(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7299971号
(P7299971)

(45)発行日　令和5年6月28日(2023.6.28)

(24)登録日　令和5年6月20日(2023.6.20)

(51)国際特許分類			FI		
H04L	*9/32*	*(2006.01)*	H04L	9/32	200B
G06F	*21/64*	*(2013.01)*	G06F	21/64	350
G06Q	*20/40*	*(2012.01)*	G06Q	20/40	
G09C	*1/00*	*(2006.01)*	G09C	1/00	640D

請求項の数　18　（全49頁）

(21)出願番号　特願2021-514956(P2021-514956)
(86)(22)出願日　令和1年6月25日(2019.6.25)
(65)公表番号　特表2021-524216(P2021-524216A)
(43)公表日　令和3年9月9日(2021.9.9)
(86)国際出願番号　PCT/US2019/039073
(87)国際公開番号　WO2020/006001
(87)国際公開日　令和2年1月2日(2020.1.2)
審査請求日　令和2年11月17日(2020.11.17)
(31)優先権主張番号　62/689,462
(32)優先日　平成30年6月25日(2018.6.25)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/712,974
(32)優先日　平成30年8月1日(2018.8.1)
最終頁に続く

(73)特許権者　520450950
オース９ インコーポレイテッド
アメリカ合衆国 カリフォルニア州 ９４４０４ フォスター シティ ヴァスコ ダガマ レーン ９７３
(74)代理人　100094569
弁理士　田中 伸一郎
(74)代理人　100103610
弁理士　▲吉▼田 和彦
(74)代理人　100109070
弁理士　須田 洋之
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100109335
弁理士　上杉 浩
最終頁に続く

(54)【発明の名称】　デジタルシールされたアセットを作成および登録し、デジタルシールされたアセットが本物であるかを確認するための方法、コンピュータプログラム製品および装置

(57)【特許請求の範囲】

【請求項１】

登録された証明済みシールを生成するための装置であって、前記装置は、少なくとも１つのプロセッサと、コンピュータコード化命令をその中に有する少なくとも１つのメモリとを備え、前記コンピュータコード化命令は、前記プロセッサによって実行されたとき、

エンティティから、証明済みシールを生成する要求を受信することであって、前記要求は、公開鍵秘密鍵ペアの公開鍵を備えるデジタル署名されたエンティティ証明証明書を備える、受信することと、

前記デジタル署名されたエンティティ証明証明書によって識別された証明機関の証明者エンティティデータにアクセスすることと、

前記デジタル署名されたエンティティ証明証明書と関連付けられ、前記証明機関からアクセスされる前記証明者エンティティデータに少なくとも部分的に基づいて、前記デジタル署名されたエンティティ証明証明書が本物であるか確認することと、

前記デジタル署名されたエンティティ証明証明書が本物であることを確認したら、前記証明済みシールのシールデータ鍵を備えるシールデータを受信することと、

前記エンティティの前記シールデータをデジタルシールレジストリ内に保存することであって、前記デジタルシールレジストリは、前記シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である、保存することと、

シールされたアセットが本物であるか確認する要求を受信することであって、前記シールされたアセットは、前記エンティティによって生成され、前記シールデータ鍵を識別し

、前記シールデータ鍵は前記エンティティによって生成され且つ前記シールされたアセットの確認されたデジタル署名と一致する、受信することと、
前記シールデータ鍵に少なくとも部分的に基づいて前記デジタルシールレジストリに問い合わせることと、
前記シールされたアセットによって識別された前記シールデータ鍵に少なくとも部分的に基づいて、前記シールされたアセットが本物であるか確認することと
を前記装置に行わせるように構成されている、装置。
【請求項２】
前記デジタル署名されたエンティティ証明証明書が、前記証明機関によって前記エンティティを証明する、請求項１に記載の装置。
【請求項３】
前記証明機関は、 少なくとも１つの一意のエンティティ識別子に基づいて、前記エンティティが真正であるかどうかを判定することと、
前記エンティティが真正であると判定した後、前記デジタル署名されたエンティティ証明証明書を生成するために、前記少なくとも１つの一意のエンティティ識別子を備えるアイデンティティエンティティデータにデジタル署名すること
を前記装置に行わせるようにさらに構成されている、請求項１に記載の装置。
【請求項４】
前記デジタルシールレジストリが、サービスとしてのソフトウェア（ＳａａＳ）レジストリサービスである、請求項１に記載の装置。
【請求項５】
前記シールデータは、電子シールと、シールメタデータと、前記シールの使用目的、前記シールの使用方法、または前記電子シールが有効である時間範囲のうちの少なくとも１つを示すシーラー情報とを備える、請求項１に記載の装置。
【請求項６】
前記シールデータ鍵が、前記証明済みシールのシール公開鍵、および前記証明済みシールを一意に識別するためのシールデータのうちの少なくとも１つを備える、請求項１に記載の装置。
【請求項７】
登録された証明済みシールを生成するためのコンピュータ実装方法であって、前記方法は、
エンティティから、証明済みシールを生成する要求を受信することであって、前記要求は、公開鍵秘密鍵ペアの公開鍵を備えるデジタル署名されたエンティティ証明証明書を備える、受信することと、
前記デジタル署名されたエンティティ証明証明書によって識別された証明機関の証明者エンティティデータにアクセスすることと、
前記デジタル署名されたエンティティ証明証明書と関連付けられ、前記証明機関からアクセスされる前記証明者エンティティデータに少なくとも部分的に基づいて、前記デジタル署名されたエンティティ証明証明書が本物であるか確認することと、
前記デジタル署名されたエンティティ証明証明書が本物であることを確認したら、前記証明済みシールのシールデータ鍵を備えるシールデータを受信することと、
前記エンティティの前記シールデータをデジタルシールレジストリ内に保存することであって、前記デジタルシールレジストリは、前記シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である、保存することと、
シールされたアセットが本物であるか確認する要求を受信することであって、前記シールされたアセットは、前記エンティティによって生成され、前記シールデータ鍵を識別し、前記シールデータ鍵は前記エンティティによって生成され且つ前記シールされたアセットの確認されたデジタル署名と一致する、受信することと、
前記シールデータ鍵に少なくとも部分的に基づいて前記デジタルシールレジストリに問い合わせることと、

前記シールされたアセットによって識別された前記シールデータ鍵に少なくとも部分的に基づいて、前記シールされたアセットが本物であるか確認することと
を含む、方法。
【請求項８】
前記デジタル署名されたエンティティ証明証明書が、前記証明機関によって前記エンティティを証明する、請求項７に記載のコンピュータ実装方法。
【請求項９】
前記証明機関が、
少なくとも１つの一意のエンティティ識別子に基づいて、前記エンティティが真正であるかどうかを判定し、
前記エンティティが真正であると判定した後、前記デジタル署名されたエンティティ証明証明書を生成するために、前記少なくとも１つの一意のエンティティ識別子を備えるエンティティデータにデジタル署名する、
ように構成されている、請求項７に記載のコンピュータ実装方法。
【請求項１０】
前記デジタルシールレジストリが、サービスとしてのソフトウェア（ＳａａＳ）レジストリサービスである、請求項７に記載のコンピュータ実装方法。
【請求項１１】
前記シールデータは、電子シールと、シールメタデータと、前記シールの使用目的、前記シールの使用方法、または前記電子シールが有効である時間範囲のうちの少なくとも１つを示すシーラー情報とを備える、請求項７に記載のコンピュータ実装方法。
【請求項１２】
前記シールデータ鍵が、前記証明済みシールのシール公開鍵、および前記証明済みシールを一意に識別するためのシールデータのうちの少なくとも１つを備える、請求項７に記載のコンピュータ実装方法。
【請求項１３】
登録された証明済みシールを生成するためのコンピュータプログラム製品であって、前記コンピュータプログラム製品は、非一時的コンピュータ可読記憶媒体、およびそこに記憶されたコンピュータプログラム命令を備え、コンピュータが、
エンティティから、証明済みシールを生成する要求を受信することであって、前記要求は、公開鍵秘密鍵ペアの公開鍵を備えるデジタル署名されたエンティティ証明証明書を備える、受信することと、
前記デジタル署名されたエンティティ証明証明書によって識別された証明機関の証明者エンティティデータにアクセスすることと、
前記デジタル署名されたエンティティ証明証明書と関連付けられ、前記証明機関からアクセスされる前記証明者エンティティデータに少なくとも部分的に基づいて、前記デジタル署名されたエンティティ証明証明書が本物であるか確認することと、
前記デジタル署名されたエンティティ証明証明書が本物であることを確認したら、前記証明済みシールのシールデータ鍵を備えるシールデータを受信することと、
前記エンティティの前記シールデータをデジタルシールレジストリ内に保存することであって、前記デジタルシールレジストリは、前記シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である、保存することと、
シールされたアセットが本物であるか確認する要求を受信することであって、前記シールされたアセットは、前記エンティティによって生成され、前記シールデータ鍵を識別し、前記シールデータ鍵は前記エンティティによって生成され且つ前記シールされたアセットの確認されたデジタル署名と一致する、受信することと、
前記シールデータ鍵に少なくとも部分的に基づいて前記デジタルシールレジストリに問い合わせることと、
前記シールされたアセットによって識別された前記シールデータ鍵に少なくとも部分的に基づいて、前記シールされたアセットが本物であるか確認することと、

を行うためのプログラム命令を記憶した、コンピュータプログラム製品。
【請求項１４】
前記デジタル署名されたエンティティ証明証明書が、前記証明機関によって前記エンティティを証明する、請求項１３に記載のコンピュータプログラム製品。
【請求項１５】
前記証明機関が、
少なくとも１つの一意のエンティティ識別子に基づいて、前記エンティティが真正であるかどうかを判定し、
前記エンティティが真正であると判定した後、前記デジタル署名されたエンティティ証明証明書を生成するために、前記少なくとも１つの一意のエンティティ識別子を備えるアイデンティティエンティティデータにデジタル署名する、
ためのプログラム命令をさらに記憶した、請求項１３に記載のコンピュータプログラム製品。
【請求項１６】
前記デジタルシールレジストリが、サービスとしてのソフトウェア（ＳａａＳ）レジストリサービスである、請求項１３に記載のコンピュータプログラム製品。
【請求項１７】
前記シールデータは、電子シールと、シールメタデータと、前記シールの使用目的、前記シールの使用方法、または前記電子シールが有効である時間範囲のうちの少なくとも１つを示すシーラー情報とを備える、請求項１３に記載のコンピュータプログラム製品。
【請求項１８】
前記シールデータ鍵が、前記証明済みシールのシール公開鍵、および前記証明済みシールを一意に識別するためのシールデータのうちの少なくとも１つを備える、請求項１３に記載のコンピュータプログラム製品。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本特許出願は、２０１８年６月２５日に出願された米国仮特許出願第６２／６８９，４６２号、２０１８年８月１日に出願された米国仮特許出願第６２／７１２，９７４号、および２０１８年１０月１１日に出願された米国仮特許出願第６２／７４４，５５４号からの優先権を主張し、これらはすべて、参照によりその全体が本明細書に組み込まれる。
【０００２】
本発明の実施形態は、一般に、アセットの認証に関し、より具体的には、証明済みエンティティからの真正の署名されかつシールされた証明の生成に関する。
【背景技術】
【０００３】
商取引がオンラインでますます広がるにつれて、オンラインで送信されたデータの整合性とソースを確認するための技術が重要になっている。
【０００４】
しかしながら、少なくとも部分的には、インターネットベースのトランザクションの本質的に匿名の性質、ならびに情報送信が傍受および／または改ざんされる機会の増加により、デジタルデータの受信者は、デジタルデータの真実性をしばしば確認することができないか、またはその送信者はデジタルデータを見るだけである。したがって、受信機に送信されるデータの真実性は、以前の技術を使用する通信の代替メカニズムによってのみ確認することができた。
【０００５】
したがって、本発明の目的は、上記の問題を解決することができ、デジタルデータが送受信されるときにエンティティ確認およびアセット認証を実現することができる技術を提供することである。結果として、デジタル署名されかつシールされたアセットを認証する

ことができるメカニズムを提供することが望ましい場合がある。さらに、デジタルデータおよびトランザクションの真正性を妥当性検査するために、一般的に信頼できるメカニズムまたはプラットフォームを提供することが望ましい場合がある。

【発明の概要】

【０００６】

概して、本明細書で提供される本発明の実施形態は、登録された証明済みシールを生成し、アセットをシールし、シールされたアセットが本物であるか確認するための方法、装置、およびコンピュータプログラム製品を含む。

【０００７】

いくつかの実施形態では、登録された証明済みシールを生成するための装置が、少なくとも１つのプロセッサと、コンピュータコード化命令をその中に有する少なくとも１つのメモリとを備えて提供され得る。いくつかの実施形態では、本装置は、プロセッサによって実行されたとき、エンティティから、登録された証明済みシールを生成する要求を受信することであって、要求は、公開鍵秘密鍵ペアの公開鍵を備えるデジタル署名されたエンティティ証明証明書を備える、受信することと、証明証明書によって識別された証明機関の証明者エンティティデータにアクセスすることと、証明証明書と関連付けられ、証明機関からアクセスされる証明者エンティティデータに少なくとも部分的に基づいて、デジタル署名されたエンティティ証明証明書が本物であるか確認することとを本装置に行わせるように構成されたコンピュータ命令を備える。デジタル署名されたエンティティ証明証明書が本物であることを確認したら、本装置は、プロセッサによって実行されたとき、証明済みシールのシールデータ鍵を備えるシールデータを受信することと、エンティティのシールデータをデジタルシールレジストリ内に保存することであって、デジタルシールレジストリは、シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である、保存することとを本装置に行わせるようにさらに構成されたコンピュータ命令を含む。デジタルシールレジストリは、サービスとしてのソフトウェア（ＳａａＳ）レジストリサービスである。

【０００８】

例示的な実施形態では、デジタル署名されたエンティティ証明証明書は、証明機関によってエンティティを証明する。

【０００９】

本装置は、少なくとも１つの一意のエンティティ識別子に基づいて、エンティティが真正であるかどうかを判定し、エンティティが真正であると判定した後、エンティティ証明証明書を生成するために、少なくとも１つの一意のエンティティ識別子を備えるアイデンティティエンティティデータにデジタル署名するようにさらに構成される。

【００１０】

別の例示的な実施形態では、シールデータは、電子シールと、シールメタデータと、シールの使用目的、シールの使用方法、または電子シールが有効である時間範囲のうちの少なくとも１つを示すシーラー情報とを備える。シールデータ鍵は、証明済みシールのシール公開鍵、および証明済みシールを一意に識別するためのシールデータを備える。

【００１１】

さらに別の例示的な実施形態では、コンピュータコード化命令は、プロセッサによって実行されたとき、シールされたアセットが本物であるか確認する要求を受信することであって、シールされたアセットは、エンティティによって生成され、シールデータ鍵を識別する、受信することと、シールデータ鍵に少なくとも部分的に基づいてデジタルシールレジストリに問い合わせることと、シールデータ鍵に少なくとも部分的に基づいて、シールされたアセットが本物であるか確認することとを本装置に行わせるようにさらに構成される。

【００１２】

登録された証明済みシールを生成するための方法がさらに提供され、本方法は、エンティティから、登録された証明済みシールを生成する要求を受信することであって、要求は

、デジタル署名されたエンティティ証明証明書を備える、受信することと、証明証明書によって識別された証明機関の証明者エンティティデータにアクセスすることと、証明証明書と関連付けられ、証明機関からアクセスされる証明者エンティティデータに少なくとも部分的に基づいて、デジタル署名されたエンティティ証明証明書が本物であるか確認することとを備える。

【００１３】

本方法は、デジタル署名されたエンティティ証明証明書が本物であることを確認したら、証明済みシールのシールデータ鍵を備えるシールデータを受信することであって、シールデータは、エンティティによって一意に生成される、受信することと、エンティティのシールデータをデジタルシールレジストリ内に保存することであって、デジタルシールレジストリは、シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である、保存することとをさらに備える。

【００１４】

本方法は、少なくとも１つの一意のエンティティ識別子に基づいて、エンティティが真正であるかどうかを判定することと、エンティティが真正であると判定した後、エンティティ証明証明書を生成するために、少なくとも１つの一意のエンティティ識別子を備えるアイデンティティエンティティデータにデジタル署名することとをさらに備える。

【００１５】

さらに別の例示的な実施形態では、本方法は、シールされたアセットが本物であるか確認する要求を受信することであって、シールされたアセットは、エンティティによって生成され、シールデータ鍵を識別する、受信することと、シールデータ鍵に少なくとも部分的に基づいてデジタルシールレジストリに問い合わせることと、シールデータ鍵に少なくとも部分的に基づいて、シールされたアセットが本物であるか確認することとを備える。

【００１６】

登録された証明済みシールを生成するためのコンピュータプログラム製品も提供され、コンピュータプログラム製品は、非一時的コンピュータ可読記憶媒体、およびそこに記憶されたコンピュータプログラム命令を備え、コンピュータプログラム命令は、エンティティから、登録された証明済みシールを生成する要求を受信することであって、要求は、デジタル署名されたエンティティ証明証明書を備える、受信することと、証明証明書によって識別された証明機関の証明者エンティティデータにアクセスすることと、証明証明書と関連付けられ、証明機関からアクセスされる証明者エンティティデータに少なくとも部分的に基づいて、デジタル署名されたエンティティ証明証明書が本物であるか確認することとを行うように構成されたプログラム命令を備える。デジタル署名されたエンティティ証明証明書が本物であることを確認したら、コンピュータプログラム製品は、証明済みシールのシールデータ鍵を備えるシールデータを受信することであって、シールデータは、エンティティによって一意に生成される、受信することと、エンティティのシールデータをデジタルシールレジストリ内に保存することであって、デジタルシールレジストリは、シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である、保存することとを行うようにさらに構成される。デジタルシールレジストリは、サービスとしてのソフトウェア（ＳａａＳ）レジストリサービスである。

【００１７】

コンピュータプログラム製品は、少なくとも１つの一意のエンティティ識別子に基づいて、エンティティが真正であるかどうかを判定し、エンティティが真正であると判定した後、エンティティ証明証明書を生成するために、少なくとも１つの一意のエンティティ識別子を備えるアイデンティティエンティティデータにデジタル署名するようにさらに構成される。

【００１８】

例示的な実施形態では、プログラム命令を備えるコンピュータプログラム命令は、シールされたアセットが本物であるか確認する要求を受信することであって、シールされたアセットは、エンティティによって生成され、シールデータ鍵を識別する、受信することと

、シールデータ鍵に少なくとも部分的に基づいてデジタルシールレジストリに問い合わせることと、シールデータ鍵に少なくとも部分的に基づいて、シールされたアセットが本物であるか確認することとを行うようにさらに構成される。

【００１９】

別の例示的な実施形態では、アセットをシールするための装置が提供され、本装置は、少なくとも１つのプロセッサ、およびコンピュータコード化命令をその中に有する少なくとも１つのメモリを備え、コンピュータ命令は、プロセッサによって実行されたとき、エンティティのアセットと関連付けられたアセットデータを生成することであって、アセットデータは、アセットおよびエンティティを一意に識別する、生成することと、独立したシールデータレジストリにその中の記憶のためにシールデータを送信することであって、シールデータレジストリは、エンティティに対応するエンティティ証明データを備え、シールデータは、エンティティ固有公開鍵秘密鍵ペアの公開鍵を備える、送信することと、エンティティ固有公開鍵秘密鍵ペアの秘密鍵を介して、アセットと関連付けられたアセットデータにデジタル署名して、署名されたアセットデータを生成することと、署名されたアセットレジストリ内の記憶のために、署名されたアセットデータを送信することであって、署名されたアセットレジストリは、エンティティ固有公開鍵秘密鍵ペアの公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にするために１つ以上のベリファイアによってアクセス可能である、送信することと、署名されたアセットレジストリ内の署名されたアセットデータ、およびシールデータレジストリ内のシールデータへのアクセスを１つ以上のベリファイアに提供することとを本装置に行わせるように構成される。

【００２０】

例示的な実施形態では、コンピュータコード化命令をその中に有する少なくとも１つのメモリ、コンピュータ命令は、プロセッサによって実行されたとき、デジタル署名されたエンティティ証明証明書を介して、証明済みシールのためにシールデータにデジタル署名することと、証明証明書を介して、デジタル署名されたエンティティ証明証明書にデジタル署名して、証明済みシール署名を生成することと、証明済みエンティティ署名でアセットデータにデジタル署名することと、デジタルシールレジストリのレジストリエントリ内の記憶のために、署名されたアセットデータを送信することであって、デジタルシールレジストリは、エンティティ固有公開鍵秘密鍵ペアの公開鍵、および証明済みシールのシール公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にするために公的にアクセス可能である、送信することとを本装置にさらに行わせるように構成される。

【００２１】

アセットをシールするための方法が提供され、本方法は、エンティティのアセットと関連付けられたアセットデータを生成することであって、アセットデータは、アセットおよびエンティティを一意に識別する、生成することと、独立したシールデータレジストリにその内の記憶のためにシールデータを送信することであって、シールデータレジストリは、エンティティに対応するエンティティ証明データを備え、シールデータは、エンティティ固有公開鍵秘密鍵ペアの公開鍵を備える、送信することと、エンティティ固有公開鍵秘密鍵ペアの秘密鍵を介して、アセットと関連付けられたアセットデータにデジタル署名して、署名されたアセットデータを生成することと、署名されたアセットレジストリ内の記憶のために、署名されたアセットデータを送信することであって、署名されたアセットレジストリは、エンティティ固有公開鍵秘密鍵ペアの公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にするために１つ以上のベリファイアによってアクセス可能である、送信することと、署名されたアセットレジストリ内の署名されたアセットデータ、および独立したシールデータレジストリ内のシールデータへのアクセスを１つ以上のベリファイアに提供することとを備える。

【００２２】

例示的な実施形態では、本方法は、デジタル署名されたエンティティ証明証明書を介し

て、証明済みシールおよびアセットデータのためにシールデータにデジタル署名することと、証明証明書を介して、デジタル署名されたエンティティ証明証明書にデジタル署名して、証明済みシール署名を生成することと、証明済みエンティティ署名でアセットデータにデジタル署名することと、デジタルシールレジストリのレジストリエントリ内の記憶のために、署名されたアセットデータを送信することであって、デジタルシールレジストリは、エンティティ固有公開鍵秘密鍵ペアの公開鍵、および証明済みシールのシール公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にするために公的にアクセス可能である、送信することとをさらに備える。

【００２３】

別の例示的な実施形態では、アセットをシールするためのコンピュータプログラム製品も提供され、コンピュータプログラム製品は、非一時的コンピュータ可読記憶媒体、およびそこに記憶されたコンピュータプログラム命令を備え、コンピュータプログラム命令は、エンティティのアセットと関連付けられたアセットデータを生成することであって、アセットデータは、アセットおよびエンティティを一意に識別する、生成することと、独立したシールデータレジストリにその内の記憶のためにシールデータを送信することであって、シールデータレジストリは、エンティティに対応するエンティティ証明データを備え、シールデータは、エンティティ固有公開鍵秘密鍵ペアの公開鍵を備える、送信することと、エンティティ固有公開鍵秘密鍵ペアの秘密鍵を介して、アセットと関連付けられたアセットデータにデジタル署名して、署名されたアセットデータを生成することと、署名されたアセットレジストリ内の記憶のために、署名されたアセットデータを送信することであって、署名されたアセットレジストリは、エンティティ固有公開鍵秘密鍵ペアの公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にするために１つ以上のベリファイアによってアクセス可能である、送信することと、署名されたアセットレジストリ内の署名されたアセットデータ、および独立したシールデータレジストリ内のシールデータへのアクセスを１つ以上のベリファイアに提供することとを行うように構成されるプログラム命令を備える。

