(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5064417号
(P5064417)

(45)発行日　平成24年10月31日(2012.10.31)　(24)登録日　平成24年8月17日(2012.8.17)

(51)Int.Cl.　　F I
G06K 17/00 (2006.01)　　G06K 17/00 T
G09C 1/00 (2006.01)　　G06K 17/00 E
　　G09C 1/00 660A

請求項の数 2　(全 14 頁)

(21)出願番号　特願2008-558669 (P2008-558669)
(86)(22)出願日　平成19年2月27日 (2007.2.27)
(65)公表番号　特表2009-529738 (P2009-529738A)
(43)公表日　平成21年8月20日 (2009.8.20)
(86)国際出願番号　PCT/EP2007/001677
(87)国際公開番号　WO2007/104423
(87)国際公開日　平成19年9月20日 (2007.9.20)
審査請求日　平成22年2月10日 (2010.2.10)
(31)優先権主張番号　102006011402.7
(32)優先日　平成18年3月11日 (2006.3.11)
(33)優先権主張国　ドイツ(DE)

(73)特許権者　504142961
バイエル・イノヴェイション・ゲゼルシャフト・ミット・ベシュレンクテル・ハフツング
Ｂａｙｅｒ　Ｉｎｎｏｖａｔｉｏｎ　ＧｍｂＨ
ドイツ５１３７３レーフェルクーゼン、カイザー－ヴィルヘルム－アレー２０番
(74)代理人　100101454
弁理士　山田　卓二
(74)代理人　100081422
弁理士　田中　光雄
(74)代理人　100125874
弁理士　川端　純市

最終頁に続く

(54)【発明の名称】機密情報を安全に処理する方法及び装置

(57)【特許請求の範囲】
【請求項１】
署名及び／又は暗号化方式を用いて、情報を安全に処理するシステム（１）であって、少なくとも、
一義的識別番号ＩＤＳ$_i$を有する第１の情報を読み出し可能に格納する移動可能で且つ受動的な第１の記憶部（２）と、
インデックスｉは、前記システム（１）に属する第１の記憶部（２）の番号を特定し、
情報を処理するために、前記第１の記憶部（２）と情報のやりとりを行う処理装置（３）と、
を有し、
前記処理装置（３）は、
一義的識別番号ＩＤＶ$_n$と、
インデックスｎは、前記システム（１）に属する処理装置（３）の番号を特定し、
前記第１の情報に対応する第２の情報を安全に格納する、外部から読み出されることが不可能で、操作が保護された第２の記憶部（６）と、
情報を処理する計算部（５）と、
前記第１及び／又は前記第２の記憶部（２，６）から前記計算部（５）に情報を送信し、且つ前記処理装置（３）と接続周辺装置（９）間で情報を送信する情報送信部（４）と、を有し、

秘密鍵ｔが属するグローバルな証明書＜ＴＣ＞が、外部から読み出すことが不可能で、操作が保護された前記第２の記憶部（６）に格納されており、
秘密鍵k_iが属する、前記グローバルな証明書＜ＴＣ＞から導き出される証明書$＜ＩＤＳ_i＞_t$が、前記システムに属する少なくとも１つの第１の記憶部$ＩＤＳ_i$（２）に格納されており、
Ｓ：＝Ｓｉｇ（ｍ，k_i）として鍵k_iを用いて情報ｍから生成された署名Ｓが、前記システムに属する少なくとも一つの第１の記憶部$ＩＤＳ_i$（２）に格納されている、ことを特徴とするシステム。

【請求項２】
請求項１に記載のシステム（１）を用いて、情報を安全に処理し／取り扱い／送信する方法であって、
情報送信部（４）により、第１の移動可能な記憶部（２）からシステム（１）の処理装置（３）の一つに情報を送信するステップと、
送信された情報が暗号化されている場合、操作が保護された第２の記憶部（６）に格納されている鍵Ｋを用いて、送信された情報を必要に応じて復号するステップと、
証明書$＜ＩＤＳ_i＞_t$が存在する場合、前記操作が保護された第２の記憶部（６）に格納されている証明書＜ＴＣ＞を用いて、前記証明書$＜ＩＤＳ_i＞_t$を必要に応じて調べるステップと、
署名Ｓ：＝Ｓｉｇ（ｍ，k_i）が存在する場合、前記証明書$＜ＩＤＳ_i＞_t$を用いて、前記署名Ｓ：＝Ｓｉｇ（ｍ，k_i）を必要に応じて調べるステップと、
署名Ｓ：＝Ｓｉｇ（ｍ，ｔ）が存在する場合、前記証明書＜ＴＣ＞を用いて、前記署名Ｓ：＝Ｓｉｇ（ｍ，ｔ）を必要に応じて調べるステップと、
情報送信部（４）により、前記システム（１）から接続周辺装置（９）に情報を送信するステップと、
を有することを特徴とする方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報、特に機密情報を安全に処理するシステム及び方法に関し、請求項１、１２、１３、１４の対応する前置き部分のシステム及び方法の使用に関する。

