(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7389235号
(P7389235)

(45)発行日　令和5年11月29日(2023.11.29)

(24)登録日　令和5年11月20日(2023.11.20)

(51)国際特許分類

H04L 9/32 (2006.01)	H04L	9/32	200D
H04L 9/08 (2006.01)	H04L	9/32	200B
G06F 21/64 (2013.01)	H04L	9/08	F
	G06F	21/64	

請求項の数　14　（全34頁）

(21)出願番号　特願2022-514565(P2022-514565)
(86)(22)出願日　令和3年3月16日(2021.3.16)
(65)公表番号　特表2022-551389(P2022-551389A)
(43)公表日　令和4年12月9日(2022.12.9)
(86)国際出願番号　PCT/US2021/022495
(87)国際公開番号　WO2022/010548
(87)国際公開日　令和4年1月13日(2022.1.13)
審査請求日　令和4年4月13日(2022.4.13)
(31)優先権主張番号　275947
(32)優先日　令和2年7月9日(2020.7.9)
(33)優先権主張国・地域又は機関
イスラエル(IL)

(73)特許権者　502208397
グーグル エルエルシー
Ｇｏｏｇｌｅ ＬＬＣ
アメリカ合衆国 カリフォルニア州 ９４０４３ マウンテン ビュー アンフィシアター パークウェイ １６００
１６００ Ａｍｐｈｉｔｈｅａｔｒｅ Ｐａｒｋｗａｙ ９４０４３ Ｍｏｕｎｔａｉｎ Ｖｉｅｗ， ＣＡ Ｕ．Ｓ．Ａ．
(74)代理人　100108453
弁理士　村山 靖彦
(74)代理人　100110364
弁理士　実広 信哉
(74)代理人　100133400
弁理士　阿部 達彦

最終頁に続く

(54)【発明の名称】　匿名イベント認証

(57)【特許請求の範囲】

【請求項１】

コンピュータ実装方法であって、

デバイス完全性コンピューティングシステムによって、およびクライアントデバイスから、N個のデバイス完全性要素についての要求を受信するステップであって、

Nは2以上の整数であり、

前記要求は、前記クライアントデバイスについてのデバイスレベル不正検出信号を含み、

前記N個のデバイス完全性要素の各々について、公開鍵データが、(i)前記デバイス完全性要素用のそれぞれの公開鍵、または(ii)前記デバイス完全性要素用の前記それぞれの公開鍵の派生物のうちの少なくとも1つを含む、ステップと、

前記デバイス完全性コンピューティングシステムによって、および前記デバイスレベル不正検出信号に少なくとも基づいて、前記クライアントデバイスの信用性の判断を判定するステップと、

前記N個のデバイス完全性要素の各々について、前記デバイス完全性コンピューティングシステムによって、少なくとも前記デバイス完全性要素についての前記公開鍵データを使用して前記デバイス完全性要素を生成するステップであって、

前記デバイス完全性要素は、前記デバイス完全性要素についての前記公開鍵データを含む内容のセットに基づいて生成されたデジタル署名を含む、ステップと、

前記デバイス完全性コンピューティングシステムによって、前記N個のデバイス完全性

要素を前記クライアントデバイスへ送信するステップと
を含むコンピュータ実装方法。
【請求項２】
各デバイス完全性要素は、前記デバイス完全性要素についての前記内容のセットを含むそれぞれのデバイス完全性トークンを含み、
前記デバイス完全性要素についての前記内容のセットは、信用性の前記判断が判定された時間を示すタイムスタンプ、および前記デバイス完全性要素についての前記公開鍵データを含み、
各デバイス完全性要素を生成するステップは、前記デバイス完全性コンピューティングシステムの秘密鍵を使用して、前記デバイス完全性要素についての前記内容のセットにデジタル署名するステップを含む、請求項1に記載のコンピュータ実装方法。
【請求項３】
前記デバイス完全性要素についての前記内容のセットは、信用性の前記判断をさらに含む、請求項2に記載のコンピュータ実装方法。
【請求項４】
各デバイス完全性要素を生成するステップは、ブラインド署名方式を使用して、前記デバイス完全性要素についての前記公開鍵データのブラインド署名を生成するステップを含み、
前記デバイス完全性要素は前記ブラインド署名である、請求項1に記載のコンピュータ実装方法。
【請求項５】
クライアントデバイスについてのＭ個の信用性レベルに対応するＭ個のブラインド署名検証鍵を公開し、前記Ｍ個のブラインド署名検証鍵に対応するＭ個のそれぞれの署名鍵を保持するステップをさらに含む、請求項4に記載のコンピュータ実装方法。
【請求項６】
信用性の前記判断の前記判定は、前記Ｍ個の信用性レベルから選択された信用性のレベルを前記クライアントデバイスに割り当てることを含む、請求項5に記載のコンピュータ実装方法。
【請求項７】
各デバイス完全性要素についての前記公開鍵データは、前記デバイス完全性要素用の前記公開鍵の前記派生物を含み、
前記デバイス完全性要素用の前記公開鍵の前記派生物は、前記ブラインド署名方式を使用してブラインドされたブラインド化公開鍵を含む、請求項6に記載のコンピュータ実装方法。
【請求項８】
前記デバイス完全性要素用の前記公開鍵の前記派生物は、前記デバイス完全性要素用の前記公開鍵のブラインド化短縮暗号学的ハッシュを含む、請求項7に記載のコンピュータ実装方法。
【請求項９】
前記ブラインド署名方式は非公開検証可能ブラインド署名方式を含む、請求項4から8のいずれか一項に記載のコンピュータ実装方法。
【請求項１０】
前記非公開検証可能ブラインド署名方式はIETF VOPRFブラインド署名方式である、請求項9に記載のコンピュータ実装方法。
【請求項１１】
前記ブラインド署名方式は公開検証可能ブラインド署名方式を含む、請求項4から8のいずれか一項に記載のコンピュータ実装方法。
【請求項１２】
前記公開検証可能ブラインド署名方式はブラインドRSA署名方式である、請求項11に記載のコンピュータ実装方法。