【００２４】

例示的な実施形態では、コンピュータプログラム製品は、デジタル署名されたエンティティ証明証明書を介して、証明済みシールおよびアセットデータのためにシールデータにデジタル署名することと、証明証明書を介して、デジタル署名されたエンティティ証明証明書にデジタル署名して、証明済みシール署名を生成することと、証明済みエンティティ署名でアセットデータにデジタル署名することと、デジタルシールレジストリのレジストリエントリ内の記憶のために、署名されたアセットデータを送信することであって、デジタルシールレジストリは、エンティティ固有公開鍵秘密鍵ペアの公開鍵、および証明済みシールのシール公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にするために公的にアクセス可能である、送信することとを行うようにさらに構成される。

【００２５】

さらに別の例示的な実施形態では、シールされたアセットが本物であるか確認するための装置が提供され、本装置は、少なくとも１つのプロセッサ、およびコンピュータコード化命令をその中に有する少なくとも１つのメモリを備え、コンピュータ命令は、プロセッサによって実行されたとき、シールされたアセットと関連付けられたアセット識別子を受信することであって、アセット識別子は、シールレジストリ内のシールされたアセットにリンクする、受信することと、アセット識別子に関係するレジストリデータを記憶するシールレジストリを識別することと、アセット識別子に関係するレジストリデータを取り出すためにシールレジストリに問い合わせることであって、レジストリデータは、証明済みエンティティによって生成されたシールデータ鍵を備え、シールされたデータ鍵は、証明済みエンティティによって生成されたシールされたアセットの確認されたデジタル署名と一致する、問い合わせることと、シールされたアセットが本物であるか確認するために、アセット識別子のデジタル署名がレジストリデータのシールデータ鍵と一致するかどうか

を判定することとを本装置に行わせるように構成される。
【００２６】
コンピュータコード化命令をその中に有する少なくとも１つのメモリ、コンピュータ命令は、プロセッサによって実行されたとき、シールされたアセットが本物であるか確認するために、証明済みエンティティがレジストリデータのエンティティデータと一致するかどうかを本装置に判定させるように構成される。
【００２７】
本装置は、シールされたアセットが本物であるか確認するために、レジストリデータの証明者エンティティ署名が証明証明書と一致することを確認し、シールされたアセットが本物であるか確認するために、証明証明書と関連付けられた証明者エンティティ署名の証明者が本物であるか確認するようにさらに構成される。
【００２８】
別の例示的な実施形態では、シールされたアセットが本物であるか確認するための方法が提供され、本方法は、シールされたアセットと関連付けられたアセット識別子を受信することであって、アセット識別子は、シールレジストリ内のシールされたアセットにリンクする、受信することと、アセット識別子に関係するレジストリデータを記憶するシールレジストリを識別することと、アセット識別子に関係するレジストリデータを取り出すためにシールレジストリに問い合わせることであって、レジストリデータは、証明済みエンティティによって生成されたシールデータ鍵を備え、シールされたデータ鍵は、証明済みエンティティによって生成されたシールされたアセットの確認されたデジタル署名と一致する、問い合わせることと、シールされたアセットが本物であるか確認するために、アセット識別子のデジタル署名がレジストリデータのシールデータ鍵と一致するかどうかを判定することとを備える。
【００２９】
本方法は、シールされたアセットが本物であるか確認するために、認定済みエンティティがレジストリデータのエンティティデータと一致するかどうかを判定することと、シールされたアセットが本物であるか確認するために、レジストリデータの証明者エンティティ署名が証明証明書と一致することを確認することと、シールされたアセットが本物であるか確認するために、証明証明書と関連付けられた証明者エンティティ署名の証明者が本物であるか確認することとをさらに備える。
【００３０】
さらに別の例示的な実施形態では、シールされたアセットが本物であるか確認するためのコンピュータプログラム製品が提供され、コンピュータプログラム製品は、非一時的コンピュータ可読記憶媒体、およびそこに記憶されたコンピュータプログラム命令を備え、コンピュータプログラム命令は、シールされたアセットと関連付けられたアセット識別子を受信することであって、アセット識別子は、シールレジストリ内のシールされたアセットにリンクする、受信することと、アセット識別子に関係するレジストリデータを記憶するシールレジストリを識別することと、アセット識別子に関係するレジストリデータを取り出すためにシールレジストリに問い合わせることであって、レジストリデータは、証明済みエンティティによって生成されたシールデータ鍵を備え、シールされたデータ鍵は、証明済みエンティティによって生成されたシールされたアセットの確認されたデジタル署名と一致する、問い合わせることと、シールされたアセットが本物であるか確認するために、アセット識別子のデジタル署名がレジストリデータのシールデータ鍵と一致するかどうかを判定することとを行うように構成されるプログラム命令を備える。
【００３１】
シールされたアセットが本物であるか確認するために、証明済みエンティティがレジストリデータのエンティティデータと一致するかどうかを判定するようにさらに構成されたプログラム命令を備えるコンピュータプログラム命令。
【００３２】
例示的な実施形態では、コンピュータプログラム製品は、シールされたアセットが本物

であるか確認するために、レジストリデータの証明者エンティティ署名が証明証明書と一致することを確認し、シールされたアセットが本物であるか確認するために、証明証明書と関連付けられた証明者エンティティ署名の証明者が本物であるか確認するようにさらに構成される。

【００３３】

このように本発明の実施形態を一般的な用語で説明してきたが、ここで、必ずしも一定の縮尺で描かれていない添付の図面を参照する。

【図面の簡単な説明】

【００３４】

【図１】本発明の例示的な実施形態から利益を得ることができるシステムを示す基本ブロック図である。

【図２Ａ】本開示の例示的な実施形態に従って特別に構成され得るブロック図を示す。

【図２Ｂ】本開示の例示的な実施形態によるレジストリを示すブロック図を示す。

【図３】本開示の例示的な実施形態に従って特別に構成され得るブロック図を示す。

【図３ａ】証明済みエンティティのシールを登録し、登録済みシールでアセットをシールし、シールされたアセットが本物であるか確認するための動作ステップを示す例示的な動作データフローの基本ブロック図を示す。

【図４】本発明の例示的な実施形態から利益を得ることができる証明済みシールレコードを示す基本ブロック図である。

【図５】本発明の例示的な実施形態から利益を得ることができる、登録された証明済みシールレコードを示す基本ブロック図である。

【図５ａ】本発明の例示的な実施形態から利益を得ることができる、ＲｅｇＳｅａｌを備えるレジストリエントリ内の証明済みシールレコードを示す基本ブロック図である。

【図６】既存のデジタル署名の作成および確認の動作ステップを示す例示的な動作データフローの基本ブロック図である。

【図６ａ】本開示の例示的な実施形態による、強制されたデジタル署名の作成および確認の動作ステップを示す例示的な動作データフローの基本ブロック図である。

【図６ｂ】本開示の例示的な実施形態による、二重暗号化された鍵を有する強制されたデジタル署名の作成および確認の動作ステップを示す例示的な動作データフローの基本ブロック図である。

【図７】本開示の例示的な実施形態に従って実行される様々な動作を示すフローチャートを示す。

【図８】本開示の例示的な実施形態に従って実行される様々な動作を示すフローチャートを示す。

【図９】本開示の例示的な実施形態に従って実行される様々な動作を示すフローチャートを示す。

【図１０】本開示の例示的な実施形態による例示的な実世界の使用例を示す。

【図１１】本開示の例示的な実施形態による例示的な実世界の使用例を示す。

【図１２】本開示の例示的な実施形態による例示的な実世界の使用例を示す。

【図１３】本開示の例示的な実施形態による例示的な実世界の使用例を示す。

【図１４】本明細書で考察されるいくつかの実施形態による、本明細書で「コンピューティングデバイス」と呼ばれることもある、１つ以上のマシンの１つ以上の表示画面によって提示することができる表示例を示す。

【図１４ａ】本明細書で考察されるいくつかの実施形態による、本明細書で「コンピューティングデバイス」と呼ばれることもある、１つ以上のマシンの１つ以上の表示画面によって提示することができる表示例を示す。

【図１４ｂ】本明細書で考察されるいくつかの実施形態による、本明細書で「コンピューティングデバイス」と呼ばれることもある、１つ以上のマシンの１つ以上の表示画面によって提示することができる表示例を示す。

【図１４ｃ】本明細書で考察されるいくつかの実施形態による、本明細書で「コンピュー

ティングデバイス」と呼ばれることもある、１つ以上のマシンの１つ以上の表示画面によって提示することができる表示例を示す。

【発明を実施するための形態】

【００３５】

本発明の例示的な実施形態を、本発明のすべてではないがいくつかの実施形態が示されている添付の図面を参照して、以下でより完全に説明する。実際に、これらの発明は、多くの異なる形態で具体化することができ、本明細書に記載の実施形態に限定されると解釈されるべきではなく、むしろ、これらの実施形態は、本開示が適用可能な法的要件を満たすように提供される。全体を通して同様の参照番号は、同様の要素を指す。本明細書で使用される場合、「データ」、「コンテンツ」、「情報」という用語、および同様の用語は、本開示の実施形態に従って送信、受信および／または記憶することができるデータを指すために互換的に使用され得る。したがって、そのような用語の使用は、本開示の実施形態の趣旨および範囲を制限するように取られるべきではない。

【００３６】

Ｉ．概要

様々な実施形態は、すべての関係者によって容易に使用および展開され、すべてに透過的であり、すべてに信頼される、新しく強化されたシステムおよび方法に向けられている。本発明の様々な態様は、上記の問題に個別におよび集合的に対処することができる。

【００３７】

本発明の一態様は、デジタルシールレジストリおよびシールされたアセットレジストリが、リモートで維持され、ネットワークを介した、例えばＷｅｂブラウザやアプリなどの多数のエンティティ（例えばシンクライアント経由）によってアクセスされ得るサーバおよびデータリポジトリなどのコンピューティングハードウェア上でホストされる、一般に共有およびホストされるサービスとしてのソフトウェア（ＳａａＳ）構成に向けられており、これにより、アセットが特定のエンティティによって実際に発行され、アセットが改ざんされていないこと、および特定のエンティティが信頼できるエンティティ証明者によって実際に証明されていることが保証される。このような構成の少なくとも１つの利点は、共通または分散レジストリ（例えば、デジタルシールレジストリ、シールされたアセットレジストリ）がデータを安全な方法で維持すると同時に、認証ソリューションを提供し、権限のないエンティティが、事前にルックアップ鍵を知りかつ付与されることなしにレジストリのコンテンツに問い合わせることに対する防御を提供することである。

【００３８】

追加または代替として、パブリックネットワークとプライベートネットワークに分散された多数のレジストリがあり、各々がデータを記憶している場合がある。多数のレジストリの同期を維持して、１つのレジストリに登録し、後で別のレジストリから登録データを取り出すことができるようにし得る。別の例示的な実施形態では、レジストリは、特定のネットワークドメインの外部でデータを共有しないことがある。

【００３９】

本発明の別の態様は、アセットベリファイアが（各エンティティがそれ自体のバージョンを作成してクライアントアプリケーションの増加がもたらされるよりも）展開するのがはるかに容易であるように、多数のエンティティによって一般に共有されるクライアントアプリケーションに向けられる。（ネットワークを介して共通または分散のシールレジストリにアクセスするために）共通のシールレジストリと共通の確認アプリケーションを組み合わせることにより、透明性、セキュリティ、および同じプラットフォームでの採用の容易さを伴って、デジタルまたは物理的アセットをデジタル化し、確認することができる。

【００４０】

本開示の別の態様は、デジタルシールを作成し、デジタルシールをアセットに適用し、シールされたアセットが本物であるか確認するための方法および技法を提供する。例えば、エンティティを証明し、エンティティの公開鍵（例えば、エンティティ公開鍵）証明書（例えば、エンティティ証明書）を作成するように構成されているシステムが提供される

。別の実施形態では、システムは、証明済みデジタルシール（例えば、ＣｅｒｔＳｅａｌ）を作成するために、エンティティ証明書とともに証明済みエンティティの第２の公開鍵（例えば、シール公開鍵）をデジタル署名するために構成される。次に、証明済みデジタルシールは、証明済みシールを記憶および検索するための共有オンラインＳａａＳとして構成されているシールレジストリに登録される。証明済みシールは、登録されると、登録済みシールまたは登録された証明済みシールと呼ばれる場合がある。追加または代替として、シールおよびアセットデータはベリファイアに送信される。

【００４１】

登録済みシールを有し、証明者エンティティによってエンティティが証明されたら、エンティティは、シール秘密鍵を使用してアセットデータのデジタル署名を作成し、かつシールされたアセットレジストリに、シールされたアセットを登録することにより、登録シール（例えば、ＲｅｇＳｅａｌ）を用いてアセットをシールすることができる。登録されたシールされたアセットは、システムによって検索および確認され得る。

【００４２】

本開示の別の態様では、システムは、シールされたアセットを確認して、対応する登録シール署名および証明エンティティが正しいこと、かつさらに、シールされたアセットデータが、認証／確認されるアセットと一致することを確証する確認メカニズムを提供する。

【００４３】

デジタルシールの用途には、ユーザＩＤの確認、物理的およびデジタルアセットの識別および／または認証、不正の検出と保護、通貨、クーポン、リワードポイント、ギフトカードポイント、クレジットカード、ローン、株式、先物などの価値のあるアセットのデジタル化、アセットおよびトランザクションのデジタル化、契約への署名、ならびに／またはスマート契約の作成および実行などが含まれるが、これらに限定されない。

【００４４】

本発明の様々な態様は、デジタルアセットまたは物理的アセットをデジタルシールまたはスタンプするためのシステムおよび方法を提供することによって、前述の問題に対処しようとする。本発明の一態様では、シールレジストリは、すべての認証を統合するのに役立つ。本発明の別の態様は、偽造されることができないようなデジタルシールまたはスタンプの作成に向けられている。また、単一の統一されたクライアントアプリは、デジタルシールを用いて任意のアセットを認証することができる。より具体的には、様々な実施形態は、デジタルまたは物理的アセットデータを登録するためのアセットレジストリサービスを提供し、アセットデータが真に改ざんされておらず、アセットが真に当該エンティティによって発行されていることを証拠立てるために任意の関与または許可される当事者によって確認されることが可能である確認可能／証明可能エンティティによって関連するデジタルシールまたはスタンプを作成するための方法に関係する。

【００４５】

特定の実施形態におけるアセットデータ（３４２）は、構造化データを含み得る。非限定的な特定の例として、アセットが運転免許証である場合、データは、（例えば、ＪＳＯＮ形式で提供され得る）運転者の識別情報であり得る。このように、認証された（および／または構造化された）データはまた、別のシステムにおける情報の自動入力のような様々な目的のためにコンピュータプログラムによって処理され得る。

【００４６】

用語

以下の考察を参照して、本出願を通して次の用語を考察する。

【００４７】

本明細書で使用される場合、「エンティティ」という用語は、シールを発行する、アセットを所有する、または確認を行うことができる任意の個人、組織、会社、政府機関、マシンまたはプログラムであり得る。

【００４８】

「エンティティ証明者」、「信頼できるエンティティ証明者」、「証明書機関」、「証

明機関」という用語、および同様の用語は、証明書機関または証明機関に類似しているがこれらに限定されない、デジタル証明書を発行するエンティティを指す。

【００４９】

「証明済みシール」、「ＣｅｒｔＳｅａｌ」、および同様の用語は、エンティティ証明者によって確認および証明されたシール所有者（例えば、エンティティ）によって作成されたシールを指す場合があり、シールの真正性が確認されている。言い換えれば、証明済みシールは、シールの内容（シールされたアセット）が改ざんされておらず、シール発行者（例えば、証明済みエンティティ）によって発行されたものとまったく同じであることを示すシールを含む場合があり、シール発行者のアイデンティティが確認されている。

【００５０】

「登録された証明済みシール」、「登録シール」、「ＲｅｇＳｅａｌ」という用語、および同様の用語は、デジタルシールレジストリに入力される証明済みシールを指す場合がある。証明済みシールがデジタルシールレジストリのエントリまたはレコードになると、ベリファイアは登録シールにアクセス可能になる。

【００５１】

「アセット」という用語は、確認、使用、または消費される可能性のあるものを指す場合がある。例えば、アセットは、デジタル（例えば、記録されたデータ、銀行口座、コンピュータアカウント、デジタル契約、電子メールアドレスおよび／または同様のもの）、または物理的（例えば、有形オブジェクト、物理的ＩＤ、卒業証書、パスポート、バッグ、薬、現金および／または同様のもの）であり得る。

【００５２】

「シールされたアセット」という用語は、登録シールのデジタル署名を持つ任意のアセットを指す場合がある。デジタル署名はアセットを「シール」する。

【００５３】

「登録済みアセット」という用語は、シールされたアセットレジストリのエントリまたはレコードとなるシールされたアセットを指す場合がある。登録されると、登録済みアセットはベリファイアがアクセス可能になる。

【００５４】

「シール」、「デジタルシール」という用語は、真正性の立証および／または証拠として機能するためにデジタルアセットまたは物理的アセットに追加されたインタラクティブタグを指す場合がある。非限定的な例として、シールは、金属片上の物理的スタンプであり得、物理的スタンプは、インタラクティブＵＲＬ（ユニフォームリソースロケータ）接続コード、運転免許証ＩＤ上のＱＲコード（登録商標）（クイックレスポンスコード）、ＭＳタグおよび／または同様のものを含む。シールは、本明細書で考察されるように、シールされたアセットＩＤまたはＲｅｇＳｅａｌ　ＩＤを備え得、および／またはそれらとして具体化され得る。シールは、アセットとは別に使用することもできる。

【００５５】

「ベリファイア」という用語は、アセットに適用されるシールが真正であることを確認するように構成または実装されているソフトウェアおよびハードウェアコンポーネントならびにプログラムコードを含む（例えば、ユーザによって動作される）任意のコンピューティングデバイスを指す場合がある。

【００５６】

ＩＩ．コンピュータプログラム製品、方法、およびコンピューティングエンティティ

本発明の実施形態は、製造品を含むコンピュータプログラム製品としてを含む、様々な方法で実装することができる。そのようなコンピュータプログラム製品は、例えば、ソフトウェアオブジェクト、メソッド、データ構造および／または同様のものを含む１つ以上のソフトウェアコンポーネントを含み得る。ソフトウェアコンポーネントは、様々なプログラミング言語のいずれかでコードすることができる。例示的なプログラミング言語は、特定のハードウェアアーキテクチャおよび／またはオペレーティングシステムプラットフォームと関連付けられたアセンブリ言語などの低水準プログラミング言語であり得る。ア

センブリ言語命令を含むソフトウェアコンポーネントは、ハードウェアアーキテクチャおよび／またはプラットフォームで実行する前に、アセンブラによって、実行可能なマシンコードに変換する必要がある場合がある。別のプログラミング言語の例は、多数のアーキテクチャ間で移植可能な高水準プログラミング言語であり得る。高水準プログラミング言語命令を含むソフトウェアコンポーネントは、実行前にインタプリタまたはコンパイラによる中間表現への変換を必要とする場合がある。

【００５７】

プログラミング言語の他の例には、マクロ言語、シェルまたはコマンド言語、ジョブ制御言語、スクリプト言語、データベースクエリまたは検索言語、および／またはレポート作成言語が含まれるが、これらに限定されない。１つ以上の例示的な実施形態では、プログラミング言語の前述の例のうちの１つにおける命令を含むソフトウェアコンポーネントは、最初に別の形態に変換される必要なしに、オペレーティングシステムまたは他のソフトウェアコンポーネントによって直接実行され得る。ソフトウェアコンポーネントは、ファイルまたは他のデータ記憶構造として記憶することができる。同様のタイプまたは機能的に関連するソフトウェアコンポーネントは、例えば、特定のディレクトリ、フォルダ、またはライブラリなどに一緒に記憶することができる。ソフトウェアコンポーネントは、静的（例えば、事前に確立もしくは固定）または動的（例えば、実行時に作成もしくは変更）である場合がある。

【００５８】

コンピュータプログラム製品は、アプリケーション、プログラム、プログラムモジュール、スクリプト、ソースコード、プログラムコード、オブジェクトコード、バイトコード、コンパイルされたコード、解釈されたコード、マシンコード、実行可能命令および／または同様のもの（本明細書では、実行可能命令、実行命令、コンピュータプログラム製品、プログラムコード、および／または本明細書で互換的に使用される同様の用語とも呼ばれる）を記憶する非一時的コンピュータ可読記憶媒体を含み得る。そのような非一時的コンピュータ可読記憶媒体には、（揮発性および非揮発性媒体を含む）すべてのコンピュータ可読媒体が含まれる。

【００５９】

一実施形態では、不揮発性コンピュータ可読記憶媒体は、フロッピーディスク、フレキシブルディスク、ハードディスク、ソリッドステートストレージ（ＳＳＳ）（例えば、ソリッドステートドライブ（ＳＳＤ）、ソリッドステートカード（ＳＳＣ）、ソリッドステートモジュール（ＳＳＭ）、エンタープライズフラッシュドライブ、磁気テープ、または他の非一時的磁気媒体および／または同様のものを含み得る。不揮発性コンピュータ可読記憶媒体はまた、パンチカード、紙テープ、光学マークシート（または穴のパターンもしくは他の光学的に認識可能な表示を有する他の物理媒体）、コンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、コンパクトディスク書き換え可能（ＣＤ－ＲＷ）、デジタル多用途ディスク（ＤＶＤ）、Ｂｌｕ－ｒａｙ（登録商標）ディスク（ＢＤ）、他の非一時的光学媒体および／または同様のものを含み得る。そのような非揮発性コンピュータ可読記憶媒体はまた、読み取り専用メモリ（ＲＯＭ）、プログラム可能な読み取り専用メモリ（ＰＲＯＭ）、消去可能なプログラム可能読み取り専用メモリ（ＥＰＲＯＭ）、電気的に消去可能なプログラム可能読み取り専用メモリ（ＥＥＰＲＯＭ）、フラッシュメモリ（例えば、シリアル、ＮＡＮＤ、ＮＯＲおよび／または同様のもの）、マルチメディアメモリカード（ＭＭＣ）、セキュアデジタル（ＳＤ）メモリカード、ＳｍａｒｔＭｅｄｉａ（登録商標）カード、ＣｏｍｐａｃｔＦｌａｓｈ（ＣＦ）カード、メモリスティックおよび／または同様のものを含み得る。さらに、不揮発性コンピュータ可読記憶媒体はまた、導電性ブリッジングランダムアクセスメモリ（ＣＢＲＡＭ）、位相変化ランダムアクセスメモリ（ＰＲＡＭ）、強誘電体ランダムアクセスメモリ（ＦｅＲＡＭ）、不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）、磁気抵抗ランダムアクセスメモリ（ＭＲＡＭ）、抵抗ランダムアクセスメモリ（ＲＲＡＭ（登録商標））、シリコン－酸化物－窒化物－酸化物－シリコンメモリ（ＳＯＮＯＳ）、フローティングジャンクションゲートランダムアクセス

