(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6792647号
(P6792647)
(45)発行日　令和2年11月25日(2020.11.25)　(24)登録日　令和2年11月10日(2020.11.10)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
G06F 21/31 (2013.01)　H04L 9/00 601F
G06F 21/62 (2013.01)　G06F 21/31
　　G06F 21/62 318

請求項の数 20　(全 23 頁)

(21)出願番号　特願2018-563664(P2018-563664)
(86)(22)出願日　平成29年4月14日(2017.4.14)
(65)公表番号　特表2019-525519(P2019-525519A)
(43)公表日　令和1年9月5日(2019.9.5)
(86)国際出願番号　PCT/US2017/027620
(87)国際公開番号　WO2018/004784
(87)国際公開日　平成30年1月4日(2018.1.4)
審査請求日　令和2年3月6日(2020.3.6)
(31)優先権主張番号　15/196,702
(32)優先日　平成28年6月29日(2016.6.29)
(33)優先権主張国・地域又は機関
　米国(US)

早期審査対象出願

(73)特許権者　508045099
シトリックス・システムズ・インコーポレイテッド
Ｃｉｔｒｉｘ　Ｓｙｓｔｅｍｓ，Ｉｎｃ．
アメリカ合衆国、フロリダ州　３３３０９、フォート・ローダーデール、ウエスト・サイプレス・クリーク・ロード　８５１
(74)代理人　110002675
特許業務法人ドライト国際特許事務所
(72)発明者　デイビッド　ロイド
英国　ＣＢ４　３ＳＱ　ケンブリッジ　ガニング　ウェイ　６
(72)発明者　アンドリュー　イネス
英国　ＣＢ２４　６ＺＧ　ケンブリッジ　ミルトン　ザ　オークス　７１
最終頁に続く

(54)【発明の名称】監査能力を備えた仮想スマートカード

(57)【特許請求の範囲】
【請求項１】
公開鍵インフラストラクチャ（ＰＫＩ：ｐｕｂｌｉｃ　ｋｅｙ　ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）スキームのコンテキストにおける秘密鍵の使用を制御するための方法であり、
クライアントコンピュータマシンにおけるシステムレベルエージェントが、仮想スマートカードサーバ（ＶＳＳ：ｖｉｒｔｕａｌ　ｓｍａｒｔ　ｃａｒｄ　ｓｅｒｖｅｒ）にユーザ認証情報を提供することにより、前記ＶＳＳに対してのみアクセス可能な安全なデータストア内の仮想スマートカードにそれぞれ割り当てられた複数の秘密鍵の検索を含む秘密鍵オペレーションを開始可能にし、
前記ＶＳＳからリモートされた前記クライアントコンピュータマシンにおけるシステムレベルエージェントが、前記ＶＳＳにおける前記クライアントコンピュータマシンのマシン認証プロトコルを開始し、信頼されたコンピュータシステムとして前記ＶＳＳに対する前記クライアントコンピュータマシンを確立すること、
前記クライアントコンピュータマシンのユーザレベルエージェントでの秘密鍵オペレーションの要求を受信したことに応答して、前記クライアントコンピュータマシンがユーザからユーザ認証情報を取得すること、
前記ユーザが前記ユーザ認証情報に基づいて認証されるに先だって、前記ユーザレベルエージェントが、前記システムレベルエージェントと交渉し前記ＶＳＳから前記秘密鍵オペレーションを許可するクッキーを取得すること、
前記ユーザレベルエージェントが、前記ＶＳＳへの秘密鍵オペレーションの要求を開始

すること、
前記ユーザレベルエージェントによって開始された前記要求の一部として、前記ユーザ認証情報および前記クッキーを、前記ユーザレベルエージェントが、前記ＶＳＳに通信すること、
前記要求に応答して、少なくとも前記ユーザに発行された前記仮想スマートカードの一つに割り当てられた秘密鍵を使用して、前記ユーザレベルエージェントによって要求された秘密鍵オペレーションを前記ＶＳＳが選択的に実行することを含む、方法。
【請求項２】
前記ＶＳＳが、前記秘密鍵オペレーションの結果を、前記クライアントコンピュータマシンの前記ユーザレベルエージェントに通信することをさらに含む、請求項１に記載の方法。
【請求項３】
前記ユーザレベルエージェントが、前記秘密鍵オペレーションの結果を前記クライアントコンピュータマシン上で実行されるアプリケーションプログラムに提供することをさらに含む、請求項２に記載の方法。
【請求項４】
前記ユーザレベルエージェントが、前記クライアントコンピュータマシン上で実行されるアプリケーションプログラムから、前記秘密鍵オペレーションの要求を受信することをさらに含む、請求項１に記載の方法。
【請求項５】
前記クッキーが、前記秘密鍵オペレーションの実行を可能にするために前記ＶＳＳにおいて一回だけ有効である、請求項１に記載の方法。
【請求項６】
前記ＶＳＳにおいて実行される前記秘密鍵オペレーションが、前記ＶＳＳに通信された署名済みデータまたは復号済みデータの安全なハッシュを生成することを含む、請求項１に記載の方法。
【請求項７】
前記ユーザ認証情報が、パスワード、ユーザバイオメトリックデータおよび物理的なスマートカードから得られるデータからなる群から選択される一つまたは複数の要素からなる、請求項１に記載の方法。
【請求項８】
前記方法は、バイオメトリックデータキャプチャデバイスおよびスマートカードリーダデバイスのうちの少なくとも一つによって、前記ユーザ認証情報をキャプチャすることをさらに含む、請求項７に記載の方法。
【請求項９】
前記ユーザレベルエージェント、前記システムレベルエージェントおよび前記ＶＳＳは、使用が要求されている特定の秘密鍵に従って決定された所定のセキュリティポリシーを選択的に適用することをさらに含む、請求項１に記載の方法。
【請求項１０】
前記ＶＳＳが、前記秘密鍵オペレーションの実行を要求する各アクションに関する情報を、安全なデータログにおいて記録することをさらに含む、請求項１に記載の方法。
【請求項１１】
公開鍵インフラストラクチャ（ＰＫＩ：ｐｕｂｌｉｃ　ｋｅｙ　ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）スキームのコンテキストにおける秘密鍵の使用を制御するための方法であり、
仮想スマートカードサーバ（ＶＳＳ：ｖｉｒｔｕａｌ　ｓｍａｒｔ　ｃａｒｄ　ｓｅｒｖｅｒ）が、信頼されたコンピュータシステムとして前記ＶＳＳからリモートされたクライアントコンピュータマシンを確立するための要求であって、予め定められたマシン認証プロトコルに従って前記クライアントコンピュータマシンにおけるシステムレベルエージェントによって開始される前記要求を前記ＶＳＳにおいて受信すること、
前記ＶＳＳが、前記クライアントコンピュータマシンのユーザが認証されるに先だって

クッキーの要求を前記システムレベルエージェントから受信すること、
前記ＶＳＳが、要求されたクッキーを前記システムレベルエージェントに提供すること、
前記ＶＳＳが、ユーザレベルエージェントから、前記クッキーと前記ユーザから前記ユーザレベルエージェントによって取得された選択されたユーザ認証情報とが一部を構成する秘密鍵オペレーションのための要求を受信すること、
前記ＶＳＳが、前記要求に応答して、前記ＶＳＳのみにアクセス可能な安全なデータストアにストアされた秘密鍵であって少なくとも前記ユーザに発行された前記仮想スマートカードの一つに割り当てられた前記秘密鍵を検索することによって、前記ユーザレベルエージェントによって要求された前記秘密鍵オペレーションを選択的に実行することを含む、方法。
【請求項１２】
複数の仮想スマートカードにそれぞれ関連付けられたコンテンツへのアクセスを制御する仮想スマートカードサーバ（ＶＳＳ：ｖｉｒｔｕａｌ　ｓｍａｒｔ　ｃａｒｄ　ｓｅｒｖｅｒ）を備える第１のコンピュータマシンと、
前記ＶＳＳから遠隔に配置された一または複数の第２のコンピュータマシンであって、おのおのが、信頼されるコンピュータシステムとして前記ＶＳＳにクライアントコンピュータマシンを確立するために、前記ＶＳＳにクライアントコンピュータマシンのマシン認証プロトコルを開始するシステムレベルエージェントを含むクライアントコンピュータシステムを備える、前記第２のコンピュータマシンと、
前記クライアントコンピュータマシンの少なくとも一つのアプリケーションプログラムによって開始される仮想スマートカードオペレーションの要求を受信する、前記クライアントコンピュータシステムにおけるユーザレベルエージェントと、
を含み、
前記ユーザレベルエージェントは前記要求に応答して、前記クライアントコンピュータシステムに、
前記クライアントコンピュータシステムのユーザから、前記仮想スマートカードオペレーションの使用を許可するのに必要なユーザ認証情報を取得させ、
前記ユーザが前記ユーザ認証情報に基づいて認証されるに先だって、前記システムレベルエージェントと交渉して、前記ＶＳＳからクッキーを取得し、
前記仮想スマートカードオペレーションを実行するための前記ＶＳＳへの要求を開始し、
前記要求の一部として前記ユーザ認証情報および前記クッキーを前記ＶＳＳに通信し、
前記ＶＳＳは、要求された仮想スマートカードオペレーションに適用可能なセキュリティポリシーが満たされる場合、仮想スマートカードオペレーションを選択的に実行することによって前記要求に応答する、仮想スマートカードシステム。
【請求項１３】
前記ＶＳＳは、前記仮想スマートカードオペレーションの結果を前記ユーザレベルエージェントに通信するように構成される、請求項１２に記載の仮想スマートカードシステム。
【請求項１４】
前記ユーザレベルエージェントは、前記仮想スマートカードオペレーションの結果を、前記仮想スマートカードオペレーションの要求を開始した前記アプリケーションプログラムに提供するように構成される、請求項１３に記載の仮想スマートカードシステム。
【請求項１５】
前記ＶＳＳは、前記クッキーが前記ＶＳＳにおける単一の仮想スマートカードオペレーションに対してのみ有効であるように構成される、請求項１２に記載の仮想スマートカードシステム。
【請求項１６】
前記仮想スマートカードオペレーションは前記ＶＳＳで実行される秘密鍵オペレーショ

ンであり、前記ＶＳＳは前記ＶＳＳに通信された署名済みデータまたは復号済みデータの安全なハッシュを生成するように構成される、請求項１２に記載の仮想スマートカードシステム。