【請求項１３】
1つまたは複数のプロセッサと、
前記1つまたは複数のプロセッサに、請求項1から12のいずれか一項に記載の方法を実践させるように構成されたコンピュータ可読命令を記憶した1つまたは複数のメモリと
を備えるシステム。
【請求項１４】
命令を記憶した非一時的コンピュータ可読記録媒体であって、前記命令は、1つまたは複数のコンピュータによって実行されると、前記1つまたは複数のコンピュータに、請求項1から12のいずれか一項に記載の方法の動作を実施させる、非一時的コンピュータ可読記録媒体。
【発明の詳細な説明】
【背景技術】
【０００１】
クライアントデバイスは、インターネットなどの公衆ネットワークを介して要求および他のデータを送信する。これらの通信は、通信を傍受する関係者および/または通信を受信し、他の関係者へフォワードする媒介など、他の関係者によって改変される場合がある。
【０００２】
クライアントデバイスは、ユーザの承知も認可もなく、不正な要求を送り得るウィルスおよびマルウェアなど、悪意のある攻撃も受ける。さらに、他の関係者が、クライアントデバイスから発したように見えるが、実際には他の関係者のデバイスから来た要求を送るように、クライアントデバイスをエミュレートする場合がある。
【０００３】
様々な認定技法が、不正および悪用を防ぐのに、ならびに公衆ネットワークを介したトランザクションの完全性を保護するのに使われ得る。同時に、これらの認定技法は、秘匿性の懸念事項を示唆し得る。たとえば、クライアントデバイスのユーザは、クライアントデバイスまたはこれらのクライアントデバイスのユーザを追跡するのに使うこともできる情報(不変デバイス識別子など)を共有することを望まない場合があり、データプロバイダは、それらがそのような情報を受信し、または扱うのを防ぐ秘匿性保護規格の下で動作する場合がある。
【発明の概要】
【課題を解決するための手段】
【０００４】
本明細書は、クライアントデバイスから送信された通信の完全性を保護し、同時に、クライアントデバイスまたはそれらのユーザを追跡するのに使われ得る不変デバイス識別子の使用を避けるための認定技法に関する技術について記載する。
【０００５】
概して、本明細書に記載する主題の第1の発明的態様は、コンピュータ実装方法において具現化されてよく、この方法は、デバイス完全性コンピューティングシステムによって、およびクライアントデバイスから、N個のデバイス完全性要素についての要求を受信するステップであって、要求は、クライアントデバイスについてのデバイスレベル不正検出信号を含み、N個のデバイス完全性要素の各々について、公開鍵データが、(i)デバイス完全性要素用のそれぞれの公開鍵、または(ii)デバイス完全性要素用のそれぞれの公開鍵の派生物のうちの少なくとも1つを含む、ステップと、デバイス完全性コンピューティングシステムによって、およびデバイスレベル不正検出信号に少なくとも基づいて、クライアントデバイスの信用性の判断を判定するステップと、N個のデバイス完全性要素の各々について、デバイス完全性コンピューティングシステムによって、少なくともデバイス完全性要素についての公開鍵データを使ってデバイス完全性要素を生成するステップであって、デバイス完全性要素は、デバイス完全性要素についての公開鍵データを含む内容のセットに基づいて生成されたデジタル署名を含む、ステップと、デバイス完全性コンピューティングシステムによって、N個のデバイス完全性要素をクライアントデバイスへ送信するス

テップとを含む。Nは、たとえば、2以上の整数であってよい。本態様の他の実装形態は、コンピュータ記憶デバイス上に符号化された、これらの方法の態様を実施するように構成された、対応する装置、システム、およびコンピュータプログラムを含む。

【０００６】

いくつかの態様では、各デバイス完全性要素は、デバイス完全性要素についての内容のセットを含むそれぞれのデバイス完全性トークンを含み、デバイス完全性要素についての内容のセットは、信用性の判断が判定された時間を示すタイムスタンプ、およびデバイス完全性要素についての公開鍵データを含み、各デバイス完全性要素を生成することは、デバイス完全性コンピューティングシステムの秘密鍵を使って、デバイス完全性要素についての内容のセットにデジタル署名することを含む。デバイス完全性要素についての内容のセットは、信用性の判断をさらに含み得る。

【０００７】

いくつかの態様では、各デバイス完全性要素を生成することは、ブラインド署名方式を使って、デバイス完全性要素についての公開鍵データのブラインド署名を生成することを含み、デバイス完全性要素はブラインド署名である。方法は、クライアントデバイスについてのM個の信用性レベルに対応するM個のブラインド署名検証鍵を公開し、M個の検証鍵に対応するM個のそれぞれの署名鍵を保持するステップをさらに含み得る。

【０００８】

いくつかの態様では、信用性の判断の判定は、M個の信用性レベルから選択された信用性のレベルをクライアントデバイスに割り当てることを含み得る。たとえば、各デバイス完全性要素についての公開鍵データは、デバイス完全性要素用の公開鍵の派生物を含んでよく、デバイス完全性要素用の公開鍵の派生物は、ブラインド署名方式を使ってブラインドされたブラインド化公開鍵を含んでよい。デバイス完全性要素用の公開鍵の派生物は、デバイス完全性要素用の公開鍵のブラインド化短縮暗号学的ハッシュを含み得る。

【０００９】

いくつかの態様では、ブラインド署名方式は、非公開検証可能ブラインド署名方式を含む。たとえば、非公開検証可能ブラインド署名方式は、IETF VOPRFブラインド署名方式であってよい。

【００１０】

他の態様では、ブラインド署名方式は、公開検証可能ブラインド署名方式を含む。たとえば、公開検証可能ブラインド署名方式は、ブラインドRSA署名方式であってよい。

【００１１】

本明細書に記載する主題の別の発明的態様は、クライアントデバイスによって実施される方法で具現化されてよく、この方法は、デバイス完全性コンピューティングシステムへ、匿名証明書についての第1の要求を送信するステップであって、要求は、クライアントデバイスについてのデバイスレベル不正検出信号を含む、ステップと、デバイス完全性コンピューティングシステムから、匿名証明書を受信するステップであって、匿名証明書は、デバイスレベル不正検出信号に少なくとも基づいて、デバイス信用性グループのセットから選択された所与の署名グループに対応し、各デバイス信用性グループは、信用性のそれぞれのカテゴリに対応する、ステップと、(i)第2の要求、および匿名認証トークンの作成の時間を示す認証トークン作成タイムスタンプ(attestation token creation timestamp)を含むデータのセット、ならびに(ii)匿名証明書を用いるグループ署名方式を使って生成された、データのセットのデジタル署名を含む匿名認証トークンを作成するステップと、認証トークンを受信側へ送信するステップとを含む。本態様の他の実装形態は、コンピュータ記憶デバイス上に符号化された、これらの方法の態様を実施するように構成された、対応する装置、システム、およびコンピュータプログラムを含む。

【００１２】

いくつかの態様では、グループ署名方式は、直接匿名認証(DAA)署名方式である。DAA署名方式は、楕円曲線暗号技術(ECC)DAA署名方式であってよい。ECC DAA署名方式は、Barreto-Naehrig曲線を用いるECC DAA署名方式であってよい。

【００１３】
いくつかの態様では、匿名証明書は、クライアントデバイスが所与の署名グループに取消し不能に割り当てられていることを示す取消し不能匿名証明書である。
【００１４】
いくつかの態様では、デバイス信用性グループのセットは少なくとも、第1の程度の信用性を有するデバイスをメンバーとして含む第1の信用性グループと、第1の程度の信用性よりも低い第2の程度の信用性を有するデバイスをメンバーとして含む第2の信用性グループとを含み、所与のグループは、第1のグループまたは第2の署名グループのうちの1つである。第1および第2の信用性グループは、デバイス完全性コンピューティングシステムによって公開された、対応する第1および第2のグループ公開鍵を有し得る。
【００１５】
いくつかの態様では、方法は、匿名証明書を、クライアントデバイス上のセキュアな秘密鍵ストアに記憶するステップをさらに含む。
【００１６】
いくつかの態様では、トークン作成タイムスタンプは、約1ミリ秒未満または約1マイクロ秒未満の時間分解能を有する。
【００１７】
いくつかの態様では、方法は、認証トークン量限度を示す情報を受信するステップと、作成するのに先立って、作成が認証トークン量限度を超えないことを検証するステップとをさらに含む。認証トークン量限度は、クライアントデバイスから、選択された宛先ドメインへ、選択された時間枠内に送られるのに適格な匿名トークンの数に対する限度であってよく、または認証トークン量限度は、クライアントデバイス上の1つもしくは複数の選択されたアプリケーションから、選択された宛先ドメインへ、選択された時間枠内に送られるのに適格な匿名トークンの数に対する限度であってよく、または認証トークン量限度は、クライアントデバイスから、選択された宛先ドメイン内の選択されたエンドポイントへ、選択された時間枠内に送られるのに適格な匿名トークンの数に対する限度であってよく、または認証トークン量限度は、クライアントデバイス上の1つもしくは複数の選択されたアプリケーションから、選択された宛先ドメイン内の選択されたエンドポイントへ、選択された時間枠内に送られるのに適格な匿名トークンの数に対する限度であってよく、またはそれらのどの組合せであってもよい。
【００１８】
本明細書において説明する主題は、以下の利点のうちの1つまたは複数を実現するために特定の実施形態において実装され得る。
【００１９】
クライアントデバイスからデータを送信するのに認証トークンを使うと、クライアントデバイスと他のエンティティのコンピュータまたは他のデバイスとの間にセキュアな通信チャネルが提供される。認証トークンとともに、認証トークンに含まれるデータのデジタル署名を含めると、エンティティは、認証トークンが作成された後、認証トークン中のデータが変更されなかったことを検証することが可能になる。さらに、トークン作成時間を認証トークンに含めると、受信側が、要求が新しいか、それともリプレイ攻撃の一部であり得るかを判定することが可能になる。
【００２０】
認証トークンは、認証トークンを送信したクライアントデバイスの完全性を示すデバイス完全性トークンも含んでよく、これは、たとえば、エミュレータまたは損なわれたデバイスからではなく、信用できるクライアントデバイスからデータが来たことを認証トークンの受信側が検証することを可能にする。デバイス完全性トークンは、信用できるデバイスアナライザ(たとえば、サードパーティデバイスアナライザ)によって生成され、デジタル署名されてよく、そうすることによって、信用できるデバイスアナライザによってクライアントデバイスが評価されたこと、およびデバイス完全性トークン中のデータが、信用できるデバイスアナライザによる作成の後に修正されていないことを、認証トークンの受