メモリ（ＦＪＧ　ＲＡＭ）、Ｍｉｌｌｉｐｅｄｅメモリ、レーストラックメモリおよび／または同様のものを含み得る。

【００６０】

一実施形態では、揮発性コンピュータ可読記憶媒体は、ランダムアクセスメモリ（ＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、スタティックランダムアクセスメモリ（ＳＲＡＭ）、高速ページモードダイナミックランダムアクセスメモリ（ＦＰＭ　ＤＲＡＭ）、拡張データ出力ダイナミックランダムアクセスメモリ（ＥＤＯ　ＤＲＡＭ）、同期ダイナミックランダムアクセスメモリ（ＳＤＲＡＭ）、ダブルデータレート同期ダイナミックランダムアクセスメモリ（ＤＤＲ　ＳＤＲＡＭ）、ダブルデータレートタイプ２同期ダイナミックランダムアクセスメモリ（ＤＤＲ２　ＳＤＲＡＭ）、ダブルデータレートタイプ３同期ダイナミックランダムアクセスメモリ（ＤＤＲ３　ＳＤＲＡＭ）、ランバスダイナミックランダムアクセスメモリ（ＲＤＲＡＭ）、ツイントランジスタＲＡＭ（ＴＴＲＡＭ）、サイリスタＲＡＭ（Ｔ－ＲＡＭ）、ゼロキャパシタ（Ｚ－ＲＡＭ）、ランバスインラインメモリモジュール（ＲＩＭＭ）、デュアルインラインメモリモジュール（ＤＩＭＭ）、シングルインラインメモリモジュール（ＳＩＭＭ）、ビデオランダムアクセスメモリ（ＶＲＡＭ）、（様々なレベルを含む）キャッシュメモリ、フラッシュメモリ、レジスタメモリなどを含み得る。コンピュータ可読記憶媒体を使用するための実施形態が説明される場合、他のタイプのコンピュータ可読記憶媒体が、上記のコンピュータ可読記憶媒体の代わりに、またはそれに加えて使用され得ることが認識されよう。

【００６１】

認識されるべきであるように、本発明の様々な実施形態はまた、方法、装置、システム、コンピューティングデバイス、コンピューティングエンティティおよび／または同様のものとして実装され得る。したがって、本発明の実施形態は、コンピュータ可読記憶媒体に記憶された命令を実行して特定のステップまたは動作を実行する、データ構造、装置、システム、コンピューティングデバイス、コンピューティングエンティティおよび／または同様のものの形態をとることができる。したがって、本発明の実施形態はまた、完全にハードウェアの実施形態、完全にコンピュータプログラム製品の実施形態、および／またはコンピュータプログラム製品と特定のステップもしくは動作を実行するハードウェアとの組み合わせを含む実施形態の形態をとることができる。

【００６２】

本発明の実施形態は、ブロック図およびフローチャート図を参照して以下に説明される。したがって、ブロック図およびフローチャート図の各ブロックは、命令、動作、ステップ、および実行のためにコンピュータ可読記憶媒体上で互換的に使用される同様の単語（例えば、実行可能な命令、実行命令、プログラムコードおよび／または同様のこと）を実行する、コンピュータプログラム製品、完全にハードウェアの実施形態、ハードウェアとコンピュータプログラム製品の組み合わせ、および／または装置、システム、コンピューティングデバイス、コンピューティングエンティティおよび／または同様のものの形態で実装することができることを認識されたい。例えば、コードの取り出し、ロード、および実行は、一度に１つの命令が取り出され、ロードされ、および実行されるように、順次実行され得る。いくつかの例示的な実施形態では、取り出し、ロード、および／または実行は、多数の命令が一緒に取り出され、ロードされ、および／または実行されるように、並行して実行され得る。したがって、そのような実施形態は、ブロック図およびフローチャート図で指定されたステップまたは動作を実行する特別に構成されたマシンを製造することができる。したがって、ブロック図およびフローチャート図は、指定された命令、動作、またはステップを実行するための実施形態の様々な組み合わせをサポートする。

【００６３】

さらに、本明細書で使用される場合、「回路」という用語は、（ａ）ハードウェアのみの回路実装（例えば、アナログ回路および／またはデジタル回路での実装）、（ｂ）本明細書で説明する１つ以上の機能を装置に実行させるために一緒に働く１つ以上のコンピュータ可読メモリに記憶されたソフトウェアおよび／またはファームウェア命令を含む回路

とコンピュータプログラム製品の組み合わせ、ならびに（ｃ）例えば、マイクロプロセッサまたはマイクロプロセッサの一部分など、ソフトウェアまたはファームウェアが物理的に存在しない場合でも、動作のためにソフトウェアまたはファームウェアを必要とする回路を指す。「回路」のこの定義は、あらゆる特許請求の範囲をも含めて、本明細書におけるこの用語のすべての使用に適用される。さらなる例として、本明細書で使用される場合、「回路」という用語は、１つ以上のプロセッサおよび／またはその部分、ならびに付随するソフトウェアおよび／またはファームウェアを含む実装も含む。別の例として、本明細書で使用される「回路」という用語は、例えば、携帯電話用のベースバンド集積回路またはアプリケーションプロセッサ集積回路、ならびにサーバ、セルラーネットワークデバイス、他のネットワークデバイス、フィールドプログラム可能ゲートアレイ、および／または他のコンピューティングデバイスにおける同様の集積回路も含む。

【００６４】

本明細書で定義されるように、物理記憶媒体（例えば、揮発性または不揮発性メモリデバイス）を指す「コンピュータ可読記憶媒体」は、電磁的信号を指す「コンピュータ可読伝送媒体」と区別され得る。

【００６５】

ＩＩＩ．例示的なシステムアーキテクチャ

図１は、本発明の例示的な実施形態から利益を得ることができるシステム１０を示す基本ブロック図である。本明細書に示され、説明されるように、システム１０は、多数の電子デバイスが有線、無線、または有線と無線の通信メカニズムの組み合わせを介して通信することができるネットワーク２０のコンテキストで使用することができる。例示的な実施形態では、電子デバイスは、本発明の実施形態に従って個人がアプリケーションを実行し、および／または互いに通信することを可能にし得るパーソナルコンピュータ（ＰＣ）または他の端末として具体化され得る。これに関連して、システム１０は、いくつかの異なる通信端末を含み得、それらの各々は、本明細書で説明するそれぞれの端末にあるとされるものを含む１つ以上の機能を実行するように構成された、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアの組み合わせのいずれかで具体化された任意のデバイスまたは手段を備え得る。例えば、システム１０は、エンティティ端末１２と、場合によってはまた、ネットワーク２０を介して互いに通信している多数の他の周辺デバイスまたはモジュールとを含むことができる。これに関連して、例えば、サーバ１８も、ネットワーク２０を介してエンティティ端末１２と通信していることがある。しかしながら、サーバ１８はまた、エンティティ端末１２と併置されるか、またはその一部分でさえあり得ることに留意されたい。ネットワーク２０と通信していることがある他のデバイスは、レジストリ１４および／または少なくとも１つの証明者端末１６を含み得る。しかしながら、サーバ１８はまた、証明者端末１６と併置されるか、またはその一部分でさえあり得ることに留意されたい。ネットワーク２０は、例えば、インターネット、ローカルエリアネットワーク（ＬＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、キャンパスエリアネットワーク（ＣＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）などを含む、いくつかの異なる通信バックボーンまたはフレームワークのいずれかであり得る。１つの例示的な実施形態では、エンティティ端末１２およびサーバ１８は、ＬＡＮまたは他のローカライズされた（例えば、特定の会社と関連付けられた）ネットワークの一部であり得、エンティティ端末１２およびサーバ１８の一方または両方は、直接的にあるいはＬＡＮのゲートウェイデバイスを介してネットワーク２０と通信していることがある。

【００６６】

ａ．例示的なサーバ

サーバ１８は、メモリおよび処理能力（例えば、図２Ａの揮発性メモリ２０７および処理要素２０５）を含み、ネットワーク２０と通信して本発明の実施形態による動作を容易にする、サーバまたは他のコンピューティングプラットフォームであり得る。いくつかの実施形態では、サーバ１８は、以下のサーバ１８に関連して説明される機能、デバイスおよび／または要素へのアクセスを提供する確認アプリをホストすることができる。

【００６７】
図２Ａは、本発明の一実施形態によるサーバ１８の概略図を提供する。一般に、コンピューティングエンティティ、エンティティ、デバイス、システムという用語、および／または本明細書で互換的に使用される同様の用語は、例えば、１つ以上のコンピュータ、コンピューティングエンティティ、デスクトップコンピュータ、携帯電話、タブレット、ファブレット、ノートブック、ラップトップ、分散システム、アイテム／デバイス、端末、サーバまたはサーバネットワーク、ブレード、ゲートウェイ、スイッチ、処理デバイス、処理エンティティ、セットトップボックス、リレー、ルータ、ネットワークアクセスポイント、基地局など、ならびに／あるいは本明細書に記載の機能、動作、および／またはプロセスを実行するように適合されているデバイスまたはエンティティの任意の組み合わせを指す場合がある。そのような機能、動作、および／またはプロセスは、例えば、送信、受信、動作、処理、表示、記憶、判定、作成／生成、監視、評価、比較、および／または本明細書で互換的に使用される同様の用語を含み得る。一実施形態では、これらの機能、動作、および／またはプロセスは、データ、コンテンツ、情報、および／または本明細書で互換的に使用される同様の用語に対して実行することができる。
【００６８】
示されるように、一実施形態では、サーバ１８はまた、送信、受信、動作、処理、表示、記憶および／または同様のことをすることができるデータ、コンテンツ、情報、および／または本明細書で互換的に使用される同様の用語を通信することによってなど、様々なコンピューティングエンティティと通信するための１つ以上のネットワークおよび／または通信インターフェース２０８を含み得る。例えば、サーバ１８は、他の分析コンピューティングエンティティ、１つ以上のユーザコンピューティングエンティティ３０および／または同様のものと通信することができる。
【００６９】
図２Ａに示されるように、一実施形態では、サーバ１８は、例えば、バスまたはネットワーク接続を介してサーバ１８内の他の要素と通信する１つ以上の処理要素２０５（プロセッサ、処理回路、および／または本明細書で互換的に使用される同様の用語とも呼ばれる）を含むかまたはそれらと通信していることがある。理解されるように、処理要素２０５は、いくつかの異なる方法で具体化することができる。例えば、処理要素２０５は、１つ以上の複雑なプログラマブルロジックデバイス（ＣＰＬＤ）、マイクロプロセッサ、マルチコアプロセッサ、コプロセシングエンティティ、アプリケーション固有命令セットプロセッサ（ＡＳＩＰ）、および／またはコントローラとして具体化され得る。さらに、処理要素２０５は、１つ以上の他の処理デバイスまたは回路として具体化され得る。回路という用語は、完全にハードウェアの実施形態、またはハードウェアとコンピュータプログラム製品の組み合わせを指す場合がある。したがって、処理要素２０５は、集積回路、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、プログラマブルロジックアレイ（ＰＬＡ）、ハードウェアアクセラレータ、他の回路および／または同様のものとして具体化され得る。したがって、理解されるように、処理要素２０５は、特定の用途のために構成され得るか、あるいは揮発性または不揮発性媒体に記憶された、またはそうでなければ処理要素２０５にアクセス可能である命令を実行するように構成され得る。したがって、ハードウェアまたはコンピュータプログラム製品によって構成されるか、あるいはそれらの組み合わせによって構成されるかにかかわらず、処理要素２０５は、相応に構成される場合、本発明の実施形態によるステップまたは動作を実行することが可能になり得る。
【００７０】
一実施形態では、サーバ１８は、不揮発性媒体（不揮発性記憶装置、メモリ、メモリ保存、メモリ回路、および／または本明細書で互換的に使用される同様の用語とも呼ばれる）をさらに含み、またはそれらと通信し得る。図１に示されているほんの一例として、サーバ１８は、別個のレジストリ１４（例えば、不揮発性データベースストレージまたはメモリ）と通信していることがある。しかしながら、レジストリ１４は、様々な実施形態に

おいてサーバ１８の一部であり得ることを理解されたい。一実施形態では、不揮発性記憶装置またはメモリは、ハードディスク、ＲＯＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、ＭＭＣ、ＳＤメモリカード、メモリスティック、ＣＢＲＡＭ、ＰＲＡＭ、ＦｅＲＡＭ、ＲＲＡＭ（登録商標）、ＳＯＮＯＳ、レーストラックメモリおよび／または同様のものなど、上記のような１つ以上の不揮発性記憶装置またはメモリ媒体２０６を含み得る。認識されるように、不揮発性記憶装置またはメモリ媒体は、データベース、データベースインスタンス、データベース管理システムエンティティ、データ、アプリケーション、プログラム、プログラムモジュール、スクリプト、ソースコード、オブジェクトコード、バイトコード、コンパイルされたコード、解釈されたコード、マシンコード、実行可能命令および／または同様のものを記憶することができる。データベース、データベースインスタンス、データベース管理システムエンティティ、および／またはコンピュータ可読記憶媒体に記憶されている情報／データの構造化または非構造化コレクションを指すために本明細書で互換的にかつ一般的な意味で使用される同様の用語。

【００７１】

記憶媒体２０６はまた、データ記憶デバイスもしくは複数のデバイスとして、（図１に示されるように）別個のデータベースサーバもしくは複数のサーバとして、またはデータ記憶デバイスと別個のデータベースサーバとの組み合わせとして具体化され得る。さらに、いくつかの実施形態では、メモリ媒体２０６は、記憶された情報／データの一部がシステム内のロケーションに中央に記憶され、他の情報／データが１つ以上のリモートロケーションに記憶されるように、分散リポジトリとして具体化され得る。あるいは、いくつかの実施形態では、分散リポジトリは、複数のリモート記憶ロケーションにのみ分散され得る。

【００７２】

メモリ媒体２０６は、サーバ１８の動作を容易にするために、サーバ１８によってアクセスおよび記憶される情報／データを含み得る。より具体的には、メモリ媒体２０６は、特定の実施形態において使用可能な情報／データを記憶するように構成された１つ以上のデータストアを包含し得る。

【００７３】

図２Ｂに示されるように、メモリ媒体２０６は、様々なエンティティ（およびそれらの対応するデジタルシール）を示す識別情報／データを有するデジタルシールレジストリ情報／データ２１１を包含し得る。メモリ媒体２０６は、シールされたアセット情報／データ２１２をさらに含み得る。シールされたアセット情報／データ２１２は、シールされたアセットの実体、アセット識別子および／または同様のものなど、シールされたアセットに関する情報／データを含み得る。アセットデータへのアクセスが、アセットデータの実体にアクセスするための暗号化鍵を有するユーザ／エンティティに制限され得るように、アセットデータは暗号化された形態で記憶され得ることを理解されたい。

【００７４】

一実施形態では、サーバ１８は、揮発性媒体（揮発性記憶装置、メモリ、メモリ保存、メモリ回路、および／または本明細書で互換的に使用される同様の用語とも呼ばれる）をさらに含み、またはそれらと通信し得る。一実施形態では、揮発性記憶装置またはメモリはまた、ＲＡＭ、ＤＲＡＭ、ＳＲＡＭ、ＦＰＭ ＤＲＡＭ、ＥＤＯ ＤＲＡＭ、ＳＤＲＡＭ、ＤＤＲ ＳＤＲＡＭ、ＤＤＲ２ ＳＤＲＡＭ、ＤＤＲ３ ＳＤＲＡＭ、ＲＤＲＡＭ、ＲＩＭＭ、ＤＩＭＭ、ＳＩＭＭ、ＶＲＡＭ、キャッシュメモリ、レジスタメモリおよび／または同様のものなど、上記のような１つ以上の揮発性記憶装置またはメモリ媒体２０７を含み得る。認識されるように、揮発性記憶装置またはメモリ媒体は、例えば、処理要素３０８によって実行されているデータベース、データベースインスタンス、データベース管理システムエンティティ、データ、アプリケーション、プログラム、プログラムモジュール、スクリプト、ソースコード、オブジェクトコード、バイトコード、コンパイルされたコード、解釈されたコード、マシンコード、実行可能命令および／または同様のものの少なくとも部分を記憶するために使用され得る。したがって、データベース、データベースイ

ンスタンス、データベース管理システムエンティティ、データ、アプリケーション、プログラム、プログラムモジュール、スクリプト、ソースコード、オブジェクトコード、バイトコード、コンパイルされたコード、解釈されたコード、マシンコード、実行可能命令および／または同様のものは、処理要素２０５およびオペレーティングシステムの助けを借りて、サーバ１８の動作の特定の側面を制御するために使用され得る。

【００７５】

示されるように、一実施形態では、サーバ１８はまた、送信、受信、動作、処理、表示、記憶および／または同様のことをすることができるデータ、コンテンツ、情報、および／または本明細書で互換的に使用される同様の用語を通信することによってなど、様々なコンピューティングエンティティと通信するための１つ以上のネットワークおよび／または通信インターフェース２０８を含み得る。例えば、サーバ１８は、他のサーバ、端末（例えば、証明者端末１６、ユーザコンピューティングエンティティ３０）および／または同様のもののコンピューティングエンティティまたは通信インターフェースと通信することができる。

【００７６】

示されるように、一実施形態では、サーバ１８はまた、送信、受信、動作、処理、表示、記憶および／または同様のことをすることができるデータ、コンテンツ、情報、および／または本明細書で互換的に使用される同様の用語を通信することによってなど、様々なコンピューティングエンティティと通信するための１つ以上のネットワークおよび／または通信インターフェース２０８を含み得る。そのような通信は、ファイバ分散データインターフェース（ＦＤＤＩ）、デジタル加入者線（ＤＳＬ）、イーサネット、非同期転送モード（ＡＴＭ）、フレームリレー、データオーバーケーブルサービスインターフェース仕様（ＤＯＣＳＩＳ）、または他の有線伝送プロトコルなどの有線データ伝送プロトコルを使用して実行することができる。同様に、サーバ１８は、汎用パケット無線サービス（ＧＰＲＳ）、ユニバーサルモバイルテレコミュニケーションズシステム（ＵＭＴＳ）、コード分割マルチアクセス２０００（ＣＤＭＡ２０００）、ＣＤＭＡ２０００　１Ｘ（１ｘＲＴＴ）、広帯域コード分割マルチアクセス（ＷＣＤＭＡ（登録商標））、モバイル通信用グローバルシステム（ＧＳＭ）、ＧＳＭエボリューション用拡張データレート（ＥＤＧＥ）、時分割同期コード分割マルチアクセス（ＴＤ－ＳＣＤＭＡ）、ロングタームエボリューション（ＬＴＥ）、発展型ユニバーサル地上波無線アクセスネットワーク（Ｅ－ＵＴＲＡＮ）、エボリューションデータオプティマイズド（ＥＶＤＯ）、高速パケットアクセス（ＨＳＰＡ）、高速ダウンリンクパケットアクセス（ＨＳＤＰＡ）、ＩＥＥＥ８０２．１１（Ｗｉ－Ｆｉ）、Ｗｉ－Ｆｉ　Ｄｉｒｅｃｔ、８０２．１６（ＷｉＭＡＸ）、超広帯域（ＵＷＢ）、赤外線（ＩＲ）プロトコル、近距離通信（ＮＦＣ）プロトコル、Ｗｉｂｒｅｅ、Ｂｌｕｅｔｏｏｔｈプロトコル、ワイヤレスユニバーサルシリアルバス（ＵＳＢ）プロトコル、および／または任意の他のワイヤレスプロトコルなど、様々なプロトコルのいずれかを使用してワイヤレス外部通信ネットワークを介して通信するように構成され得る。サーバ１８は、そのようなプロトコルおよび規格を使用して、ボーダーゲートウェイプロトコル（ＢＧＰ）、動的ホスト構成プロトコル（ＤＨＣＰ）、ドメインネームシステム（ＤＮＳ）、ファイル転送プロトコル（ＦＴＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、ＨＴＴＰオーバーＴＬＳ／ＳＳＬ／Ｓｅｃｕｒｅ、インターネットメッセージアクセスプロトコル（ＩＭＡＰ）、ネットワークタイムプロトコル（ＮＴＰ）、シンプルメール転送プロトコル（ＳＭＴＰ）、Ｔｅｌｎｅｔ、トランスポートレイヤセキュリティ（ＴＬＳ）、セキュアソケットレイヤ（ＳＳＬ）、インターネットプロトコル（ＩＰ）、伝送制御プロトコル（ＴＣＰ）、ユーザデータグラムプロトコル（ＵＤＰ）、データグラム輻輳制御プロトコル（ＤＣＣＰ）、ストリーム制御伝送プロトコル（ＳＣＴＰ）、ハイパーテキストマークアップ言語（ＨＴＭＬ）および／または同様のものを使用して通信することができる。

【００７７】

認識されるように、１つ以上の分析コンピューティングエンティティのコンポーネント

は、分散システム内など、他のサーバ１８コンポーネントから離れて配置され得る。さらに、コンポーネントのうちの１つ以上を集約することができ、本明細書で説明する機能を実行する追加のコンポーネントをサーバ１８に含めることができる。したがって、サーバ１８は、様々なニーズおよび状況に対応するように適合させることができる。

【００７８】

ｂ．例示的なユーザコンピューティングエンティティ

図３は、本発明の実施形態と併せて使用することができるユーザコンピューティングエンティティ３０を表す例示的な概略図を提供する。認識されるように、ユーザコンピューティングエンティティは、エージェントによって動作され得、サーバ１８に関連して説明されたものと同様のコンポーネントおよび機能を含み得る。さらに、図３に示されるように、ユーザコンピューティングエンティティは、追加のコンポーネントおよび機能を含み得る。例えば、ユーザコンピューティングエンティティ３０は、アンテナ３１２、送信機３０４（例えば、無線）、受信機３０６（例えば、無線）、ネットワークインターフェース３２０、ならびにそれぞれ送信機３０４および受信機３０６および／またはネットワークインターフェース３２０に信号を提供し、かつそれらから信号を受信する処理要素３０８を含むことができる。それぞれ送信機３０４および受信機３０６に提供され、かつそれらから受信される信号は、サーバ１８、別のユーザコンピューティングエンティティ３０および／または同様のものの様々なエンティティと通信するための、適用可能な無線システムのエアインターフェース規格に従う信号情報／データを含み得る。これに関連して、ユーザコンピューティングエンティティ３０は、１つ以上のエアインターフェース規格、通信プロトコル、変調タイプ、およびアクセスタイプで動作することが可能になり得る。より具体的には、ユーザコンピューティングエンティティ３０は、いくつかの有線または無線通信規格およびプロトコルのいずれかに従って動作することができる。特定の実施形態では、ユーザコンピューティングエンティティ３０は、ＧＰＲＳ、ＵＭＴＳ、ＣＤＭＡ２０００、１ｘＲＴＴ、ＷＣＤＭＡ（登録商標）、ＴＤ－ＳＣＤＭＡ、ＬＴＥ、Ｅ－ＵＴＲＡＮ、ＥＶＤＯ、ＨＳＰＡ、ＨＳＤＰＡ、Ｗｉ－Ｆｉ、ＷｉＭＡＸ、ＵＷＢ、ＩＲプロトコル、Ｂｌｕｅｔｏｏｔｈプロトコル、ＵＳＢプロトコル、および／または他のワイヤレスプロトコルなど、複数の無線通信規格およびプロトコルに従って動作することができる。