【請求項１７】

前記ユーザ認証情報は、パスワード、ユーザバイオメトリックデータおよび物理的なスマートカードから得られるデータからなる群から選択される一つまたは複数の要素からなる、請求項１２に記載の仮想スマートカードシステム。

【請求項１８】

前記クライアントコンピュータシステムは、バイオメトリックデータキャプチャデバイスおよびスマートカードリーダデバイスのうちの少なくとも一つを使用することによって、前記ユーザ認証情報をキャプチャするように構成される、請求項１７に記載の仮想スマートカードシステム。

【請求項１９】

前記ユーザレベルエージェント、前記システムレベルエージェントおよび前記ＶＳＳの各々は、使用が要求されている特定の仮想スマートカードに従って決定された所定のセキュリティポリシーを選択的に適用するように構成される、請求項１２に記載の仮想スマートカードシステム。

【請求項２０】

前記ＶＳＳは、仮想スマートカードオペレーションに対する各要求に関連する複数のイベントに関する情報をデータログに記録するように構成される、請求項１２に記載の仮想スマートカードシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

（関連出願の相互参照）

本出願は、２０１６年６月２９日に出願された米国特許出願第１５／１９６，７０２号の利益を主張し、その出願はその全体が参照により本明細書に組み込まれる。

【０００２】

本書は、認証、暗号化およびデータ記憶のための方法およびシステムに関する。より詳細には、本書がスマートカードを使用して一般に実施される企業レベルの機能を容易にするための方法およびシステムに関する。

【背景技術】

【０００３】

スマートカードはポケットサイズのカードであり、内蔵された電子回路（例えば、内蔵メモリを備えた安全なマイクロコントローラー）を含み、直接的な物理的な接続または無線周波信号の手段によってリーダ装置によって読み取ることができる。スマートカードは、暗号化から認証までの範囲の多くの用途を有する。スマートカードは少量のデータを記憶する能力を有し、特定のオンカード処理機能を実行するように設計することができる。このような情報伝達を容易にするために、従来のスマートカードは、一般にスマートカードリーダと呼ばれるハードウェア要素と情報伝達するように設計されている。

【０００４】

多くの企業は、金融取引や文書承認などの監査プロセスに厳しい要件を課している。どの従業員がどのステップをいつ許可したかを知る必要がある。同様に、従業員は彼らが承認している取引を完全に理解する必要があり、この目的のために彼らの資格認証の使用を制御することができなければならない。これらのプロセスを容易にするために、スマートカードは、認証および署名の目的で従業員に発行され得る。このようなシナリオでは、スマートカードが従来の公開鍵インフラストラクチャ（ＰＫＩ：ｐｕｂｌｉｃ　ｋｅｙ　ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）スキームに関連して使用するための秘密鍵を含むことができる。スマートカードは、個人識別番号（ＰＩＮ：ｐｅｒｓｏｎａｌ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｎｕｍｂｅｒ）パスコードまたは指紋リーダと併せて使用され、ユーザを

認証することができる。

【０００５】

スマートカードの使用に代わるものとして、本明細書で説明される目的のためのデジタル証明書は、「ソフトウェア証明書」サポートを使用してエンドユーザに直接発行されている。このような実装では、ＰＫＩシステムで使用するための秘密鍵が、従来、ユーザのローミングプロファイルに格納されてきた。知られているように、ローミングユーザプロファイルはあるコンピュータオペレーティングシステムの特徴であり、それによって、ユーザは同じネットワーク上の任意のコンピュータにログオンし、その文書ならびに他のデータ（デジタル証明書および／または秘密鍵など）にアクセスすることができる。しかし、ユーザは秘密鍵を制御できず、ハッカーが鍵を「盗む」ことは非常に容易である。

【０００６】

従来のスマートカードは、ローミングユーザプロファイルに関連付けられた証明書および秘密鍵を利用するシステムに優る特定の利点を提供する。例えば、スマートカードは、秘密鍵がコピーされないように保護する上でより優れたハードウェアベースのソリューションを容易にする。それでも、スマートカードは、紛失／窃盗の影響を受けやすく、ユーザのＰＩＮを推定できると、許可なしで使用することができる。一旦、スマートカードのようなトークンに対する物理的な制御が失われると、鍵が無許可の目的のために使用されないことをエンタープライズが保証することは困難である。例えば、そのような状況は、スマートカードが終了時に従業員によって返却されないシナリオにおいて生じ得る。

【０００７】

従来のスマートカードを使用する際の別の課題は、特定の個人の資格認証が様々なトランザクションに関連していつどのように使用されたかを再構築または追跡するために必要とされる監査プロセスを妨げる可能性があることである。スマートカードを使用するシステムは監査を容易にするように設計することができるが、これらのシステムは独自仕様であるか、または異なるアプリケーションに組み込まれる傾向がある。したがって、監査を統一することができないかまたは幾つかのアプリケーションがすべての適切な情報をログに記録しないことがある。

【発明の概要】

【０００８】

本発明の実施形態は、仮想スマートカードシステムに関する。システムは、仮想スマートカードサーバ（ＶＳＳ：ｖｉｒｔｕａｌ　ｓｍａｒｔ　ｃａｒｄ　ｓｅｒｖｅｒ）を備える第１のコンピュータマシンを含む。ＶＳＳは、複数の仮想スマートカードにそれぞれ関連付けられたコンテンツへのアクセスを制御する。一または複数の第２のコンピュータマシンがＶＳＳから離れて配置される。第２のコンピュータマシンの各々は、システムレベルエージェントを含むクライアントコンピュータシステムである。システムレベルエージェントは、ＶＳＳにおいてクライアントコンピュータマシンのマシン認証プロトコルを開始して、信頼されるコンピュータシステムとしてＶＳＳに対してクライアントコンピュータマシンを確立する。そのように確立されると、クライアントコンピュータシステムにおけるユーザレベルエージェントは、一つまたは複数の仮想スマートカードオペレーションに対する要求を受信する。例えば、要求は、クライアントコンピュータマシン上で実行されるアプリケーションプログラムによって開始されることができる。

【０００９】

ユーザレベルエージェントはクライアントコンピュータシステムに特定のオペレーションを実行させるように、そのような各要求に応答する。これらは、クライアントコンピュータシステムのユーザから、仮想スマートカードオペレーションの使用を許可するのに必要なユーザ認証情報を取得することを含む。これらのオペレーションは、システムレベルエージェントと交渉して、ＶＳＳからクッキーを取得することをさらに含むことができる。その後、ユーザレベルエージェントは、特定の仮想スマートカードオペレーションを実行するためにＶＳＳへの要求を開始する。この要求は、ユーザ認証情報およびクッキーをＶＳＳに通信することを含む。ＶＳＳは、要求された仮想スマートカードオペレーション

に適用可能なセキュリティポリシーが満たされることを条件として、仮想スマートカードオペレーションを選択的に実行するように各要求に応答するように構成される。特定の仮想スマートカードオペレーションが完了すると、ＶＳＳは、仮想スマートカードオペレーションの結果をユーザレベルエージェントに通信する。次に、ユーザレベルエージェントは、仮想スマートカードオペレーションの結果を、仮想スマートカードオペレーションの要求を開始したアプリケーションプログラムに提供する。ＶＳＳは後続の監査目的のために、仮想スマートカードオペレーションに対する各要求に関係する複数のイベントに適用される情報をデータログに記録するように構成される。

【００１０】

幾つかの実施形態は、また、公開鍵インフラストラクチャ（ＰＫＩ：ｐｕｂｌｉｃ ｋｅｙ ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）スキームのコンテキストにおいて一つまたは複数の秘密鍵の使用を制御するための方法に関する。この方法は、ＶＳＳのみに可能な安全なデータストアに複数の秘密鍵を格納することを含むことができる。その後、ＶＳＳからリモートされたクライアントコンピュータマシンのシステムレベルエージェントを使用して、ＶＳＳでクライアントコンピュータマシンのマシン認証プロトコルを開始する。このプロセスは、信頼されるコンピュータシステムとしてＶＳＳにクライアントコンピュータマシンを確立する。クライアントコンピュータマシンにおけるユーザレベルエージェントは、秘密鍵オペレーションのための一つまたは複数の要求を受信することができる。例えば、そのような要求は、クライアントコンピュータマシン上で実行するアプリケーションプログラムによって生成することができる。特定の要求に応答して、ユーザレベルエージェントはユーザからユーザ認証情報を取得し、システムレベルエージェントと交渉してＶＳＳからクッキーを取得する。ユーザレベルエージェントはまた秘密鍵オペレーションのための要求をＶＳＳに開始し、ユーザ認証情報およびクッキーをユーザレベルエージェントからＶＳＳに通信する。その要求に応答して、ＶＳＳは、認証情報が適用されるセキュリティポリシーを満たす場合、ユーザに割り当てられた秘密鍵を使用して、ユーザレベルエージェントによって要求された秘密鍵オペレーションを選択的に実行する。

【００１１】

実施形態は以下の図面を参照して説明され、図面において同様の符号は図面全体を通して同様のアイテムを表す。

【図面の簡単な説明】

【００１２】

【図１】図１は、本明細書で説明される仮想スマートカードシステムの一実施形態を理解するのに有用なシステム図である。

【図２】図２は、安全なコンピュータシステムのあるコンポーネントを理解するのに有用なアーキテクチャ図である。

【図３】図３は、仮想スマートカードシステムの様々なコンポーネント間の特定の通信を理解するのに有用な図である。

【図４Ａ】図４Ａは、安全なコンピュータで仮想スマートカードにアクセスするための例示的な方法を示すフローチャートを含む。

【図４Ｂ】図４Ｂは、安全なコンピュータで仮想スマートカードにアクセスするための例示的な方法を示すフローチャートを含む。

【図５Ａ】図５Ａは、仮想スマートカードサーバにおいて仮想スマートカードへのアクセスを提供する例示的な方法を示すフローチャートを含む。

【図５Ｂ】図５Ｂは、仮想スマートカードサーバにおいて仮想スマートカードへのアクセスを提供する例示的な方法を示すフローチャートを含む。

【図６】図６は、例示的なコンピュータシステムの構成を理解するのに有用なハードウェアブロック図である。

【発明を実施するための形態】

【００１３】

本明細書で全体的に説明し、添付の図面に示す実施形態の構成要素は、多種多様な異な

る構成で配置および設計できることが容易に理解されよう。したがって、図面に表される様々な実施形態の以下のより詳細な説明は、本開示の範囲を限定することを意図するものではなく、様々な実施形態を単に代表するものである。実施形態の様々な観点が図面に示されているが、図面は特に示されていない限り、必ずしも一定の縮尺で描かれていない。

