顧客モジュールに接続されており、これは錠１４０にも接続を有する。

【００６４】

ステップ３６８において、システム・トークン１２０（これは図１ではトークン１３２として図示されている）が、錠１４０に接続されている装置１３０の中に差し込まれる。

【００６５】

ステップ３７０において、錠１４０は１つのプログラミング・ジョブをシステム・トークン１２０から読み取り、シード１から３の復号化を行って、１つのＳＨＡ－１ハッシュを生成する。

【００６６】

ステップ３７２において、錠１４０はそのハッシュを、装置１３０の中にインストールされたシステム・トークン１２０の中に格納されている共有機密に対して検証する。

【００６７】

ステップ３７４において、検証結果が分析される。

【００６８】

検証に失敗した場合、錠１４０はエラーを設定し、施錠システム共有機密をステップ３７８で設定しない。

【００６９】

検証に成功すると、共有機密がステップ３７８で錠１４０の中に格納される。

【００７０】

処理手順はステップ３７６または３７８で終了する。

【００７１】

ステップ３６８から３７８はいくつかの錠の上で繰り返される。施錠システム共有機密をいくつかの錠に、同一の初期ステップで転送することが可能である。

【００７２】

図３Ｄは鍵共有機密が新たな鍵にセットされる１つの実施例を図示する流れ図である。

顧客モジュール１１０は共有機密の生成を制御する責務を負う。顧客モジュールは顧客端末内に存在するので、この処理はその顧客モジュールがインターネット接続されており、装置１１４が顧客端末１０８に接続されているという条件で、顧客の施設内で実施される。錠製造者または卸業者はＡＳＰサーバ１００の保守以外にこの処理手順において何の役割も担わない。１つの実施例において、顧客モジュール１１０は、以下においてそれらが顧客モジュールに割り当てられている仕事のいくつかまたは全てを、装置１１４を制御して実行する。

【００７３】

この処理手順は新たな鍵１１８および既存のシステム・トークン１２０が装置１１４の中で接続された際に、ステップ３８０で開始される。

【００７４】

ステップ３８２において、顧客モジュール１１０は鍵１１８から鍵データを読み取り、それをシステム・トークン１２０に送信する。この鍵データは鍵シリアル番号を含むはずである。

【００７５】

ステップ３８４において、システム・トークン１２０は鍵データと施錠システム共有機密とを使用して鍵共有機密を計算する。

【００７６】

ステップ３８６において、顧客モジュール１１０はその鍵共有機密を新たな鍵１１８にセットする。

【００７７】

ステップ３８７において、顧客モジュール１１０はその新たな鍵１１８を鍵システム・データベース１０２の中に登録する。この転送は、例えばＳＳＬ（安全ソケット・レイヤ：Secure Sockets Layer）で暗号化されている。

【００７８】

この処理手順は３８８で終了する。

【００７９】

上記に加えて、追加アクセス・データが施錠システムの鍵の中にプログラムされる場合がある。１つの実施例において、鍵は、鍵識別子、鍵共有機密およびアクセス・グループ・データを含むデータ構造を格納している。各々の鍵はユニークな識別子ＩＤを有し、これはその鍵を同定するために使用される。アクセス・グループ・データは１つまたは複数の、その鍵が所属するアクセス・グループを含む。

【００８０】

１つの実施例において、１つの鍵はそれへのアクセスが許されている１つのアクセス・グループにある錠が属している場合、またはその鍵がアクセスを許されている鍵識別ＩＤを有する場合に、その錠を開けることができる。

【００８１】

アクセス・グループにより、鍵の編成が大いに強化される。１つの鍵には異なる場所へのアクセスを許可するために複数のアクセス・グループが与えられている。例えば、同一の鍵がアパート（アクセス・グループ１）、地下室（アクセス・グループ２）、車庫（アクセス・グループ３）、および空き瓶置き場（アクセス・グループ４）へのアクセスが与えられる。従ってある使用者はアクセス・グループ４のみを含む１つの鍵を廃品回収業者に与える。従ってその業者は空き瓶置き場へのアクセスは与えられるが、その鍵はそのビルの別の場所へのアクセスは認可されていない。