【００７９】

これらの通信規格およびプロトコルを介して、ユーザコンピューティングエンティティ３０は、非構造化補足サービスデータ（ＵＳＳＤ）、ショートメッセージサービス（ＳＭＳ）、マルチメディアメッセージングサービス（ＭＭＳ）、デュアルトーン多重周波数シグナリング（ＤＴＭＦ）、および／またはサブスクライバアイデンティティモジュールダイアラ（ＳＩＭダイアラ）などの概念を使用して他の様々なエンティティと通信することができる。ユーザコンピューティングエンティティ３０はまた、例えば、そのファームウェア、ソフトウェア（例えば、実行可能命令、アプリケーション、プログラムモジュールを含む）、およびオペレーティングシステムへの変更、アドオン、および更新をダウンロードすることができる。

【００８０】

一実施形態によれば、ユーザコンピューティングエンティティ３０は、ロケーション判定の態様、デバイス、モジュール、機能、および／または本明細書で互換的に使用される同様の単語を含み得る。例えば、ユーザコンピューティングエンティティ３０は、例えば、緯度、経度、高度、ジオコード、コース、方向、方位、速度、ＵＴＣ、日付、および／または様々な他の情報／データを収集するように適応されたロケーションモジュールなど、屋外測位の態様を含み得る。一実施形態では、ロケーションモジュールは、視野内の衛星の数およびそれらの衛星の相対位置を識別することによって、エフェメリスデータとしても知られるデータを取得することができる。衛星は、ＬＥＯ衛星システム、ＤＯＤ衛星システム、欧州連合ガリレオ測位システム、中国コンパスナビゲーションシステム、インド地域ナビゲーション衛星システムおよび／または同様のものを含む、様々な異なる衛星

であり得る。あるいは、ロケーション情報／データ／データは、セルラータワー、Ｗｉ－Ｆｉアクセスポイントおよび／または同様のものを含む様々な他のシステムに関連して位置を三角測量することによって判定され得る。同様に、ユーザコンピューティングエンティティ３０は、例えば、緯度、経度、高度、ジオコード、コース、方向、方位、速度、時間、日付、および／または様々な他の情報／データを収集するように適応されたロケーションモジュールなど、屋内測位の態様を含み得る。屋内の態様のいくつかは、ＲＦＩＤタグ、屋内ビーコンまたは送信機、Ｗｉ－Ｆｉアクセスポイント、セルラータワー、近くのコンピューティングデバイス（例えば、スマートフォン、ラップトップ）および／または同様のものを含む様々な位置またはロケーション技術を使用する場合がある。例えば、そのような技術は、ｉＢｅａｃｏｎ（登録商標）、ジンバル近接ビーコン、ＢＬＥ送信機、近距離通信（ＮＦＣ）送信機および／または同様のものを含み得る。これらの屋内測位の態様は、インチまたはセンチメートル以内に誰かまたは何かのロケーションを判定するために様々な設定で使用することができる。

【００８１】

ユーザコンピューティングエンティティ３０はまた、１つ以上のユーザ入出力インターフェース（例えば、処理要素３０８に結合されたディスプレイ３１６および／またはスピーカ／スピーカドライバ、ならびに処理要素３０８に結合されたタッチスクリーン、キーボード、マウス、および／またはマイクロフォン）を備えるユーザインターフェースを備え得る。例えば、ユーザ出力インターフェースは、アプリケーション、ブラウザ、ユーザインターフェース、ダッシュボード、ウェブページ、ならびに／あるいは情報／データの表示または可聴提示を引き起こすためにかつ１つ以上のユーザ入力インターフェースを介したそれとのユーザ対話のために、ユーザコンピューティングエンティティ３０上で互換的に実行されかつ／またはユーザコンピューティングエンティティ３０を介してアクセス可能である本明細書で使用される同様の単語を提供するように構成され得る。ユーザ出力インターフェースは、サーバ１８との通信から動的に更新され得る。ユーザ入力インターフェースは、キーパッド３１８（ハードもしくはソフト）、タッチディスプレイ、ボイス／音声もしくはモーションインターフェース、スキャナ、リーダー、または他の入力デバイスなど、ユーザコンピューティングエンティティ３０がデータを受信することを可能にするいくつかのデバイスのいずれかを備えることができる。キーパッド３１８を含む実施形態では、キーパッド３１８は、従来の数字（０～９）および関連するキー（＃、＊）、ならびにユーザコンピューティングエンティティ３０を動作させるために使用される他のキーを含む（または表示させる）ことができ、アルファベットキーのフルセット、または英数字キーのフルセットを提供するためにアクティブ化できるキーのセットを含むことができる。入力を提供することに加えて、ユーザ入力インターフェースは、例えば、スクリーンセーバーおよび／またはスリープモードなどの特定の機能をアクティブまたは非アクティブにするために使用することができる。そのような入力を通じて、ユーザコンピューティングエンティティ３０は、情報／データ、ユーザ対話／入力および／または同様のものを収集することができる。

【００８２】

ユーザコンピューティングエンティティ３０はまた、揮発性記憶装置もしくはメモリ３２２および／または不揮発性記憶装置もしくはメモリ３２４を含むことができ、これらは、埋め込まれ得る、および／または取り外し可能であり得る。例えば、不揮発性メモリは、ＲＯＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、ＭＭＣ、ＳＤメモリカード、メモリスティック、ＣＢＲＡＭ、ＰＲＡＭ、ＦｅＲＡＭ、ＲＲＡＭ（登録商標）、ＳＯＮＯＳ、レーストラックメモリおよび／または同様のものであり得る。揮発性メモリは、ＲＡＭ、ＤＲＡＭ、ＳＲＡＭ、ＦＰＭ ＤＲＡＭ、ＥＤＯ ＤＲＡＭ、ＳＤＲＡＭ、ＤＤＲ ＳＤＲＡＭ、ＤＤＲ２ ＳＤＲＡＭ、ＤＤＲ３ ＳＤＲＡＭ、ＲＤＲＡＭ、ＲＩＭＭ、ＤＩＭＭ、ＳＩＭＭ、ＶＲＡＭ、キャッシュメモリ、レジスタメモリおよび／または同様のものであり得る。揮発性および非揮発性記憶装置またはメモリは、ユーザコンピューティングエンティティ３０の機能を実装するためのデータベース、データベースイン

スタンス、データベース管理システムエンティティ、データ、アプリケーション、プログラム、プログラムモジュール、スクリプト、ソースコード、オブジェクトコード、バイトコード、コンパイルされたコード、解釈されたコード、マシンコード、実行可能命令および／または同様のものを記憶することができる。

【００８３】

ｃ．例示的な端末

様々な実施形態では、証明者端末１６および／またはエンティティ端末１２などの端末は、上で考察されたサーバ１８と同様の構成を有することができる。これらの端末は、様々なユーザによって動作され、および／または（例えば、ユーザコンピューティングエンティティ３０を介して）アクセス可能であり得、かつ／あるいは本明細書で考察される様々な機能を提供するように構成され得る。例えば、証明者端末１６は、第三者と関連付けられ得、エンティティのアイデンティティを証明するために構成され得る。

【００８４】

ユーザコンピューティングエンティティ３０がスマートフォンまたはタブレットなどのモバイルデバイスである実施形態では、エンティティ端末１２は、「アプリ」を実行して、サーバ１８および／またはエンティティ端末１２と対話することができる。このようなアプリは通常、タブレットやスマートフォンなどのモバイルデバイス上で実行するように設計されている。例えば、ｉＯＳ（登録商標）、Ａｎｄｒｏｉｄ（登録商標）、またはＷｉｎｄｏｗｓ（登録商標）などのモバイルデバイスオペレーティングシステム上で実行されるアプリが提供される場合がある。これらのプラットフォームは通常、アプリが相互に通信したり、モバイルデバイスの特定のハードウェアおよびソフトウェアコンポーネントと通信したりできるようにするフレームワークを提供する。例えば、上記のモバイルオペレーティングシステムはそれぞれ、ロケーションサービス回路、有線および無線ネットワークインターフェース、ユーザ連絡先、ならびに他のアプリケーションと対話するためのフレームワークを提供する。アプリの外部で実行されるハードウェアおよびソフトウェアモジュールとの通信は、通常、モバイルデバイスオペレーティングシステムによって提供されるアプリケーションプログラミングインターフェース（ＡＰＩ）を介して提供される。

【００８５】

例示的な実施形態では、エンティティ端末１２を利用して、対応するアセットデータファイルとして記憶できるアセットデータ（例えば、アセットがデジタル画像、データへのリンクである場合はアセット自体、アセットデータのデジタルハッシュ、アセットデータのデジタル署名などのように、アセットに関係するデータ）を準備、変更、レビュー、トランザクション、または他の方法でインターフェースすることができる。例えば、車の所有権は、例えば、エンティティ端末１２と関連付けられ、対応するアセットファイルとして記憶されるユーザまたはエンティティによって、エンティティ端末１２に記憶され得る。車の所有権は、例えば、証明者端末１６を有する車両管理局（ＤＭＶ）などの別のエンティティによって作成することができる。さらに別の代替手段として、アセットファイルは、証明者端末１６から（例えば、インターネットを介して）ダウンロードすることができる。アセットファイルは、他のアセットファイルとともに、いずれかの端末のメモリデバイス３３および／またはアセットレジストリに記憶することができる。車の所有権は、例えば、ＰＤＦ形式で、または車の所有権を作成するために使用されるアプリケーションと関連付けられたローカル／独自形式で保存することができ、ネットワーク２０を介して様々な当事者間で電子的に共有することができる。

【００８６】

例示的な実施形態では、エンティティ端末１２は、真正性の立証または証拠として機能するように、車の所有権にシール（例えば、シールされたアセットエントリにリンクするＱＲコード（登録商標）またはＩＤなどの物理的スタンプ）を生成および／または適用するように構成され得る。適用されるシールは、ユーザまたはエンティティが車の所有権の所有者であることを証明した証明者端末（例えば、ＤＭＶまたは専門家協会）によってユーザまたはエンティティに与えられるシールであり得る。したがって、シールに署名して

シールすることにより、ユーザまたはエンティティは、アセットファイルの内容に対して専門的な責任を負う。したがって、車の所有権を含むアセットファイルは、（例えば、エンティティ端末１２、証明者端末１６、および／または１つ以上の第三者端末（図示せず）の間で）ネットワーク２０を介して電子的に共有することができるが、アセットファイルがユーザまたはエンティティによって署名およびシールされていない限り、車の所有権は信頼（例えば、認証）することができない。

【００８７】

エンティティ端末１２はさらに、サーバ１８を介して、現在証明済みシール（すなわち、確認された所有者／エンティティのアイデンティティ）を登録することができる。証明済みシールを登録することにより、エンティティ端末１２は、改ざんされていないアセットがレジストリ１４にロードされ、確認されると、証明済みシールが、サーバ１８の確認マネージャ２４を介して第三者によって確認され得ることを確立し得る。

【００８８】

証明済みシールを確立した後、エンティティ端末１２は、証明済みシールをアセット（例えば、車の所有権）にさらに適用して、そのアセットをシールされたアセットとして識別することができる。端末１２は、サーバ１８を介して、シールされたアセットをさらに登録することができ、したがって、証明済みアセットがレジストリ１４にロードされることを確立することができる。

【００８９】

本発明の実施形態は、エンティティ端末１２が車の所有権にデジタル署名およびシールし、その後、文書の署名者／シール者（例えば、エンティティ）の署名およびシールを有するシールされたアセットを作成することを可能にするセキュリティ対策を提供する。さらに、本発明の実施形態は、デジタルアセットが真正であることを保証するために、エンティティが証明機関によって証明されていることを確認され得るメカニズムを提供する。いくつかの実施形態は、特定のデジタルアセットが実際にエンティティによって発行され、デジタルアセットが改ざんされておらず、エンティティが、信頼できるエンティティ証明者（例えば証明機関）によって実際に証明されることを保証するために、多数の当事者によって共通に共有されるレジストリ１４をさらに提供する。別の例示的な実施形態では、以下でさらに詳細に説明するように、他の当事者またはエンティティが、ルックアップ鍵を事前に知らずにレジストリのコンテンツに問い合わせることは不可能である。

【００９０】

例示的な実施形態では、共通に共有されるレジストリは、一意で無関係であるエントリ／レコードを含む。実装されるセキュリティ対策には、シールＩＤおよび／またはアセットＩＤによってデータをフェッチするように共通に共有されるレジストリを構成することが含まれる場合がある。

【００９１】

エンティティ端末１２は、特定のエンティティと関連付けられた端末、または特定のエンティティと提携した企業であり得る。証明者端末１６は、証明機関、またはエンティティを証明する権限を与えられた他の第三者と関連付けることができる。本発明の実施形態は、エンティティ端末１２が、中央レジストリに登録されているシールとされたアセットから、証明済みエンティティ関連付けられたデジタル適用された署名およびシールを有する物理的またはデジタルアセットを関連付けることを可能にし得る。これに関連して、エンティティ端末１２は、サーバ１８のデジタルアプリケータ２２を含むか、そうでなければ通信している可能性がある。

【００９２】

デジタルアプリケータ２２は、以下でより詳細に説明するように、本発明の例示的な実施形態に従ってデジタル署名およびシールを適用するように構成される、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアの組み合わせで具体化されるデバイスまたは回路などの任意の手段であり得る。デジタルアプリケータ２２は、処理要素２０５の制御下で動作することができる（またはそれとして具体化することさえできる）。図１

に示される実施形態などのいくつかの実施形態では、デジタルアプリケータ２２は、サーバ１８のソフトウェアで具体化され得る。したがって、エンティティ端末１２は、シールだけでなく、シールされたアセットの登録（例えば登録済みシールのデジタル署名を有するアセット）についても生成、証明、および登録のために、サーバ１８からデジタル署名およびシールサービスにアクセスするために、クライアント／サーバ環境でデジタルアプリケータ２２と通信することができる。

【００９３】

物理的またはデジタルアセットに関連して選択することができる１つの機能は、証明済みエンティティの署名とシールを有するアセットを登録することであり得る。言い換えれば、１つの機能は、デジタルシールを作成し、そのシールを証明し、証明済みシールを登録することであり得る。その後、登録された証明済みシールを使用してアセットに署名し、シールされたアセットをレジストリ１０に登録する。したがって、選択された物理的またはデジタルアセットについて、ユーザインターフェースまたは制御コンソールから特定のオプションを選択して、デジタルアプリケータ２２に、対応するアセットにデジタルシールおよび署名を適用させることができる。エンティティがデジタルシールおよび署名の適用を指示するとき、デジタルアプリケータ２２は、例えば、証明済みエンティティと関連付けられたシールおよび署名に関するデータを取り出し、シールレジストリに対してオンラインで共有される証明済みデジタルシールを作成することができる。次に、アセットはシールされ、証明済みエンティティのシールおよび署名とともに、対応するアセットデータを有する登録済みシールに登録される。登録済みシールとともに、現在の日付スタンプをアセットに適用することもできる。例示的な実施形態によれば、登録済みシールが適用されて、シール秘密鍵を使用してシールされたアセットが作成された後、シールされたアセットは、アセットが検索可能であるように、共通または分散レジストリに登録される。そのため、シールされたアセットを確認して、対応する登録済みシールおよび証明済みエンティティが正しいこと、およびシールされたアセットデータが確認対象のアセットと一致することを確証することができる。

【００９４】

別の例示的な実施形態では、ベリファイア（例えば、第三者または消費者）がアセットをレビューしている場合、ベリファイアは、サーバ１８によって提供される確認サービスによってアセットの真正性を確認することができる。ベリファイアは、サーバ１８の確認マネージャ２４と通信している可能性がある。

【００９５】

確認マネージャ２４は、以下でより詳細に説明するように、本発明の例示的な実施形態に従って、シールされたアセットが本物であるか確認するように構成される、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアの組み合わせで具体化されるデバイスまたは回路などの任意の手段であり得る。確認マネージャ２４は、処理要素２６の制御下で動作することができる（またはそれとして具体化することさえできる）。図１に示される実施形態などのいくつかの実施形態では、確認マネージャ２４は、サーバ１８のソフトウェアで具体化され得る。したがって、エンティティ端末１２は、シール確認されたアセットの確認のためにサーバ１８から確認サービスにアクセスするために、クライアント／サーバ環境において確認マネージャ２４と通信することができる。

【００９６】

例示的な実施形態では、エンティティ端末１２は、確認マネージャ２４にアセットの一意の識別子（例えば、アセットＩＤ）を提供することができ、それに対して、確認マネージャ２４は、アセットＩＤを使用して、レジストリからシールされたアセットレコードをフェッチして、シールされたアセットレコード内の情報を確認する。例示的な実施形態では、アセットＩＤは、アセットＩＤが一意である限り、例えば、「Ａ」から「Ｚ」までの２６個のアルファベット、「０」から「９」までの１０個の数字、「！」から「＝」までの１３個の特殊文字などを含む文字を含み得る。

【００９７】

例示的な実施形態では、確認マネージャ２４は、次に、シールされたアセットの記憶ロケーション（例えば、レジストリ）にリンクされて、シールされたアセットが実際に真正であり、証明済みエンティティが添付されているかどうかを確認することができる。あるいは、第三者または顧客が、シールされたアセットと関連付けられたＩＤを受け取っているか、またはそうでなければ認識している場合、第三者または顧客は、確認目的でシールされたアセットにアクセスするために、確認マネージャ２４に関連して、シールされたアセットＩＤをアプリに入力することができる。

【００９８】

レジストリおよびシールされたアセットＩＤへのアクセスの許可に関するセキュリティを確保するために、確認マネージャ２４および／または情報サーバ１８は、第三者のアイデンティティを保証して第三者が確認マネージャ２４のサービスにアクセスできるようにするための認証サービスを提供するように構成される、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアの組み合わせで具体化されるデバイスまたは回路などの任意の手段であり得るアプリケーションを含み得る。アプリケーションは、例えば、ユーザ名または他の識別と、対応するパスワードまたはコードを提供することによって、第三者ユーザにログインを要求する場合がある。これに関連して、アプリケーションは、各第三者ユーザと関連付けられた個別のアカウントまたはレコードの保守を提供する場合がある。

【００９９】

例示的な実施形態では、エンティティ端末１２（または別の端末）は、他の周辺機器および／またはデバイスをさらに含むことができる。例えば、エンティティ端末１２は、セキュリティデバイスを含み得る。例示的な実施形態では、セキュリティデバイスは、特定のエンティティを識別する目的でセキュリティの追加のレイヤを提供するように構成される、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアの組み合わせで具体化されるデバイスまたは回路などの任意の手段であり得る。いくつかの実施形態では、セキュリティデバイスは、秘密鍵／公開鍵ペア、磁気カードリーダー、無線周波数識別（ＲＦＩＤ）リーダー、生体識別デバイスおよび／または同様のものであり得る。したがって、特定のエンティティと関連付けられた磁気カード、ＲＦＩＤタグ、または単に生理学的または行動的特性を使用して、特定のエンティティに対して証明およびデジタルアプリケータ２２のサービスへのアクセスを付与する前に、特定のエンティティの識別および認証を支援することができる。

【０１００】

したがって、いくつかの実施形態は、機能へのアクセスならびにシールおよび登録のために少なくとも２つのセキュリティレベルを含み得る。したがって、例えば、エンティティがアセットに署名してシールするために、エンティティは、デジタルアプリケータ２２によるセキュリティチェックに合格するためのログインおよびパスワードを提供し、セキュリティデバイスによるセキュリティチェックに合格するための鍵、アクセスカード（例えば、磁気もしくはＲＦＩＤ）、または他のアイデンティティの表示（例えば、多要素認証）の所有に関係するアイデンティティのさらなる証拠を提供することを要求され得る。以下でより詳細に説明するように、さらにさらなるセキュリティも提供され得る。

【０１０１】

ｄ．例示的なネットワーク

一実施形態では、ネットワーク２０は、例えば、ケーブルネットワーク、パブリックネットワーク（例えば、インターネット）、プライベートネットワーク（例えば、フレームリレーネットワーク）、ワイヤレスネットワーク、セルラーネットワーク、電話ネットワーク（例えば、公衆電話交換網）、あるいは他の好適なプライベートおよび／またはパブリックネットワークなど、異なるタイプの好適な通信ネットワークのいずれか１つまたは組み合わせを含み得るが、これらに限定されない。さらに、ネットワーク２０は、それと関連付けられた任意の好適な通信範囲を有し得、例えば、グローバルネットワーク（例えば、インターネット）、ＭＡＮ、ＷＡＮ、ＬＡＮ、またはＰＡＮを含み得る。さらに、ネ

ットワーク２０は、同軸ケーブル、ツイストペア線、光ファイバ、ハイブリッドファイバ同軸（ＨＦＣ）媒体、マイクロ波地上トランシーバ、無線周波数通信媒体、衛星通信媒体、またはそれらの任意の組み合わせ、ならびにネットワークプロバイダまたは他のエンティティによって提供される様々なネットワークデバイスおよびコンピューティングプラットフォームを含むがこれらに限定されない、ネットワークトラフィックが運ばれることができる任意のタイプの媒体を含み得る。

【０１０２】

ＩＶ．例示的なシステム動作

ここで、図３、４、５、および６を参照し、これらは、本明細書で考察されるコンピューティングエンティティによって実行される様々な機能を示している。本明細書で考察される特定の実施形態は、公開鍵暗号を利用するが、他の暗号化方法論が特定の実施形態において利用され得る。公開鍵暗号は、デジタル署名の生成および／または認証に利用することができる。使用することができる公開鍵暗号化および／またはデジタル署名スキームには、限定はされないが、リベスト－シャミア－エーデルマン（ＲＳＡ）、楕円曲線、量子セーフアルゴリズムおよび／または同様のものが含まれる。暗号化強度は、選択された暗号化スキームおよび／または利用されるセキュリティ要件に少なくとも部分的に基づいて選択することができる。

【０１０３】

ａ．デジタルシールの作成

図３ａは、本開示の例示的な実施形態に従ってシールを登録し、アセットをシールし、およびシールされたアセットをエンティティ証明者３１０、エンティティ／証明済みエンティティ３２０、デジタルシールレジストリ３３０、シールされたアセット３４０、ベリファイア３５０、およびレジストリリスト３６０を用いて確認するための動作ステップを示す動作データフロー図を示す。注目すべきことに、図３ａは、１つの例示的な実施形態の例示であり、したがって、いくつかの代替の実施形態では、追加の動作を実行することができ、またはいくつかの動作を省略してもよい。

【０１０４】

Ｉ．エンティティを確認し、デジタル証明書を発行する

ここで図３ａを参照すると、ワークフローは、エンティティ証明者３１０で開始することができ、エンティティ証明者３１０は、エンティティ３２０を確認し、デジタル証明書を発行して、エンティティ３２０を証明する。これに関連して、エンティティ証明者３１０は、エンティティ３２０の資格情報を確認し、確認すると、対応する証明のシールをエンティティ３２０に発行する。