【００１４】

スマートカードはポケットサイズのカードであり、内蔵された電子回路（例えば、内蔵メモリを備えた安全なマイクロコントローラー）を含み、直接的な物理的な接続または無線周波信号の手段によってリーダ装置によって読み取ることができる。いくつかのシナリオでは、スマートカードが公開鍵インフラストラクチャ（ＰＫＩ：ｐｕｂｌｉｃ　ｋｅｙ　ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）スキームに関連したデジタル証明書を含むことができる。この種の例示的なデジタル証明書は、Ｘ．５０９などの既知のＰＫＩ規格に従って発行されたデジタル証明書である。知られているように、そのようなデジタル証明書はエンティティの公開鍵を、その所有者（例えば、組織または人）に関する特定の属性に結びつけるために使用することができる。従来のスマートカードは、特定のユーザに割り当てられた秘密鍵に関する情報も含むことができる。スマートカード上のデジタル証明書および秘密鍵は個人（例えば、企業の従業員）によって様々な目的のために使用される。例えば、これらの要素はユーザが文書に署名しているか、またはトランザクションを承認しているときに、署名および認証の目的で使用することができる。また、それらは、他のアプリケーションの中でも、安全なドキュメント処理、および／または暗号通信のために使用されてもよい。

【００１５】

しかし、スマートカードは、様々な制限および問題を抱える。カードは忘れられるか、紛失するか、または盗まれる可能性があり、そのようなシナリオでは、センターアドミニストレーターは、スマートカードが最終的にどこになり得るかに関して、限られた可視性のみを有する。また、スマートカードが紛失または盗難された場合、カードに格納された鍵情報は管理者によって無効にされることができるだけであり、リモートで削除することはできない。従来のスマートカードに関する別の問題は、従業員が朝自宅でスマートカードを離れるときに生じる。彼らに割り当てられたスマートカードがなければ、従業員は彼らの仕事を遂行することができないかもしれない。また、スマートカードは、通常、「グループ間で共有される」ことができない。各スマートカードは個人に割り当てられなければならず、例えば、突然のビジースケジュールを処理するために４人のチームを６人に拡張する必要がある場合、この目的のために２つの追加のスマートカードを準備し、次いで、ビジー期間が完了すると準備を解除する必要がある。最後に、スマートカードを使用するコンピュータシステムはある種の監査機能を容易にすることができるが、スマートカードが使用された時および場所を判定するためにセンターアドミニストレーターが監査を実行することはしばしば非常に困難である。

【００１６】

したがって、本明細書では、一つまたは複数のユーザのそれぞれによる一つまたは複数の仮想スマートカードのそれぞれの使用を容易にするための方法およびシステムが開示される。本明細書に記載される実施形態は従来のスマートカードに関連する多くの制限を克服し、その利益の全てを保持する。ユーザは、安全なコンピュータシステムに対して彼らの身元を認証することができる。その後、（ユーザが使用するための何らかの権限を有する）適切な証明書および秘密鍵が、リモート中央サーバ上で安全に生成またはアクセスされ得る。

【００１７】

リモート中央サーバは、サーバがユーザのための様々なタイプの証明書を生成することができるように、認証局へのアクセスを有利に有することができる集中化された仮想スマートカードサーバである。知られているように、認証局はエンティティの識別を検証し、エンティティのデジタル証明書にデジタル署名することによってそのような識別を証明する組織である。すべての証明書および秘密鍵は攻撃者が秘密鍵にアクセスすることが極め

て困難になるように、場合によっては「ハードウェアセキュリティモジュール」を使用して鍵を管理して、仮想スマートカードサーバ上に安全に格納される。いくつかの実施形態では、サーバがサーバ上で物理的セキュリティを維持するために、安全な場所に保持することができる。各ユーザは、特定の仮想スマートカードの使用を許可するように設定された事前に設定されたポリシーに従って、サーバによって認証される。認証メカニズムは、ユーザ名／パスワード、セキュリティアサーションマークアップ言語（Ｓｅｃｕｒｉｔｙ　Ａｓｓｅｒｔｉｏｎ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ：ＳＡＭＬ）認証、バイオメトリックまたは任意の他の適切な方法であり得る。異なる認証要件またはセキュリティプロトコルは、その特定のユーザのためにサーバ上に格納され得るいくつかの異なる仮想スマートカードのそれぞれへのユーザアクセスのために定義され得る。

【００１８】

特定の個人に割り当てられた仮想スマートカードの一つが使用される場合、注意深く制御されたインフォームドコンセントおよび認証プロンプトが、安全なコンピュータシステムでユーザに表示される。プロンプトはユーザが何らかの目的のために（例えば、特定のトランザクションまたはプロセスを承認するために）仮想スマートカードのうちの一つを利用する必要があるときはいつでも、表示され得る。仮想スマートカードサーバは、特定の仮想スマートカードの使用に適用されるセキュリティポリシーに適切なレベルであれば何でも、ユーザを認証する。これは、以下のような、すなわちユーザ名、アプリケーションが使用されている場所、時間など情報を潜在的に含む。認証ポリシーによって要求される場合、サーバは「存在証明」認証を要求することもでき、したがって、エンドユーザは、チャレンジに応答する（パスワードを入力する、スマートカードを挿入する、指紋リーダを使用する）必要があり得る。

【００１９】

ユーザが安全なコンピュータシステムに対して認証されると、適切な証明書（すなわち、仮想スマートカード）が、標準的なコンピュータオペレーティングシステム（ＡＰＩｓ）を使用することによって、ユーザがアクセスできるアプリケーションに公開される。標準的なオペレーティングシステムＡＰＩｓの使用は、アプリケーションの最も広い選択との互換性を促進する。スマートカードが実際に使用される場合（例えば、ユーザがトランザクションまたはプロセスを承認する必要がある場合）、注意深く制御されたインフォームドコンセントおよび認証プロンプトがユーザに表示される。

【００２０】

より大きなセキュリティを保証するために、ユーザの秘密鍵（ユーザの仮想スマートカードに関連付けられる）は、リモート中央サーバから決して離れないことが有利である。したがって、たとえユーザが様々な秘密鍵を使用することを許可されたとしても、ユーザは、それらの秘密鍵への直接アクセスを決して許可されない。ユーザに利用可能な各秘密鍵の各使用は、集中化された仮想スマートカードサーバに委任される。したがって、中央サーバは、各秘密鍵の使用毎に安全な監査ログを作成することができる。さらに、異常が検出された場合（例えば、悪意のある従業員が終了した場合）、リモート中央サーバは、管理者からのコマンドに応答して、そのようなユーザに割り当てられた秘密鍵へのアクセスを直ちに終了することができる。この効力発生に遅れはない。

【００２１】

図１は、本明細書で説明する仮想スマートカードシステムの一実施形態を理解するのに有用なシステム図である。便宜上、本明細書で説明される特定の実施形態は秘密鍵情報（例えば、ＰＫＩスキームのコンテキストで使用され得る秘密鍵情報）を備える一つまたは複数の仮想スマートカードのコンテキストで開示される。しかし、本明細書に記載される仮想スマートカードシステムはこの点において限定されず、代わりに、従来の物理的スマートカードにおいて提供され得る任意のコンテンツまたは機能に関連して使用され得ることが理解されるべきである。

【００２２】

図１のシステムは、認証局（ＣＡ）１０４、安全なデータストア１０３およびメインデ

ータストア１０５へのアクセスを有する仮想スマートカードサーバ（ＶＳＳ）１０２を含む。一つまたは複数の安全なコンピュータシステム１０６$_1$－１０６$_n$は、コンピュータデータネットワーク１０８を使用してＶＳＳと通信する。ＶＳＳ１０２は、クライアントの安全なコンピュータシステム１０６$_1$－１０６$_n$に仮想スマートカードサービスを提供するコンピュータプログラムおよび関連するコンピュータハードウェアを備えることができる。

【００２３】

安全なデータストア１０３は、個々のユーザに割り当てられた、または発行された一つまたは複数の秘密鍵に関する秘密鍵データ１１４を含むことができる。いくつかの実施形態では、安全なデータストア１０３がデジタル鍵を記憶するように特に設計されたハードウェアセキュリティモジュール（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ：ＨＳＭ）とすることができる。したがって、安全なデータストア１０３は、ＶＳＳに接続するプラグインカードまたは外部デバイスとすることができる。

【００２４】

メインデータストア１０５は、秘密鍵の使用を許可するかどうかを決定するときにＶＳＳによって課せられる条件および要件を定義する一つまたは複数のＶＳＳセキュリティポリシー１１０を含むことができる。メインデータストアは、ユーザ認証データ１１２、デジタル証明書１１６、およびトランザクションログ１１８も含むことができる。トランザクションログ１１８はＶＳＳによって使用されて、後続の監査目的のために、本明細書で説明するように、秘密鍵動作を伴うトランザクションを記録する。

【００２５】

コンピュータデータネットワーク１０８は、本明細書で説明する仮想スマートカードシステムを実装するのに必要なファイル、データおよび他のタイプの情報の通信を容易にするのに適している。コンピュータネットワーク１０８は、また、ＶＳＳ１０２で利用可能な特定のコンピュータリソースを安全なコンピュータシステム１０６$_1$－１０６$_n$と共有することを容易にすることができる。この目的のために使用することができる例示的なネットワークは、任意の既知の通信プロトコルに従って動作するパケットデータネットワークを含むことができる。そのようなネットワークの組織的範囲は、イントラネット、エクストラネットおよびインターネットのうちの一つまたは複数を含むことができる。