【００８２】

図３Ｅは錠１４０が鍵１１８で開けられる際の、１つの実施例を図示する流れ図である。

【００８３】

この処理手順は、使用者が鍵１１８を錠１４０の中に挿入した際に、ステップ３９０から開始される。この段階で、自己給電式錠はその鍵が錠の中に挿入されるので、その鍵の

動きから電力を発生する。これに代わって錠が電池を含んでいても構わない。

【００８４】

ステップ３９１において、錠１４０は鍵データおよび１つのハッシュを鍵１１８から読み取る。

【００８５】

ステップ３９２において、錠１４０は鍵データとその錠内の施錠システム共有機密とを使用して１つのＳＨＡ－１ハッシュを計算する。

【００８６】

ステップ３９３において、錠１４０はその錠で計算されたハッシュを鍵１１８から読み取られたハッシュに照らして検証する。

【００８７】

ステップ３９４において、検証結果が分析される。

【００８８】

ステップ３９９において、検証に失敗した場合、錠１４０はエラーを設定し解錠すること無く処理は終了する。

【００８９】

検証に成功すると、錠１４０はその鍵アクセス・データをステップ３９６で検証する。

【００９０】

ステップ３９７において、検証結果が分析される。この鍵アクセス・データはその鍵が所属している可能なアクセス・グループの情報を含む。錠はその鍵が所属しているアクセス・グループとその錠が解錠されるようにプログラムされているアクセス・グループとが整合するかチェックする。

【００９１】

検証に失敗すると、錠１４０はエラーを設定し解錠はしない。これはステップ３９９で行われる。

【００９２】

検証に成功すると、錠１４０はステップ３９８で解錠される。

【００９３】

処理手順はステップ３９８または３９９で終了する。

【００９４】

図４は錠１４０へのアクセス権が使用者により、顧客モジュール１１０を用いて変更される際の１つの例を図示する。顧客モジュール１１０はこのアクセス権変更の初期部分を制御する責任を負う。顧客モジュールは顧客端末１０８の中に存在するので、この処理手順はその顧客モジュールがインターネット接続を有するという条件で顧客の施設内で実行される。この処理手順が開始される前に、システム・トークン１２０は装置１１４の中に設置され、この装置１１４は顧客端末１０８と顧客モジュール１１０に接続されている。加えて、顧客モジュールはＡＳＰサーバ１００にログインする。

【００９５】

ＡＳＰサーバはデータベース１０２を保守しており、此処に施錠システムの錠、鍵およびアクセス権に関する情報が格納されている。しかしながら、アクセス権はＡＳＰサーバで変更されることは無い。アクセス権の変更には顧客モジュール１１０、１２６および装置１１４、１３０を介して顧客モジュールに接続しているシステム・トークンを使用する必要がある。

【００９６】

１つの実施例において、顧客モジュールはシステムの使用者に対して、アクセス権を変更し、錠および鍵をプログラムするためのインタフェースを提供する。顧客モジュール１１０は新たな錠アクセス・データを使用者から受信するように構成されている。その様なデータを受信すると、顧客モジュール１１０は“Program Lock”（錠をプログラム）メッセージ４０２をＡＳＰサーバ１００で保守されているデータベース１０２に送信する。

【００９７】

ＡＳＰサーバ１００は受信したデータをデータベース１０２の中に格納し、修正された錠アクセス・データを顧客モジュール１１０に“Send Job”（ジョブ送信）メッセージ４０４として送信し返す。顧客モジュール１１０はそのメッセージを受信し、そのデータを“Crypt Job”（ジョブ暗号化）メッセージ４０６として装置１１４に接続されているシステム・トークン１２０に送信する。システム・トークン１２０はアクセス・データを施錠システム共有機密で暗号化し、その暗号化された錠アクセス・データを顧客モジュール１１０へ“Send Crypted Job”（暗号化されたジョブ送信）メッセージ４０８として送信する。顧客モジュールは暗号化されたデータを受信し、それをＡＳＰサーバ１００に“Send Crypted Job”（暗号化されたジョブ送信）メッセージ４１０として送信する。ＡＳＰサーバ１００はそのデータをデータベース１０２の一部である作業待ち行列（work queue）４００の中に設置する。作業待ち行列４００は後ほど錠へ転送される、暗号化されたアクセス・データ・メッセージのリストである。顧客モジュール１１０はＡＳＰサーバ１００からログアウトする。

【００９８】

この処理手順の残りのステップはその錠がインストールされている現場で実施される。最初に、使用者は顧客モジュール１２６からＡＳＰサーバ１００にログインする。使用者のコマンドで、顧客モジュールはＡＳＰサーバに接触し、錠に対してプログラムされるべき１つのジョブを作業待ち行列４００からメッセージ４１２と共に選択する。作業待ち行列４００は暗号化された錠アクセス・データをメッセージ４１４の中で送信することにより応答する。顧客モジュール１２６はそのジョブを受信し、それを顧客端末１２４のメモリ内に格納する。そのジョブ・データで含まれている錠アクセス・データは暗号化されており、そのデータを顧客端末１２４の中に格納することは安全上の危険では無い。