【０１０５】

「確認済みエンティティ」または「証明済みエンティティ」になるためには、各エンティティは、エンティティ証明者３１０またはエンティティ発行者によって設定される要件に準拠する必要がある。例えば、エンティティ証明者３１０は、例えば、エンティティ３２０が、特定の基準に準拠するかまたは準拠することに同意する合法的なビジネス商人であることを確認し得る。例えば、エンティティ証明者３１０は、エンティティがプライバシーまたはセキュリティ要件に準拠していることを確認する組織であり得る。あるいは、例えば、エンティティ証明者３１０は、連絡先情報、製造、生産または販売施設、納税番号、住所、登録、ライセンス、社会保障番号、電子メール、電話、バイオメトリクス、個人アイデンティティ、コンピューティングデバイスおよびソフトウェアアプリケーションにインストールされた秘密／公開鍵、またはこれらの任意の組み合わせの確認などのデジタル証明書を発行する前に、名目的な量の証明を実行することができる。

【０１０６】

例示的な実施形態では、エンティティ証明者は、エンティティ３２０自体であり得、そのようなものとして、自己証明サービスまたは証明機関を提供する。追加または代替として、エンティティ証明者３１０は、政府機関、プリティグッドプライバシー（ＰＧＰ）プログラム、ブロックチェーン、またはエンティティのアイデンティティを確認することが

できるかもしくは確認するのに信頼することができる別のエンティティであり得る。別の例示的な実施形態では、エンティティ証明者３１０は、証明者の階層であり得、ルート証明者の署名公開鍵は公開されている。より高いレベルの確実性が必要である場合、１つの証明済みエンティティ証明書は、多数の証明者がデジタル署名する必要がある場合がある。エンティティが証明者３１０によって証明されると、エンティティは、本明細書では証明済みエンティティ３２０と呼ばれる。

【０１０７】

例示的な実施形態では、エンティティ３２０は、デジタルシール（例えば、ＱＲコード（登録商標）として表され得る公開鍵）をすでに所有している可能性があるか、またはシールは、デジタルアプリケーション２２によって生成される。例えば、エンティティ３２０は、デジタルアプリケーション２２による証明のためにそれらのデジタルシールを送信することができる。

【０１０８】

例示的な実施形態では、デジタル署名およびデジタルシールの完全性、機密性および真正性を実施するために、証明者３１０は、デジタルアプリケータ２２によって適用されるシールおよび署名の証明書を提供するように構成される、ハードウェア、ソフトウェア、またはハードウェアとソフトウェアの組み合わせで具体化されるデバイスまたは回路などの任意の手段であり得る。通常、エンティティ３２０は、秘密／公開鍵ペアを作成し、証明者３１０は、エンティティによって作成された公開鍵とエンティティ識別データにデジタル署名して、証明書発行者自身の秘密鍵を使用して公開鍵証明書を作成する。エンティティは、それの秘密鍵を秘密に保つ。

【０１０９】

エンティティ３２０のアイデンティティの証明を示すデータは、証明者３１０（例えば、証明者３１０を介して提供されるルート証明書）までさかのぼって、エンティティ３２０のアイデンティティが、信頼できる第三者の証明者３１０によって証明されたという信頼を確立することができる。証明者のデータを追跡するために利用されるデータは、デジタルシール内で提供され得、および／またはデジタルシールとともに提供されるデータに少なくとも部分的に基づいてアクセスされ得る。

【０１１０】

ｉｉ．証明済みシールの作成

例示的な実施形態では、証明者３１０は、シールおよび署名を証明するための中間証明機関として働くことができる。これに関連して、例えば、証明者３１０は、暗号プロトコル（例えば、セキュアソケットレイヤ（ＳＳＬ））を利用し、デジタルアプリケータ２２によって適用される任意のシールおよび署名を伴う証明書を発行することができる。一実施形態では、デジタルアプリケータ２２は、デジタル電子シールおよび署名を、証明者３１０を介して確認可能なシールおよび署名に変換するように構成され得る。証明者３１０によって発行された証明書は、アセットにアセットの完全性を提供するために、シールおよび署名の真正性をさらに確認するために使用され得る。さらに、例示的な実施形態では、証明者３１０は、証明者３１０によって通常ならば発行される証明書の代わりにまたはそれに加えて、外部エージェンシーからの証明書を含めることを要求することを可能にし得る。これに関連して、例えば、専門エージェンシーまたは他の証明エージェンシーが、特定のデジタルシールおよび署名が真正であることを示すために特定の証明書を提供する場合、証明者３１０は、デジタルアプリケータ２２によって発行されたデジタルシールおよび署名の信頼できる証明書機関確認が完了したことを示すために専門エージェンシーのエンティティと通信し、署名およびその上のシールの真正性のさらなる証拠として、ならびに専門エージェンシーまたは外部エージェンシーの要件も満たされていることの証拠としてアセットに含めるために、特定の証明書が証明書発行者に発行されることを要求することができる。

【０１１１】

例示的な実施形態では、エンティティ証明者３１０は、エンティティ３２０から証明済

みエンティティ証明書発行要求を受信することができ、この要求は、エンティティのための少なくとも１つの一意の識別子と、秘密鍵／公開鍵ペアの公開鍵とを含む。その後、証明者３１０は、少なくとも１つの一意の識別子に基づいてエンティティが真正であるかどうかを判定し、エンティティが真正であると判定した後、秘密鍵とともに少なくとも１つの一意の識別子を備えるアイデンティティエンティティデータにデジタル署名して、証明済みエンティティ証明書を生成することができる。言い換えれば、証明者３１０は、エンティティ３２０によって受信および作成された公開鍵およびエンティティデータにデジタル署名して、図４に示されるような証明済みエンティティ証明書４６０を作成する。

【０１１２】

証明済みシールを取得するために、エンティティ３２０は、図４に示されるように、シール公開鍵４１０およびシール秘密鍵４２０として別の公開鍵／秘密鍵ペアを作成する。例示的な実施形態では、エンティティ３２０は、選択されたシールデータをデジタルアプリケーション２２に送信することができる。選択されたシールデータには、シールの使用目的（例えば、医薬品の製造業者の証明）、シールのタイプおよび／またはカテゴリ（例えば、薬品の出所の証明、卒業証書の真正性の証明および／または同様のもの）、シールの使用目的（例えば、制限および／または他の手順の指示の提供）、ならびに／あるいはシールが有効である時間範囲（例えば、１週間、２４時間）が含まれる場合がある。

【０１１３】

例示的な実施形態では、シール公開鍵４１０自体または公開鍵４１０、および選択されたシールデータ４４０のいくつかは、シールＩＤ４８０として使用される。シールＩＤ４８０は、証明済みシールを一意に識別するために使用される。本明細書で使用される場合、「シールデータ鍵」は、証明済みシールを一意に識別するために使用されるシールＩＤを指す場合がある。証明済みシール４７０を作成するために、デジタルアプリケーション２２は、証明済みエンティティ４６０の対応する秘密鍵４３０を用いてシールＩＤ４８０およびシールデータ４４０にデジタル署名して、証明済みエンティティ３２０のデジタル署名４５０を作成する。

【０１１４】

例示的な実施形態では、証明機関によって証明済みエンティティに付与されたエンティティ証明書４６０は、証明済みシール４７０に記憶されたリンクまたはエンティティ証明書自体４６３を含み得る。

【０１１５】

追加または代替として、デジタルアプリケーション２２は、エンティティ証明書４６０およびその対応するエンティティ秘密鍵４３０を使用する代わりに、別の証明済みシール４７０を使用して別の証明済みシールを作成することができる。

【０１１６】

ｉｉｉ．証明済みシールの登録

次に、デジタルアプリケーション２２は、証明済みシール／登録済みシールを有するレジストリエントリ３７０として、図３に示されるように、証明済みシール４７０をデジタルシールレジストリ３３０に登録する。証明済みシール４７０が登録されると、それは登録シールと呼ばれることがある。登録シールは、デジタルシールレジストリ３３０から、対応するレジストリエントリ３７０と関連付けられているそのシールＩＤ４８０によって検索可能であり得る。いつでも、登録シールは、そのエンティティ署名４５０を用いて証明済みエンティティ３２０によって取り消され得る。

【０１１７】

例示的な実施形態では、登録シールは、デジタルシールレジストリ３３０からそのシールＩＤ４８０によって検索可能である。デジタルシールレジストリ２１１として働く１つまたは多数のオンラインサービスが存在する可能性があり、これらのレジストリは、登録されたレコードを交換することができる。登録シールは、証明済みエンティティ３２０のデジタル署名４５０を用いて、その証明済みエンティティによって取り消され得る。

【０１１８】

レジストリは、一般に公開されるか、または非公開に保たれ得る。１つ以上の接続された公開レジストリの利点は、アプリケーションを１つのプラットフォームに統合することができることである。図３Ａに示されるように構成されたデジタルシールレジストリ３３０は、サーバ１８を使用して、レジストリおよびそのレコードまたはエントリ３７０の動作を管理する。

【０１１９】

ｂ．アセットのシール

シールされたアセット３４０を作成するために、エンティティ３２０は、デジタルアプリケーション２２を介して、証明済みシール／登録済みシール４７０内のシール公開鍵４１０の対応するシール秘密鍵４２０を用いてアセットＩＤ３８０またはアセットのシールＩＤにデジタル署名して、登録済みシール署名５３０を有するシールされたアセット５００をもたらすことができる。次に、署名されたシールされたアセットおよびそれに対応するシールＩＤ４８０は、シールされたアセット５００を含む単一のレジストリエントリとしてレジストリに保存される。例示的な実施形態では、レジストリは、アセットおよび／またはシールをフェッチするためにベリファイアに提供されるリンクを用いて、証明済みエンティティによって管理され得る。シールされたアセットを有することは、アセットＩＤ５１０およびアセットデータ５２０が、シールＩＤ５８０を有する証明済みシール／登録済みシール４７０の登録シール署名５３０をもつエンティティ証明書４６０によってシールされていることの確認を提供する。言い換えれば、他のエンティティは、シールされたアセットがそれらによってシールされていると主張することはできない。アセットＩＤ５１０は、公開鍵または乱数のような新しいＩＤ、または証明済みシール４７０の図４のシール公開鍵４１０、またはシール公開鍵４１０と何らかのアセットデータ３４２であり得る。シールされたアセット３４０は、そのアセットＩＤ３８０またはシールＩＤによって検索可能であり、シールされたアセットレコード５００を得ることができる。

【０１２０】

追加または代替として、アセットをシールするために、アセットデータ５２０ａは、アセットをシールするために使用される証明済みシール／登録シール３７０のレジストリエントリに入力され得る。これは、アセットレジストリエントリ／シールされたアセット５１０ａによって示されるように、シールされたアセットレコード５００を証明済みシールレコード４７０と組み合わせる。証明済みシール４７０のシールＩＤ４８０は、図５ａにおけるようにアセットＩＤ（シールＩＤ／アセットＩＤ５８０ａ）として使用することができる。これを達成するために、デジタルアプリケータ２２は、証明済みエンティティ証明書４６０を用いてシールＩＤ４８０およびアセットデータ５２０ａにデジタル署名し、エンティティ署名５５０ａをもたらし、次に、エンティティ証明書４７０を用いてエンティティ署名４５０にデジタル署名して、証明済みシール（ＣｅｒｔＳｅａｌ）署名５３０ａを作成する。この場合、証明済みエンティティ証明書５６０ａは、レコード５１０ａ（例えば、アセットレジストリエントリ／シールされたアセット）に添付されるか、またはそれへのリンクが提供されるので、エンティティ署名５５０ａが本物であるか確認することができる。ＣｅｒｔＳｅａｌ署名５３０ａが本物であるか確認するための公開鍵は、Ｓｅａｌ＿ＩＤ５８０ａであるか、あるいはＳｅａｌ＿ＩＤ５８０ａから派生している。

【０１２１】

ワイン、医薬、食品および／または同様のものなどの消耗品である物理的なシールされたアセットの場合、１つのシールＩＤ／アセットＩＤは、アセット／パッケージの外側に配置することができる。２番目のシールＩＤは、アセット／パッケージ内に配置することができる。そのような実施形態では、各シールＩＤが１回だけ使用される場合、それはより効果的である。偽造者の場合、外側のシールと内側のシールの両方をバッチでコピーするのが最も費用効果が高い。内側のシールのうちの１つが本物であることが確認された場合、バッチ全体は、高いレベルの確実性で偽造されていることがわかる。

【０１２２】

ｃ．デジタル署名確認の実施

既存の現在のデジタル署名および確認プロセスを図６に示す。図６に示すように、文書またはデータ６１０の公開／秘密鍵のペアを使用してデジタル署名を作成するためのプロセスは、最初にデータ６１０のデジタルハッシュ６２０を計算し、次に、秘密鍵を用いて結果のハッシュ６２０を暗号化して、暗号化されたハッシュ６３０を作成することである。通常、データ６１０および暗号化されたハッシュ６３０は、一緒に（例えば、互いに関連して）記憶され、デジタル署名された文書と呼ばれる。対応する公開鍵６０２はまた、鍵所有者のアイデンティティを証拠立てるためのデジタル証明書、または公衆によく知られている公開鍵および所有者のいずれかとともに、デジタル署名された文書とともに記憶され得る。図６に示すように、デジタル署名が本物であるか確認するために、最初に、公開鍵または証明書６０２を使用して、暗号化されたハッシュ６３０を復号化して、復号化された署名６４０を取得し、次に、データ６１０のハッシュ６２０を、デジタル署名の作成の場合と同じアルゴリズムを使用して計算し、最後に、ハッシュ６２０が、復号化された署名６４０と比較され、それらが同じである場合、デジタル署名は有効であると判定される。

【０１２３】

ただし、上記のアプローチの問題は、デジタル署名が本物であるか確認されたという証拠がないことである。任意のエンティティは、デジタル署名された文書からデータ６１０を取り、添付されたデジタル署名を確認したと主張することができる。

【０１２４】

上記の問題を解決するために、様々な実施形態は、図６ａに示されるように、デジタル署名確認を実施することを提供する。本開示は、公開鍵暗号化、デジタル署名、対称暗号化、およびハッシュ計算のうちの１つ以上を利用することがある。追加または代替として、量子コンピューティングセーフアルゴリズムも利用することができる。暗号化の強度は、使用するスキームとセキュリティ要件に基づいて選択することができる。

【０１２５】

図６ａを参照すると、動作ステップは、最初に、暗号化ハッシュ関数を使用してデータ６１０ａのハッシュ６２０ａを計算することを含む。その後、暗号化されたデータ６４０ａを得るための鍵として、上記で計算されたハッシュ６２０ａを用いてデータ６１０ａを暗号化する。次に、署名の秘密鍵を使用してハッシュ６２０ａを暗号化して、暗号化されたハッシュ６３０ａを得る。

【０１２６】

暗号化されたデータ６４０ａおよび暗号化されたハッシュ６３０ａは、この実施形態では、デジタル署名された（暗号化された）文書である。署名公開鍵６０２ａまたはその公開鍵証明書は、図６ａに示されるように、署名された文書６００ａに添付することができる。公開鍵６０２ａまたはその公開鍵証明書は、例示的な実施形態では、署名された文書から分離することができる。

【０１２７】

この実施形態に従って生成されたデジタル署名が本物であるか確認するために、確認動作ステップは、暗号化されたハッシュ６３０ａを署名公開鍵６０２ａを用いて復号化してデータハッシュ６２０ａを取得すること、上記のステップからのハッシュ６２０ａを使用して、暗号化されたデータ６４０ａを復号化すること、次に、復号化されたデータ６５０ａを取得することを含む。

【０１２８】

復号化されたデータ６５０ａが意味のある場合（例えば、暗号化された暗号として判読不能でない場合）、デジタル署名は有効であると判定される。

【０１２９】

さらに、エントロピー６１２ａ（例えば、乱数）は、データをさらに保護するためにハッシュされる前に、データ６１０に追加され得る。例示的な実施形態では、エントロピー６１２ａのサイズは、少なくとも部分的にセキュリティ要件に基づくことができる。

【０１３０】

本発明の別の実施形態は、図６ｂに示されるように、デジタル署名確認を実施することである。動作プロセスステップは、暗号化鍵６２０ｂの生成を含む。例示的な実施形態では、暗号化鍵は、対称鍵または秘密／公開鍵ペアであり得る。後続のステップは、暗号化鍵６２０ｂを用いて署名されるデータ６１０ｂを暗号化して、暗号化されたデータ６４０ｂを得ること、暗号化されたデータ６４０ｂのハッシュ６２２ｂを計算すること、デジタル署名の秘密鍵を用いて暗号化鍵６２０ｂを暗号化すること、暗号化された暗号化鍵６３０ｂを得ること、および上記の暗号化された鍵６３０ｂをハッシュ６２２ｂを用いて暗号化して、二重暗号化された鍵６５０ｂを取得することを含む。

【０１３１】

暗号化されたデータ６４０ｂおよび二重暗号化された暗号化鍵６５０ｂは、デジタル署名された（暗号化された）文書を表すことができる。署名公開鍵６０２ｂまたはその公開鍵証明書は、図６ｂに示されるように、署名された文書６００ｂに添付することができる。公開鍵またはその公開鍵証明書６０２ｂは、それが配置され得る限り、署名された文書から分離もされ得る。

【０１３２】

例示的な実施形態では、この実施形態に従って生成されたデジタル署名が本物であるか確認するための方法は、図６ｂに示されるように以下の動作ステップを含む：暗号化されたデータ６４０ｂのハッシュを計算して、暗号化されたデータハッシュ６２２ｂを取り戻すこと、上記で導出されたハッシュ６２２ｂを用いて、二重暗号化された鍵６５０ｂを復号化して、暗号化された鍵６３０ｂを得ること、暗号化された暗号化鍵６３０ｂを署名の公開鍵６０２ｂを用いて復号化して暗号化鍵６２０ｂを取り戻すこと、上記のステップからの暗号化鍵６２０ｂを使用して、暗号化されたデータ６４０ｂを復号化して、結果的に、復号化されたデータ６５０ｂをもたらすこと。

【０１３３】

例示的な実施形態では、デジタル署名は、復号化されたデータ６５０ｂが意味のある（例えば、判読不能または文字化けしていない）場合に有効であると判定される。

【０１３４】

追加または代替として、暗号化鍵６２０ｂは、データ６１０ｂの図６ｂのハッシュ６２０ｂであり得る。

【０１３５】

別の例示的な実施形態では、暗号化鍵６２０ｃを二重暗号化して、二重暗号化された鍵６５０ｂを得る順序を逆にすることができ、それは依然として機能する。この場合、確認の復号化順序も逆になる。

【０１３６】

さらに別の例示的な実施形態では、公開鍵またはその証明書６０２ｂを暗号化するためのハッシュ６２２ｂを、暗号化された鍵６３０ｂを暗号化する代わりに利用することができる。言い換えれば、デジタル署名ベリファイアは、暗号化されたデータ６４０ｂのハッシュを計算し、公開鍵６０２ｂを使用していくつかのデータを復号化してから、暗号化されたデータ６４０ｂを復号化して、復号化されたデータ６５０ｂを得る。

【０１３７】

上記の実施形態の例示的なケースは、暗号化鍵６２０ｂが、データ６１０ａの図６ａのハッシュ６２０ａであり得ることである。特定の実施形態では、暗号化鍵６２０ｂを二重暗号化して、二重暗号化された鍵６５０ｂを得る順序を逆にすることができる。この場合、確認の復号化順序も逆にする必要がある。二重暗号化の他の方法は、特定の実施形態に従って提供され得る。例えば、暗号化された鍵６３０ｂを暗号化する代わりに、ハッシュ６２２ｂを使用して公開鍵またはその証明書６０２ｂを暗号化するなど。本質は、デジタル署名ベリファイアを強制して、暗号化されたデータ６４０ｂのハッシュを計算し、公開鍵６０２ｂを使用していくつかのデータを復号化してから、暗号化されたデータ６４０ｂを復号化して、復号化されたデータ６１０ｂを得ることができることである。

【０１３８】

ｃ．シールされたアセットの確認

図３に戻ると、シールされたアセット３４０が本物であるか確認するために、確認マネージャ２４は、シールされたアセットと関連付けられたアセット識別子を受信することができる。追加または代替として、確認マネージャは、シールされたアセットのシール識別子を受信することができる。次に、確認マネージャ２４は、レジストリを位置特定するか、または既知のシールレジストリリストサービスからレジストリロケーションを得るか、またはアセット識別子もしくはシール識別子（例えば、ロケーションＵＲＩのＱＲコード（登録商標））に埋め込まれたロケーションデータからレジストリロケーションを得ることができる。

【０１３９】

次に、確認マネージャ２４は、レジストリに問い合わせて、アセット識別子またはシール識別子に関係するレジストリデータを有するレコードを取り出すことができる。レジストリデータは、証明済みエンティティによって生成されたシールデータ鍵を含み、シールされたデータ鍵は、証明済みエンティティによって生成されたシールされたアセットの確認されたデジタル署名と一致する。その後、確認マネージャ２４は、アセット識別子のデジタル署名がレジストリデータのシールデータ鍵と一致するかどうかを判定して、シールされたアセットが本物であるか確認することができる。

【０１４０】

言い換えれば、確認マネージャ２４は、レコードの登録シールが、正しい証明済みエンティティのエンティティ証明書によって署名されていることを確認するように構成される。確認マネージャ２４は、レコード内のエンティティ証明書が、正しい証明済みエンティティを証明すること、および証明済みエンティティが、正しいエンティティ証明者によって実際に証明されていることをさらに確認することができる。確認マネージャはまた、（例えば、機械学習アルゴリズム、直接マッチングアルゴリズムおよび／または同様のものなどの１つ以上のマッチングアルゴリズムを介して）エンティティ証明者が有効であるおよび／または信頼することができることを確認することができる。レコード内のアセットデータが確認対象のアセットと一致すること、および／またはＲｅｇＳｅａｌが正しいタイプであるかどうかを確認するために、確認マネージャによってさらなる確認ステップが実装される。

【０１４１】

図７、８、および９は、本発明の例示的な実施形態によるシステム、方法、およびコンピュータプログラム製品のフローチャートである。フローチャートの各ブロックまたはステップ、およびフローチャート内のブロックの組み合わせは、ハードウェア、ファームウェア、および／または１つ以上のコンピュータプログラム命令を含むソフトウェアなどの様々な手段によって実装できることが理解されよう。例えば、上記の手順のうちの１つ以上は、コンピュータプログラム命令によって具体化され得る。これに関連して、上記の手順を具体化するコンピュータプログラム命令は、例えば、端末またはサーバのメモリデバイスによって記憶され、それぞれの処理要素２０５によって実行され得る。理解されるように、そのようなコンピュータプログラム命令は、コンピュータまたは他のプログラム可能な装置（すなわち、ハードウェア）にロードされて、マシンが製造され得、その結果、コンピュータまたは他のプログラム可能な装置上で実行される命令は、フローチャートブロックまたはステップ内で指定された機能を実装するための手段を作成する。これらのコンピュータプログラム命令はまた、コンピュータまたは他のプログラム可能な装置に特定の方法で機能するように指示することができるコンピュータ可読メモリに記憶され得、その結果、コンピュータ可読メモリに記憶された命令は、フローチャートブロックまたはステップ内で指定された機能を実装する命令手段を含む製造品を生じる。コンピュータプログラム命令はまた、コンピュータまたは他のプログラム可能な装置にロードされて、コンピュータまたは他のプログラム可能な装置上で一連の動作ステップが実行させられて、コンピュータ実装プロセスが生じ得、その結果、コンピュータまたは他のプログラム可能な装置上で実行される命令は、フローチャートブロックまたはステップ内で指定された機能