【背景技術】
【０００２】
情報、特に機密情報を安全に処理する、システム、方法及び／又は使用が一般的に知られている。

【０００３】
例えば、磁気ストリップカード、チップカード、又はスマートカードなどによる、時にはＰＩＮと組み合わせた、認証を介したアクセスのみを提供する、自動現金支払機などのアクセス制御システムが知られている。機密情報は、権限のない使用に対する保護として、他の情報（例えば、ＰＩＮ）の取り調べを必要とするカードに格納される。電子マネー取引のための磁気ストリップカード又はチップカードの場合、暗号化されたデータが格納される。磁気ストリップカードのような受動的カードの場合、これらのデータは、外部から、すなわち、別の読み取り装置により、復号される。能動的カードの場合、チップなどの計算部がカードに組み込まれている。この場合、情報はチップ上で復号化されうる。チップカードの悪用を防ぐために、チップへのアクセスは、例えば、ピン（pin）により、又は生体特徴を取り調べることにより、制御される。

【発明の開示】
【発明が解決しようとする課題】
【０００４】
磁気カード及びチップカードには、例えば、機械の又は電磁気の影響により、損害、汚染、又は他の障害を容易に受けやすいという欠点がある。また、磁気カード及びチップカ

ードは、カードの所定の寸法のせいで、非常に小さい限られた記憶容量しか持たない。磁気ストリップカードと比較すると、チップカードは、より大きな記憶容量を持ち、さらに、操作とコピーに対してより安全である。

【０００５】

以上により、現在、いくつかの認証方法はチップカードに限定されている。例えば、人が機密情報の信憑性とインテグリティを電子的に証明可能な署名カードは、チップカードとしてのみ製造されている。

【０００６】

しかし、チップカードは、製造するのに非常に費用がかかり、多くの場合、磁気ストリップカードなどよりも非常に高価である。

【０００７】

本発明は、広い分野の応用と様々な使用のために用いることができ、特に、一般の人々が容易に操作可能な、機密情報を安全に送信するシステム及び／又は方法を創造することを目的とする。

【０００８】

さらに、本発明は、大量のデータを確実に高速で送信可能で、障害の影響をほとんど受けず、不正使用又は不正利用を防ぐことが可能な、機密情報を安全に送信する、信頼性のあるシステム及び／又は方法を提供することを目的とする。

【０００９】

この目的は、請求項１の前置き部分に記載のシステムと、請求項１２及び／又は請求項１３の前置き部分に記載の方法とにより、達成される。

【課題を解決するための手段】

【００１０】

本発明は、署名及び／又は暗号化方式を用いて、情報、特に機密情報を確実に処理するシステムが、少なくとも、第１の情報を読み出し可能に格納する第１の移動可能で且つ受動的な記憶部と、情報を処理するために、第１の記憶部と情報のやりとりを行うように設計された処理装置と、を有し、処理装置が、第１の情報に対応する第２の情報を読み出し可能に格納する、復号が保護された第２の記憶部と、情報を処理する、好ましくは暗号化処理する計算部と、第１及び／又は第２の記憶部の情報を計算部に送信する情報送信部と、を有するという、技術的教示を含む。

【００１１】

以下、処理は、一般的に、入力、処理、出力（格納）のＩＰＯ（Ｓ）原則に従った処理のことを意味するものと理解される。より一般的には、これは、取り扱い情報と呼ばれる。

【００１２】

情報は、具体的には、全ての情報であると理解されるが、特に、不正なアクセスから保護されなければならない情報、すなわち、一般的に機密情報及び／又は秘密情報のことを言う。機密情報及び／又は秘密情報は、診断された病気のパターン、治療、銀行取引データなどの金融データを含む、個人データである。

【００１３】

第三者による不正なアクセスから情報を保護し、及び／又は情報のインテグリティ及び／又は信憑性を調べるために、署名及び／又は暗号化方式が処理するために提供される。

【００１４】

情報を処理するシステム又は装置は、少なくとも、第１の情報を読み出し可能に格納する第１の移動可能な記憶部を有する。第１の記憶部は、相応じて物又は人に関連し、物又は人により管理され、そこに格納される。第１の記憶部は、物又は人と共に移動可能な、移動式に適応している。必要に応じて対応する装置により読み出しが可能なデータ又は情報が、移動可能な第１の記憶部に格納される。情報は、例えば、１対の鍵である秘密鍵などの電子式鍵、及び／又は署名又は電子署名を含む。さらに、情報は、他人のアクセスから保護されなければならない又はアクセスできないようにして格納されなければならない

データを含むことができる。これは、例えば、銀行口座データ、臨床データ、及び識別データなどである。好ましくは、この情報は、対応する鍵で暗号化され及び／又は署名される。

【００１５】

必要に応じてこの情報を処理することができるように、システム内に処理装置が設けられる。処理装置は、秘密情報を処理装置により読み出せるように又は第１の記憶部に格納できるように、第１の記憶部と情報のやりとりを行う。

【００１６】

処理装置は、少なくとも一つの第２の記憶部を有する。第２の記憶部は、好ましくは、復号に対して安全となるように適合している。これは、例えば、許可なしではアクセスできない密封容器などの物理的な保護により、及び／又はデータ保護などの他の保護装置により、実行されうる。

【００１７】

第２の記憶部には、第２の情報が格納される。第２の情報、具体的には、第２の機密及び／又は秘密情報は、第１の記憶部の第１の情報に対応している。例えば、第２の情報は、一対の鍵を形成するために、第１の記憶部の鍵に対応する計数鍵を含むことができる。さらに、第１の記憶部のデータに対応する認証についての関連データが、第２の記憶部に格納されうる。