信側が検証することができる。

【００２１】

認証トークンは、クライアントデバイスから送信された通信の完全性を保護するが、認証トークンの使用に関連付けられた潜在的秘匿性問題が存在する。第1の秘匿性問題は、複数の認証トークン内での同じデバイス完全性トークンの再利用が、同じクライアントデバイスによって送信された複数の要求を、認証トークン受信側が相関させ、相関に基づいてユーザデータを集約することを潜在的に可能にし得ることである。本文書に記載する技法は、クライアントデバイスの一意の公開鍵を各々が含む、複数のデバイス完全性トークンを使うことによって、そのような相関に対して秘匿性を強化することができる。たとえば、クライアントデバイスは、N個の公開/秘密鍵ペアのバッチを生成し、次いで、N個の公開鍵を、N個の対応するデバイス完全性トークンのバッチを受信するためにサードパーティデバイスアナライザへ送ればよい。次いで、クライアントデバイスは、たとえば、新しいデバイス完全性トークンを各要求のために使ってよく、もしくはクライアントデバイスは、同じデバイス完全性トークンを、一定の時間間隔内のすべての要求のために使ってよく、もしくはクライアントデバイスは、同じデバイス完全性トークンを、クライアントデバイス上の同じアプリケーションから発したすべての要求のために使ってよく、またはそれらの何らかの組合せであってよい。各公開鍵の使用を制限すると、公開鍵に基づいて受信側が相関し得る要求の量が制限される。このバッチ手法を使うと、また、より少ない要求を処理させることによって、デバイスアナライザに対する負担が削減され、ネットワーク帯域幅の消費が削減され、場合によっては、デバイス完全性トークンが必要とされた度にデバイス完全性トークンについての要求をクライアントデバイスが送った場合にもち込まれる、デバイス完全性トークンを含む要求を送信するときの、クライアントデバイスにおける待ち時間が削減される。

【００２２】

第2の秘匿性問題は、クライアントデバイスの不変公開鍵をデバイスアナライザと共有することで、デバイスアナライザがクライアントデバイスを追跡することを潜在的に可能にし得ることである。たとえば、デバイスアナライザと共謀することによって、複数の別個の認証トークンの受信側は、デバイスアナライザがそれらの認証トークンを同じデバイスからの同じバッチ要求の中で受信したことを知ることができ、したがって、そのような認証トークンの受信側は、同じクライアントデバイスによって送信された複数の要求を相関させ、相関に基づいてユーザデータを集約することができる。本文書に記載する技法は、公開鍵の未加工値ではなく、公開鍵のブラインド化バージョンをデバイスアナライザへ送ることによって、そのような追跡に対して秘匿性を強化することができる。たとえば、クライアントデバイスは、N個の公開-秘密鍵ペアのバッチを生成し、N個の公開鍵(または公開鍵の暗号ハッシュ)をブラインドし、次いで、N個のブラインド化鍵をデバイスアナライザへ送ることができ、サードパーティデバイスアナライザは、クライアントデバイス公開鍵の未加工値を一度も受信することなく、N個の対応するブラインド署名のバッチを戻す。

【００２３】

本開示のさらなる態様は、公開鍵署名方式ではなくグループ署名方式を使うことによって、信用できるデバイスアナライザによる、および認証トークン受信側による両方の追跡に対して秘匿性を強化するという利点を提供し得る。たとえば、サードパーティデバイスアナライザは、クライアントデバイスの信用性のレベルに対応する署名グループにクライアントデバイスを割り当て、署名グループ用の匿名証明書をクライアントデバイスに与えればよい。次いで、クライアントは、匿名証明書を用いるグループ署名方式を使って各認証トークンに署名すればよく、認証トークン受信側は、サードパーティデバイスアナライザによって公開される公開グループ鍵を使って匿名署名を確認すればよい。この手法を使うと、クライアントデバイスのリソースに対して、多くの公開/秘密鍵ペアを作成するという負担が軽減され、デバイスアナライザのリソースに対して、各公開鍵用のデバイス完全性トークンを作成するという負担が軽減される。こうすることにより、他の機能を実施す

るためにそれぞれのリソースが解放され、デバイスアナライザは、解放されたリソースを使って、より多くのクライアントデバイスをより短い時間期間で評価することが可能になる。したがって、グループ署名方式の使用は、公開/秘密鍵ペアの生成が削減されるので、より効率的なプロセスを提供する。

【００２４】

前述の主題の様々な特徴および利点は、以下で、図面に関して説明される。追加の特徴および利点は、本明細書で説明する主題および特許請求の範囲から明らかである。

【図面の簡単な説明】

【００２５】

【図１】デジタルコンポーネントシステムがデジタルコンポーネントを配信する環境のブロック図である。

【図２】N個のデバイス完全性トークンのバッチを要求し、受信するための例示的プロセスを示す流れ図である。

【図３】認証トークンを送り、受信し、確認するための例示的プロセスを示す流れ図である。

【図４】N個のブラインド署名されたデバイス完全性トークンのバッチを要求し、受信するための例示的プロセスを示す流れ図である。

【図５】ブラインド署名された認証トークンを送り、受信し、確認するための例示的プロセスを示す流れ図である。

【図６】署名グループ用の匿名秘密鍵を要求するための例示的プロセスを示す流れ図である。

【図７】匿名で署名された認証トークンを送り、受信し、確認するための例示的プロセスを示す流れ図である。

【図８】公開されたトークン量限度に従うように認証トークンをスロットリングするための例示的プロセスを示す流れ図である。

【図９】例示的コンピュータシステムのブロック図である。

【発明を実施するための形態】

【００２６】

様々な図面における同様の参照番号および名称は、同様の要素を示す。

【００２７】

概して、本明細書に記載するシステムおよび技法は、クライアントデバイスと、デジタルコンポーネントを、デジタルコンポーネント配信システムによる配信のために作成し、提供する、コンテンツパブリッシャー、デジタルコンポーネント配信システム、およびデジタルコンポーネントプロバイダなど、他のエンティティとの間のセキュアな通信チャネルを提供することができる。クライアントデバイスは、要求およびネットワークを介した他のデータ送信とともに、他のエンティティによって、要求の完全性およびクライアントデバイスの完全性を確認するのに使われる認証トークンを提供することができる。要求は、たとえば、ユーザのデータを管理するための(たとえば、ユーザ関連データを消去するための)要求、コンテンツに対する要求、および/または他のコンテンツとともに提示するためのデジタルコンポーネントに対する要求を含み得る。認証トークンを使って通信チャネルをセキュアにすることにより、不正なユーザは、ユーザデータを変更し、消去し、または場合によってはユーザデータにアクセスすることも、要求の内容を変更することも、たとえば、デジタルコンポーネント配信システムおよび/もしくはプロバイダを欺くために、新しい要求を作成することも確実にできなくなる。