を実装するためのステップを提供する。

【０１４２】

したがって、フローチャートのブロックまたはステップは、指定された機能を実行するための手段の組み合わせ、指定された機能を実行するためのステップの組み合わせ、および指定された機能を実行するためのプログラム命令手段をサポートする。フローチャートの１つ以上のブロックまたはステップ、およびフローチャート内のブロックまたはステップの組み合わせは、特定の機能もしくはステップ、または特別な目的のハードウェアとコンピュータ命令の組み合わせを実行する特別な目的のハードウェアベースのコンピュータシステムによって実装することができることも理解されよう。

【０１４３】

これに関連して、図７に示されるように、登録された証明済みシールを生成する方法の一実施形態は、エンティティから、登録された証明済みシールを生成する要求を受信することを含み得、要求は、ブロック７００に示されるように、デジタル署名されたエンティティ証明証明書を備える。

【０１４４】

例示的な実施形態では、この方法は、追加の動作を含み得る。例えば、この方法は、ブロック７１０に示されるように、証明証明書によって識別された証明機関の証明者エンティティデータにアクセスする動作をさらに含み得る。

【０１４５】

ブロック７２０において、この方法は、証明証明書と関連付けられ、証明機関からアクセスされる証明者エンティティデータに少なくとも部分的に基づいて、デジタル署名されたエンティティ証明証明書が本物であるか確認することをさらに含み得る。

【０１４６】

この方法は、ブロック７３０に示されるように、デジタル署名されたエンティティ証明証明書が本物であることを確認したら、証明済みシールのシールデータ鍵を含むシールデータを受信するための動作をさらに含み得、シールデータは、エンティティによって一意に生成される。

【０１４７】

ブロック７４０に示されるように、この方法は、デジタルシールレジストリ内にエンティティのシールデータを保存することをさらに含み、デジタルシールレジストリは、シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である。

【０１４８】

別の実施形態では、図８に示されるように、アセットをシールするための方法が提供される。この方法は、ブロック８００に示されるように、エンティティのアセットと関連付けられたアセットデータを生成することを備え、アセットデータは、アセットおよびエンティティを一意に識別する。

【０１４９】

例示的な実施形態では、この方法は、追加の動作を含み得る。例えば、この方法は、ブロック８１０に示されるように、シールデータを独立したシールデータレジストリに送信してそこに記憶する動作をさらに含み得、シールデータレジストリは、エンティティに対応するエンティティ証明データを含み、シールデータは、エンティティ固有公開鍵秘密鍵ペアの公開鍵を含む。

【０１５０】

ブロック８２０において、この方法は、エンティティ固有公開鍵秘密鍵ペアの秘密鍵を介してアセットと関連付けられたアセットデータにデジタル署名して、署名されたアセットデータを生成することをさらに備える。

【０１５１】

この方法は、ブロック８３０に示されるように、署名されたアセットデータを送信して、署名されたアセットレジストリに記憶することをさらに備え、署名されたアセットレジストリは、１つ以上のベリファイアによってアクセス可能であって、エンティティ固有公

開鍵秘密鍵ペアの公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にする。

【０１５２】

別の例示的な実施形態では、この方法は、ブロック９４０に示されるように、１つ以上のベリファイアに、署名されたアセットレジストリ内の署名されたアセットデータ、および独立したシールデータレジストリ内のシールデータへのアクセスを提供することをさらに備える。

【０１５３】

図９に示されるように、さらに別の例示的な実施形態では、シールされたアセットが本物であるか確認するための方法が提供され、この方法は、アセット識別子に関係するレジストリデータを記憶するシールレジストリを識別すること（ブロック９００を参照）、およびシールレジストリに問い合わせて、アセット識別子に関係するレジストリデータを取り出すことを備え、レジストリデータは、証明済みエンティティによって生成されたシールデータ鍵を備え、シールされたデータ鍵は、ブロック９１０に示されるように、証明済みエンティティによって生成されたシールされたアセットの確認されたデジタル署名と一致する。

【０１５４】

ブロック９２０において、この方法は、アセット識別子のデジタル署名がレジストリデータのシールデータ鍵と一致するかどうかを判定して、シールされたアセットが本物であるか確認することをさらに備える。

【０１５５】

例示的な実施形態では、この方法は、アセットシール識別子を受信し、シール識別子と関連付けられたアセットレジストリを識別し、アセットレジストリからレジストリエントリまたはレコードをルックアップし、シール識別子と関連付けられたレジストリエントリまたはレコードをルックアップするための手段を含む。この方法は、登録済みシールが有効であり、レジストリエントリ内の登録シールが証明済みエンティティによって作成されていることを確認するための手段をさらに備える。この方法はまた、登録済みシールの証明済みエンティティが有効であり、信頼できる証明機関によって証明されていることを確認する手段を含む。

【０１５６】

図７、８、および９に関して上記で説明された動作は、例示のみを目的として具体的に説明されている。いくつかの実施形態では、シールされたアセットと別の認証タイプが関連付けられ得ることが認識されるべきである。さらに、いくつかの実施形態では、別のタイプの登録済みシールが、対応するレベルの真正性を提供し得ることを認識されたい。したがって、図７、８、および９に示される特定の実施形態は、本開示の範囲および繻子を制限するものと解釈されるべきではない。

【０１５７】

図７、８、および９に示される特定のステップは、いくつかのシステムによって、独立したシステムによって、またはシステムの組み合わせによって実行され得ることが認識されよう。追加または代替として、いくつかの実施形態では、ステップ代替動作、代替動作、および／または動作の異なる配置は、本明細書の開示の範囲内の実施形態によって実行され得る。したがって、図３～９に示される特定のフローは、単なる例示であり、限定を目的とするものではない。

【０１５８】

使用例１－医療保険詐欺防止

保険会社は、その保険カードごとにデジタルシールされたアセットを作成する。アセット識別子またはシールＩＤは、例えば、対応する物理カードにＱＲコード（登録商標）として印刷することができる。サーバ１８と通信しているモバイルデバイスは、ＱＲコード（登録商標）を読み取り、発行保険会社が、確認された登録シールを有し、したがって保険カードデータが正しいことを、シールレジストリ１４を用いて確認することができる。

例示的な実施形態では、保険カードデータ自体を図５のアセットレジストリレコードエントリ５００に保存することができ、またはリンクをエントリに保存することができ、リンクは、保険カードが保存されるロケーションへのリンクである。サーバ１８の確認マネージャ２４は、アセットレジストリから保険カードデータをフェッチする。カードデータは、保険契約者ユーザの画像を含み得る。確認マネージャと通信しているモバイルデバイスのユーザは、保険契約者の画像を有するフェッチされた保険データをカード所有者と比較して、保険カードが実際に保険会社によって正しい保険契約者に発行されていること、およびさらに、カードがいかなる方法でも改ざんされていないことを確証することができる。例示的な実施形態では、確認プロセスのための電子レコード、モバイルデバイスのロケーション、およびタイムスタンプは、保険カードおよび保険契約者が確認されたことの証拠として保存することができる。例示的な実施形態では、すべての正しいデータが確認デバイスによって返され得るので、保険カードは、シールＩＤのＱＲコード（登録商標）のみを含むことができる。例えば、モバイルデバイス上の画像のようなデジタル形態のシールＩＤは、保険カードとしても働く。

【０１５９】

（例えば、ウォレット内の）様々な物理カードのいずれも、上記の保険カードの例で考察されたのと同様の方法でデジタル化することができる。追加または代替として、個人を識別するための顔認識などのバイオメトリクスが、確認マネージャ２４によって利用され得る。例えば、証明済みエンティティ３２０は、個人に関する情報を含む、個人のためのシールされたアセット３４０を作成することができる（図３を参照）。バイオメトリックデータの固有の特性は、証明されたアセットのアセットＩＤ３８０またはシールＩＤにリンクすることができる。例えば、保険会社は、その保険カードシールＩＤとしてシールＩＤと保険カードタイプを使用することができる。保険カードタイプはアセットデータ３４２の一部である。シールされた保険カードは、カード保険カードシールＩＤを鍵として使用してレジストリ１４をルックアップすることにより、フェッチおよび確認することができる。カード保険カードシールＩＤの少なくとも一部は、顔認識のようなバイオメトリクスによって取得された個人（例えば、エンティティ）のシールＩＤである。さらに、カードシールＩＤの２番目の部分は、保険カードタイプである場合がある。同様に、個人のシールＩＤは、他のタイプの識別目的にも使用することができる。

【０１６０】

図１のレジストリ１４は、ベリファイア１５０に許可を与えることによって保護することができる。これを達成するために、例えば、証明済みエンティティ１２０は、別個の許可ＲｅｇＳｅａｌを登録し、このＲｅｇＳｅａｌを使用して、ベリファイアアプリケーションをシールする。この場合、アプリケーションは、それ自体の鍵ペアを持つシールされたアセットである。シールされたアセット鍵ペアを使用して、アプリケーションを認証し、アプリケーションがアクセスすることができるデータを制御することもできる。

【０１６１】

使用例２－金融アセットのデジタル化

ブロックチェーンと関連する多くの困難を伴わずに、金融アセット（例えば、通貨）をデジタル化するために様々な実施形態を利用することができる。図１０は、証明済みの銀行が、図２に示されるようなプロセスで現金または小切手を発行するための登録シールを登録する一実施形態による現金のデジタル化の例示的な描写である。例えば、シールデータには、通貨のタイプ、サポートされる支払いまたはトランザクションプロトコルが含まれる場合があり、他のデータを登録することができる。デジタル小切手を発行するために、サーバ１８と通信している顧客デバイスは、公開鍵秘密鍵ペアを作成し、公開鍵をウォレットＩＤまたはアドレスとして使用することができる。次に、銀行は、小切手の一意のＩＤを作成し、ＩＤ、顧客のウォレットＩＤ、および小切手金額データ（例えば、シールデータ）を通貨シールの秘密鍵のデジタル署名を用いてシールして、デジタル小切手レコードを作成する。

【０１６２】

デジタル小切手を使用するには、支払人が小切手ＩＤ、受取人のウォレットＩＤ、および小切手金額に署名して、ウォレットデジタル署名を作成する。受取人は、署名されたデータまたは支払いトランザクションレコードを銀行に送信し、銀行は、新しいデジタル小切手を受取人に発行する。古い小切手は銀行によって無効にされる。残りの金額は、新しいデジタル小切手で支払人に発行することができる。１回の支払いトランザクションで多数の小切手トランザクションを完了することができる。多数のデジタル署名を使用して、デジタル小切手のセキュリティを強化することもできる。デジタル署名の代わりに、ビットコインやイーサリアム用に提供されているものなど、一部のスクリプトやソフトウェアプログラミング言語を使用して、認証およびトランザクションプロセスをより柔軟で用途の広いものにすることもできる。

【０１６３】

あるいは、上記のように新しいデジタル小切手を発行して古い小切手をキャンセルする代わりに、銀行は、通貨証明済みシール２７０を用いてトランザクションレコードに署名して、トランザクションにおいてデジタル署名４５０を作成することができる。したがって、署名またはシールされたトランザクションは、同じ小切手ＩＤと、新しいウォレットに再分配される金額とを持つ新しい小切手として働くことができる。これらのシールされたトランザクションは、新しいデジタル小切手と交換するために銀行に提出することができる。さらに他の実施形態では、（他のエンティティに対応する）他のＲｅｇＳｅａｌを利用して、元のエンティティの承認に基づいて、トランザクションを承認することができる。特定の実施形態では、シールレジストリおよび／またはアセットレジストリは、特定の実装に従ってブロックチェーンとして実装され得る。別の例示的な実施形態では、他のエンティティが元のエンティティに代わってトランザクションをシールできることに元のエンティティが同意する限り、他のエンティティからの別のＲｅｇＳｅａｌを使用してトランザクションを承認することができる。

【０１６４】

様々な実施形態では、最初に、受取人は、支払人のデバイスが読み取るためのＱＲコード（登録商標）などの入力を有する。次に、支払人はデバイスを使用して入力を読み取り、支払人に支払うことに同意する。入力は受取人のアカウントにリンクされる。支払人が同意してプロセスを終えると、支払いは支払人のアカウントから受取人のアカウントに送金される。しかしながら、そのような実施形態には、入力が悪意のある当事者によって置き換えられて支払いが盗まれる可能性があるなどの問題がある。セルフサービスの自転車レンタルの場合など、支払い入力（ＱＲコード（登録商標））を放置すると、それはより脆弱になる。このようなモバイルデバイスの支払いを保護するために、ＲｅｇＳｅａｌを使用して支払い入力（ＱＲコード（登録商標））に署名することができる。支払人は、潜在的な顧客が支払いに同意する前に、支払い入力が適切にシールされていること、および支払い入力のその証明済み所有者（エンティティ１２０）が本物であるか確認することができる。他の誰かが偽の支払い入力を作成して、本当の所有者のふりをすることはできない。確認プロセスを支払いプロセスに組み込んで、偽造された支払い入力を検出した場合に支払人に警告することができる。

【０１６５】

上記の実施形態は、価値のあるアセットをデジタル化するための例としてのみ役立つ。銀行は、デジタルアセットを発行するための証明済みエンティティ（アセット発行者）の例でもある。発行されたデジタルアセットは、１つ以上の秘密／公開鍵ペアによって保護されたウォレットにリンクされる。発行されたアセットは、アセット発行者の対応するアセットシール（ＲｅｇＳｅａｌ）によって保護される。

【０１６６】

使用例３－アセットトランザクション

同じまたは異なるアセットシールを用いて発行されたデジタルアセットは、図１２に示すように、対応するシールを適用して取引することができる。アセット取引トランザクション１２００は、アセットＩＤ１２１０、対応する宛先ウォレットＩＤおよび支払いデー

タ１２４４、アセットまたはウォレット所有者が受取人に支払うことに同意することを確認するための対応するウォレットのデジタルウォレット署名１２４６、ならびにアセットが対応するウォレットによって所有されており、トランザクションがコミットされたときに金額が正しく利用可能であることを確認するための対応するアセットＲｅｇＳｅａｌのアセットシール／ＲｅｇＳｅａｌ署名１２３０から構成される。別の例示的な実施形態では、アセットシール／ＲｅｇＳｅａｌ署名１２３０は、アセットＲｅｇＳｅａｌによって承認された他のプロキシＲｅｇＳｅａｌの署名であり得る。すべてのウォレットおよびＲｅｇＳｅａｌの署名がトランザクションレコード１２００に収集されると、所有者は、トランザクションレコード１２００を対応するアセット発行者に送信して、交換または取引から生じた新しいデジタルアセットと交換することができる。

【０１６７】

使用例４－スマート契約

例示的な実施形態では、スマート契約は、アセットＩＤ１３１０、対応する宛先ウォレットＩＤおよびデータ１３４４、契約が有効であるために満たされなければならない１つ以上の条件１３５０、アセットまたはウォレットの所有者が、条件が満たされたら契約でトランザクションをコミットすることに同意することを確認するための対応するウォレットのデジタル署名１３４６を備え、アセット発行者の対応するアセットシール１３３０のデジタル署名を使用して、アセットが対応するウォレットによって所有されており、金額が正しく、アセットが、トランザクションがコミットまたはキャンセルされるまで予約されることを確認する。例えば、年末におけるＳ＆Ｐ５００インデックス（ＳＰ）がしきい値Ｔを下回った場合、ユーザＡがユーザＢに通貨Ｃで金額ＡＭＴを支払うことに同意することを指定する契約。スマート契約は、１）ウォレットＡ内の証明済みシールを用いて発行された通貨Ｃの金額ＡＭＴのアセットＩＤ１３１０を有するデジタル小切手、２）デジタル小切手がウォレットＢに支払われるという支払いトランザクション、３）条件が、年末にＳＰ＜Ｔであり、Ｓ＆Ｐ５００インデックスベリファイアＶによって確認されること、４）Ａが契約に同意することを確認するためのウォレットＡの署名１３４６、５）小切手ＣＩＤが有効であり、小切手が契約の終了時に利用可能であることを確認するための通貨Ｃの証明済みシールのデジタル署名１３３０、ならびに６）ＳＰ＜Ｔであることを確認するための年末におけるベリファイアＶのデジタル署名１３６０から構成される。契約が署名され、上記の条件が満たされると、ユーザＢは、通貨発行者にトランザクションを送信し、それをデジタル小切手と交換することができる。この例示的な実施形態では、すべての肯定的条件が満たされると、契約を実行することができる。１つの否定的な条件が確認された場合、契約はキャンセルされる場合がある。１つ以上の条件を確認するために、契約において１つ以上の条件ベリファイアが必要になる場合がある。

【０１６８】

使用例５－デジタル契約または文書の署名

別の例示的な実施形態では、図１３に示されるように、１つ以上の証明済みエンティティは、開示されたスキームを用いてデジタル契約または文書に署名することができる。各エンティティは、文書１３１０ａのハッシュ１３２０ａにそのＲｅｇＳｅａｌを用いて署名して、デジタル署名１３３０ａを作成する。結果として得られるレコード１３００ａは、デジタル署名された文書または契約である。

【０１６９】

例えば、２人の個人間の契約には、契約に署名するために使用されたシールされた運転免許証が含まれる場合がある。運転免許証は政府機関によってシールされ得る。シールされた運転免許証が偽造されておらずかつ偽造することができないことを保証するために、シールＩＤは運転免許証番号として使用することができ、その対応する秘密鍵は発行者またはＤＭＶによって所有される。さらに、シールされたアセットレコードを用いて追加の秘密公開鍵ペアをシールすることができ、個人または運転手が秘密鍵を所有する。２人の個人は、図１３のように秘密鍵を使用して契約に署名して、デジタル署名１３３０ａを作成する。シールされた文書１３００ａは、契約が２人の個人または運転手によって本当に

署名されていることを証拠立てる。
【０１７０】
別の例は、ＲｅｇＳｅａｌを使用して電子メールアドレスを証明し、その秘密鍵を使用して電子メールに署名することである。これは、電子メールが実際にＲｅｇＳｅａｌの所有者によって送信されたことを証拠立てることができる。その結果、フィッシング電子メールやスパム電子メールを高いレベルで確実にフィルタ除外することができる。
【０１７１】
使用例６－アイデンティティ確認
エンティティがＲｅｇＳｅａｌを用いて証明されると、対応する秘密鍵と公開鍵のペアをアイデンティティ確認に使用することができる。例えば、秘密鍵と公開鍵のペアは、パスワードなしのログインに使用することができる。例えば、Ｗｅｂサイトはエンティティに乱数を送信することができ、エンティティは、その秘密鍵を用いて乱数を暗号化し、暗号化された暗号をＷｅｂサイトに送り返す。Ｗｅｂサイトは、公開鍵を用いて暗号を復号化して乱数を取得し、これは、エンティティに送信された元の乱数と一致する必要がある。
【０１７２】
使用例７－認証サービス
現在の環境では、クレジットカード詐欺は一般に、権限のないユーザによるクレジットカードの権限のない使用と関連している。デジタル化されたクレジットカード（デジタルアセット）を使用することにより、商店は、カードが実際に適切なクレジットカード会社（ＣｅｒｔＥｎｔｉｔｙ）によって発行され、ユーザアイデンティティを証明するためのデジタル署名を作成したのは所有者の秘密鍵であることを確証することができる。デジタル署名は毎回異なる（例えば、秘密鍵のみが同じである）ため、ハッカーは、デジタル署名を盗むことによって利益を得ることができない。カード所有者のデジタル署名と彼らのデジタルクレジットカードを組み合わせることで、トランザクションを行うために、正しい証明済みの人物が適切なカードを使用していることが保証される。
【０１７３】
リワードポイントとギフトカードポイントのトランザクションに関する別の例を提供する。証明済みエンティティには、リワードプログラムの発行者（航空会社、ホテル、レストランなど）および／またはｅコマース会社が含まれる場合がある。シールされたアセットには、リワードポイント、取引トランザクション、デジタルウォレットが含まれる場合がある。デジタルキャッシュの例と同様に、リワードポイントおよびポイント取引は、安全にデジタル化することができる。本明細書の開示に基づいて、消費者が、様々なｅコマースプラットフォーム上で彼らの個人的なリワードを販売することを可能にする、新規で安全な方法が提供される。例えば、消費者は、リワード発行者（ＣｅｒｔＥｎｔｉｔｙ）によって証明されたデジタルリワード（デジタルアセット）を得る。さらに、ｅコマース企業はリワードの真正性を容易に確認することができ、注文が行われると、トランザクションはリワード所有者によってスタンプされ、トランザクションをクリアするためにリワード発行者に送信され得る。
【０１７４】
さらに別の例では、政府証明書は、ここで提供される動作手順に従って政府エージェンシーがデジタル証明書をそれに対して発行することができる、政府エージェンシーなどの証明済みエンティティを含み得る。シールされたアセットには、例えば、パスポート識別、政府発行の証明書、免許証などが含まれる場合がある。そのようなシールされたアセットの審査官は、政府発行の文書が実際に対応する機関によって発行されたことを、高い信頼レベルで確認することができる。
【０１７５】
身元調査の実施に関連して、学校および／または雇用主などの証明済みエンティティは、卒業証明書、従業員の職歴、成績証明書などのシールされたアセットを有する学生卒業生を証明することを提供し得る。例えば、学生が卒業すると、学生の学校は、彼らの学位のデジタル証明書を発行することができる。別の例は、従業員が会社を辞めたときに提供

され、雇用主は従業員の職歴が本物であるかを証明するデジタル証明書を発行することができ、従業員が新しい雇用主における新しい仕事に応募する場合、新しい雇用主は、本明細書で考察される様々な実施形態を介して発行当事者を容易にチェックすることができるので、従業員は、自信を持ってデジタル学位および職歴を新しい雇用主に送信することができる。そのため、時間のかかる身元調査を回避することができる。他の使用例の例は、ローン会社が、本明細書で考察される発明を使用して文書の真正性を確認することができるので、消費者が彼らの信用スコアのデジタルコピーをローン会社に直接送信することができる信用チェックに関係し得る。さらに、秘密鍵を使用して、電話や電子メールなどの通信が実際に正当な所有者からのものであることを確認することができるため、アイデンティティ情報の盗難のケースを防ぐことができる。

【０１７６】

使用例８－デジタル署名／証明書を使用する許可の管理

例示的な実施形態では、公開鍵暗号化および／またはデジタル署名／証明書は、許可を管理するために実装される。保護されるデータは、一意の識別子（ＵＩＤ）を用いて割り当てられる／リンクされる。データは、データ自体にすることも、データへのＵＲＬにすることもできる。例えば、上記のように、データとそのＵＩＤは証明済みシール（ＣｅｒｔＳｅａｌ）によってシールすることができ、ＣｅｒｔＳｅａｌは証明済みエンティティによって証明される。データの許可を管理するために、図１１のルート許可証明書１１００が作成され、これは、公開鍵、およびオプションで許可のタイプ（例えば、読み取り、書き込みアクセス）、および証明済みエンティティのデジタル署名または証明済みシール、またはデータを備える。例示的な実施形態では、ルート許可証明書１１００は、例えば、ＵＩＤ１１３２としての公開鍵によってデータ１１４０のデジタル署名を使用してデジタル署名され、秘密鍵を使用してデジタル署名に署名する。ルート許可証明書の署名は、許可がデータの所有者によって付与されていることの証明として働く。別の例示的な実施形態では、デジタル署名は、そのＵＩＤとして公開鍵を使用し、秘密鍵を使用して署名に署名することによって、データ１１４０を使用して取得することができる。