【００１８】

暗号化及び／又は署名される第１の情報の少なくとも一部を処理するために、これは最初に復号化されなければならない、及び／又は署名が調べられなければならない。そのため、処理装置は、処理、具体的には、情報を暗号化処理する計算部を有する。この計算部は、第１の記憶部のキャリヤにより実行されなければならない処理が実行されうるように、少なくとも部分的に暗号化及び／又は署名されたデータを処理する。

【００１９】

また、第１及び／又は第２の記憶部から計算部に情報を送信するために、情報送信部が設けられる。情報送信部は、対応情報を安全に送信するために用いられうる。

【００２０】

記憶部の少なくとも一つは、秘密情報、具体的には第１の情報が非電子的に記憶部に格納され及び／又は記憶部から読み出されうるような、非電子記憶部として構成されることが好ましい。非電子記憶部は、例えば、磁気又は光学式の記憶部を含む。

【００２１】

特に、記憶部の少なくとも１つは、秘密情報、具体的には第１の情報が光学的に格納され及び／又は読み出されうる記憶媒体として、光でアドレス可能なポリマー基を含む光学式記憶部として構成されることが好ましい。

【００２２】

光でアドレス可能なポリマーは、指向的な複屈折が光により物質に書き込まれるという事実により区別される種類の物質を形成する（Polymers as Electrooptical and Photooptical Active Media, V.P. Shibaev (編集者), シュプリンガー出版社（Springer Verlag）, ニューヨーク, 1995; Natansohn et al., Chem. Mater. 1993, 403-411）。これらの光でアドレス可能なポリマーとして、例えば、US-A 5,173,381に記載のアゾベンゼン官能基側鎖を備えたポリマーがある。

【００２３】

情報の光学式記憶によって、これは確実に配置され、外的影響から十分に保護され、非常に小さなスペースで多量であり得る。具体的には、光学的に記憶された情報は、磁場又は電気誘導などの影響から安全に置かれる。光学式記憶により、記憶する量に対する容量の比率が最適になる。さらに、光学式記憶部は、チップなどの電子記憶部よりも、より有利に生産される。よって、光学式記憶は、価格に対する容量の比率を最適にすることができる。

【００２４】

記憶部の少なくとも一つは、チップカード、ストレージカード、スマートカードの群の中から選択されたカードの形式で構成されることが好ましい。カードとして設計することにより、容易に取り扱い、メモリを移動可能にすることができる。好ましくは、カードは、日常使用されている他のカード、例えばクレジットカードと同一の寸法を持つ。このようにカードを形成することにより、この目的のために特別な記憶部を生成する必要なく、例えば、財布などの中で簡単に持ち続けることができる移動可能なメモリを実現できる。それ故、カードのフォーマットは、ＩＳＯ／ＩＥＣ７８１０規格で規定されているＩＤ－１であることが好ましい。このフォーマットは、好ましくは、従来のリーダなどでも使用されうる。

【００２５】

カード及び／又は移動可能な記憶部にできるだけ多くの情報及び／又はデータを格納するために、記憶部の少なくとも１つは、好ましくは０．５メガバイト、より好ましくは１．０メガバイト、さらに好ましくは１．５メガバイトより多くの記憶容量を有することが好ましい。磁気ストリップ、チップなどの従来のメモリは、非常に限られた数の情報項目を格納するためだけの、より小さな記憶容量を持っている。そのため、格納できる情報は少ししかない。より多くの情報を格納することができない。本発明の好ましい記憶容量を用いて、できる限りより念入りに暗号化された、より大量のデータが格納されうる。

【００２６】

大記憶容量を確保するため、記憶部、具体的には第１の移動可能な記憶部を形成するのに用いられる記憶媒体は、ポリマーとして、具体的には、光でアドレス可能なポリマー基のポリマーとして、適している。

【００２７】

具体的には、情報は、移動可能なメモリにホログラフ的に、特に、好ましくは、１以上の偏光ホログラムとして、格納されうる。情報のホログラフィック記憶により、さらなる人による権限のない処理、例えばコピーや他の操作からの効果的な及び改善された情報の保護が実現される。

【００２８】

ホログラフィック記憶は、アナログの記憶方法である。すなわち、情報は、第１の移動可能なメモリにアナログ形式で存在する。

【００２９】

第１の移動可能なメモリに格納される機密情報は、好ましくは、移動可能なメモリに格納される前及び／又は移動可能なメモリから読み出された後、デジタル形式で存在する。

【００３０】

移動可能なメモリに格納される前及び／又は移動可能なメモリから読み出された後、好ましくは、機密情報は暗号化され及び／又は署名される。

【００３１】

好ましい実施形態において、記憶部の少なくとも１つ、好ましくは第２の記憶部は、情報がデジタル的に格納され及び／又は読み出される、デジタル記憶部として構成される。情報は、好ましくは、対応する記憶部、具体的には第２の記憶部に、記憶スペースの関係で最後ではなく、デジタル的に格納される。デジタルの秘密情報は、好ましくはデジタル的に暗号化及び／又は署名される。機密情報が署名される場合、署名は好ましくは機密情報と共に記憶部に格納される。これにより、記憶部の少なくとも１つ、好ましくは第２の記憶部は、暗号化が可能な記憶部として構成されることが好ましい（第１の秘密情報が、暗号化されて、該記憶部に格納され及び／又は該記憶部から読み出されうる）。

【００３２】

多量の情報を格納するために、対応する記憶部は、好ましくは、受動的メモリとして構成される。特に、移動可能な記憶部は、多量の情報を格納する。よって、受動的記憶部は、対応するアルゴリズムにより、情報の計算、処理、復号などが能動的に実行される領域を持たない。