【００９９】

次にシステム・トークン１３６が装置１３０の中に設置される。装置１３０と顧客端末１２４および顧客モジュール１２６の間の接続が確立される。顧客モジュールは、使用者から“Program Lock”（錠をプログラムせよ）命令を受信した場合に暗号化された錠アクセス・データ４１６をシステム・トークン１３６へ送信するように構成されている。使用者は装置１３０を錠１４０にプログラムされるように接続する。錠１４０が装置１３０と接続が確立されたことを検出した場合に、その錠は錠アクセス・データをシステム・トークン１３６から要求する４１８ように構成されている。１つの実施例において、錠はそのデータを要求する前にシステム・トークンを認証するように構成されている。

【０１００】

システム・トークン１３６は暗号化されたデータ４２０を送信することで応答する。錠１４０はそのデータの復号化を行い、その署名を錠の中に格納されている共有機密を用いて検証する。そのデータが有効な場合、錠１４０はそのデータを格納し、錠プログラミング状態を含む暗号化された肯定応答メッセージ４２２をシステム・トークン１３６へ送信し、その錠のアクセス・データのプログラムが完了したことを示す。そのデータが有効でなかった場合、錠１４０はそのデータを無視し、否定確認４２２をシステム・トークン１３６へ送信し、錠のプログラムが失敗したことを示す。１つの実施例において、装置１３０は使用者に対して錠プログラミングの成功を可視表示、例えば緑または赤色の発光ダイオードで通知するように構成されている。

【０１０１】

システム・トークン１３６は暗号化された錠プログラミング状態４２４を顧客モジュール１２６に送信する。この顧客モジュール１２６は暗号化された錠プログラミング状態４２６を作業待ち行列４００に送信する。

【０１０２】

この錠プログラミング状態は作業待ち行列４００の中に、システム・トークン１２０に接続された顧客モジュールがＡＳＰサーバ１００とセッションを確立するまで残される。顧客モジュールはＡＳＰサーバ１００に接続された際に作業待ち行列４００をチェック４２８するように構成されているはずである。問い合わせメッセージ４２８に対する応答と

して、ＡＳＰサーバ１００は暗号化された錠プログラミング状態を顧客モジュール１１０へ送信する４３０。

【０１０３】

暗号化された状態メッセージ４３０を受信した際に、顧客モジュール１１０はそのメッセージをシステム・トークン１２０に送信し４３２、これはデータを復号化してその復号化されたデータ４３４を顧客モジュール１１０に送信することで応答する。顧客モジュールは錠１４０状態を含むそのデータ４３６をＡＳＰサーバ１００に送信し、これはその錠状態をデータベース１０２の中に格納する。

【０１０４】

図３Ｃに関連して説明した処理手順は、施錠システム共有機密を１つの錠にインストールする。その施錠システム共有機密がインストールされる前は、錠は初期状態にある。初期状態錠はいずれの施錠システムにも属していない。それはいずれの鍵の認証もまた鍵のアクセス・データの検証を行うようには構成されていない。施錠システム共有機密はまた１つの鍵から図３Ｃの処理手順に類似の手順で取り除かれるはずである。１つの実施例において、顧客モジュール１１０は鍵を初期状態に戻すための命令を含む、錠アクセス・データ・パケットを生成するように構成されている。共有機密がアンインストールされた後は、その錠は再び初期状態に戻り、それは安全上のリスク無しで別の施錠システムで再使用できる。施錠システム共有機密を持たない錠は、安全上注意すべき情報は格納されていない。

【０１０５】

施錠システム共有機密が図３Ｃの処理手順を用いて錠の中にインストールされると、その錠はその施錠システムの１メンバーである。その施錠システムに属する鍵のみがその錠を開けることができる。しかしながら、その錠はいずれの追加アクセス・データを検証することは無い。錠のこの状態は委任状態（commissioned state）と呼ばれる。

【０１０６】

施錠システム共有機密は使用者から与えられたシードを基に、図３Ａに説明されているように装置１１４内のシステム・トークン１２０または顧客モジュール１１０で生成される。施錠システム共有機密は、システム・トークンの書き込み専用メモリの中に格納されている。

【０１０７】

記述された錠管理システムで管理されている１つのシステムに属する錠は、施錠システム共有機密をシステム・トークンとして計算する能力を有する。鍵は各々の鍵のユニークな識別子と施錠システム共有機密から生成されたユニークな機密を有する。錠は鍵から読み取られたユニークな識別子とその錠内に格納されている施錠システム共有機密に基づき、鍵機密を生成するように構成されている。