【００２６】

ここで図２を参照すると、安全なコンピュータシステム１０６$_n$の特定のコンポーネントを把握するのに役立つアーキテクチャ図が示されている。安全なコンピュータシステムはコンピュータハードウェアコンポーネント２１４（例えば、中央処理装置またはＣＰＵ）、メインメモリ２１６および特定のネットワークインターフェースデバイス２１８を備え、本明細書で説明するネットワーク通信を容易にすることができる。安全なコンピュータシステムは、安全なコンピュータシステム上で利用可能なハードウェアおよびソフトウェアリソースを管理するためのオペレーティングシステム２１２も含むことができる。オペレーティングシステム２１２は、アプリケーションプログラム２０２が使用できる事前コンパイルされたルーチンまたは機能のライブラリ２０８へのアクセスを容易にすることができる。ライブラリ内で提供される様々な機能およびルーチンは、一つまたは複数のアプリケーションプログラミングインターフェース（ＡＰＩ：ａｐｐｌｉｃａｔｉｏｎ　ｐｒｏｇｒａｍｍｉｎｇ　ｉｎｔｅｒｆａｃｅ）２１０を使用してアプリケーションに公開することができる。

【００２７】

セキュリティ保護されたコンピュータシステム１０６$_n$は、システムレベルエージェント２０４およびユーザレベルエージェント２０６をさらに含む。システムレベルエージェント２０４およびユーザレベルエージェント２０６は本明細書で説明する仮想スマートカードの使用を容易にするために、安全なコンピュータシステムにおいてある種のセキュリティおよび認証関連機能を実行するコンピュータプログラムである。これらのエージェントの各々は、ＶＳＳ１０２との特定の通信にも関与する。システムレベルエージェント２

０４は主に、安全なコンピュータシステム１０６$_n$に関する認証オペレーションに関与する。ユーザレベルエージェントは主に安全なコンピュータシステム１０６$_n$のユーザに関する認証に関与する。システムレベルエージェントは、安全なコンピュータシステムの起動プロセス中にインスタンス化される。ユーザレベルエージェント２０６は、安全なコンピュータシステム１０６$_n$にログインしたユーザ毎に有利にインスタンス化される。ユーザに対してインスタンス化されるユーザレベルエージェント２０６は、そのユーザに代わって動作するようにシステムレベルエージェント２０４によって信頼される。

【００２８】

メインメモリ２１６は本明細書で説明するように、一つまたは複数の仮想スマートカード（例えば、秘密鍵情報を含む仮想スマートカード）の使用を許可するために適用されるセキュリティポリシーを制御するように構成された一つのまたは複数の定義されたセキュリティポリシーを含むことができる。例えば、メインメモリは、各仮想スマートカードの使用のためにシステムレベルエージェント２０４によって適用されるセキュリティポリシーを定義する複数のシステムレベルエージェント（ｓｙｓｔｅｍ　ｌｅｖｅｌ　ａｇｅｎｔ：ＳＬＡ）セキュリティポリシー２２０を含むことができる。同様に、メインメモリは、各仮想スマートカードの使用のためにユーザレベルエージェント２０６によって適用されるセキュリティポリシーを定義する複数のユーザレベルエージェントセキュリティポリシー２２２を含むことができる。

【００２９】

一態様によれば、ユーザレベルエージェント２０６は、ＶＳＳ１０２に対して直接ユーザを認証する。しかし、そのたびに、一回使用のクッキーを取得するためにシステムレベルエージェント２０４と最初に交渉しなければならない。システムレベルエージェント２０４はＶＳＳ１０２から一回使用のクッキーを取得することによって応答し、それをユーザレベルエージェント２０６に提供する。したがって、ＶＳＳ、システムレベルエージェント２０４、およびユーザレベルエージェント２０６はすべて、どの認証または秘密鍵アクションが実行されているかを知っている。これらのエンティティのオペレーションは以下でさらに詳細に説明され、それらの目的は議論が進むにつれてより明らかになるのであろう。

【００３０】

次に図３を参照すると、仮想スマートカードシステムの様々なコンポーネント間のある種の相互作用を理解するのに有用なコミュニケーションダイアグラムが示されている。これらの対話はＶＳＳ１０２と、システムレベルエージェント２０４およびユーザレベルエージェント２０６を含む安全なコンピュータシステム（例えば、安全なコンピュータシステム１０６$_n$）を含む様々なエンティティとの間の通信を含むことができる。これらの相互作用のいくつかは、図４Ａ－４Ｂおよび図５Ａ－５Ｂに関連してさらに詳細に説明される。より明確にするために、単一の仮想スマートカードのみの使用が、図３に示される通信において説明される。さらに、ユーザは安全なコンピュータシステムにログオンした特定のセッション中に、ＶＳＳ１０２から一つまたは複数の許可された仮想スマートカードに同様にアクセスすることができることを理解されたい。これらの異なる仮想スマートカードの各々は異なる目的を有することができ、いくつかの実施形態では、異なるセキュリティポリシーに従ってアクセスすることができる。

【００３１】

通信セッション３００は、システムレベルエージェント２０４がステップ３０２で通信して、ＶＳＳへの安全なコンピュータクライアント認証を開始したときに開始することができる。このプロセスは、適切な認証プロトコルを使用して、安全なコンピュータシステム１０６$_n$をＶＳＳに対して識別することを含むことができる。このプロセスは、認証が肯定応答または完了したことを示すために、ＶＳＳからシステムレベルエージェントへの通信３０３を含み得る。通信３０３は、また、利用可能なスマートカードおよび適切な使用ポリシーのリストを備えることができる。スマートカードおよび適切な使用ポリシーのこのリストは、その後、後の使用のために安全なコンピュータシステムにおいてシステム

レベルエージェント２０４によって格納される。

【００３２】

本明細書に記載される目的のために使用され得る例示的な機械認証プロトコルは、よく知られているＫｅｒｂｅｒｏｓ識別プロトコルを含み得、それによって、安全なコンピュータシステム１０６ｎおよびＶＳＳ１０２の両方がそれぞれ、他方の同一性を検証する。あるいは、従来のトランスポート層セキュリティ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ：ＴＬＳ）クライアント認証プロトコルをこの目的のために使用することができる。このステップでマシン認証に使用される正確なプロセスは安全なコンピュータシステムおよびＶＳＳ１０２の各々が他のマシンのアイデンティティを認証することができる限り、重要ではない。したがって、現在知られているかまたは将来知られている任意の適切な機械認証プロセスを使用することができる。使用される特定の認証プロトコルに応じて、他のコンピュータシステムとの追加の通信を機械認証プロセスに関与させることができることを理解されたい。例えば、そのような通信は、信頼できる権威サーバへの通信を含むことができる。明瞭にするために、これらの付加的なステップは、図３では意図的に省略されている。

【００３３】

機械認証プロセスが３０３で完了すると、ＶＳＳはその後、特定のシステムレベルエージェント２０４からの要求を信頼し、受け入れる。ユーザが安全なシステムコンピュータ１０６$_n$にログオンすると、システムレベルエージェント２０４は、ユーザが到着したことをＶＳＳ１０２に通知する（３０４）。これは、ＶＳＳが適切な仮想スマートカードがそのユーザによる使用のために利用可能であることを確実にすることを可能にする。システムレベルエージェントはまたそのユーザのためのユーザレベルエージェント２０６をインスタンス化する。この時点で、ユーザは、一つまたは複数のアプリケーションプログラム２０２を使用して処理動作を開始することができる。

【００３４】

ある時点で、これらの処理オペレーションはある秘密鍵オペレーション（例えば、物理的なスマートカードに格納された秘密鍵の使用によって従来取り扱われている秘密鍵オペレーション）を必要とする可能性があり、例示的な秘密鍵オペレーションは、認証オペレーション、署名オペレーション、プロセス承認オペレーションおよび／または暗号オペレーションを含むことができる。一つまたは複数のそのようなオペレーションは、ＰＫＩシナリオのコンテキストにおける秘密鍵の使用を含むことができる。このようなイベントがアプリケーションプログラム２０２の一つに関連して発生すると、アプリケーションプログラムは秘密鍵オペレーションの要求３０６を開始する。例えば、そのようなオペレーションを開始するために、アプリケーションは、安全なコンピュータシステム１０６ｎ上で利用可能な一つまたは複数のスタンダードオペレーティングシステムＡＰＩ’ｓ２１０に要求を通信することができる。

【００３５】

これに応答して、ユーザレベルエージェント２０６は、３０８において、本明細書で開示されるような特定の仮想スマートカードの使用に関するユーザの同意を要求する一つまたは複数のユーザプロンプトを表示する。これらの同意プロンプトは、ユーザ認証３１０を含むアクションを含むことができる。システム内の各ユーザは、それらに割り当てられた一つまたは複数の仮想スマートカードのうちの特定の一つ使用するために定義された構成されたポリシーに従って認証される。この点に関して、特定のユーザに割り当てられた異なる仮想スマートカードは、異なるセキュリティポリシーを添付することができることに留意されたい。したがって、特定のインスタンスにおけるユーザ認証メカニズムは、特定の仮想スマートカードの使用のために適所にあるセキュリティポリシーに適切であり得る、ユーザ名／パスワードの組み合わせ、ＳＡＭＬ認証、またはバイオメトリック認証のうちの一つまたは複数を含み得る。いくつかのシナリオでは、物理的なスマートカードをこの認証プロセスの一部として使用することもできる。したがって、ユーザは、３１０で認証情報を提供することによってプロンプトに応答する。

【００３６】
最終的に、ユーザレベルエージェント２０６は３０６において特定のアプリケーションプログラムによって要求された秘密鍵オペレーションを実行するために、ＶＳＳと通信する必要がある。しかし、そのようにする前に、サービスレベルエージェント（ＳＬＡ）２０４と交渉して（３１２）、一回使用のクッキーを受信しなければならない。一回使用のクッキーは暗号化され得る小さなデータファイル（例えば、テキストファイル）から構成され得る。一回使用のクッキー（その名前が意味する）は、単一の秘密鍵オペレーションのみを許可するために有効である。これらのオペレーションはユーザレベルエージェントが仮想スマートカードトランザクションに従事しているときに、システムレベルエージェント２０４が常に認識されることを保証する。システムレベルエージェント２０４は、ユーザレベルエージェント２０６が仮想スマートカードを使用する許可を求めたことをＶＳＳ１０２に知らせることによってユーザレベルエージェント２０６に応答する（３１４）。このアクションはＶＳＳにトランザクションを警告し、ＶＳＳが３１６でシステムレベルエージェント２０４に一回使用のクッキーを提供することになる。システムレベルエージェントはこの一回使用のクッキーを受信し、それを３１８でユーザレベルエージェント２０６に提供する。