【００３３】

一方、情報を処理するためのアルゴリズムが第２の記憶部に格納されうるため、大部分が第２の記憶部に格納される情報はあまりない。よって、第２の記憶部は、能動的記憶部であることが好ましい。従来のシステムにおいては、移動可能な記憶部が能動的メモリとして構成されるか（チップカード）、又は移動可能な記憶部が非常に小さな安全なメモリを持っている（ホログラフィックメモリカード）。

【００３４】

第１の移動可能なメモリを大記憶容量を備えた受動的で安全なメモリとして構成し、第２のメモリを能動的メモリ又は能動的記憶部として構成することにより、安全で頑丈で費用効率が高いシステムが形成される。具体的には、第２の記憶部は、第２の情報が電子的に格納され及び／又は読み出されうる電子記憶部であることが好ましい。磁気又は非電子記憶部としての構成と対照的に、特に機密情報とアルゴリズムは、好ましくは電子的に電子記憶部に格納され、計算部との対応する通信が、問題なく、例えば、アナログ／デジタル変換器を間に挟むことなく、実行されうる。

【００３５】

好ましい実施形態では、第１のメモリは光メモリ、すなわち、受動的メモリとして構成され、第２のメモリは電子メモリとして構成される。第２のメモリは計算部に接続されるため、対応する第２のメモリを備えたカードは、能動的記憶カードと呼ばれる。

【００３６】

それ故、情報は、光学的に、好ましくはホログラフ的に第１のメモリに格納される。その後、情報送信部によりデータを第２の電子記憶部に送信するために、データはアナログ形式から電子又はデジタル形式に変更されなければならない。このため、光源が、情報送信部として、カメラと併用して使用される。第１の記憶部のホログラムは、光源により照らされる。ホログラムでの光ビームの回折により、格納された情報の画像が生成される。このように生成された画像（機密情報を含む。）は、カメラによりとらえられ、その結果、そこで画像化される。カメラは、光信号から第２の記憶部に対応する電子信号又はデジタル信号を生成する。

【００３７】

機密情報を処理するため、第２のメモリが第１の計算部に接続される。第１の計算部は、単独で第２のメモリの情報にアクセスする。権限のない人が、第２のメモリに蓄積された情報を外部から読み出す及び／又は操作する実現性はない。データが両者間で送信されるように、第２の記憶部と通信できるのは第１の計算部のみである。

【００３８】

第１の計算部は、情報を暗号及び復号し又は署名する暗号機能を有する。具体的には、その機能は、署名を生成及び／又は調べる実現性を含む。第２の記憶部が権限のない人によるアクセスから保護されるのと同時に、第１の計算部もまた権限のない人によるアクセスから保護される。

【００３９】

計算部、第２の記憶部、及び情報送信部は、一つのユニット又は一つの設備において、計算部と第２のメモリ間で、データを交換するのに適していることが好ましい。このユニットを用いて、情報は、第１と第２のメモリ間で交換されうる。

【００４０】

計算部は、スマートカードやチップカードの形式で、第２の記憶部に一体化されて構成されることが好ましい。不正操作を防ぐために、計算部と記憶部のユニットは、好ましくは、例えば「一般基準」、具体的にはＥＡＬ４＋以上を達成する基準に従った証明書と共に提供される。これにより、非常に高いセキュリティが実現される。

【００４１】

上述したように、移動可能な第１のメモリと第２のメモリ間の情報送信部は、少なくとも１つのビーム経路を介して、情報を送信するために、光学式情報送信部として構成されることが好ましい。

【００４２】

計算部は、少なくとも１つの伝送チャネル（該チャネルを介して、他の計算部との間で情報が送受信される。）を有することが好ましい。

【００４３】

伝送チャネルは、好ましくは、保護されたチャネルとして適合される。保護されたチャネルは、暗号化されたチャネルでありうる（論理保護）。しかしながら、保護されたチャネルは、例えば、監視環境に配置され、又はアクセスできないため、権限のない人が外部から攻撃できないようなチャネルであることも可能である（物理保護）。

【００４４】

異なる計算部間でデータを交換するために、データ交換の前に、計算部は互いに認証しなければならない。

【００４５】

情報送信部は、好ましくは、書き込み部及び／又は読み出し部として構成されうる。

【００４６】

好ましい実施形態では、光学式情報送信部が、少なくとも１つのビームにより光学的に情報を送信するために、レーザ群を含む偏光を放射するように構成される。

【００４７】

他の計算部（例えば、セキュリティを増加させる計算部）を提供することが可能であるのと同時に、第１及び／又は第２の情報に対応する第３の情報を格納するための第３の記憶部がさらに設けられることが好ましい。これにより、例えば、虹彩スキャン、ＰＩＮの入力、指紋などの他の生物測定データの取得の形式で、さらなるセキュリティの取り調べを実行することが可能となる。

【００４８】

種々のユーザの鍵の番号及び／又は証明書などを管理するために、鍵の番号及び／又は署名を管理する鍵管理部がさらに設けられることが好ましい。

【００４９】

また、本発明は、情報の安全な暗号処理、取り扱い、及び／又は伝送の方法を提供する技術的教示を含む。その方法は、第１の暗号化された情報を第１の受動的で移動可能なメモリ上から読み出す及び／又は第１の受動的で移動可能なメモリ上に格納するステップと、第１の情報に対応する第２の情報を読み出す及び／又は格納するステップと、第１の暗号化された情報を計算部に送信するステップと、第２の情報を計算部に送信するステップと、計算部の第２の情報により、第１の情報を暗号化処理するステップと、を含み、第１の情報の読み出し及び／又は格納ステップ、及び／又は第１の情報の送信ステップは、少なくとも部分的に非電子式で実行される。