【０１７７】

この例では、ルート許可証明書がデータ１１４０によって署名されている場合、データは、証明済みシールによって証明される必要はない。ユーザ、組織、デバイス、またはサービスなどに許可を付与するために、ユーザは別の秘密鍵公開鍵ペアを生成し、公開鍵は、ルート許可証明書を用いてデジタル署名され、オプションで、ユーザに許可を提供する別の許可証明書を作成するための許可タイプを用いて署名される。いくつかの例では、許可証明書は、図１１の１１１０許可証明書に示されているように、ツリー構造を形成する他の許可証明書に署名することができる。

【０１７８】

ユーザがデータへの許可を有することを確認するために、ユーザは、許可証明書１１３０の秘密鍵の所有権の証拠を提供し、許可証明書は、ルートアクセス許可証明書１１００への許可証明書１１１０のチェーンによって確認され、ルート証明書１１００は、データ自体によって証明されるか、あるいはデータの証明済みシールによってまたはデータ１１７０の証明済みエンティティによって証明される。これらの証明書は、ユーザ許可証明書をデータにリンクする。この例では、ホストされている当事者ではなく、データの所有者が許可を制御する。

【０１７９】

別の例示的な実施形態では、データを保護する１つの方法は、その所有者がデータ自体をホストし、データへのＵＲＬリンクのみを提供できることである。ＵＩＤおよび／または許可証明書は、第三者によってホストされる場合がある。ユーザがデータにアクセスするとき、その所有者は、最初に、本明細書の実施形態に従って、ユーザが適切な許可を有することを確認することができる。

【０１８０】

さらに別の例示的な実施形態では、データは暗号化される。データの暗号化鍵は、許可

証明書に暗号化鍵を埋め込むことによってエンドユーザに渡される。暗号化鍵は、許可証明書１１３２の公開鍵を使用して暗号化することができる。許可証明書の所有者は、対応する秘密鍵を用いて暗号化鍵を得ることができる唯一の人物である。この方法で、暗号化鍵を証明書ツリーに渡すことができる。公開鍵暗号化された暗号化鍵はまた、許可証明書とは別に記憶することができ、例えば、本明細書に記載の例示的な実施形態によれば、許可証明書公開鍵をルックアップ鍵としてレジストリなどの１つのデータベースに保存することができる。

【０１８１】

この例示的な実施形態では、データおよびその許可は、デジタル署名を使用して一緒にバインドすることができ、許可は、デジタル署名を使用してユーザに付与され得る。ユーザは、他のユーザに許可を与えることができ、許可は、他者に許可を与える許可を含むことができる。

【０１８２】

使用例９－個人アイデンティティ証明

例えば、公証人および郵便局などの上記のようなエンティティは、エンティティ証明者によって証明されることができる。次に、証明済みエンティティは、それらのＲｅｇＳｅａｌを使用して個人を証明し、その個人に対してＲｅｇＳｅａｌを発行することができる。次に、この個人は、例えば、契約書への署名、ローンの申し込み、クレジットカード、保険カードの使用の権限付与、アセットの売却、医師訪問の証拠のためのデジタル署名の作成などのケースにおいて、それらのＲｅｇＳｅａｌを使用して、それらのアイデンティティの証明、デジタル署名、存在の証拠の作成などを行うことができる。

【０１８３】

個人アイデンティティ証明書は、クレジットカード詐欺と戦うために使用することができる。クレジットカードの権限のない使用は、今日非常に一般的な問題である。カード所有者の住所に新しいクレジットカードが郵送されると、メールが盗難に遭い、クレジットカードが悪用される可能性がある。そのため、企業にはユーザの真正性を保証する信頼できる方法がない。さらに、カードの使用（例えばオンライン購入）時にカード所有者がいない場合、そのようなクレジットカードトランザクションにおいて本当の所有者がカードを使用していることを保証するのは困難である。

【０１８４】

本発明の実施形態を使用して、クレジットカード会社は、公証人によって公証されたカード所有者の公開鍵を登録することができる。確認を求めて所有者にメッセージが送信されると、メッセージは、上で考察されたように所有者の公開鍵を使用して暗号化される場合がある。所有者は、メッセージを受信した後、それに応じてアクションを取ることができる。所有者だけがその秘密鍵を持っているので、所有者だけが復号化して応答することができる。他の人は、メッセージを確認することができない。

【０１８５】

別の例では、エンティティは、権限のあるベリファイアのみがサーバ情報にアクセスすることを望む場合がある。例えば、保険会社は、その権限のある診療所だけが患者の保険カード情報にアクセスできるようにしたい場合がある。軍事エージェンシーは、カードを紛失したときに機密情報（例えば、ユーザの写真、出生データ、社会保障番号など）が暴露されないように、物理的なカード上で限られた情報のみを発行したい場合がある。ただし、権限のあるユーザは、ベリファイアを使用してシールされたアセットをチェックすることにより、より多くの情報を取得することができる。これを実現するために、ベリファイアアプリケーションのユーザは、ベリファイアアプリケーションを使用して、エンティティ証明者で公開鍵を証明して、上記のようにＲｅｇＳｅａｌを得ることができる。次に、ユーザは、ＲｅｇＳｅａｌを使用してベリファイアアプリケーションにそれらのアイデンティティを登録して、それらのアイデンティティを証明することができる。したがって、許可は、証明済みのアイデンティティに基づいて付与される。このようにして、その後の証明書公開鍵を使用することによってすべての将来の通信を暗号化して、権限のあるベ

リファイアのみが特定の情報を確認できるようにする。

【０１８６】

個人の公開鍵が証明書として公証されると、個人の秘密鍵は、パスワード、指紋、音声認識、顔認識、または他のセーフティ方法を介してアクセス可能な電話あるいは任意のハードウェアデバイスまたはサーバ上のデジタルウォレットに保存することができる。ウォレットは、Ａｐｐｌｅ　Ｐａｙ、クレジットカード、デビットカードなどの多数の支払い方法を記憶する場合があり、例えばｅコマースＷｅｂサイト上などで、支払いカードが使用されている場合は常に、チェックアウト前に、ｅコマース会社は、購入したアイテム、金額などの情報を含むショッピングカート情報を個人のデバイスに通信することになる。この情報は、個人の公開鍵を使用して暗号化することができるため、支払いカードの所有者のみがメッセージを解読することができる。メッセージを受信すると、個人は、支払い方法を選択し、オプションで配送先住所を入力し、それらの秘密鍵を使用してメッセージを暗号化することによって支払い方法の使用に権限を与えることができる。この場合、ｅコマース会社と、選択された支払いカード会社の両方は、それらの秘密鍵のみがメッセージを復号化することができるため、トランザクションが真のカード所有者によって権限を与えられ、承認されることを知っている。そのため、署名された権限付与に基づいて、支払いに迅速かつ正常に権限を与えることができる。この新規の方法は、本当の所有者がカードを使用していることを確証することにより、潜在的な権限のないカード購入の多くを排除することができる。

【０１８７】

例示的な実施形態では、本当のカード所有者に送信される公開鍵暗号化されたメッセージは、例えば、保険カードがスキャンされている、登録された本当の所有者にアラートが送信されるなどのイベントによってトリガされ得る。ｅコマース企業は、チェックアウト時に表示するために、ＱＲコード（登録商標）など、デバイスで読み取り可能なコードの形態ですべてのショッピングカート情報を提示することもでき、これに対して、個人は、ウォレットデバイス上のスキャナを使用してコードをスキャンすることができる。デバイスは、ウォレットからの支払い方法の選択を促すことができる。次に、ウォレットは、支払い情報を暗号化し、クレジットカード会社による権限付与のためにｅコマース会社に送信して、チェックアウトを迅速化することができる。ユーザが実店舗での対面支払いにウォレットを使用している場合も、同じ方法を適用することができる。この場合、ユーザは、販売者によって提示されたコードをスキャンして支払いに権限を与えることができる。

【０１８８】

ユーザインターフェースの例

図１４、１４ａ、１４ｂ、および１４ｃは、様々な実施形態による例示的な構成を実装するための１つ以上のコンピューティングデバイス（例えば、ユーザコンピューティングデバイス）の１つ以上のディスプレイ画面によって提示され得る例示的な表示を示す。例えば、図１４、１４ａ、１４ｂ、および１４ｃの表示は、デスクトップまたはラップトップコンピュータによって、またはモバイルのハンドヘルドマーチャントデバイスによってユーザに提示することができる。これらの表示は、あるユーザから別のユーザへのシールされた文書の取得および送信を容易にするのに役立つ場合がある。

【０１８９】

図１４、１４ａ、１４ｂ、および１４ｃの表示を使用して、エンティティが、シールされたアセットを要求し、システムを使用してシールされたアセットを送信するための比較的単純、迅速、かつ直感的な方法を提供することができる。図１４、１４ａ、１４ｂ、および１４ｃの表示を、例えば、ポータルとして使用して、シールアセットを作成し、ユーザまたはエンティティに対する選択および送信のために、シールされたアセットを提供し、かつシールされたアセットの確認を提供して、シールされたアセットが、証明済みエンティティによってシールされており、アセットがシールされた時間以降、改ざんまたは変更されていないことを確認することができる。

【０１９０】

一例では、図１４の表示１４００は、ユーザが、新しいシールされたアセットの作成を開始することを可能にする一連のフィールドを含むものとして示されている。この例では、ユーザのＪａｎｅ　Ｓｍｉｔｈは、シールされた雇用証明を要求している可能性があるＪｏｈｎ　ＭｃＣｌａｎｅの、過去の雇用主である。例えば、表示１４００は、新しいシールされた雇用証明１４０４を選択するユーザ入力を受信するために構成され得る。新しいシールされた文書またはアセット、この場合は雇用証明を作成することを選択すると、ユーザＪａｎｅ　Ｓｍｉｔｈは、過去の従業員Ｊｏｈｎ　ＭｃＣｌａｎｅ１４０２の個人的詳細を入力することができる。１４０１によって示されるように、表示は、ユーザＪａｎｅ　Ｓｍｉｔｈが、雇用証明を提供する選択された文書をエンベロープに追加することを可能にし得る。表示１４００は、雇用証明文書１４０２を含むエンベロープをシールおよび証明するためのアクションを提供する。表示はさらに、シールされた雇用証明を、従業員、例えば、従業員と関連付けられたユーザコンピューティングエンティティに送信することを提供する。次に、従業員は、シールされた雇用証明書を他のユーザ（例えば、将来の新規雇用者）に（ユーザコンピューティングエンティティを介して）送信して、シールされたデータにアクセスできるようにする。

【０１９１】

別の例では、図１４ａの表示１４００ａは、ユーザＪａｎｅ　Ｓｍｉｔｈに、検索入力グラフィカル要素１４０１ａを介して、シールされたアセットを検索する能力を提供するものとして示されている。ユーザが検索基準（例えば、従業員の社会保障番号）を入力すると、検索結果１４０２ａが表示１４００ａ上に提示される。各検索結果について、表示１４００ａは、シールされたアセットを転送する、シールされたアセットをコピーする、閲覧またはアクセス許可を管理する、シールされたアセットおよび／または同様のものを削除するなどのアクションを提供する。表示１４００ａはさらに、新しいシールされたアセット１４０３ａを作成するアクションを提供する。

【０１９２】

一例では、図１４ｂ表示１４００ｂが示され、従業員Ｊｏｈｎ　ＭｃＣｌａｎｅは、彼が所有するシールされたアセットのリストを見ることができる。１４０１ｂに示されるように、リストには、２つの異なるタイムスタンプにおいて作成された雇用証明、および卒業証書が含まれている。図示の例の表示１４００ｂは、最新の雇用証明など、少なくとも１つの選択されたシールされたアセット１４０２ｂを転送するオプションをユーザに提供する。

【０１９３】

図１４ｃの表示１４００ｃによって示されるように、シールされたアセット送付の受信者は、シールされたアセットにアクセスするためのリンク１４０１ｃを提供され得る。表示１４００ｃは、証明者、エンティティ、シールが確立された日付、一意のシールＩＤ、アクセス満了日および／または同様のもののうちの１つ以上を含む情報１４０２ｃを伴うエンベロープ（例えば、シールされたアセット）を含むものとして示されている。エンベロープを含む表示１４００ｃは、エンベロープが以下のエンティティによってシールされた（証明機関によって確認された）こと、および証明者によって確認されるようにエンベロープがシールされた時間以降、エンベロープの内容が誰によっても改ざんまたは変更されていないことの確認を提供する。

【０１９４】

本明細書で考察される例示的な表示によって提示される情報のすべてまたは一部は、システムの１つ以上のコンポーネントによって受信、生成および／または維持されるデータに基づくことができることに留意されたい。

【０１９５】

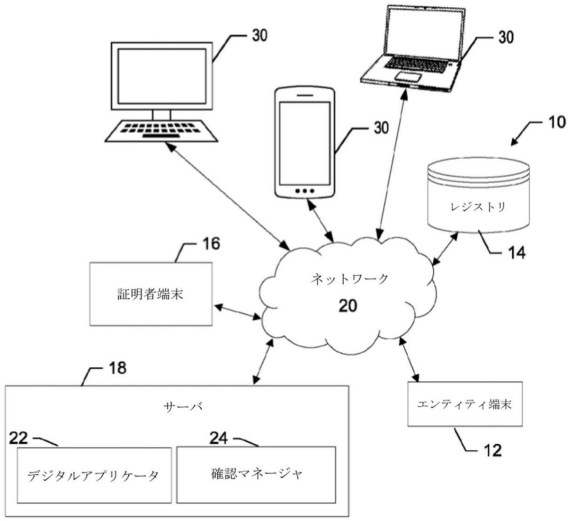
いくつかの実施形態では、上記の動作のいくつかは、変更またはさらに増幅され得る。さらに、いくつかの実施形態では、追加のオプションの動作が含まれ得る。上記の動作に対する変更、増幅、または追加は、任意の順序および任意の組み合わせで実行することができる。

【０１９６】

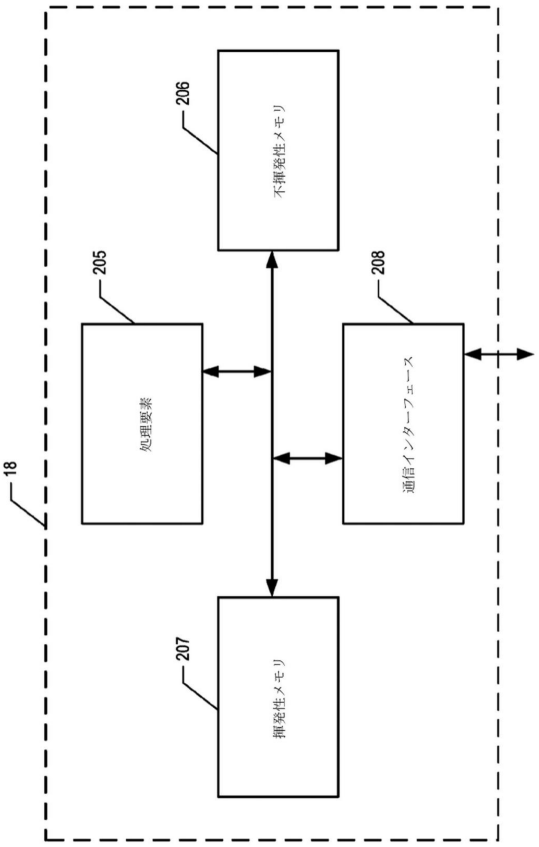
本明細書に記載された本開示の多くの変更形態および他の実施形態は、前述の説明および関連する図面に提示された教示の恩恵を受けて、これらの開示が関係する当業者に思い浮かぶことであろう。したがって、本開示は、開示された特定の実施形態に限定されるべきではなく、変更形態および他の実施形態は、添付の特許請求の範囲の範囲内に含まれることが意図されることを理解されたい。さらに、前述の説明および関連する図面は、要素および／または機能の特定の例示的な組み合わせを背景として例示的な実施形態を説明しているが、代替の実施形態によって、添付の特許請求の範囲の範囲から逸脱することなく、要素および／または機能の異なる組み合わせを提供し得ることを認識されたい。これに関連して、例えば、添付の特許請求の範囲のいくつかに記載されているように、上記で明示的に説明されたものとは異なる要素および／または機能の組み合わせも企図されている。本明細書では特定の用語が使用されているが、それらは、一般的かつ説明的な意味でのみ使用されており、限定を目的としていない。

【図面】

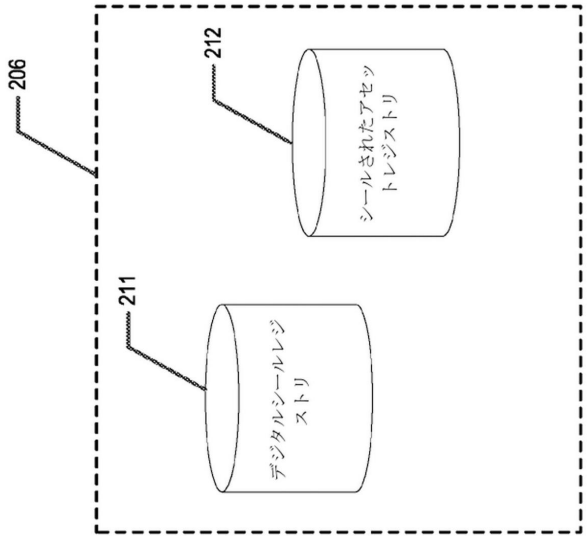
【図１】



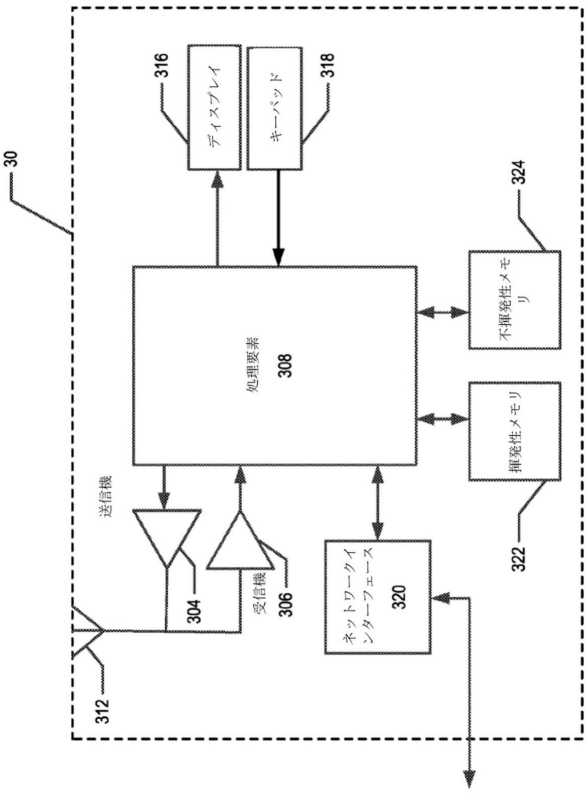
【図２Ａ】



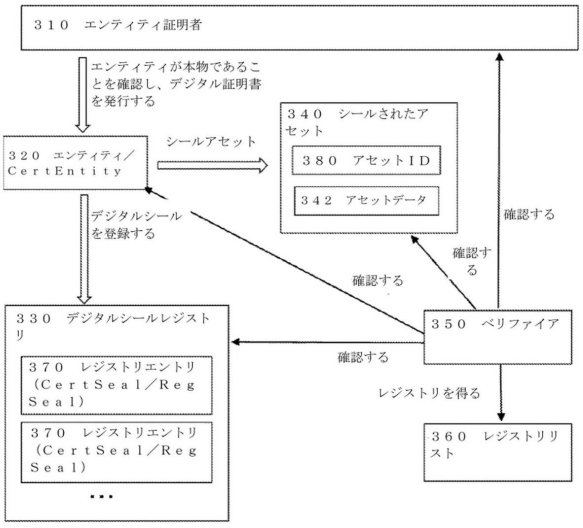
【図２Ｂ】


206
212
シールされたアセットレジストリ
211
デジタルシールレジストリ

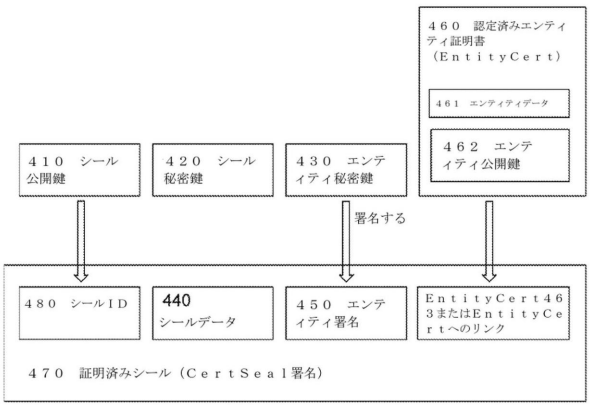
【図３】


30
316
ディスプレイ
318
キーパッド
324
不揮発性メモリ
処理要素
308
揮発性メモリ
322
送信機
304
受信機
306
ネットワークインターフェース
320
312

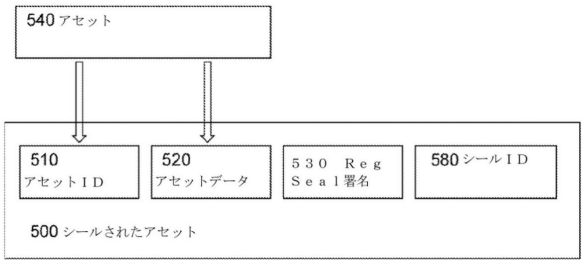
【図３ａ】


３１０　エンティティ証明者
エンティティが本物であることを確認し、デジタル証明書を発行する
３２０　エンティティ／CertEntity
シールアセット
３４０　シールされたアセット
３８０　アセットＩＤ
３４２　アセットデータ
デジタルシールを登録する
確認する
確認する
確認する
３３０　デジタルシールレジストリ
３７０　レジストリエントリ（CertSeal／RegSeal）
３７０　レジストリエントリ（CertSeal／RegSeal）
…
３５０　ベリファイア
確認する
レジストリを得る
３６０　レジストリリスト

【図４】


４６０　認定済みエンティティ証明書（EntityCert）
４６１　エンティティデータ
４６２　エンティティ公開鍵
４１０　シール公開鍵
４２０　シール秘密鍵
４３０　エンティティ秘密鍵
署名する
４８０　シールＩＤ
440
シールデータ
４５０　エンティティ署名
EntityCert463またはEntityCertへのリンク
４７０　証明済みシール（CertSeal署名）