【００２８】

いくつかの手法では、認証トークンは、クライアントデバイスの秘密鍵を使ってデジタル署名され得る。クライアントデバイスは、秘密鍵を内密に維持することができる。認証トークンは、とりわけ、秘密鍵に対応する公開鍵、ペイロード、およびデバイス完全性トークンを含み得る。デバイス完全性トークンは、信用できるデバイス完全性システム、たとえば、クライアントデバイスのユーザおよび認証トークンの受信側とは異なるエンティ

ティによって維持されるサードパーティデバイス完全性システムによって判定される、クライアントデバイスの完全性のレベルを示す判断を含み得る。デバイス完全性トークンは、デバイス完全性トークンをクライアントデバイスにバインドするための、クライアントデバイスの公開鍵(または公開鍵の暗号ハッシュ)も含み得る。

【００２９】

デバイス完全性トークンは、デバイス完全性システムが機密にしておく秘密鍵を使って、デバイス完全性システムによってデジタル署名され得る。この秘密鍵に対応する公開鍵は受信側に与えられてよく、そうすることによって、受信側は、クライアントデバイスがデバイス完全性システムによって、たとえば、公開鍵を使ってデバイス完全性トークンのデジタル署名を検証することによって評価されたと信用し得る。2つの鍵ペアを使うというこの組合せは、受信側がクライアントデバイスの完全性と、クライアントデバイスから受信された通信の完全性とを確認することを可能にするセキュアな通信チャネルを提供し、デバイス完全性トークンをクライアントデバイスにバインドし、そうすることによって、他のデバイスは、それらの完全性を偽造するためにデバイス完全性トークンを使うことができない。

【００３０】

いくつかの手法では、デバイス完全性システムは、デバイス完全性トークンに含めるための、公開鍵の未加工データを受信しない。そうではなく、クライアントデバイスは、ブラインド署名方式を使って公開鍵またはその派生物をブラインドすることによって、ブラインド化公開鍵または公開鍵のブラインド化派生物(たとえば、公開鍵のブラインド化短縮暗号ハッシュ)を送ればよい。ブラインド署名方式を用いて、デバイス完全性システムは、クライアントデバイスの公開鍵の未加工値を受信せずに、クライアントデバイスの完全性を証明することができ、公開鍵による潜在的追跡の危険性を削減することによってクライアントデバイスまたはユーザの秘匿性を強化する。デバイス完全性システムは、受信側がブラインド署名を検証するのに使うことができるブラインド署名検証鍵を公開してよい。

【００３１】

他の手法では、グループ署名方式は、グループマネージャとしてのデバイス完全性システムとともに使われ得る。たとえば、デバイス完全性システムは、M個の信用性グループ用のM個のグループ検証鍵を公開し、M個の信用性グループのうちの1つにクライアントデバイスを割り当て、クライアントデバイスへ匿名証明書を送達することができる。クライアントデバイスは、匿名証明書を使って認証トークンに匿名で署名することができ、これらの匿名署名は、公開されたグループ検証鍵を使って受信側によって検証され得る。グループ署名方式を用いると、デバイス完全性システムも認証トークンの受信側も、クライアントデバイスの公開鍵の未加工値を受信する必要がなく、公開鍵による潜在的追跡の危険性を削減することによって、クライアントデバイスまたはユーザの秘匿性をさらに強化する。

【００３２】

図1は、デジタルコンポーネントシステム150がデジタルコンポーネント129を配信する環境100のブロック図である。例示的環境100は、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)、インターネット、モバイルネットワーク、またはそれらの組合せなどのデータ通信ネットワーク105を含む。ネットワーク105は、クライアントデバイス110、パブリッシャー130、ウェブサイト140、デジタルコンポーネント配信システム150、およびデバイス完全性システム170(デバイス完全性コンピューティングシステムとも呼ばれ得る)を接続する。例示的環境100は、多くの異なるクライアントデバイス110、パブリッシャー130、ウェブサイト140、デジタルコンポーネント配信システム150、およびデバイス完全性システム170を含み得る。

【００３３】

ウェブサイト140は、ドメイン名に関連付けられ、1つまたは複数のサーバによってホストされる1つまたは複数のリソース145である。例示的ウェブサイトは、テキスト、画像、マルチメディアコンテンツ、およびスクリプトなどのプログラミング要素を含み得る

、HTMLでフォーマットされたウェブページの集合である。各ウェブサイト140は、ウェブサイト140を制御、管理、および/または所有するエンティティであるパブリッシャー130によって維持される。

【００３４】

リソース145は、ネットワーク105を介して提供することができる任意のデータである。リソース145は、リソース145に関連付けられたリソースアドレス、たとえばユニバーサルリソースロケータ(URL)によって識別される。リソースには、ほんのいくつかの例を挙げれば、HTMLページ、ワードプロセッシングドキュメント、およびポータブルドキュメントフォーマット(PDF)ドキュメント、画像、ビデオ、およびフィードソースが含まれる。リソースは、埋め込まれた情報(ハイパーリンク内のメタ情報など)および/または埋め込まれた命令(スクリプトなど)を含み得る、単語、語句、画像、および音声などのコンテンツを含むことができる。

【００３５】

クライアントデバイス110は、ネットワーク105を介して通信することが可能な電子デバイスである。例示的なクライアントデバイス110は、パーソナルコンピュータ、モバイル通信デバイス、たとえば、スマートフォン、デジタルメディアプレーヤ、スマートスピーカー、着用可能デバイス(たとえば、スマートウォッチ)、およびネットワーク105を介してデータを送り、受信することができる他のデバイスを含む。クライアントデバイス110は、一般に、ネットワーク105を介してデータの送付および受信を円滑にする、ウェブブラウザおよび/またはネイティブアプリケーションなどのアプリケーション111を含む。ネイティブアプリケーションは、特定のプラットフォームまたは特定のデバイスに対して開発されたアプリケーションである。パブリッシャー130は、固有アプリケーションを開発し、クライアントデバイス110に提供することができる。

【００３６】

いくつかのリソース145、アプリケーションページ、または他のアプリケーションコンテンツは、デジタルコンポーネントにリソース145またはアプリケーションページを提示するためのデジタルコンポーネントスロットを含むことができる。本文書全体を通して使われる限り、「デジタルコンポーネント」というフレーズは、デジタルコンテンツまたはデジタル情報の個別単位(たとえば、ビデオクリップ、オーディオクリップ、マルチメディアクリップ、画像、テキスト、または別のコンテンツ単位)を指す。デジタルコンポーネント129は、単一のファイルとして、またはファイルの集合として物理メモリデバイスに電子的に記憶することができ、デジタルコンポーネントは、ビデオファイル、オーディオファイル、マルチメディアファイル、画像ファイル、またはテキストファイルの形をとり、広告情報を含むことができ、したがって、広告は、デジタルコンポーネントの一種である。たとえば、デジタルコンポーネント129は、アプリケーション111によって提示されるウェブページ、リソース、またはアプリケーションページのコンテンツを補足することが意図されるコンテンツであってよい。より具体的には、デジタルコンポーネント129は、リソースコンテンツに関連するデジタルコンテンツを含み得る(たとえば、デジタルコンポーネントは、ウェブページコンテンツと同じトピック、または関連するトピックに関連し得る)。デジタルコンポーネント配信システム150によるデジタルコンポーネントの提供により、したがって、ウェブページコンテンツを補足し、概して強化することができる。