【００５０】

具体的には、秘密情報を処理する本発明の方法は、以下の本文に記述されたステップを含む。

【００５１】

情報、特に移動可能なメモリに予め格納されている機密情報は、情報送信部により、第１の移動可能なメモリから第１の計算部に送信される。情報がデジタル的に暗号化されている場合、その情報は、第１の計算部と、第２のメモリに格納された情報、例えば、暗号化鍵とにより、復号される。情報が署名されている場合、署名が相応じて調べられる。

【００５２】

具体的には、第１の移動可能なメモリ内の情報は、対称暗号化システムにより暗号化されている。このため、例えば、ＡＥＳ等の種類の暗号化方法が用いられうる。署名のために、好ましくは、電子暗号化の標準の手順が用いられる。このため、例えば、ＲＳＡ又はＥＣＤＳＡ（Elliptic Curve Digital Signature Algorithm）タイプの方法が用いられうる。

【００５３】

「第１の情報の読み出し及び／又は格納」ステップ及び／又は「第１の情報の送信」ステップは光学的に実行されることが好ましい。この方法において、送信は、伝送速度とデ

ータの機密保護に関し最適化されて実行されうる。

【００５４】

本発明の方法のステップの少なくとも１つは、デジタル的に実行されることが好ましい。デジタル処理は、Ａ／Ｄ変換器を必要とせず、コンピュータにより容易に処理できるという利点をもたらす。これは、より簡易な構成とより簡易な方法の実行を可能にする。

【００５５】

権限のある立場の人だけが情報をアクセスできるようにするため、「読み出し及び／又は格納」ステップ及び／又は「送信」ステップの少なくとも１つは、暗号化されて実行されることが好ましい。これにより、高度なデータセキュリティが確保される。光学的なデジタル処理の場合、特に、暗号化は、この方法を用いて非常に秘密の情報が処理されうるような、最高度のデータセキュリティを達成する。全体的に、この方法を用いることにより、データセキュリティにおいて、非常に高度なセキュリティを達成することができる。

【００５６】

第１の情報は、光学的に送信可能な形式で利用できることが好ましい。さらに、「読み出し及び／又は格納」ステップ及び／又は「第２の情報の送信」ステップは、電子的に実行されることが好ましい。不正アクセスから保護される第２の情報は、いずれの場合でも、一般に、移動可能な記憶部に格納されることはない。これにより、計算部により容易に処理されうる。このため、特に、従来から既に知られているメモリ及び／又は処理媒体は、本発明の対応する応用に適した各ケースにおいて、用いられうる。

【００５７】

第２の情報の「読み出し及び／又は格納」ステップと暗号処理ステップは、一構成部品において実行されることが、特に有利である。この方法では、暗号及び復号に必要な装置が、一構成部品内でスペースを取らない方法で提供されうる。この構成部品は、外部からの又は第三者によるアクセスに対して、相応じて保護される。これらのステップが一構成部品において実行されるという事実によって、時間のかからない送信媒体が、データを送信するために提供される必要がある。一構成部品に一体化することにより、望まれないアクセスから保護されなければならないのは、この一構成部品のみとなる。

【００５８】

情報の有効な保護又は認証を行うために、情報は、署名されるか及び／又は暗号化されて提供される。これにより、「読み出し及び／又は格納」ステップは、「署名及び／又は鍵データの読み出し及び／又は格納」ステップを含む場合に有利になる。署名及び／又は鍵データは、移動可能な記憶部などの種々の記憶部で保管されうる。データがホログラフ的に格納される場合、署名と鍵の読み出しを少なくともほとんど不可能にする、高水準のセキュリティが実行されうる。

【００５９】

特に、ホログラムは第三者が容易に又は簡易な方法で読み出すことができないため、偏光ホログラムを含むホログラムとして、秘密情報が読み出し及び／又は格納されるとき、これらは望まれていない又は望ましくないアクセスから最適に保護される。

【００６０】

さらに、ホログラムとしての記憶は、操作及び／又はコピーに対して有効な保護を提供する。

【００６１】

できるだけ多くのユーザの情報を管理するため、好ましくは、ユーザの情報の全てが署名され、又は対応する個々の鍵で暗号化されうる。特に、機密情報は、鍵管理により管理されることが好ましい。鍵管理は、本発明の構成部品である。

【００６２】

特に機密情報の安全な処理が確実となるように、鍵管理において、鍵と証明書は定義され、選択され、及び／又は導かれ、及びシステムの種々の構成部品に割り当てられる。さらに、鍵管理は、鍵及び／又は証明書の完全な交換を必要とせずに、構成部品がシステムから取り除かれ及び／又はシステムに統合されうることを確実にする。