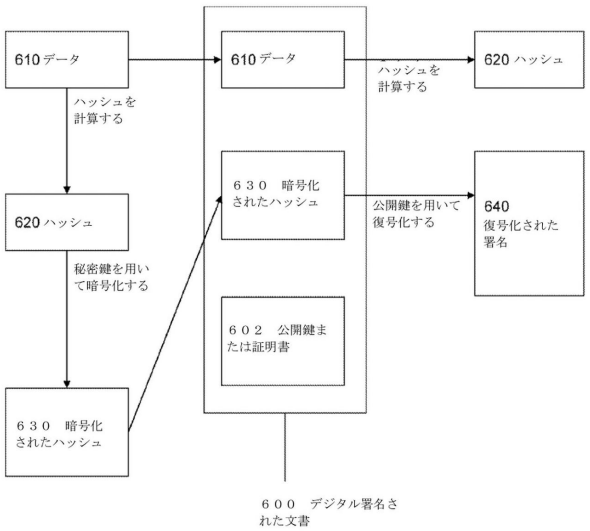
【図５】



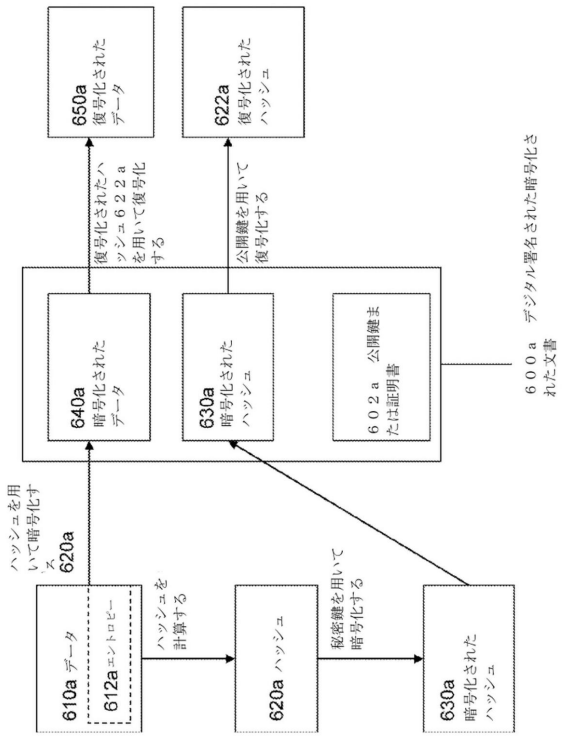
【図５ａ】

【図６】

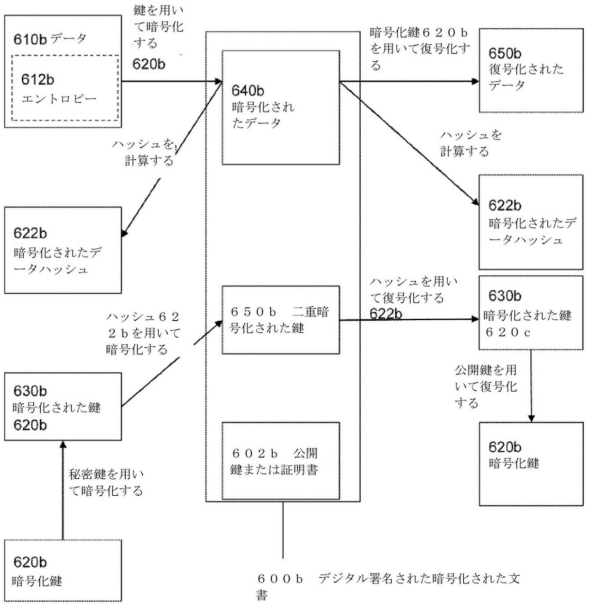
（従来技術）



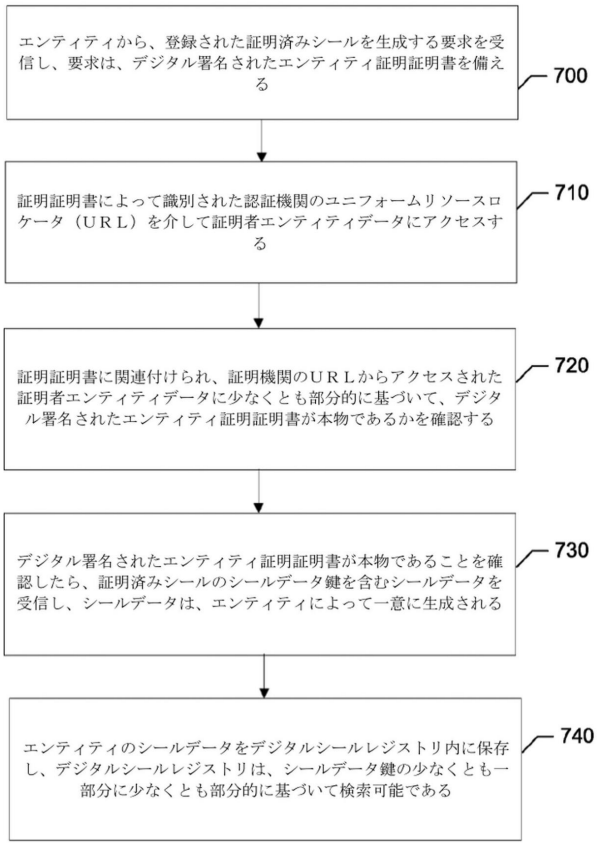
【図６ａ】



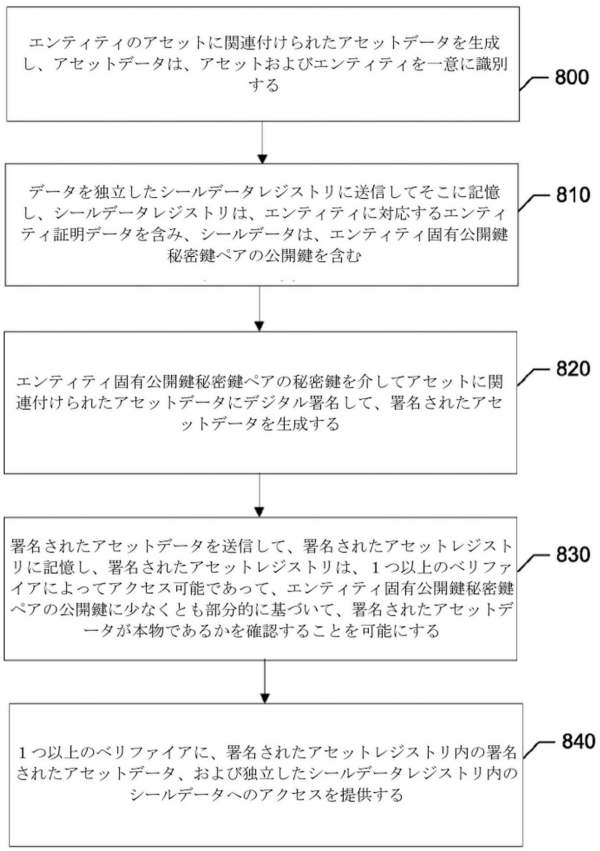
【図６ｂ】


610b データ
612b エントロピー
鍵を用いて暗号化する
620b
640b 暗号化されたデータ
暗号化鍵６２０ｂを用いて復号化する
650b 復号化されたデータ
ハッシュを計算する
622b 暗号化されたデータハッシュ
ハッシュを計算する
622b 暗号化されたデータハッシュ
６５０ｂ 二重暗号化された鍵
ハッシュを用いて復号化する 622b
630b 暗号化された鍵６２０ｃ
ハッシュ６２２ｂを用いて暗号化する
630b 暗号化された鍵 620b
公開鍵を用いて復号化する
６０２ｂ 公開鍵または証明書
620b 暗号化鍵
秘密鍵を用いて暗号化する
620b 暗号化鍵
６００ｂ デジタル署名された暗号化された文書

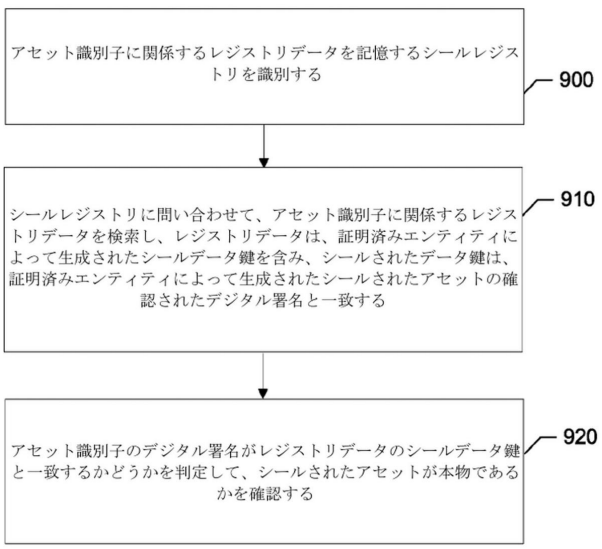
【図７】


エンティティから、登録された証明済みシールを生成する要求を受信し、要求は、デジタル署名されたエンティティ証明証明書を備える
700
証明証明書によって識別された認証機関のユニフォームリソースロケータ（ＵＲＬ）を介して証明者エンティティデータにアクセスする
710
証明証明書に関連付けられ、証明機関のＵＲＬからアクセスされた証明者エンティティデータに少なくとも部分的に基づいて、デジタル署名されたエンティティ証明証明書が本物であるかを確認する
720
デジタル署名されたエンティティ証明証明書が本物であることを確認したら、証明済みシールのシールデータ鍵を含むシールデータを受信し、シールデータは、エンティティによって一意に生成される
730
エンティティのシールデータをデジタルシールレジストリ内に保存し、デジタルシールレジストリは、シールデータ鍵の少なくとも一部分に少なくとも部分的に基づいて検索可能である
740

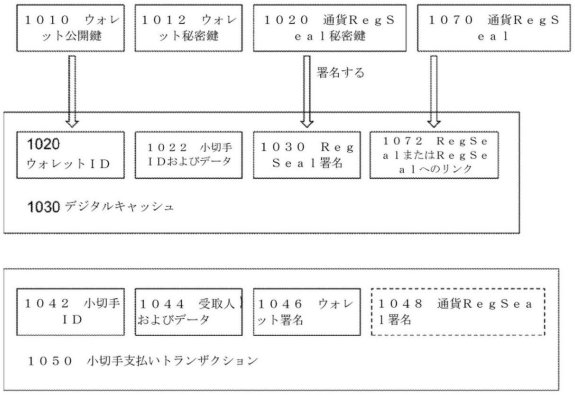
【図８】


エンティティのアセットに関連付けられたアセットデータを生成し、アセットデータは、アセットおよびエンティティを一意に識別する
800
データを独立したシールデータレジストリに送信してそこに記憶し、シールデータレジストリは、エンティティに対応するエンティティ証明データを含み、シールデータは、エンティティ固有公開鍵秘密鍵ペアの公開鍵を含む
810
エンティティ固有公開鍵秘密鍵ペアの秘密鍵を介してアセットに関連付けられたアセットデータにデジタル署名して、署名されたアセットデータを生成する
820
署名されたアセットデータを送信して、署名されたアセットレジストリに記憶し、署名されたアセットレジストリは、１つ以上のベリファイアによってアクセス可能であって、エンティティ固有公開鍵秘密鍵ペアの公開鍵に少なくとも部分的に基づいて、署名されたアセットデータが本物であるかを確認することを可能にする
830
１つ以上のベリファイアに、署名されたアセットレジストリ内の署名されたアセットデータ、および独立したシールデータレジストリ内のシールデータへのアクセスを提供する
840

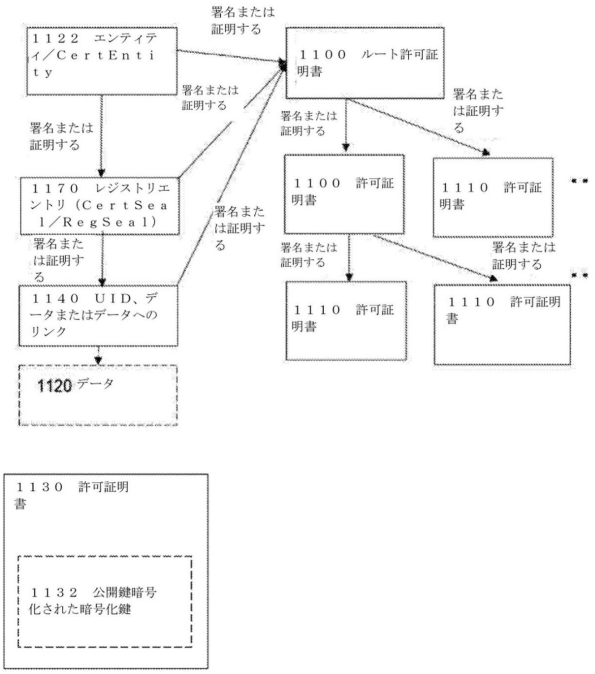
【図９】


アセット識別子に関係するレジストリデータを記憶するシールレジストリを識別する
900
シールレジストリに問い合わせて、アセット識別子に関係するレジストリデータを検索し、レジストリデータは、証明済みエンティティによって生成されたシールデータ鍵を含み、シールされたデータ鍵は、証明済みエンティティによって生成されたシールされたアセットの確認されたデジタル署名と一致する
910
アセット識別子のデジタル署名がレジストリデータのシールデータ鍵と一致するかどうかを判定して、シールされたアセットが本物であるかを確認する
920

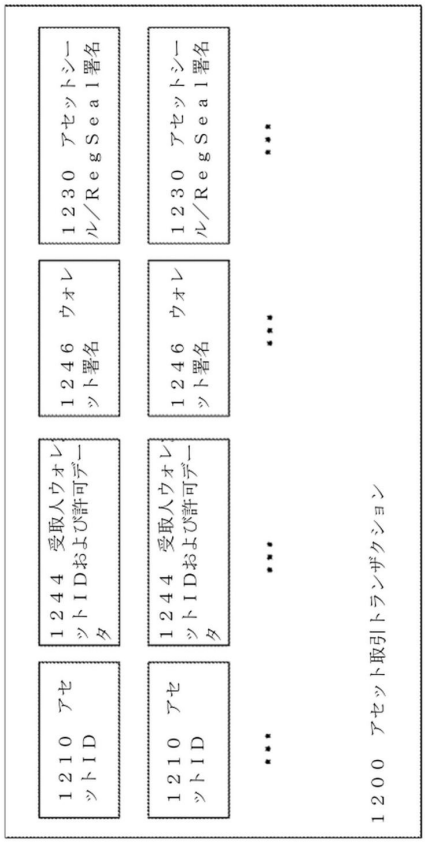
【図１０】



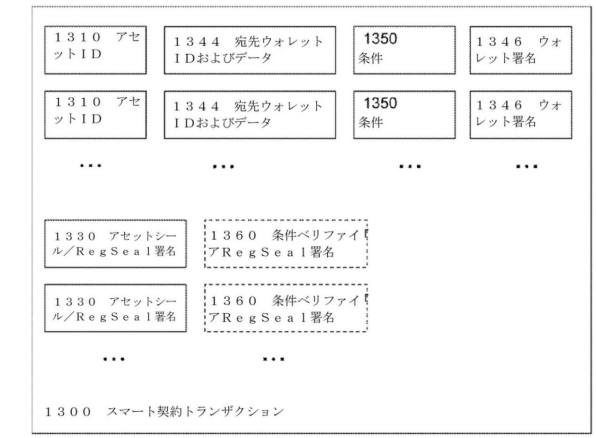
【図１１】



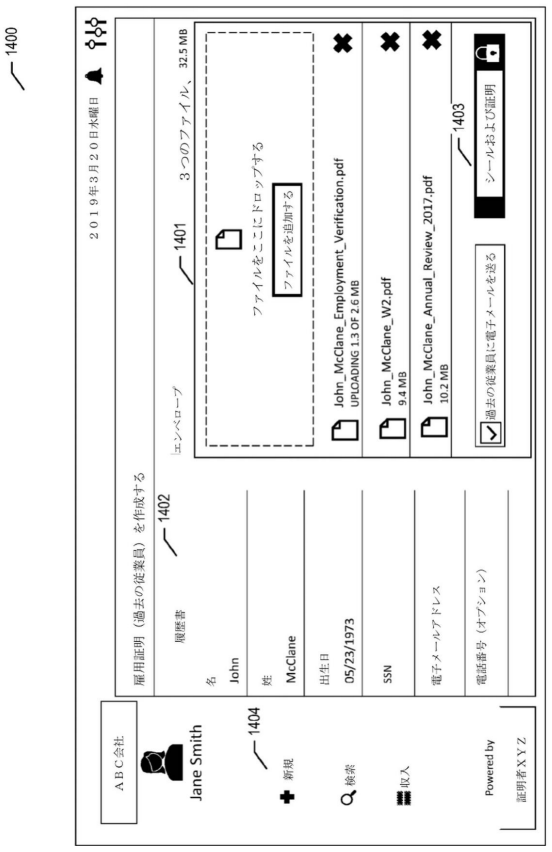
【図１２】



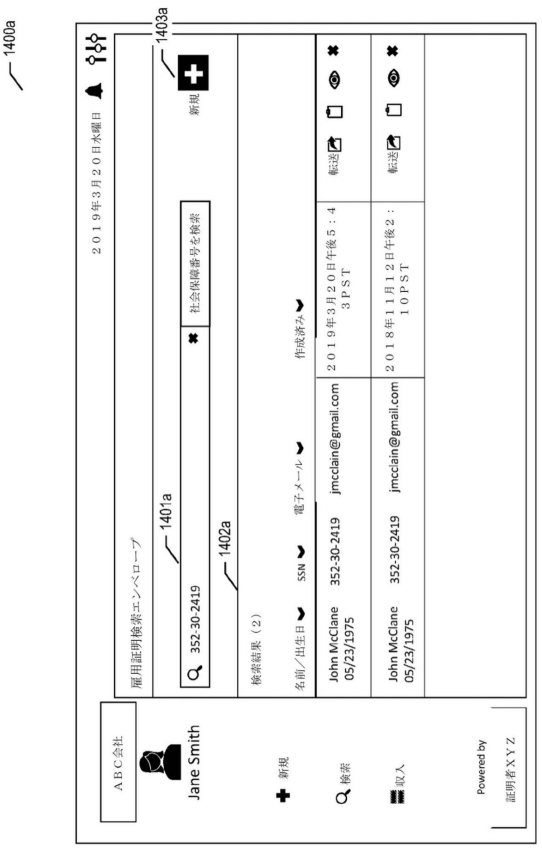
【図１３】



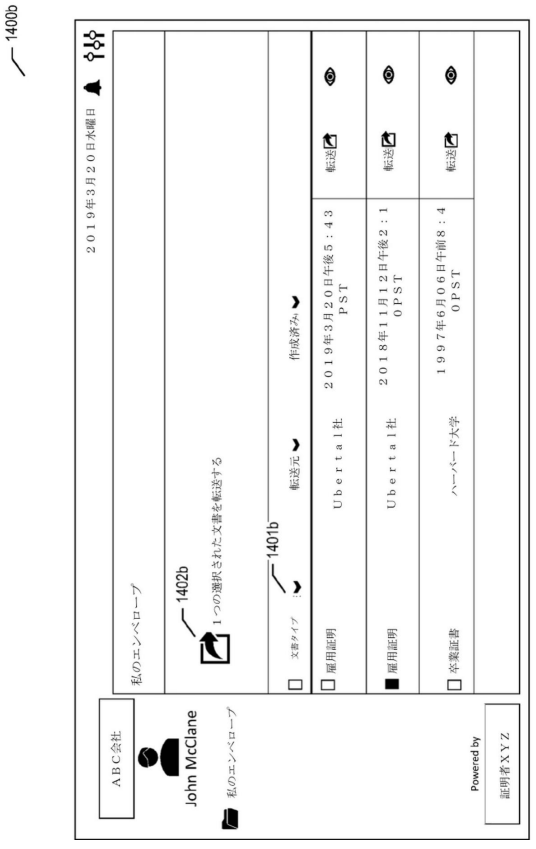
【図１４】



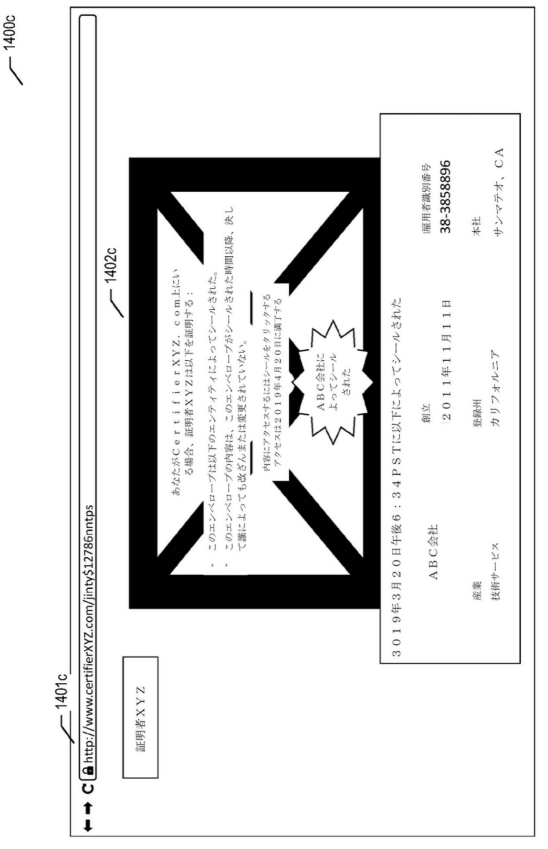
【図１４ａ】



【図１４ｂ】



【図１４ｃ】



フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/744,554
(32)優先日 平成30年10月11日(2018.10.11)
(33)優先権主張国・地域又は機関
米国(US)
前置審査
(74)代理人 100120525
弁理士 近藤 直樹
(74)代理人 100139712
弁理士 那須 威夫
(74)代理人 100122563
弁理士 越柴 絵里
(72)発明者 リ ホンジュン
アメリカ合衆国 カリフォルニア州 ９４４０４ フォスター シティ ヴァスコ ダ ガマ レーン ９７３ オース９ インコーポレイテッド内
(72)発明者 シュ ニング
アメリカ合衆国 カリフォルニア州 ９４４０４ フォスター シティ ヴァスコ ダ ガマ レーン ９７３ オース９ インコーポレイテッド内
審査官 青木 重徳
(56)参考文献 特開２０１１－１６０３６１（ＪＰ，Ａ）
特表２００８－５１５７４１（ＪＰ，Ａ）
特開２０１６－２２００６２（ＪＰ，Ａ）
特表２０１６－５０３９８８（ＪＰ，Ａ）
米国特許出願公開第２０１０／００８２９９４（ＵＳ，Ａ１）
米国特許出願公開第２０１７／０２７９７８５（ＵＳ，Ａ１）
韓国公開特許第１０－２００９－０００７４０（ＫＲ，Ａ）
東角 芳樹 ほか，コンソーシアムチェーンにおける証明書管理に関する一考察，２０１７年暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１７）予稿集 ［ＵＳＢ］，日本，２０１７年 暗号と情報セキュリティシンポジウム実行，2017年01月24日，１Ｆ２－３，ｐ．１－４
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｑ ２０／４０
Ｇ０９Ｃ １／００
Ｇ０６Ｆ ２１／６４