【００３７】

アプリケーション111が、1つまたは複数のデジタルコンポーネントスロットを含むリソース145またはアプリケーションコンテンツをロードすると、ウェブブラウザであってよいアプリケーション111は、デジタルコンポーネント配信システム150に対して、各スロット用のデジタルコンポーネント129を要求することができる。デジタルコンポーネント配信システム150は、デジタルコンポーネントプロバイダ160に対してデジタルコンポーネントを要求することができる。デジタルコンポーネントプロバイダ160は、デジタルコンポーネントを、リソース145および/または他のコンテンツとの表示のために提供するエンティティである。例示的デジタルコンポーネントプロバイダは、広告を提供する広告

主である。
【００３８】
いくつかの場合には、デジタルコンポーネント配信システム150は、1つまたは複数のデジタルコンポーネントパートナー152に対してデジタルコンポーネントを要求することもできる。デジタルコンポーネントパートナー152は、デジタルコンポーネント要求に応答して、デジタルコンポーネントプロバイダ160の代わりにデジタルコンポーネントを選択するエンティティである。
【００３９】
デジタルコンポーネント配信システム150は、様々な基準に基づいて、各デジタルコンポーネントスロット用のデジタルコンポーネントを選択してよい。たとえば、デジタルコンポーネント配信システム150は、デジタルコンポーネントプロバイダ160および/またはデジタルコンポーネントパートナー152から受信されたデジタルコンポーネントから、リソース145または他のアプリケーションコンテンツとの関連性、デジタルコンポーネントの性能(たとえば、ユーザがデジタルコンポーネントと対話する割合)などに基づいて、デジタルコンポーネントを選択することができる。デジタルコンポーネント配信システム150は次いで、選択されたデジタルコンポーネントを、リソース145または他のアプリケーションコンテンツとの表示のためにクライアントデバイス110に提供すればよい。デジタルコンポーネント配信システム150は、選択されたデジタルコンポーネント129を、クライアントデバイス110上で動作するアプリケーション111による表示のために、1つまたは複数のクライアントデバイス110へ送信してよい。
【００４０】
アプリケーション111がネットワーク105を介して要求120を送るとき、アプリケーション111は、要求とともに認証トークン122を送ることができる。たとえば、アプリケーション111が、デジタルコンポーネント配信システム150へデジタルコンポーネント要求を送る場合、この要求は、認証トークン122を含み得る。同様に、アプリケーション111が別のエンティティへ(たとえば、パブリッシャー130、デジタルコンポーネント配信システム150、デジタルコンポーネントパートナー152、またはデジタルコンポーネントプロバイダ160へ)、そのエンティティによって記憶されるデータを管理する、たとえば消去するために要求を送る場合、この要求は、認証トークン122を含み得る。
【００４１】
いくつかの実装形態では、アプリケーション111は、指定されたタイプの要求のための認証トークン122を送るように構成される。たとえば、認証トークン122を送る各アプリケーション111は、アプリケーション111に、認証トークン122を生成させ、かつ/または送らせるソフトウェア開発キット(SDK)またはアプリケーションプログラミングインターフェース(API)を含み得る。SDKは、要求のセット、たとえば、ユーザデータを管理し、デジタルコンポーネントを要求するための、認証トークン122が含まれるべき要求などを指定することができる。他のタイプの要求、たとえば、ニュースウェブページを要求することは、認証トークン122を求めない場合がある。
【００４２】
クライアントデバイス110は、アプリケーション111用の認証トークンを生成する、信用できるプログラム114も含むことができる。信用できるプログラム114は、偽造が困難な信頼できるソースからの信用できるコードを含み得る。たとえば、信用できるプログラム114は、オペレーティングシステム、オペレーティングシステムの一部分、ウェブブラウザなどであってよい。概して、信用できるプログラム114は、侵入が困難であり、犯罪者が信用できるプログラム114を改ざんするために拡張することが必要になる時間および労力の量が極めて高い。加えて、信用できるプログラム114は信頼できるソースによって提供され維持されるため、高まるいかなる脆弱性もソースによって対処され得る。信用できるプログラムは侵入が困難であるため、そのような信用できるプログラムをこのように使用することは、クライアントデバイスにおけるセキュリティを増大する技術的利点を提供する。加えて、信用できるプログラムは信頼できるソースによって維持されるため、こ

のプログラムは信用できるプログラム内の脆弱性を低減する利点を提供する。

【００４３】

信用できるプログラム114は、クライアントデバイス110に対して局所的であってよい。たとえば、信用できるプログラム114は、クライアントデバイス110のオペレーティングシステムのデバイスドライバであってよい。いくつかの実装形態では、信用できるプログラム114は、クライアントデバイス110に対して完全に局所的に動作し、ユーザ情報を送信する必要を低減する。いくつかの実装形態では、信用できるプログラム114は、クライアントデバイス110に対して局所的に、およびネットワーク105などのネットワークを介して、動作し得る。たとえば、信用できるプログラム114は、ユーザデバイス110上にインストールされ、ネットワーク105を介して情報を送信および受信するウェブブラウザであってよい。

【００４４】

信用できるプログラム114は、以下でより詳しく説明するように、暗号化鍵(たとえば、公開/秘密鍵ペア)を生成し、暗号化鍵をセキュアなストレージ115(たとえば、セキュアなキャッシュ)に記憶し、デバイス完全性トークンをセキュアなストレージ115に記憶し、認証トークンを生成し、暗号鍵もしくはその派生物のブラインド署名を生成し、かつ/または証明書をフェッチし、記憶することができる。いくつかの実装形態では、信用できるプログラム114は、データを、デバイス完全性システム170へ送り、そこから受信するために、デバイス完全性クライアントと対話する。いくつかの実装形態では、信用できるプログラム114は、指定されたタイプの要求、たとえば、ユーザ秘匿性設定を変更するための要求のセットの各々のための認証トークン122を生成するように構成される。

【００４５】

認証トークン122は、エンティティによって、要求の完全性およびクライアントデバイス110の完全性を確認するのに使われる。たとえば、ユーザが、他のエンティティによって記憶されている自分のデータを管理することを可能にすることにより、悪意のあるユーザが他のユーザのデータを管理し、かつ/または盗むことを試みる可能性を広げる場合がある。デジタルコンポーネントに対して、いくつかの悪意のあるエンティティが、要求を実際よりも価値があるように見えるようにするために、デジタルコンポーネント要求のパラメータを偽造しようと、たとえば、デジタルコンポーネントとともに与えられる予定の異なるリソースを指定しようと、および/またはデジタルコンポーネントが提示される予定の異なるユーザを指定しようと試みる場合がある。さらに、何人かの悪意のある関係者が、無法な目的のために他者のクライアントデバイスをエミュレートしようと試みる場合がある。

【００４６】

認証トークン122は、他者が要求120を改変するのを防ぐとともに、要求120が、確認されたクライアントデバイス110から来たことを保証する、媒介を通した、クライアントデバイス110と他のエンティティのコンピュータまたは他のデバイスとの間のセキュアな通信チャネルを提供する。