【００６３】
鍵の選択と鍵の割り当てのために、構成部品群は、最初に、構成部品の全てがシステムに属するように定義される。各システムにおいて、複数の移動可能なメモリと、移動可能なメモリ用の少なくとも１以上の読み出し／書き込み装置とがある。読み出し／書き込み装置は、それぞれ、計算部と併用して、既に記述した第２のメモリの形式の少なくとも１つのメモリを含む。
【００６４】
このようなシステムは、例えば、アクセス制御適用のために、使用人カードを全ての使用人に発行する会社である。この場合、使用人カードと読み出し／書き込み装置とが、システムに属する構成部品となる。
【００６５】
また、システムは、例えば、銀行のカードを顧客に発行する銀行である（移動可能なメモリ）。この場合、銀行のカードと読み出し／書き込み装置とが、システムに属する構成部品となる。
【００６６】
システムのために、グローバル鍵Ｋがある。この鍵は、（システムの各読み出し／書き込み装置の）第２のメモリに安全に格納される。システムに属する各移動可能なメモリ（$ＩＤ_i$）に対して、唯一の鍵$Ｋ_i$＝ｆ（Ｋ，$ＩＤ_i$）が導き出される。ここで、ｆは鍵導出関数である。秘密情報は、第１の移動可能なメモリ上で鍵$Ｋ_i$で暗号化される。復号中、$Ｋ_i$で暗号化されて移動可能なメモリに格納された情報は、情報送信部により、第１の計算部に送信され、第２のメモリに保管されている鍵Ｋを用いて復号される。
【００６７】
また、システムは、例えば、信託センター（ＴＣ）により発行されたグローバルな証明書＜ＴＣ＞を持っている。＜ＴＣ＞証明書は、秘密鍵ｔを含む。グローバルな証明書は、（システムの各読み出し／書き込み装置の）第２のメモリに格納される。移動可能なメモリ$ＩＤ_i$毎に証明書$＜ＩＤ_i＞_t$がある。情報ｍの信憑性及び／又はインテグリティを立証するために、情報ｍは、対応する秘密鍵$ｋ_i$を用いて、移動可能なメモリにおいて、Ｓ：＝Ｓｉｇ（ｍ，$ｋ_i$）として署名される。証明書と共に署名Ｓは、移動可能なメモリに格納される。署名のチェック中、データｍ、署名Ｓ、及び証明書$＜ＩＤ_i＞_t$は、情報送信部により、移動可能なメモリから第１の計算部に送信される。第１の計算部と第２のメモリに格納されたグローバルな証明書＜ＴＣ＞により、証明書$＜ＩＤ_i＞_t$が最初に照合される。それから、署名Ｓが、証明書$＜ＩＤ_i＞_t$により照合される。全ての照合が成功すると、署名は受諾される。
【００６８】
本発明のさらなる実施形態では、より高いレベルのユニット（ＴＣ）は、秘密鍵ｔを用いて、直接データｍを署名する。これは、生物測定アクセス制御などのために重要でありうる。この取り決めの場合、より高いレベルのユニットは、最初に、移動可能なメモリに格納される情報が、実際にそこに属するかどうかを調べる。生物測定アクセス制御の場合、より高いレベルの組織が、識別カード（移動可能なメモリ）に格納される生物測定データ（情報ｍ）が、そのカードの所有者に実際に属するかどうかを調べ、正当性に署名する。
【００６９】
その後、上述した署名についてのシステムは、情報ｍがＳ：＝Ｓｉｇ（ｍ、ｔ）として署名されるように変更される。署名Ｓは、データｍと共に、移動可能なメモリに格納される。それは、＜ＴＣ＞を適用することにより、照合されうる。
【００７０】
最初に情報に署名し、それからデータと署名を暗号化することと、最初にデータを暗号化し、それから暗号化されたデータを署名することの両方が可能である。
【００７１】
上述したように、第１の計算部が、伝送チャネルを介して、他の計算部に接続されるこ

とが考えられる。これらのさらなる計算部は、機密情報の安全な送信と結び付いていることは、特に関心のあることである。この場合、他の計算部は、より高いレベルの装置と呼ばれるシステムに属する。

【００７２】

システムには、対応する秘密鍵ｇと共に、グループ証明書＜Ｇ＞がある。グループ証明書＜Ｇ＞は、システムに属する各装置に格納される。識別番号$ＩＤ_i$の各装置は、秘密鍵ｇで署名された証明書$＜ＩＤ_i，Ａ_i＞_g$を有する。それは、装置の種類（例えば、生物測定取得システム、データベース）についての情報を提供しうる属性$Ａ_i$を含む。暗号化されたチャネルを介して、互いに通信する２つの装置は、証明書を交換する。それらは、＜Ｇ＞を適用することにより、証明書$＜ＩＤ_i，Ａ_i＞_g$の署名を照合し、属性を照合する。署名がエラーなく調べられたときのみ、安全な送信経路が装置間に設けられる。

【００７３】

有効期間を制限して証明書$＜ＩＤ_i，Ａ_i＞_g$を提供することが好ましい。証明書は、交換が簡単にできるように、例えば、スマートカードの形式で、装置に導入されうる。

【００７４】

証明書の有効性が満期になった後、鍵は更新される。スマートカードの場合、装置のスマートカードを交換することにより、これは簡単になされる。

【００７５】

安全な情報交換から装置を除外するために、それらはブロックされる。各装置は、無効になった証明書のリスト（ＣＲＬ）を有する。これらの証明書は、グループ証明書又は装置証明書でありうる。グループ証明書の場合、グループ全体の装置がブロックされ、装置証明書の場合、個々の装置がブロックされる。無効になった装置についてのブロックリストは、各装置にロードされなければならない。ブロックリストは、上述の証明書＜ＴＣ＞などのグローバルな証明書で署名される。それから、ブロックリストは、署名Ｓｉｇ（ＣＲＬ，ｔ）と共に、装置にロードされる。その結果、アタッカーが盗んだ装置を使用して、秘密情報にアクセスする可能性を持たないように、アタッカーにより盗まれた装置は、ブロックされうる。