【０１０８】

図４に記述された処理手順を用いて、錠アクセス・グループが錠の中にインストールされると、その錠は鍵を認証し鍵アクセス・データを検証することができる。鍵アクセス・データ検証は、更に欧州特許明細書０７１１２６７５に説明されており、これは参考として此処に組み込まれている。

【０１０９】

図５は鍵１１８および錠１４０の１例を図示する。図５の例において、鍵１１８は接触配列５０２と鍵フレームに接続された電子回路５００を含む。電子回路５００は、メモリ・ユニットを含んでもよい。図１の電子機械式錠１４０は自己給電式錠である。錠１４０は電力伝達機構５０４を含み、これは使用者からの機械エネルギーを発電機５０６に転換し、鍵１１８が錠１４０に挿入された際に電子回路５０８に電力を供給する。この例において、電子回路５０８は鍵の電子回路５００と接触配列５１０および鍵の接触配列５０２を通して通信するように構成されている。この通信は無線接続または物理的伝導により実現される。

【０１１０】

電子回路５０８は、鍵が挿入された時点で、鍵１１８の電子回路５００から鍵データを読み取るように構成されている。電子回路５０８は更に、先に説明したように鍵を認証しアクセス・データを検証するように構成されている。電子回路はプロセッサと、データならびにプロセッサ用に必要とされるソフトウェアを格納するためのメモリ・ユニットを含む。ソフトウェアは施錠システム共有機密、アクセス・データの更新および鍵の認証に関する先に説明した処理手順を実行するように構成されている。

【０１１１】

図５の錠は更に、解錠命令を受けてその錠を機械的に解錠可能な状態に設定するように構成されている作動装置５１２を含む。作動装置は発電機５０６で産出された電力を給電されている。作動装置５１２は機械的に施錠状態にセットされるが、これの詳細な解説は、本実施例を明示するためには不要であろう。

【０１１２】

作動装置５１２がその錠を機械的に解錠可能状態に設定すると、例えばボルト機構５１４は鍵１１８を回転することで動かされる。必要な機械的力もまた、使用者が扉の取っ手またはノブ（図５には図示せず）を回転することにより発生される。その他の好適な回転機構もまた同様に使用できる。

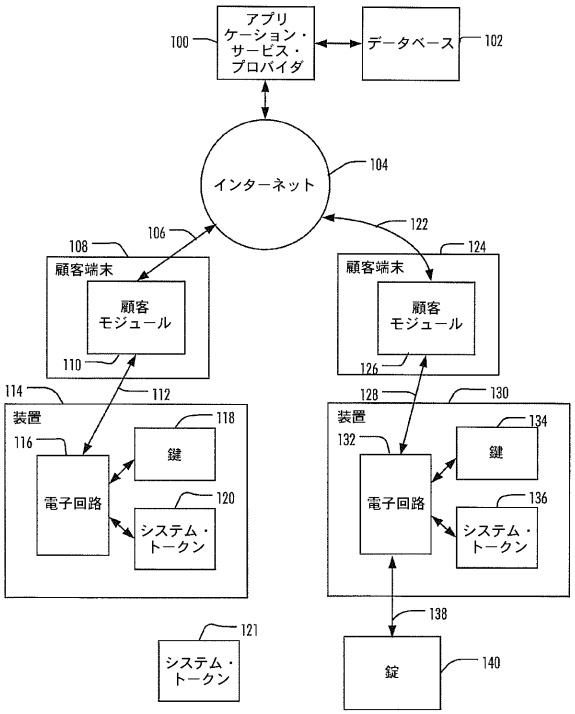
【０１１３】

上記のステップおよび関連する機能はその時間的順序は絶対的なものでは無く、いくつかのステップは同時にまたは指定されたものとは異なる順序で実施できる。その他の機能もまた、いくつかのステップ間またはステップの中で実行できる。いくつかのステップまたはステップの一部もまた省略するか、または対応するステップまたはステップの一部で置き換えることが出来る。

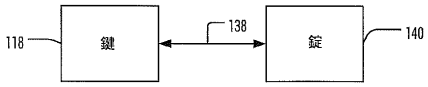
【０１１４】

当業者には明らかなように、技術の進歩に伴い、本発明の概念は種々の方法で実現できる。本発明およびその実施例は上記の例に制限されるものではなく、特許請求の範囲に入るものである。