【００４７】

信用できるプログラム114は、異なる形を有する、または異なる内容を含む、異なるタイプの認証トークン122を生成することができる。いくつかの実装形態では、認証トークン122は、クライアントデバイス110の公開鍵113と、認証トークン122が作成される時間を示すトークン作成時間と、ペイロードデータと、クライアントデバイス110から受信されたデータを使って、デバイス完全性システム170によって、または信用できるプログラム114によって生成されるデバイス完全性トークンとを含む内容のセットを含む。認証トークン122は、認証トークン122および内容のセットに含まれる公開鍵113に対応する秘密鍵112を使って、信用できるプログラム114によって生成されたデジタル署名も含み得る。つまり、信用できるプログラム114は、秘密鍵112を使って内容のセットにデジタル署名し、得られたデジタル署名を内容のセットとともに認証トークン122に含めることができる。

【００４８】
いくつかの実装形態では、認証トークン122は、ペイロードデータと、認証トークン122が作成される時間を示す認証トークン作成時間と、内容のセットのデジタル署名とを含む内容のセットを含む。この例では、信用できるプログラム114は、グループ署名方式と、デバイス完全性システム170によってクライアントデバイス110に対して発行された証明書とを使って、デジタル署名を生成することができる。
【００４９】
いずれの例でも、クライアントデバイス110は、デジタルコンポーネント配信システム150または他の受信側へ送られる要求120に、認証トークン122を含めることができる。認証トークン122の受信側は、認証トークン122および/または認証トークン122に含まれるデバイス完全性トークン(適切な場合)を確認しようと試み得る。認証トークン122の確認が成功した場合、受信側は、クライアントデバイス110が信用できるデバイスであるかどうかを判定し、それに応じて要求を処理すればよい。認証トークン122の確認が成功しなかった場合、受信側は、たとえば、要求120に応答することもそれに応答してデータを変更することもなく、要求120を無視または消去すればよい。認証トークン122を含む要求を生成し、認証トークンを確認するための例示的プロセスを、図2～図8に示し、以下で説明する。
【００５０】
認証トークン作成時間は、認証トークン122が作成された時間を示す。信用できるプログラム114は、信用できるプログラム114が認証トークンを作成する作成時間を記録し得る。この認証トークン作成時間は、高分解能タイムスタンプ(たとえば、秒まで、ミリ秒まで、またはマイクロ秒まで正確)であってよい。認証トークン作成時間は、認証トークン122を含む要求120が新しいまたは最近の要求であるかどうかを判定するのに使うことができる。たとえば、認証トークン122を受信するエンティティは、トークン作成時間を、現在時刻または認証トークン122が受信された時間と比較すればよい。2つの時間の間の差が閾を超える場合、以下でより詳しく説明するように、エンティティは、要求が新しくないか、または無効であると判定してよい。
【００５１】
認証トークン作成時間は、リプレイ攻撃を検出するのに使うこともできる。たとえば、同じ認証トークン作成時間を含む同じデータのセットを有する複数の要求が受信される場合、要求を受信するエンティティは、要求が複製である、および/または要求がリプレイ攻撃の一部であると判定してよい。
【００５２】
認証トークン作成時間は、他のデータとの組合せで、要求120についてのトランザクション識別子としても働き得る。たとえば、トランザクション識別子は、認証トークン122の認証トークン作成時間と、認証トークン122が公開鍵113を含む実装形態では認証トークン122の公開鍵113のうちの2つ以上の組合せであってよい。トランザクション識別子は、複数のチャネルから受信された同じ要求の複数のバージョンを複製解除するのに使うことができる。たとえば、デジタルコンポーネントプロバイダ160-3は、デジタルコンポーネント配信システム150とデジタルコンポーネントパートナー152の両方から同じ要求を受信し得る。この例では、トランザクション識別子は、認証トークン122のトークン作成時間および認証トークン122の公開鍵113に基づき得る。デジタルコンポーネントプロバイダ160-3は、2つ以上の要求の中の2つのデータを比較して、要求が複製であるかどうかを判定すればよい。
【００５３】
ペイロードは、個々の要求120についてのデータを含み得る。たとえば、要求120がデジタルコンポーネントについてである場合、ペイロードは、デジタルコンポーネントを選択するのに使うことができるデータを含み得る。このペイロードは、デジタルコンポーネントスロット(またはリソース145についてのURL)、リソース145についての情報(たとえば、リソースのトピック)、デジタルコンポーネントスロットについての情報(たとえば、

スロットの数、スロットのタイプ、スロットのサイズなど)、ユーザがこの特徴を可能にしている場合はクライアントデバイス110についての情報(たとえば、デバイスのタイプ、デバイスのIPアドレス、クライアントデバイス110の地理的ロケーション)を有するリソース145、および/または他の適切な情報を含んでもよい。

【００５４】

要求120が、パブリッシャー130、デジタルコンポーネント配信システム150、デジタルコンポーネントパートナー152、デジタルコンポーネントプロバイダ160、または別のエンティティにおいてユーザのデータを管理するためのものである場合、要求120は、要求される変更を指定するデータを含み得る。たとえば、ユーザが、デジタルコンポーネントプロバイダ160-2からユーザのデータをすべて削除することを選択した場合、ペイロードは、このデータ削除と、デジタルコンポーネントプロバイダ160-2とを指定するデータ(たとえば、デジタルコンポーネントプロバイダ160-2についての識別子またはネットワークアドレス)を含むことになる。

【００５５】

デバイス完全性システム170は、クライアントデバイス110から、たとえば、信用できるプログラム114から受信されたデバイスレベル不正検出信号を評価し、デバイスレベル不正検出信号に基づいて、クライアントデバイス110の信用性(または完全性)のレベルを判定する。デバイスレベル不正検出信号は、クライアントデバイスが損なわれているかどうか、またはクライアントデバイスが通常のクライアントデバイス、もしくはエミュレートされたクライアントデバイスとして動作しているかを判定するために使用され得る、クライアントデバイスの動作特性またはメトリックを表すデータを含み得る。いくつかの動作特性およびメトリックは、エミュレータと比べて、真のクライアントデバイスでは異なることがよくある。いくつかの実装形態では、デバイスレベル不正検出信号は、信用トークンを要求しているアプリケーション111の動作特性およびメトリックを含むアプリケーションレベルの不正検出信号を含む。信用できるプログラム114は、これらのデバイスレベル不正検出信号を収集し、これらの信号を信用トークンに対する要求内に含めることができる。

【００５６】

デバイス完全性システム170は、クライアントデバイス110の信用性(または完全性)のレベルを示す判断を発行することができる。受信側は、判断を含む要求120を信用するべきかどうかを判定するのに、判断を使う。たとえば、クライアントデバイス110は信用性がないことを判断が示す場合、受信側は要求を無視し、たとえば、要求に応答しなくてよい。

【００５７】

上述したように、いくつかの手法では、デバイス秘密/公開鍵ペア(ならびにデバイス公開鍵に関連付けられたデバイス完全性トークン)は、クライアントデバイスまたはユーザの秘匿性を、認証トークン受信側による追跡に対して強化するために、複数の認証トークンにわたって変えられてよい。たとえば、クライアントデバイスは、秘密/公開鍵ペアのバッチを生成し、デバイス完全性トークンの対応するバッチをデバイス完全性サーバから取り出してよく、そうすることによって、デバイス完全性トークンの再利用が減らされるか、またはなくされる。このバッチプロセスの説明のための例を、図2に示す。