【００７６】

また、ブロックリストは更新されうるか、又は中央サーバに問い合わせを行うことにより、取り調べられうる。サーバでは、今調べている証明書についてのエントリがあるかどうかが、チェックされる。

【００７７】

本発明によるシステム及び／又は本発明による方法は、具体的には、
アクセス制御システム、
入口制御システム、
自動現金支払システム、
識別システム、
医療データ（健康手帳など）管理システム、
として及び／又はその中で使用されることが好ましい。

【００７８】

さらに、好ましい特徴が、従属形式の下位請求項又は下記の図面により、より詳細に記述される。

【発明を実施するための最良の形態】

【００７９】

図１は、情報、特に本発明による機密情報を処理する、本発明のシステム１を図式的に示している。システム１は、記憶部２を有する。記憶部２は、ここでは、移動可能な記憶部として、特に、移動可能な受動的記憶部として構成される。記憶部は、任意の形式で構成されうるが、ここではメモリカード（対応する箱内に象徴的に示されている。）として構成される。この場合、記憶部２は、情報又はデータを光学的に格納するように構成される。格納される情報は、秘密情報又は機密情報である。具体的には、秘密情報又は機密情

報は、生物測定データ及び／又はエラー訂正データを含む署名データを含む。データは、記憶部２にホログラフ的に置かれ及び／又はデジタル的に暗号化される。

【００８０】

記憶部２に加えて、システム１は、処理装置３（破線で図示されている。）を有する。処理装置３は、記憶部２と情報のやりとりを行い、具体的には、記憶部２からの読み出し及び／又は記憶部２への書き込みができるように、構成される。記憶部２から処理装置３への矢印とその逆の矢印は、記憶部２からのデータの読み出し及び書き込みを図示している。

【００８１】

記憶部２からの情報を送信するために、処理装置３は第１の情報送信部４を有する。第１の情報送信部４は、ここでは、信号処理に適したセンサ部（カメラ）４ａを含む。情報送信部は、一般的に、異なるユニットや構成要素間の全ての送信手段を含む。第１の情報送信部４ａへの対応する矢印により図示され、そこからそれぞれ離れているように、第１の情報送信部４とセンサ部４ａは、それぞれ情報を送信するために使用される。

【００８２】

さらに、システム１は、情報を暗号化処理する計算部５を有する。このため、データ又は情報は、センサ部４ａから又はさらに一般的には第１の情報送信部４から、計算部５に送信され、それぞれそこから離れる。

【００８３】

システム１は、第２の記憶部６をさらに有する。第２の記憶部６は、復号から保護されように構成され、第１の情報に対応する第２の情報を読み出し可能に格納するために使用される。具体的には、第１の情報と共に、アクセス又はエントリを提供する、さらなるセキュリティ関連データがある。他の物のうち、第２の記憶部は、機密情報を復号するための対応鍵が格納される領域６ａを有する。その領域内で読み出されうる他のデータは、復号、署名、ＭＡＣ（メッセージ認証コード）のためのデータ、又は、暗号又は認証などの他の使用におけるデータでありうる。

【００８４】

第１の記憶部２から読み込まれるデータに対応する対応データは、第２の記憶部６又は６ａから計算部５に、安全な第２の情報送信部７を介して送信される。情報送信部７は、通信の監視及び／又は交換されるデータの操作が可能にならないように、アタッカーに対する効果的な保護メカニズムを有するように構成される。

【００８５】

図１において、計算部５は、例えば、２つのモジュール５ａ、５ｂからなるように構成される。モジュール５ａが暗号計算を行うのに対して、モジュール５ｂは全シーケンスを制御し、他の接続要素（８，９）との通信に関与する。

【００８６】

移動可能な記憶部２の対象とするキャリヤの個人入力によるさらなる保護を確立するため、システム１は移動可能な記憶部２の対象とするキャリヤとの外部通信を提供する。このため、システムは、処理装置において、外部通信のためのインターフェース８を有する。

【００８７】

第１のインターフェース８ａは、キャリヤを照合するのに使用される入力要求又は問い合わせを入力し及び表示するために用いられる。ここでは、この第１のインターフェース８ａは、ディスプレイとして構成される。ディスプレイは、例えば、個人識別番号（ＰＩＮ）を入力させる入力要求を表示する。

【００８８】

第２のインターフェース８ｂは、処理装置３のユーザによる情報入力のために使用される。この第２のインターフェース８ｂは、ここでは、カーソルの移動による入力制御の可能性を備えた数値入力として実行される。処理装置３のユーザは、制御パラメータ又はＰＩＮなどの個人データをこの入力又は入力部を介して、入力することができる。

