【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和2年4月16日(2020.4.16)

【公表番号】特表2019-525519(P2019-525519A)
【公表日】令和1年9月5日(2019.9.5)
【年通号数】公開・登録公報2019-036
【出願番号】特願2018-563664(P2018-563664)
【国際特許分類】
*Ｈ０４Ｌ　9/08　(2006.01)*
*Ｇ０６Ｆ　21/31　(2013.01)*
*Ｇ０６Ｆ　21/62　(2013.01)*
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｇ０６Ｆ　21/31
Ｇ０６Ｆ　21/62　３１８

【手続補正書】
【提出日】令和2年3月6日(2020.3.6)
【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】
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にそれぞれ割り当てられている複数の秘密鍵を、仮想スマートカードサーバ（ＶＳＳ：ｖｉｒｔｕａｌ　ｓｍａｒｔ　ｃａｒｄ　ｓｅｒｖｅｒ）に対してのみアクセス可能な安心なデータストアに格納すること、
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におけるシステムレベルエージェントを使用して、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秘密鍵操作の要求を受信したことに応答して、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に前記システムレベルエージェントと交渉させて前記ＶＳＳから前記秘密鍵操作を許可するクッキーを取得させること、
前記ユーザレベルエージェントから前記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から前記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で選択的に実行することを含む、方法。
【請求項２】
前記秘密鍵オペレーションの結果を前記ＶＳＳから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、前記ユーザレベルエージェントにおける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ＶＳＳにおける前記クッキーの使用を制限し、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ようにすることをさらに含む、請求項１に記載の方法。
【請求項６】
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ために、前記ＶＳＳにおいて実行される前記秘密鍵オペレーションを選択することをさらに含む、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において、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】
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前記ＶＳＳに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にそれぞれ割り当てられている複数の秘密鍵を、仮想スマートカードサーバ（ＶＳＳ：ｖｉｒｔｕａｌ　ｓｍａｒｔ　ｃａｒｄ　ｓｅｒｖｅｒ）に対してのみアクセス可能な安心なデータストアに格納すること、
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前記ＶＳＳにおいて受信すること、
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において、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前記ＶＳＳで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。