【００５８】

この例では、クライアントデバイス200が、Nという個数の公開/秘密鍵ペアを作成する(201)。たとえば、クライアントデバイス200の信用できるプログラムが、公開/秘密鍵ペアを生成し得る。公開/秘密鍵ペアは、対称鍵ペアであってよい。各公開/秘密鍵ペアは、秘密鍵と、秘密鍵に対応するとともにそれに数学的にリンクされる公開鍵とを含む。秘密鍵を使ってデジタル署名されているデータは、対応する公開鍵を使ってのみ、検証することができる。同様に、公開鍵を使って暗号化されているデータは、対応する秘密鍵を使ってのみ、解読することができる。

【００５９】

クライアントデバイス200は、N個のデバイス完全性要素について、デバイス完全性コンピューティングシステム220へ要求を送る(202)。数Nは、2以上の整数であってよい。この例では、デバイス完全性要素はデバイス完全性トークンであり、要求は、N個の公開/秘密鍵ペアに対応するN個のデバイス完全性トークンについてである。信用できるプログラムは、信用できるプログラムが一意のデバイス完全性トークンを要求の中で使う頻度に基づいて、要求するべきデバイス完全性トークンの数Nを判定することができる。クライアントデバイスは、各要求されたデバイス完全性トークン用の公開/秘密鍵ペアを生成し、公開鍵データを要求の中に含めればよい。この例では、公開鍵データは公開鍵自体であってよい。要求はしたがって、クライアントデバイス200のN個の公開鍵211をデバイス完全性サーバ220に渡すことを伴う。この例では、N個の公開鍵211は、実際の公開鍵、たとえば、N個の公開鍵211の未加工データを含む。要求は、デバイスレベル不正検出信号も含むことができる。たとえば、信用できるプログラムは、デバイスレベル不正検出信号を収集し、これらの信号を要求内に含めることができる。

【００６０】

デバイス完全性コンピューティングシステム220は、要求を受信する(221)。クライアントデバイスから受信されたデバイスレベル不正検出信号に基づいて、デバイス完全性コンピューティングシステム220は、クライアントデバイスの信用性のレベルを判定する(222)。たとえば、デバイス完全性コンピューティングシステムは、各々がそれぞれの判断に対応する、M個の可能な信用性のレベルを有する可能性がある。この例では、デバイス完全性コンピューティングシステム220は、上述したように、デバイスレベル不正検出信号に基づいて、これらのM個の可能な信用性のレベルのうちの1つを選択し得る。

【００６１】

デバイス完全性コンピューティングシステム220は、N個のデバイス完全性要素を生成する(223)。この例では、各デバイス完全性要素は、デバイス完全性トークンの形をしている。つまり、デバイス完全性コンピューティングシステム220は、各受信された公開鍵用に、それぞれのデバイス完全性トークンを生成する。

【００６２】

各デバイス完全性トークンは、信用性判断と、信用性の判断についてのタイムスタンプと、クライアントデバイス200のN個の公開鍵211のうちの1つとを含み得る。タイムスタンプは、デバイス完全性トークンが生成される時間を示す。デバイス完全性システムは、N個の公開鍵211のうちの1つに基づいて、各デバイス完全性トークンを生成することができる。たとえば、デバイス完全性システム220は、クライアントデバイス200の公開鍵、信用性判断、およびタイムスタンプを含むデータのセットを組み立てることができる。信用性の判断がただ2つの可能な判断(信用性のある、および信用性のない)を含む、いくつかの手法では、信用性の判断はデバイス完全性トークンから省かれてよい。言い換えると、これらの手法では、デバイス完全性システムは、信用性のあるデバイス用のデバイス完全性トークンを(信用性の暗示された判断を省くトークンとともに)生成し、信用性のないデバイス用のデバイス完全性トークンを生成するのを単に断ればよい。

【００６３】

デバイス完全性コンピューティングシステム220は、N個のデバイス完全性トークンの各々にデジタル署名する(224)。たとえば、デバイス完全性コンピューティングシステム220は、デバイス完全性システムの秘密鍵を使って、ならびにデバイス完全性トークンの他のデータ(たとえば、信用性判断、クライアントデバイス200の公開鍵、およびタイムスタンプ)に基づいて、デジタル署名を生成することができる。

【００６４】

デバイス完全性コンピューティングシステム220は、N個のデバイス完全性トークンをクライアントデバイスへ送信する(225)。クライアントデバイス200は、デバイス完全性トークンのバッチを受信し、後で使うために記憶する(203)。クライアントデバイス200は、デバイス完全性トークンをローカルに、たとえば、信用できるプログラムによって維持されるキャッシュまたはセキュアなストレージに記憶することができる。各キャッシュ

されたデバイス完全性トークンは、たとえば、(1)デバイス完全性コンピューティングシステム220によって判定される信用性の判断、(2)デバイス完全性トークンの作成についてのタイムスタンプ、(3)クライアントデバイスの公開鍵および(4)デバイス完全性コンピューティングシステム220の秘密鍵を使って署名された、トークンコンポーネントのデジタル署名を含み得る。

【００６５】

デバイス完全性トークンのバッチを取得してから、図2の例に示されるように、クライアントデバイスは、上述したように、デジタルコンポーネントプロバイダまたは他の認証トークン受信側へ向かう様々な要求の一部として、認証トークンを組み立て、送るのにデバイス完全性トークンを使うことができる。そのような要求の説明のための例が、図3にプロセスフロー図として示される。

【００６６】

要求を準備するために、クライアントデバイス300は、クライアントデバイスのローカルストレージからデバイス完全性トークンを取り出せばよい(301)。様々な手法において、クライアントデバイス300は、たとえば、(1)各要求についての新しいデバイス完全性トークンを使うこと、または(2)選択された時間間隔(たとえば、H時間連続)に対して同じデバイス完全性トークンを使い、その間隔が経過したときは、異なるデバイス完全性トークンを使うこと、または(3)同じアプリケーションもしくはウェブサイト(たとえば、各アプリケーションもしくはウェブサイト用に異なるデバイス完全性トークンが使われる)から発したすべての要求に対して同じデバイス完全性トークンを使うこと、または(4)これらのトークン再利用手法のうちの2つ以上の組合せを使うこと(たとえば、選択された時間間隔内に同じアプリケーションもしくはウェブサイトから発した、すべての要求に対して同じデバイス完全性トークンを使う)を行うことができる。したがって、クライアントデバイス300は、要求が生成されるアプリケーションもしくはウェブサイトまたは要求が生成される現在時刻に基づいてデバイス完全性トークンを取り出すことができる。

【００６７】

クライアントデバイス300は、要求を生成し得る(302)。要求311は、たとえば、ペイロードデータ(上述した)、要求作成タイムスタンプ、取り出されたデバイス完全性トークン、デバイス完全性トークンに対応するデバイス公開鍵、および要求コンポーネントのデジタル署名を含み得る。クライアントデバイスの信用できるプログラム、またはクライアントデバイスのオペレーティングシステムの信用できる構成要素が、ペイロードデータおよびデバイス完全性トークンにアクセスすることによって、認証トークンを含むか、またはその形であってよい要求311を生成することができる。信用できるプログラムは、要求作成タイムスタンプとして、現在時刻を判定することもできる。信用できるプログラムは、クライアントデバイスの秘密鍵(たとえば、要求の中に含まれるデバイス公開鍵に対応する秘密鍵)を使って、ペイロードデータのデジタル署名、公開鍵およびタイムスタンプを生成することができる。いくつかの手法では、認証トークンサイズを削減するための簡単な最適化として、認証トークンはデバイス公開鍵を省き、というのは、デバイス公開鍵は、認証トークンのコンポーネントとして含まれるデバイス完全性トークンの中にすでに存在するからである。