【００８９】
第１のインターフェース８ａは、計算部５に、より正確には、安全な第２の情報送信部７を介して第２のモジュール５ｂに、一方向に接続される。その方向は、第２のモジュールから第１のインターフェース８ａに向いている。
【００９０】
第２のインターフェース８ｂは、計算部５に、より正確には、安全な情報送信部７を介して第２のモジュール５ｂに、一方向に接続される。その方向は、第２のインターフェース８ｂから第２のモジュール５ｂに向いている。
【００９１】
図１に示すシステム１は、システムの中核を形成する移動可能な記憶部２と処理装置３の他に、データ又は情報が対応する接続を介して交換可能となる、他の周辺装置９又は接続システムを有する。この周辺装置９は、生物測定の取得と情報の整合のための第１の接続システム９ａを備えることが可能である。このため、第２のモジュール５ｂは、制御信号を送信するために、第１の接続システム９ａに双方向に接続される。一方、第２のモジュール５ｂは、生物測定データを送信し、照合の結果を送り返すために、安全な接続を介して、第１の接続システム９ａに双方向に接続される。安全な接続は、外部からアタッカーにアクセスできない接続である。第１の接続システム９ａは、例えば、虹彩スキャン装置、又は指紋、虹彩パターン、声などの生物測定データを検出する他の装置でありうる。
【００９２】
さらに、周辺装置９は、第２の接続システム９ｂを備えることができる。この第２の接続システム９ｂは、例えば、コンピュータネットワーク、又は単にサーバを含む、データベースでありうる。データベースには、照合後ユーザにより読み出し可能な対応情報が格納されうる。第２の接続システム９ｂは、処理装置３、より正確には、安全な又は簡易な接続を介して、第２のモジュール５に接続される。データ又は情報Ｍは、これらの間で送信される。機密情報を交換する場合、接続は、安全な第２の情報送信部７として構成される。無批判（uncritical）な情報を交換する場合、簡易な第１の情報送信部４が選択されうる。
【００９３】
さらに、周辺装置９は、第３の接続システム９ｃを備えることができる。第３の接続システム９ｃは、情報又はユーザの照合又は認証後にアクセスを許可するドアロックなどのアクセスとして構成されうる。第３の接続システム９ｃは、双方向接続を介して、計算部５に接続される。アタッカーがアクセスを開放するために外部からのアクセスとして構成される接続システム９ｃに信号を送信することを防ぐために、好ましくは、接続システム９ｃは、安全な接続７を介して、計算部５に接続される。
【００９４】
さらに、周辺装置９は、第４の接続システム９ｄを備えることができる。第４の接続システム９ｄは、例えば、時間の取得又は時間が限られたアクセスを許可する、時間処理装置でありうる。第４の接続システム９ｄは、安全な接続を介して、計算部５に双方向に接続される。他の物のうち、時間情報が送信される。
【００９５】
機密情報を交換する場合、接続は、それぞれ安全な接続又は第２の情報送信部７として、構成される。無批判な情報を交換する場合、簡易接続又は第１の情報送信部４が選択されうる。
【００９６】
周辺装置９は、一般に、各ケースにおいて、接続システム９ａ～９ｄのうち一つだけを含むこともできるし、又は接続システムの任意の組み合わせを含むこともできる。
【図面の簡単な説明】
【００９７】
【図１】署名及び／又は暗号化方式を用いて情報を処理する、本発明のシステムを図式的に示す図

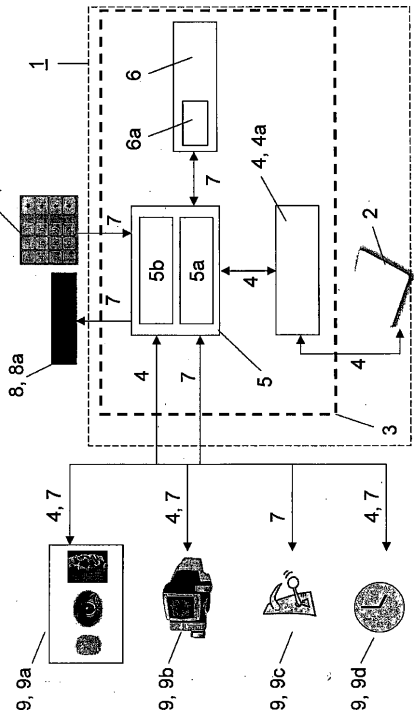
【符号の説明】

【００９８】

１　　システム
２　　第１の記憶部
３　　処理装置
４　　第１の情報送信部
４ａ　カメラ
５　　計算部
５ａ　第１のモジュール
５ｂ　第２のモジュール
６　　第２の記憶部
７　　（安全な）第２の情報送信部
８　　インターフェース
８ａ　第１のインターフェース
８ｂ　第２のインターフェース
９　　周辺装置
９ａ　第１の接続システム
９ｂ　第２の接続システム
９ｃ　第３の接続システム
９ｄ　第４の接続システム

【図１】

Fig. 1



フロントページの続き

(72)発明者　シュテファン・フェルケニング
ドイツ連邦共和国デー－５０６７０ケルン、シリングシュトラーセ２６－２８番
(72)発明者　ハルディ・ユンガーマン
ドイツ連邦共和国デー－１０８２３ベルリン、アカーツィエンシュトラーセ４番
(72)発明者　トルステン・フーペ
ドイツ連邦共和国デー－８２０４１オーバーハッヒング、フォルデレス・グライセンタール１４番

審査官　関　博文

(56)参考文献　特開平０９－２８２４３３（ＪＰ，Ａ）
米国特許第０５６９４４７１（ＵＳ，Ａ）
米国特許出願公開第２００５／０１６０２７７（ＵＳ，Ａ１）
特開２００１－０９２７８７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06K 17/00
G06K 19/00-19/08
G09C 1/00