【００３７】
この時点で、ユーザレベルエージェントは、ＶＳＳからの秘密鍵オペレーションを要求するのに必要な要素のすべてを有する。それは、３１０で受信されたユーザ認証情報を有し、ＶＳＳから秘密鍵オペレーションを取得することを可能にする、必要とされる一回使用のクッキーを有する。したがって、ユーザレベルエージェント２０６は、３２０において、秘密鍵オペレーションの要求を開始する。この要求は、３１０で取得された一回使用のクッキーおよびユーザ認証データを含む情報を含むことができる。ＶＳＳ１０２はこの情報を受信し、それを評価して、要求された秘密鍵オペレーションを実行すべきかどうかを判定する。その場合、ＶＳＳはそのような秘密鍵オペレーションを実行し、その結果をユーザレベルエージェント２０６に通信する（３２２）。例えば、結果は、秘密鍵を使用して復号化された署名付き文書および／またはデータの安全なハッシュを含むことができる。これらの結果がユーザレベルエージェントで受信されると、３２４において、秘密鍵オペレーションの要求を開始したアプリケーションプログラム２０２にこれらの結果が提供される。

【００３８】
次に図４Ａおよび図４Ｂを参照すると、安全なコンピュータ１０６ｎにおける仮想スマートカードシステムの例示的な方法を示すフローチャートが提供されている。プロセスは４０２で始まり、４０４に進み、システムレベルエージェントによって安全なコンピュータシステムがＶＳＳに対して認証される。このステップは、安全なコンピュータシステムにインストールされている様々なアプリケーションプログラムが使用できるようにすべき使用可能なスマートカードのリストを、安全なコンピュータシステムのＶＳＳから受信することも含むことができる。この情報は、安全なコンピュータシステムに格納され、ユーザレベルエージェント２０６によってアクセスされることができる。ユーザが安全なコンピュータシステムにログインすると（４０６：Ｙｅｓ）、システムレベルエージェントに通知される。システムレベルエージェントは、４０８において、ユーザが到着したことをＶＳＳに通知する。さらに、システムレベルエージェントは、４１０において、ユーザレベルエージェントをインスタンス化する。その後、ユーザは、安全なコンピュータシステムで利用可能な一つまたは複数のアプリケーションプログラムを利用することができる。

【００３９】
ある時点で、コンピュータシステム上で使用中のアプリケーションプログラムは、秘密鍵オペレーション（４１２：Ｙｅｓ）を必要とすることがある。このとき、秘密鍵オペレーションの要求は、ユーザレベルエージェントに向けられる。このプロセスをよりよく理解するために、よく知られた或るオペレーティングシステム（例えば、Ｗｉｎｄｏｗｓベースのオペレーティングシステム）では、公開鍵および証明書が秘密鍵を参照しながら「

ユーザの証明書ストア」内に配置されることに留意されたい。同様に、安全なコンピュータシステム内のスマートカードデータベースは、証明書およびカードを参照するスマートカードリーダおよび「既知の」スマートカードのリストを含む。ユーザレベルエージェントは、秘密鍵のロケーションが「最新の状態に保たれる」ことを確実にする（これはスマートカードをオンザフライで切り替えることが必要になった場合に定期的に生じる）。また、いくつかのスマートカードは特定の場所（例えば、「オフィスでのみ」）でのみ使用できるように制限され、コーヒーショップでラップトップから作業する場合、ユーザはこのようなスマートカードの使用を妨げられる。本明細書で説明する実施形態ではアプリケーションプログラムがスマートカードデータベースおよび証明書ストアを通常通り使用するが、格納された「参照先」のリストによって、ユーザレベルエージェント２０６が秘密鍵へのアクセスを得る目的で呼び出される。

【００４０】

４１２において、ユーザレベルエージェントが秘密鍵オペレーションの要求を受信すると、４１４において、ユーザレベルエージェントはプロンプト（例えば、ユーザ表示画面に表示されたプロンプト）を開始し、ユーザに秘密鍵オペレーションの実行に同意するように要求する。この要求は、特定のユーザ証明書の要求も含むことができる。例えば、ユーザは、チャレンジに応答する（パスワードを入力する、スマートカードを挿入する、指紋リーダを使用する）必要があるかもしれない。本明細書で説明されるユーザレベルエージェントは、有利には仮想スマートカードの特定の「ユーザビリティ」機能を管理する役割を果たす。例えば、ユーザは、特定のアプリケーションに対して仮想スマートカードを使用するように一回だけ、または場合によっては５分毎に一回だけプロンプトされるべきであると決定されてもよい。

【００４１】

必要な同意および必要な資格証明データがいったん得られると、ユーザレベルエージェントは、システムレベルエージェントと交渉して（４１６）、一回使用のクッキーを得る。また、このプロセスは、ユーザが秘密鍵オペレーションの要求に関与していることをシステムレベルエージェントに通知する役割も果たす。システムレベルエージェントはまたプライベートマシンにおけるオペレーションのロギングおよび監査を担当する。したがって、システムレベルエージェントは、ユーザが秘密鍵オペレーションの要求を開始するたびに適切なログ入力を行うことができる。これは、後に、ＶＳＳに保持された中央レコードに対してクロスチェックすることができる。

【００４２】

４１８において、システムレベルエージェントはユーザが秘密鍵オペレーションを許可したことをＶＳＳに通知し、ＶＳＳは、４２０において、必要とされる一回使用のクッキーを提供することによって応答する。システムレベルエージェントは４２２において、一回使用のクッキーをユーザレベルエージェントに通信し、それにより、ユーザレベルエージェントがＶＳＳから直接秘密鍵オペレーションを求めることを可能にする。より詳細には４２４において、ユーザレベルエージェントは必要な認証データ、一回使用のクッキーおよび秘密鍵要求データをＶＳＳに通信する。ユーザの資格証明（例えば、パスワード、バイオメトリックスキャンデータ）に加えて、認証データは、以下のような、すなわち、ユーザ名、認証オペレーションが要求されている場所、認証要求の時刻、どのアプリケーションプログラムが要求を開始したかなどの情報を含むことができる。秘密鍵オペレーションがＶＳＳで承認された場合、ユーザレベルエージェントは、４２６で、ＶＳＳから秘密鍵オペレーション応答を引き続き受信する。次いで、４２８において、ユーザレベルエージェントは、要求を開始したアプリケーションが秘密鍵応答データを利用可能にする。その後、プロセスは４３０で終了するか、または続行することができる。

【００４３】

以下、ＶＳＳの動作を図５Ａおよび５Ｂを参照して説明する。プロセスは５０２で開始し、５０４に進み、ＶＳＳはコンピュータシステム認証プロセスに参加するために、リモートコンピュータのシステムレベルエージェントによって開始された要求を受信する。プ

ロセスは５０６に進み、ＶＳＳはクライアントコンピュータシステムとの認証プロセスに従事する。この目的のために使用することができる例示的な機械認証プロトコルは、よく知られているＫｅｒｂｅｒｏｓ識別プロトコルまたは従来のトランスポート層セキュリティ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ：ＴＬＳ）クライアント認証プロトコルを含むことができる。５０８において、認証プロセスが成功したかどうかに関する判定が行われる。そうである場合（５０８：はい）、プロセスは５１２に進み、リモートクライアントコンピュータは、その後、信頼されるコンピュータシステムとしてＶＳＳにリストされる。認証プロセスが失敗した場合、認証要求は５１０で拒否され、プロセスは次の要求を処理するために５０４に戻る。

【００４４】

次の時点で、ＶＳＳは、リモートクライアントコンピュータシステムのシステムレベルエージェントから新しいユーザ通知を受信することができる（５１４）。そのような通知が受信されると、ＶＳＳは、秘密鍵オペレーションのために特定のユーザの仮想スマートカードを準備することができる（５１６）。例えば、これらの動作は、ユーザの仮想スマートカードのうちの一つまたはそれ以上に関連付けられた秘密鍵データ１１４を安全なデータベースから検索することを含むことができる。一般に、秘密鍵データは、安全なデータストア１０３に記憶される。あるいは、秘密鍵が暗号化されてメインデータストア１０５に格納されてもよく、その場合、秘密鍵はそれが使用されるときに、安全なデータストア１０３にインポートされ得る。ユーザが以前にシステムを使用しなかった場合、ＶＳＳは、「証明書プロビジョニング」を実行する権限を与えられ得る。これは、スマートカードをユーザに発行する際にシステム管理者が実行するステップの自動バージョンである。事実上、ＶＳＳは、システム管理者と同様に信頼され、特定のユーザグループのための新しいスマートカードおよび証明書を登録する。これは、登録オーソリティとしてＶＳＳを中央認証オーソリティに統合することによって行われる。

【００４５】

ＶＳＳは、ユーザの存在の発生またはリモートクライアントコンピューティングシステムにおけるログインをトランザクションログ１１８に記録することもできる。その後、ＶＳＳは、５１８において、リモートクライアントコンピュータシステムで実行されるシステムレベルエージェントから秘密鍵要求が受信されるのを待つ間、他のアクションを実行することができる。システムレベルエージェントからの秘密鍵要求は、ユーザが秘密鍵オペレーションを実行しようと試みているかまたは実行しようとしていることの指示として働く。要求が受信された場合（５１８：Ｙｅｓ）、ＶＳＳは、一回使用のクッキーを生成する。次いで、このクッキーは、５２０で、要求を開始したリモートクライアントコンピュータシステムのシステムレベルエージェントに通信される。ＶＳＳは、監査目的でクッキーの生成および配信イベントを記録することもできる。

【００４６】

ＶＳＳは、本明細書で説明される特定のイベントに関してロギング動作を実行することに限定されないことに留意されたい。その代わりに、ＶＳＳは、仮想スマートカード使用の監査およびロギングに関して関連があるとみなされ得る多種多様なイベントおよびデータをログすることができる。例えば、ＶＳＳは使用されている特定の仮想スマートカード、実行されている仮想スマートカードオペレーション（例えば、署名または解読）、安全なコンピュータシステムにおいて仮想スマートカードを使用している特定のアプリケーションプログラム、仮想スマートカードを使用する要求を許可したユーザ、許可が発生した安全なコンピュータシステム、およびユーザが最初にログインした位置を記録することができる。