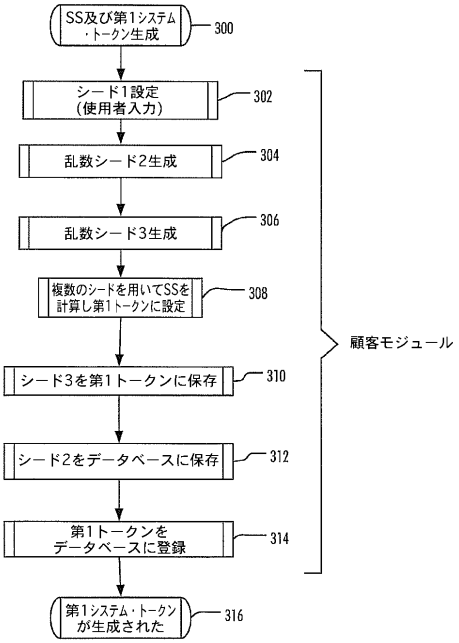
【図１】



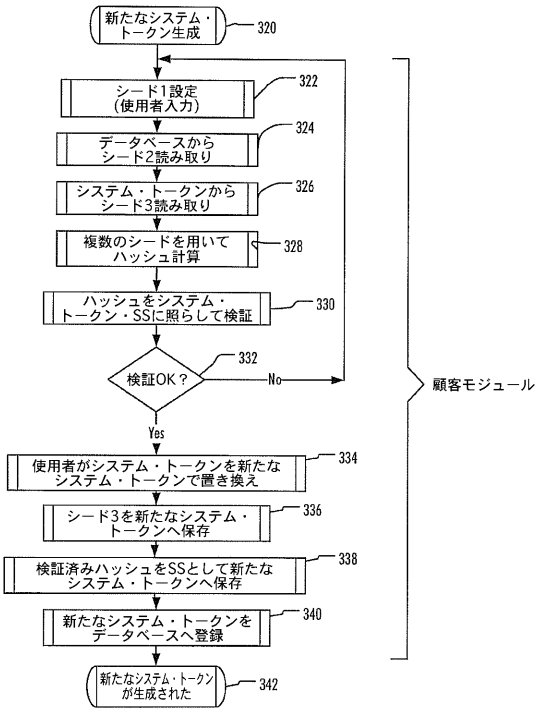
【図２】



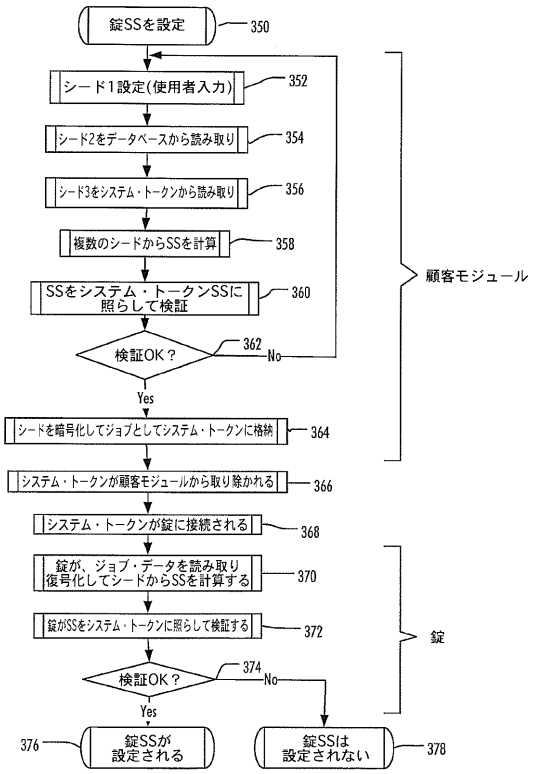
【図３Ａ】



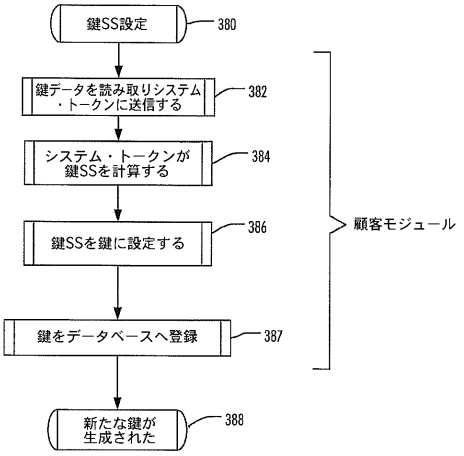
【図３Ｂ】



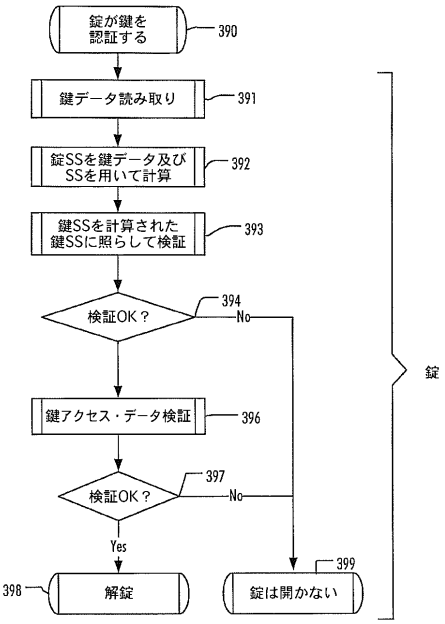
【図３Ｃ】



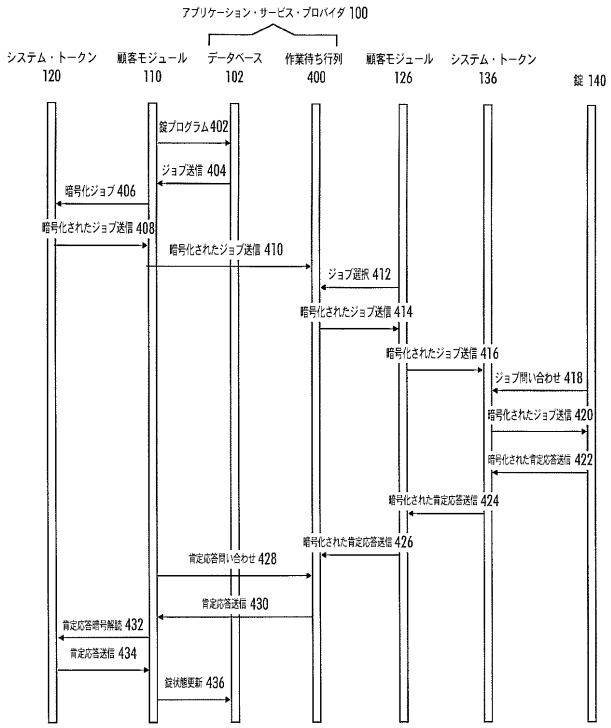
【図３Ｄ】


鍵SS設定
380
鍵データを読み取りシステム・トークンに送信する
382
システム・トークンが鍵SSを計算する
384
鍵SSを鍵に設定する
386
鍵をデータベースへ登録
387
新たな鍵が生成された
388
顧客モジュール

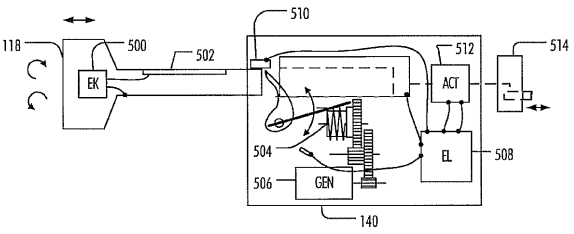
【図３Ｅ】


錠が鍵を認証する
390
鍵データ読み取り
391
錠SSを鍵データ及びSSを用いて計算
392
鍵SSを計算された鍵SSに照らして検証
393
検証OK？
394
No
鍵アクセス・データ検証
396
検証OK？
397
No
Yes
解錠
398
錠は開かない
399
錠

【図４】


アプリケーション・サービス・プロバイダ 100
システム・トークン 120
顧客モジュール 110
データベース 102
作業待ち行列 400
顧客モジュール 126
システム・トークン 136
錠 140
錠プログラム 402
ジョブ送信 404
暗号化ジョブ 406
暗号化されたジョブ送信 408
暗号化されたジョブ送信 410
ジョブ選択 412
暗号化されたジョブ送信 414
暗号化されたジョブ送信 416
ジョブ問い合わせ 418
暗号化されたジョブ送信 420
暗号化された肯定応答送信 422
暗号化された肯定応答送信 424
暗号化された肯定応答送信 426
肯定応答問い合わせ 428
肯定応答送信 430
肯定応答暗号解読 432
肯定応答送信 434
錠状態更新 436

【図５】


118
500
502
EK
510
512
514
ACT
504
506
GEN
EL
508
140

【手続補正書】
【提出日】平成22年5月27日(2010.5.27)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
自己給電式錠の錠管理システムであって：
各々が錠システムに関連する情報を格納するように構成された、１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバ、少なくとも１つの錠、少なくとも１つの顧客モジュール、第１装置および１つのシステム・トークン；を含み、
前記システム・トークンが鍵および錠をプログラムするための施錠システム機密を格納するように構成されおり；
前記少なくとも１つの顧客モジュールが、
暗号化および復号化用に共有機密を生成することによって、前記第１装置がシステム・トークンを用いて鍵をプログラムすることを制御し、
暗号化および復号化用に共有機密を生成することによって、前記第１装置がシステム・トークンを用いて錠アクセス・パケットをプログラムすることを制御し、
前記データ・パケットを公衆ネットワークを用いて前記ＡＳＰサーバに転送し、
暗号化された状態パケットを前記ＡＳＰサーバから公衆ネットワークを用いて受信し、
前記状態パケットの復号化を、システム・トークンを用いて制御し、
復号化された状態パケットに関する情報を前記ＡＳＰサーバへ公衆ネットワークを用いて送信するように構成されており；
前記ＡＳＰサーバが、
インターネットに接続され、
錠および鍵アクセス・データを格納し、一時的に錠アクセス・パケットおよび暗号化された状態パケットを格納するためのデータベースを保守するように構成されており、
少なくとも１つの錠が、
データ・パケットを前記ＡＳＰサーバから公衆ネットワーク経由で受信し、
前記データ・パケットをシステム・トークンを用いて復号化し、暗号化された状態パケットをＡＳＰサーバに公衆ネットワークを用いて送信するように構成されている、前記錠管理システム。
【請求項２】
請求項１記載の錠管理システムにおいて、顧客モジュールが錠が属している施錠システムに関する情報と前記錠のアクセス権に関する情報を含む、錠アクセス・データ・パケットを生成するように、前記第１装置を制御するよう構成されている、前記錠管理システム。
【請求項３】
請求項１記載の錠管理システムにおいて、顧客モジュールが錠を初期状態に戻すための命令を含む、錠アクセス・データ・パケットを生成するように、前記第１装置を制御するよう構成されている、前記錠管理システム。
【請求項４】
請求項１記載の錠管理システムにおいて、前記第１装置が、鍵、顧客モジュールと接続し、前記システム・トークンと通信するように構成されている、前記錠管理システム。
【請求項５】
請求項１記載の錠管理システムにおいて、錠と接続し、前記システム・トークンと通信するように構成されている第２装置を含む、前記錠管理システム。

【請求項６】
請求項５記載の錠管理システムにおいて、前記ＡＳＰサーバと公衆回線で接続し、前記第２装置と有線または無線接続で接続するように構成された、第２顧客モジュールを含む、前記錠管理システム。
【請求項７】
請求項６記載の錠管理システムにおいて、前記第２顧客モジュールが錠アクセス・データ・パケットを前記ＡＳＰサーバから受信し、前記錠アクセス・データ・パケットを前記第２装置経由で錠に転送するように構成されている、前記錠管理システム。
【請求項８】
請求項６記載の錠管理システムにおいて、前記第２顧客モジュールが暗号化された状態パケットを錠から前記第２装置経由で受信し、前記状態パケットを前記ＡＳＰサーバに転送するように構成されている、前記錠管理システム。
【請求項９】
請求項６記載の錠管理システムにおいて、前記第２顧客モジュールと前記ＡＳＰサーバとの間の接続は少なくとも一部分が無線である、前記錠管理システム。
【請求項１０】
請求項６記載の錠管理システムにおいて、該錠管理システムが第２顧客モジュールを携帯端末の中に含む、前記錠管理システム。
【請求項１１】
自己給電式錠用システムを管理するための方法であって：
暗号化および復号化用に共有機密を生成することによって、第１装置がシステム・トークンを用いて鍵をプログラムすることを、顧客モジュールによって制御し、
暗号化および復号化用に共有機密を生成することによって、第１装置がシステム・トークンを用いて錠アクセス・データ・パケットをプログラムすることを、顧客モジュールによって制御し、
生成された前記錠アクセス・データ・パケットを、前記システム・トークンを用いて暗号化し；
暗号化された前記錠アクセス・データ・パケットをＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバに公衆ネットワークを用いて転送し；
暗号化された前記錠アクセス・データ・パケットを前記ＡＳＰサーバ内に格納し；
暗号化された前記錠アクセス・データ・パケットを１つの錠により前記ＡＳＰサーバから公衆ネットワーク経由で読み取り；
前記錠アクセス・データ・パケットを前記錠の中で復号化し；
前記錠の中で暗号化された状態パケットを生成し、該状態パケットを前記ＡＳＰサーバへ転送し；
１つの状態パケットを前記ＡＳＰサーバから読み取り、顧客モジュールによる前記状態パケットの復号化を制御し；
復号化された前記状態パケットに関する情報を前記顧客モジュールから前記ＡＳＰサーバに転送する、ことを含む、錠管理方法。
【請求項１２】
請求項１１記載の方法が更に：
顧客モジュール内で、錠が属している施錠システムに関する情報と前記錠のアクセス権に関する情報を含む、錠アクセス・データ・パケットを生成することを含む、前記錠管理方法。
【請求項１３】
請求項１１記載の方法が更に：
顧客モジュール内で、錠命令「初期状態に復元」を含む錠アクセス・データ・パケットを生成することを含む、前記錠管理方法。
【請求項１４】