【００４７】

プロセスは５２２に進み、ＶＳＳは、リモートクライアントコンピュータのユーザレベルエージェントから秘密鍵オペレーション要求を受信するのを待つ。ＶＳＳは、そのような要求を待つ間、他の動作を実行することができる。秘密鍵オペレーション要求が受信された場合（５２２：Ｙｅｓ）、プロセスは５２４に進み、提供された認証情報がＶＳＳに

よって評価される。この評価プロセスは、ユーザ認証情報を、安全なデータベースに含まれるユーザ認証データ１１２と比較することを含むことができる。ＶＳＳは、将来の監査の目的で、評価イベントをトランザクションログ１１８に記録することもできる。

【００４８】

ＶＳＳは、異なる仮想スマートカードを使用する権限を制御するために選択的に適用することができるセキュリティポリシー１１０の一つまたは複数のセットを有することができる。ユーザ証明書が受け入れられない場合（５２６：Ｎｏ）、秘密鍵オペレーション要求は拒否され、イベントが５２８で記録される。そのようなシナリオでは、プロセスはユーザ認証データが受信されるのを待つために、オプションとして５２２に戻ることができる。しかし、ユーザ証明書が受け入れられた場合（５２６：はい）、ＶＳＳは、５３０において、リモートクライアントコンピュータシステムにおけるユーザレベルエージェントによって要求された特定の秘密鍵オペレーションを実行することができる。ＶＳＳで実行されるこれらの秘密鍵オペレーションは例えば、ＶＳＳに通信された署名済みまたは解読済みデータの安全なハッシュを生成することを含むことができる。

【００４９】

その後、プロセスはステップ５３２に進み、秘密鍵オペレーションの結果（例えば、署名されたデータまたは解読されたデータの安全なハッシュ）が、リモートクライアントコンピュータシステムのユーザレベルエージェントに通信される。このイベントは、将来の監査目的のためにＶＳＳによってログ記録することもできる。このプロセスは、その後、５３４で終了するか、または続行することができる。

【００５０】

ほとんどの従来のスマートカードは、ＲＳＡまたは楕円曲線秘密鍵のためにハードコードされている。したがって、本明細書で説明される方法およびシステムは秘密鍵を使用する署名および認証を容易にするために（すなわち、ＶＳＳサーバで秘密鍵オペレーションを実行することによって）使用することができる。しかし、当然のことながら、実施形態はこの点に関して限定されない。従来のスマートカードには、利用可能な限られたメモリ内に収まる任意のプログラムをロードすることができる。最も進歩したタイプの従来のスマートカードは、カード上で指紋照合または虹彩スキャンアルゴリズムを実行することができる。したがって、本明細書で開示される様々な実施形態では、そのような動作の態様が代わりに、ＶＳＳにおける仮想スマートカードによって実行することができる。実際、本明細書に記載される仮想スマートカードは物理的スマートカードが可能な任意の機能を提供するために使用することができるが、コストは大幅に低減される。

【００５１】

さらに、図３－５に関して開示されているプロセスは、ユーザがリモートクライアントコンピュータシステムに既にログインしている場合に、一つまたは複数の仮想スマートカードを使用するというコンテキストで説明したことに留意されたい。しかし、本明細書で説明する方法およびシステムは、ログインプロセスにも拡張できることを理解されたい。例えば、安全なクライアントコンピュータに接続されたカスタムデバイスは、バイオメトリックスキャンおよびパスワードプロンプトを使用することができる。この組み合わせはほとんどのオペレーティングシステムにとって異常な認証オプションであるが、本明細書で説明する実施形態はこのプロセスを標準的なスマートカードログオンのように見せることができる。

【００５２】

本明細書で説明するシステムおよび方法ではユーザが一つまたは複数の仮想スマートカードに関連付けられた一つまたは複数の秘密鍵を使用することは許可されるが、そのような情報への直接アクセスは決して許可されない。一つまたは複数の秘密鍵の各使用は、ＶＳＳに委任される。したがって、ＶＳＳは、特定の仮想スマートカードに関連付けられた各秘密鍵のあらゆる使用の安全な監査ログを作成することができる。さらに、必要が生じた場合、管理者は、一つまたは複数の仮想スマートカード／秘密鍵への特定のユーザのアクセスを終了するようにＶＳＳに直ちに指示することができる。従業員から物理的なスマ

ートカードを収集する必要はなく、スマートカードを使用する能力を無効にする際の遅延もない。新しい（または一時的な）スマートカードがユーザに発行される必要がある場合、プロセスはＶＳＳ管理者によって直ちに実行され、仮想スマートカードはユーザによって直ちに仮想的にアクセスされることができる。

【００５３】

本明細書で説明されるシステムのさらなる利点に関しては、システムレベルエージェント、ユーザレベルエージェント、およびＶＳＳは、ユーザがアクセスを許可される各仮想スマートカードの使用に合わせて調整された異なる柔軟なセキュリティポリシーのセットをそれぞれ適用できることである。システムレベルエージェント、ユーザレベルエージェント、およびＶＳＳの各々で適用されるこれらのポリシーは、プロセスに関与する他のエンティティの各々によって適用されるポリシーとは独立して、選択的に適用することができる。

【００５４】

また、仮想スマートカードを使用するときに必要とされる実際の物理的トークンがないので、エンドユーザがそのようなトークンを失ったり、忘れたりする機会がない。したがって、特定のトランザクションを許可する証明書は、ユーザのアイデンティティから分離される。この利点をよりよく理解するために、セキュリティ監査人のグループを含む例示的な使用事例を考える。監査人は、書類の見直しのために交替勤務をしていると仮定する。そのようなシナリオでは、当局が各監査員に独自のカードを与える必要があるか、または交代の終わりに次の監査員に物理的に渡される一つのカードを共有する必要がある。これらのシステムのいずれも特に満足できるものではない。多くのスマートカードの存在は、紛失または誤用の可能性を増大させる手段となる。しかし、一つのスマートカードを共有することは、特に２人の人が同時に働くか、または異なる場所で働く場合に問題がある。多数のユーザが同じＶＳＳにアクセスすることができるので、ＶＳＳは、同じスマートカードを多数のユーザに同時に提供することができる。同様に、電話などのいくつかのモバイルデバイスに対する重大な制限である、特定のベンダーのスマートカードリーダーハードウェアの必要性はもはやない。ハードウェアを必要としないことは、そのようなシステムの購入および所有のコストも低減する。

【００５５】

最後に、個々の所有権のあるスマートカードベンダーによって提供されるソフトウェアから離れることによって、本明細書で説明される仮想スマートカードソリューションは、ユーザが見るプロンプトのカスタマイズ、およびより柔軟な認証オプションを可能にする。プロンプトおよび認証オプションは、スマートカード製造業者によって供給されるスマートカードミドルウェアドライバのバージョンとは無関係になる。特に、どのアプリケーションが、どの識別証明およびどのくらいの頻度でユーザにプロンプトを出すかについての制御が提供される。対照的に、ハードウェアソリューションは、次のような制限的なハードコード化要求を有する傾向がある。「ユーザが４桁のＰＩＮを入力する限り、ユーザがアクションを実行するたびに繰り返し、任意のコンピュータ上の任意のアプリケーションがこれを使用することができる。」

【００５６】

本明細書に開示される本発明の構成の実施形態は、一つのコンピュータシステムにおいて実現することができる。代替される実施形態は、いくつかの相互接続されたコンピュータシステムで実現することができる。本明細書に記載の方法を実行するように適合された任意の種類のコンピュータシステムまたは他の装置が適している。ハードウェアとソフトウェアの典型的な組み合わせは、汎用コンピュータシステムであり得る。汎用コンピュータシステムは、本明細書で説明する方法を実行するようにコンピュータシステムを制御することができるコンピュータプログラムを有することができる。

【００５７】

次に図６を参照すると、例示的なコンピュータシステム６００を備えるマシンの構成を理解するのに有用なハードウェアブロック図が示されている。マシンは本明細書で論じら

れる方法のうちの任意の一つまたはそれ以上を実行させるために使用される命令のセットをコンピュータシステムに含むことができる。ネットワーク化された配備では、マシンがサーバまたはクライアントマシンとして機能することができる。一つまたは複数の実施形態では、例示的なコンピュータシステム６００が安全なコンピュータシステム１０６$_1$－１０６$_n$のそれぞれおよび／またはＶＳＳ１０２に対応することができる。いくつかの実施形態では、コンピュータ６００がスタンドアロンデバイスとして独立して動作することができる。しかし、複数の実施形態はこの点に関して限定されず、他のシナリオではコンピュータシステムが分散環境内の他のマシンに動作可能に接続（ネットワーク化）して、本明細書で説明する特定の動作を容易にすることができる。したがって、単一のマシンのみが示されているが、本発明の実施形態は本明細書で説明されるような命令の一つまたは複数のセットを個々にまたは共同で実行するマシンの任意の集合を含むとみなすことができることを理解されたい。

【００５８】

コンピュータシステム６００は、プロセッサ６０２（例えば中央処理部やＣＰＵ）、メインメモリ６０４、スタティックメモリ６０６、機械可読媒体６２０からなるドライブユニット６０８、入力／出力デバイス６１０、ディスプレイユニット６１２（液晶ＬＣＤ）、固体ディスプレイ、ブラウン管（ＣＲＴ）、ネットワークインターフェースデバイス６１４で構成されている。これらの様々なコンポーネント間の通信は、データバス６１８によって容易にすることができる。一つまたは複数の命令セット６２４は、メインメモリ６０４、スタティックメモリ６０６およびドライブユニット６０８のうちの一つまたは複数に完全にまたは部分的に格納することができる。また、命令はコンピュータシステムによるプロセッサ６０２の実行中に、プロセッサ６０２内にあるようにすることもできる。

【００５９】

入力／出力デバイス６１０はキーボード、マウス、マルチタッチ表面（例えば、タッチスクリーン）、マイクロフォン、カメラなどを含むことができる。安全なコンピュータシステム１０６$_1$－１０６$_n$では、入力／出力デバイスがユーザの生態情報をキャプチャするのに適した一つまたは複数のバイオメトリックキャプチャデバイスをさらに含むことができる。このようなユーザ生体情報は、ユーザ認証情報を含むことができる。このような情報は安全なコンピュータシステムに対するユーザによる最初のログインを容易にするために、安全なコンピュータシステム１０６$_1$－１０６$_n$によって使用され得る。あるいは、このような情報がＶＳＳに対するユーザの認証のために使用され得る。例えば、ユーザ生体情報は、秘密鍵オペレーションの要求の一部としてユーザを認証するためにＶＳＳに通信され得る。同様に、そのようなシナリオにおける入力／出力デバイス６１０は、ユーザによって提示される物理的なスマートカードに含まれる情報を読み取ることができる物理的なスマートカードリーダを含むことができる。スマートカードに含まれる情報は秘密鍵オペレーションが要求されたときに、安全なコンピュータへのユーザログインを円滑にするために、および／またはユーザ認証情報として用いることができる。