自己給電式錠用の錠管理システム内の１つの顧客モジュールであって：
暗号化および復号化のための共有機密の生成を制御し；
鍵データと前記共有機密から１つのシステム・トークンを用いて１つのユニークな鍵機密を生成し；
前記システム・トークンを用いて錠アクセス・データ・パケットを生成して暗号化し；
前記錠管理システムのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバと公衆ネットワークを用いて、錠システムに関する情報を通信するように構成されている、前記顧客モジュール。
【請求項１５】
自己給電式錠用の錠管理システム内の錠であって：
データ・パケットを、前記錠管理システムの１つのＡＳＰ（アプリケーション・サービス・プロバイダ：application service provider）サーバから受信し；
前記データ・パケットをシステム・トークンを用いて復号化し、共有機密を前記データ・パケット情報を用いて生成し、前記共有機密を格納し、暗号化された状態パケットを前記ＡＳＰサーバへ、公衆ネットワークを用いて送信するように、構成されている前記錠。
【請求項１６】
請求項１５記載の錠において、前記錠が：
鍵と通信し；
鍵データと前記共有機密からユニークな鍵機密を生成し；
前記生成された鍵機密が前記鍵内に格納されている鍵機密に対応する場合に前記鍵を認証するように構成されている、前記錠。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/FI2008/050529

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 602 536 A (HENDERSON WALTER G [US] ET AL) 11 February 1997 (1997-02-11) abstract column 1, line 30 - column 52, line 63 figures 1-29	1-18
X	EP 1 549 020 A (ACTIVCARD INC [US]) 29 June 2005 (2005-06-29) abstract paragraph [0006] - paragraph [0073] figures 1-3b	1-18
X	EP 1 653 415 A (IMMOTEC SYSTEMS [FR]) 3 May 2006 (2006-05-03) abstract paragraph [0008] - paragraph [0054] figures 1-6	1-18

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 March 2009	25/03/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pañeda Fernández, J

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FI2008/050529

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 132 871 A (SIMONS & VOSS GMBH [DE]) 12 September 2001 (2001-09-12) abstract paragraph [0002] - paragraph [0031] figures 1-3	1-18
A	EP 1 024 239 A (IBM [US]) 2 August 2000 (2000-08-02) paragraph [0008] - paragraph [0072] abstract figure 1	1-18
A	WO 2006/136662 A (MOHINET OY [FI]; KOLJONEN JOUNI [FI]) 28 December 2006 (2006-12-28) abstract paragraph [0002] - paragraph [0028] figures 1,2 claim 8	1-18
A	EP 1 249 797 A (ALLIED TELESIS K K [JP]) 16 October 2002 (2002-10-16) the whole document	1-18

3

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FI2008/050529

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5602536 A	11-02-1997	US 6842105 B1	11-01-2005
		US 2005168320 A1	04-08-2005
EP 1549020 A	29-06-2005	US 2005138380 A1	23-06-2005
		US 2008059798 A1	06-03-2008
EP 1653415 A	03-05-2006	FR 2877468 A1	05-05-2006
EP 1132871 A	12-09-2001	DE 10011035 A1	20-09-2001
EP 1024239 A	02-08-2000	AU 1793400 A	18-08-2000
		CA 2323146 A1	03-08-2000
		DE 69924349 D1	28-04-2005
		DE 69924349 T2	09-02-2006
		ES 2236973 T3	16-07-2005
		WO 0045016 A1	03-08-2000
		JP 3485254 B2	13-01-2004
		JP 2000224163 A	11-08-2000
		TW 462173 B	01-11-2001
		US 6981142 B1	27-12-2005
WO 2006136662 A	28-12-2006	EP 1897066 A1	12-03-2008
EP 1249797 A	16-10-2002	JP 3474548 B2	08-12-2003
		JP 2002314572 A	25-10-2002
		KR 20020079458 A	19-10-2002
		SG 114519 A1	28-09-2005
		TW 242735 B	01-11-2005
		US 2002145506 A1	10-10-2002

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100159525
弁理士 大日方 和幸
(74)代理人 100138346
弁理士 畑中 孝之
(74)代理人 100147658
弁理士 岩見 晶啓
(72)発明者 ロヒニヴァ、セッポ
フィンランド国、オウル、カンサンカトゥ ５７ シー ８３
(72)発明者 プカリ、ミカ
フィンランド国、オウル、トートリンティエ ５

Ｆターム(参考) 2E250 AA01 BB08 BB47 CC12 EE09 FF35 GG06