【００６０】

ネットワークインターフェースデバイス６１４はデータネットワーク６１６によって利用されるネットワーク通信プロトコルに従って有線または無線ネットワークデータ通信を容易にするために、ハードウェアコンポーネントおよびソフトウェアまたはファームウェアを備えることができる。

【００６１】

ドライブユニット６０８は機械可読媒体６２０を備えることができ、機械可読媒体６２０には、本明細書で説明する方法および機能のうちの一つまたは複数を容易にするために使用される一つまたは複数の命令セット６２４（たとえば、ソフトウェア）が格納される。「機械可読媒体」という用語は、本開示の方法論のうちの任意の一つまたは複数を容易にする命令またはデータ構造を記憶することができる任意の有形媒体を含むと理解されたい。例示的な機械可読媒体は、磁気媒体、固体メモリ、光媒体などを含むことができる。より詳細には、本明細書で説明する有形媒体が磁気ディスク、光磁気ディスク、ＣＤ－Ｒ

ＯＭディスクおよびＤＶＤ－ＲＯＭディスク、半導体メモリデバイス、電気的消去可能プログラマブル読み出し専用メモリ（ＥＥＰＲＯＭ）およびフラッシュメモリデバイスを含むことができる。本明細書に記載されるような有形の媒体は伝播する信号を含まない限り、非一時的な媒体である。

【００６２】

本明細書で参照されるコンピュータシステムは、サーバコンピュータ、クライアントユーザコンピュータ、パーソナルコンピュータ（ＰＣ）、タブレットＰＣ、ラップトップコンピュータ、デスクトップコンピュータ、制御システム、ネットワークルータ、スイッチまたはブリッジ、またはそのデバイスによってとられるべき動作を指定する命令のセット（シーケンシャルまたはその他）を実行することができる任意の他のデバイスを含む、様々なタイプのコンピューティングシステムおよびデバイスを備えることができる。さらに、単一のコンピュータが示されているが、「コンピュータシステム」という語句は本明細書で論じられる方法のうちの任意の一つまたは複数を実行するための命令のセット（または複数のセット）を個々にまたは共同で実行するコンピューティングデバイスの任意の集合を含むと理解されるべきである。

【００６３】

したがって、コンピュータシステム６００は、様々な実施形態に関連して使用することができるコンピュータシステムの一つの可能な例であることを理解されるべきである。しかし、本発明は、この点に関して限定されず、任意の他の適切なコンピュータシステムアーキテクチャも、限定なしに使用することができる。特定用途向け集積回路、プログラマブル論理アレイ、および他のハードウェアデバイスを含むが、これらに限定されない、専用ハードウェア実装を、同様に、本明細書で説明される方法を実装するように構築することができる。様々な実施形態の装置およびシステムを含むことができるアプリケーションは、様々な電子システムおよびコンピュータシステムを広く含む。いくつかの実施形態は、モジュール間およびモジュールを介して通信される関連する制御信号およびデータ信号に関する２つ以上の特定の相互接続されたハードウェアモジュールまたはデバイスまたは特定用途向け集積回路の一部として、機能を実装することができる。したがって、例示的なシステムは、ソフトウェア、ファームウェアおよびハードウェア実装に適用可能である。

【００６４】

さらに、実施形態は有形のコンピュータ使用可能記憶媒体（例えば、ハードディスクまたはＣＤ－ＲＯＭ）上のコンピュータプログラム製品の形態をとることができることを理解されたい。コンピュータ使用可能記憶媒体は、媒体内に具現化されたコンピュータ使用可能プログラムコードを有することができる。本明細書で使用されるコンピュータプログラム製品という用語は、本明細書で説明される方法の実施を可能にするすべての特徴を備えるデバイスを指す。コンピュータプログラム、ソフトウェアアプリケーション、コンピュータソフトウェアルーチンおよび／または本コンテキストにおけるこれらの用語の他の変形は情報処理能力を有するシステムに、直接または次の、すなわち、ａ)別の言語、コード、または表記への変換、またはｂ）異なる材料形式での複製のいずれかまたは両方の後に、特定の機能を実行させることを意図した命令セットの、任意の言語、コード、または表記による任意の表現を意味する。

【００６５】

本発明は、本発明の思想及び基本的特徴から逸脱することなく、他の特定の形で具体化され得る。説明した実施形態は、あらゆる点で例示的なものにすぎず、限定的なものではないとみなすべきである。したがって、本発明の範囲は、この詳細な説明ではなく、添付の特許請求の範囲によって示される。特許請求の範囲と等価の意味および範囲内にある全ての変更は、その範囲内で含まれるものとする。

【００６６】

本明細書全体を通して、特徴、利点または類似の言葉への参照は本発明で実現され得る特徴および利点の全てが、本発明の任意の単一の実施形態にあるべきまたはあることを意

味しない。むしろ、特徴および利点を参照する言葉は、一実施形態に関連して説明された特定の特徴、利点または特性が本発明の少なくとも一つの実施形態に含まれることを意味すると理解される。したがって、本明細書全体にわたる特徴および利点ならびに類似の言葉の議論は必ずしもそうとは限らないが、同じ実施形態を参照することができる。

【００６７】

さらに、本発明の記載された特徴、利点および特徴は、一つ以上の実施形態において任意の適切な様式で組み合わされ得る。当業者は、本明細書の説明に照らして、特定の実施形態の特定の特徴または利点のうちの一つまたは複数なしに本発明を実施できることを認識するのであろう。他の例では、追加の特徴および利点が本発明のすべての実施形態に存在しなくてもよい特定の実施形態において認識されてもよい。

【００６８】

本明細書全体を通して、「一実施形態」、「実施形態」または類似の言葉への参照は、示された実施形態に関連して記載された特定の機能、構成または特徴が少なくとも一つの実施形態に含まれることを手段する。したがって、本明細書全体にわたる「一実施形態では」、「一実施形態では」、および類似の言葉は必ずしもそうとは限らないが、すべてが同じ実施形態を指す場合がある。

【００６９】

本明細書で使用されるように、単数形「ａ」、「ａｎ」、および「ｔｈｅ」は文脈が明確に別段の指示をしない限り、複数の参照を含む。別途定義しない限り、本明細書で使用するすべての技術的および科学的用語は、当業者によって一般に理解されるのと同じ意味を有する。本明細書で使用されるように、「備える」という語は「含むが、これに限定されない」を手段する。

【００７０】

当業者は、図６に示すコンピュータシステムアーキテクチャがコンピュータシステムの一つの可能な例であることを理解するのであろう。しかし、本発明は、この点に関して限定されず、任意の他の適切なコンピュータシステムアーキテクチャも限定なしに使用することができる。特定用途向け集積回路、プログラマブル論理アレイ、および他のハードウェアデバイスを含むが、これらに限定されない、専用ハードウェア実装を、同様に、本明細書で説明される方法を実装するように構築することができる。様々な実施形態の装置およびシステムを含むことができるアプリケーションは、様々な電子システムおよびコンピュータシステムを広く含む。いくつかの実施形態は、モジュール間およびモジュールを介して通信される関連する制御信号およびデータ信号に関する２つ以上の特定の相互接続されたハードウェアモジュールまたはデバイスまたは特定用途向け集積回路の一部として、機能を実装することができる。したがって、例示的なシステムは、ソフトウェア、ファームウェアおよびハードウェア実装に適用可能である。

【００７１】

本発明の様々な実施形態によれば、本明細書で説明される方法は、ソフトウェアプログラムとして機械可読記憶媒体に格納され、コンピュータプロセッサ上で動作するように構成される。さらに、ソフトウェア実装は分散処理、コンポーネント／オブジェクト分散処理、並列処理、仮想マシン処理を含むことができるが、これらに限定されず、これらもまた、本明細書で説明される方法を実装するように構築することができる。本発明の様々な実施形態では、ネットワーク環境に接続されたネットワークインターフェースデバイス６１４が命令６２４を使用してネットワーク上で通信する。

【００７２】

機械可読記憶媒体６２０は例示的な実施形態では単一の記憶媒体として示されているが、「機械可読記憶媒体」という用語は一つまたは複数の命令セットを記憶する単一の媒体または複数の媒体（例えば、集中型または分散型データベース、ならびに／または関連するキャッシュおよびサーバ）を含むと解釈されるべきである。用語「機械可読記憶媒体」はまた、機械による実行のための命令のセットを記憶し、符号化し、または運搬することができ、機械に本開示の方法論のうちの任意の一つまたは複数を実行させる任意の有形媒

体を含むと解釈されるべきである。

【００７３】

したがって、「機械可読記憶媒体」という用語は限定しないが、一つまたは複数の読み取り専用（不揮発性）メモリ、ランダムアクセスメモリ、または他の書き換え可能（揮発性）メモリを収容するメモリカードまたは他のパッケージなどの固体メモリ、ディスクまたはテープなどの光磁気媒体または光媒体を含むと解釈されるべきである。したがって、本開示は本明細書で列挙される機械可読媒体のうちの任意の一つまたは複数を含み、本明細書のソフトウェア実装が格納される、認識された均等物および後続の媒体を含むとみなされる。

【００７４】

本発明を一つまたは複数の実施に関して例示および説明したが、本明細書および添付の図面を読んで理解すれば、同等の変更および修正が当業者に思い浮かぶことができる。さらに、本発明の特定の特徴はいくつかの実装のうちの一つのみに関して開示されている可能性があるが、そのような特徴は任意の所与のまたは特定の用途に対して所望され得、有利であり得るように、他の実装の一つまたは複数の他の特徴と組み合わされ得る。したがって、本発明の広さおよび範囲は、上述の実施形態のいずれによっても限定されるべきではない。むしろ、本発明の範囲は、以下の特許請求の範囲およびそれらの均等物に従って定義されるべきである。

【図１】

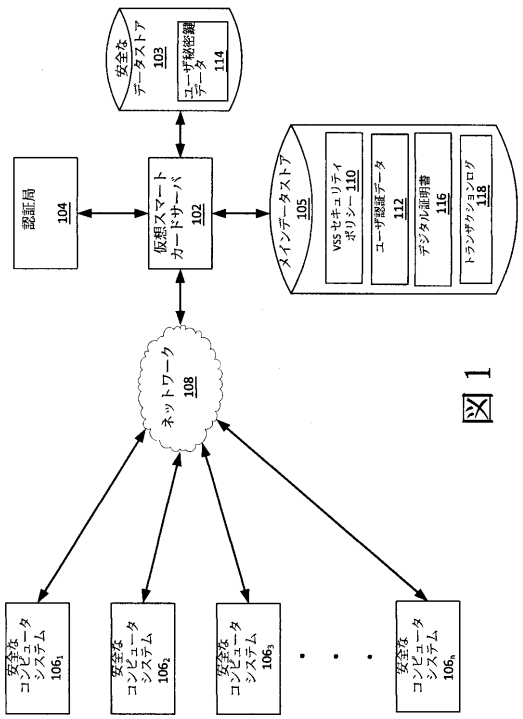

図１

【図２】

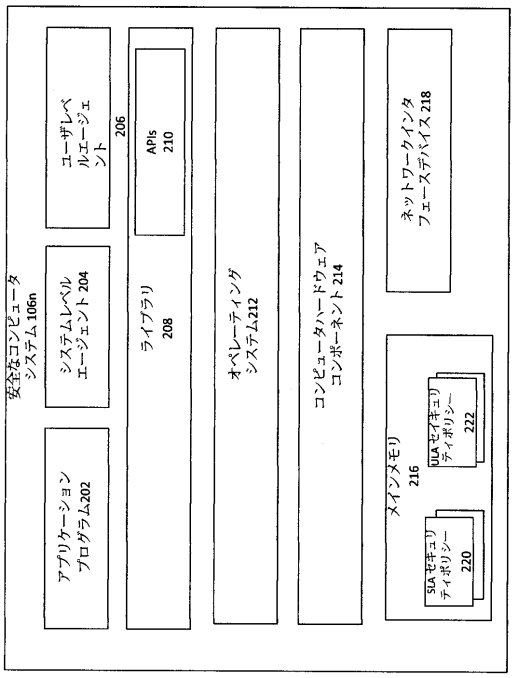

図２

【図３】

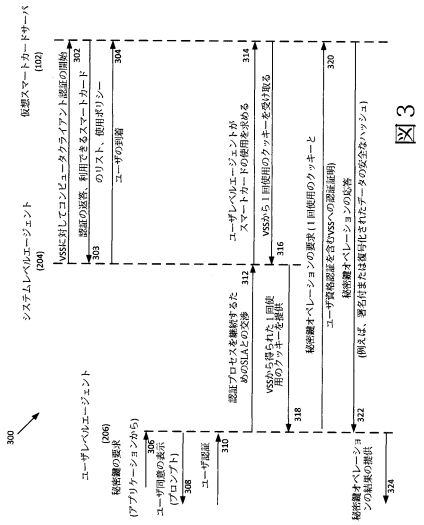

図３

【図４Ａ】

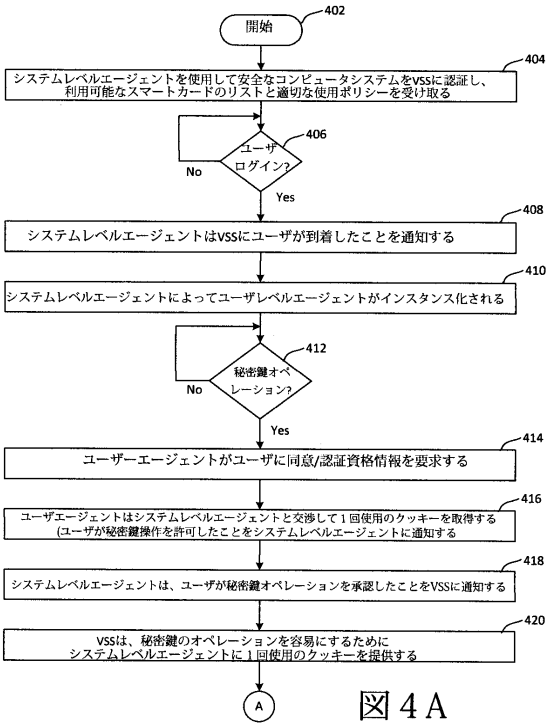

図４Ａ

【図４Ｂ】

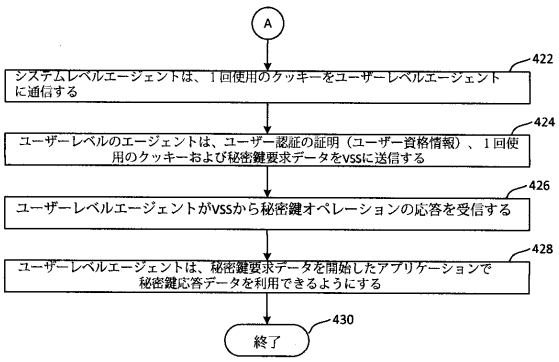

図４Ｂ

【図５Ａ】

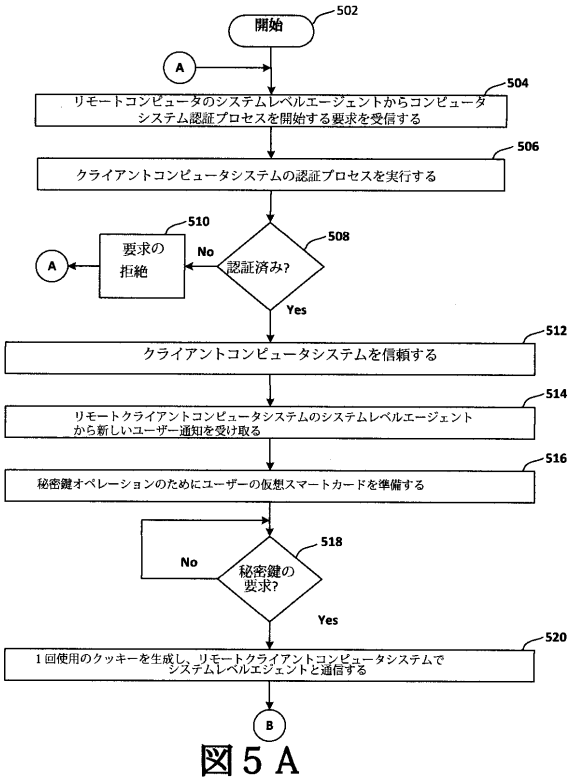

図５Ａ

【図５Ｂ】

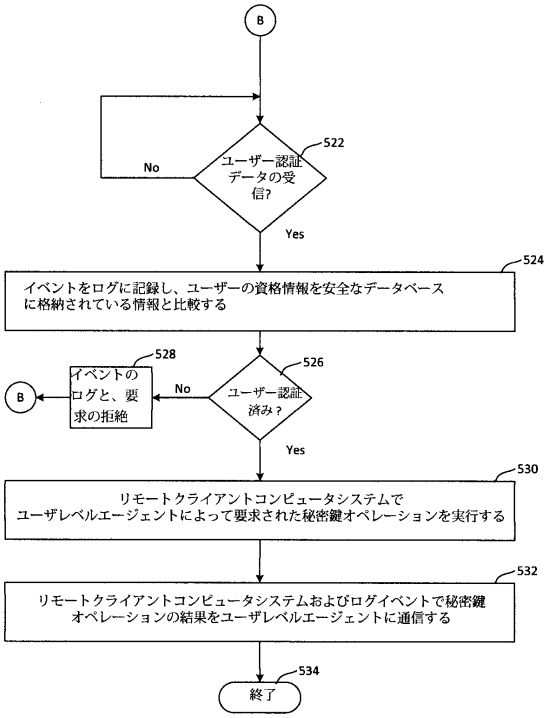
B
ユーザー認証データの受信?
522
No
Yes
イベントをログに記録し、ユーザーの資格情報を安全なデータベースに格納されている情報と比較する
524
ユーザー認証済み?
526
No
イベントのログと、要求の拒絶
528
B
Yes
リモートクライアントコンピュータシステムでユーザレベルエージェントによって要求された秘密鍵オペレーションを実行する
530
リモートクライアントコンピュータシステムおよびログイベントで秘密鍵オペレーションの結果をユーザレベルエージェントに通信する
532
終了
534

図５Ｂ

【図６】

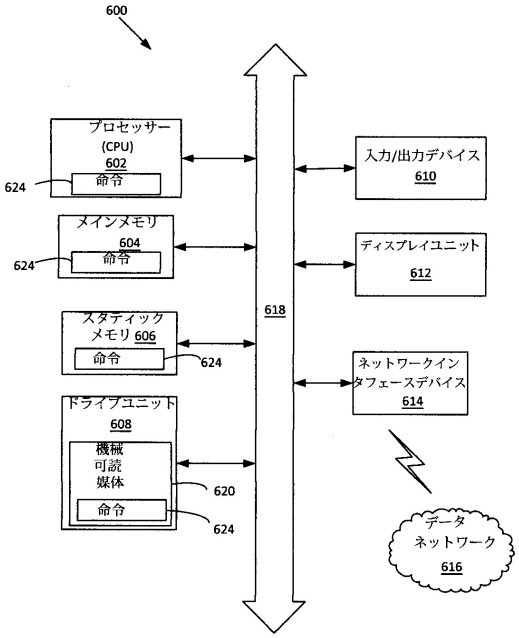
600
プロセッサー (CPU) 602
命令
624
メインメモリ 604
命令
624
スタティックメモリ 606
命令
624
ドライブユニット 608
機械可読媒体
620
命令
624
618
入力/出力デバイス 610
ディスプレイユニット 612
ネットワークインタフェースデバイス 614
データネットワーク 616

図６

フロントページの続き

審査官　行田　悦資

(56)参考文献　特開２０００－２２１８８１（ＪＰ，Ａ）
米国特許出願公開第２００２／０１８４５０７（ＵＳ，Ａ１）
特開２０１３－１９２１２５（ＪＰ，Ａ）
特表２００５－５０２２１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／６２