【００６８】

クライアントデバイス300は、受信側のコンピューティングシステム320へ要求311を送る(303)。この例では、受信側はデジタルコンポーネントプロバイダである。たとえば、クライアントデバイス300はデジタルコンポーネント配信システムへ要求311を送ればよく、デジタルコンポーネント配信システムは、1つまたは複数のデジタルコンポーネントプロバイダへ要求を送ればよい。

【００６９】

受信側コンピューティングシステム320は、要求を受信する(321)。受信側コンピューティングシステム320は、要求を確認する(322)。たとえば、受信側コンピューティングシステム320は、要求の中に含まれるデバイス公開鍵を使って要求のデジタル署名を検証

することによって、要求を確認することができる。受信側コンピューティングシステム320は、公開鍵と、クライアントデバイス300によって署名された要求の内容、たとえば、ペイロードデータ、タイムスタンプ、公開鍵、およびデバイス完全性トークンを使ってデジタル署名を検証しようと試み得る。この内容のいずれかが、デジタル署名が生成された後で変わった場合、検証は失敗する。たとえば、悪意のある関係者が、デバイス完全性トークンを別の要求に挿入し、またはより高い信用性の判断を有する、異なるデバイス完全性トークンを要求に挿入した場合、署名検証は失敗する。これにより、要求の内容は、たとえば、媒介による、要求の送信中に変更されないことが保証される。

【００７０】

受信側コンピューティングシステム320は、デバイス完全性トークンを確認する(323)。たとえば、受信側コンピューティングシステム320は、デバイス完全性コンピューティングシステムの公開鍵を使ってデバイス完全性トークンの署名を検証することによって、デバイス完全性トークンを確認することができる。こうすることにより、同様に、デバイス完全性トークンコンピューティングシステムによってデバイス完全性トークンが発行されてから、デバイス完全性トークンの内容が変わっていないことが保証される。認証トークンがデバイス公開鍵を含む場合、デバイス完全性トークンの確認は、認証トークンとともに含まれるデバイス公開鍵が、デバイス完全性トークン内に含まれるデバイス公開鍵と一致することの確認も含み得る。

【００７１】

受信側コンピューティングシステム320は、デバイス完全性トークンの適時性およびクライアントデバイスの信用性を確認して(324)、たとえば、デバイス完全性トークンが最近作成された(すなわち、H、D=1、2、3、...の場合、要求が行われた時間より前のH時間またはD日など、選択された時間間隔を超えて作成されたのではない)ことを確かめ、デバイス完全性トークンの中の信用性判断が、要求を履行するのに十分な判断であることを確かめる。

【００７２】

これらの妥当性検査すべてに通った場合、受信側コンピューティングシステム320は、上述したように、要求に応答して(325)、たとえば、設定を変更し、ユーザデータを追加または削除し、デジタルコンポーネントを送達することなどができる。妥当性検査のいずれかが失敗した場合、受信側コンピューティングシステム320は要求を無視すればよい。たとえば、受信側コンピューティングシステム320は要求に応答しなくてよく、要求された動作を実施しなくてよい、などである。

【００７３】

デジタルコンポーネントを送達することを伴う要求に対して、応答すること325は、適切なデジタルコンポーネント312を任意選択で送ることを含み得る。たとえば、受信側コンピューティングシステム320は、要求のペイロードに基づいてデジタルコンポーネントを選択し、デジタルコンポーネントプロバイダへ要求を送ったデジタルコンポーネント配信システムへデジタルコンポーネントを送ればよい。対して、デジタルコンポーネント配信システムは、クライアントデバイス300へデジタルコンポーネントを送ってよい。クライアントデバイス300は、デジタルコンポーネントを受信し得る(304)。次に、クライアントデバイス300はデジタルコンポーネントを提示すればよい。

【００７４】

上述したように、いくつかの手法では、デバイス完全性トークンを生成するためのプロセスにおいて、ブラインド署名方式が使われてよく、そうすることによって、デバイス完全性コンピューティングシステムには、クライアントデバイスの公開鍵の未加工データが見えない。たとえば、クライアントデバイスは、秘密/公開鍵ペアのバッチを生成し、次いで、公開鍵(または、公開鍵の暗号ハッシュなど、ブラインド署名方式のコミットフェーズ用の値として使うことができる、これらの公開鍵の適切な派生物、もしくはデバイスモデル番号と連結された、公開鍵の暗号ハッシュ)を、ブラインド署名方式を使ってブラインドしてから、デバイス完全性システムへ公開鍵を送って、デバイス完全性要素の対応するバ

ッチを取り出すことができる。この例では、デバイス完全性要素は、ブラインド化公開鍵のブラインド署名である。このバッチプロセスの説明のための例を、図4に示す。

【００７５】

この例では、デバイス完全性コンピューティングシステム420は、クライアントデバイスについてのM個の異なるレベルの信用性を定義し、対応するM個のレベルの信用性のためのM個の異なるブラインド署名検証鍵411を公開し得る(421)。たとえば、M個のレベルは、2つのレベル、すなわち信用性のある、および信用性のない、を含み得る。別の例では、M個のレベルは、3つのレベル、すなわち、疑わしい、満足できる、および信用できる、を含み得る。他の例では、M個のレベルは、4つのレベル、すなわち、不正、疑わしい、満足できる、および信用できる、を含み得る。他の数のレベルが使われてもよい。したがって、Mは2以上の整数であり得る。いくつかの手法では、最も低いレベルの信用性(たとえば、「信用性のない」または「不正」レベルの信用性)にブラインド署名検証鍵を割り当てるのではなく、最も低いレベルの信用性が、M個のレベルの信用性から省かれてよく、デバイス完全性コンピューティングシステムは、最も低いレベルの信用性をもつデバイスにブラインド署名を与えるのを単に断ればよい。したがって、これらの手法では、Mは1以上の整数であってよい。

【００７６】

デバイス完全性コンピューティングシステム420は、ブラインド署名方式を使って、各レベルの信用性についてのそれぞれのブラインド署名検証鍵411を生成することができる。ブラインド署名方式は、インターネット技術タスクフォース(IETF)検証可能忘却型擬似乱数関数(VOPRF)ブラインド署名方式などの非公開検証可能ブラインド署名方式であってよい。他の手法では、ブラインド署名方式は、リベスト-シャミア-エーデルマン(RSA)ブラインド署名方式などの公開検証可能ブラインド署名方式であってよい。

【００７７】

デバイス完全性コンピューティングシステム420は、クライアントデバイス400を含むクライアントデバイスがブラインド署名検証鍵411を取得することができるように、ブラインド署名検証鍵411を公開し得る。たとえば、デバイス完全性コンピューティングシステム420は、ブラインド署名検証鍵411を、ウェブサイトまたはモバイルアプリストアに公開し得る。

【００７８】

クライアントデバイス400は、これらのブラインド署名検証鍵を受信し得る(401)。たとえば、クライアントデバイス400は、ブラインド署名検証鍵411をダウンロードし、ブラインド署名検証鍵411をローカルに、たとえば、セキュアなストレージまたはキャッシュに記憶すればよい。クライアントデバイス400は、以下でさらに論じるように、デバイス完全性コンピューティングシステム420から後になって受信されたブラインド署名を検証するために、ブラインド署名検証鍵411を保持することができる。いくつかの手法では、デバイス完全性コンピューティングシステム420は、新しいブラインド署名検証鍵411を定期的に(たとえば、毎時間、毎日、毎週、または他の適切な時間期間ごとに)公開してよく、ブラインド署名検証鍵のセットのこのリフレッシュは、以下でさらに説明するように、デバイス完全性トークンの適時性を確認するのに使われてよい。

【００７９】

N個のデバイス完全性トークンのバッチを取得するために、クライアントデバイス400は、N個の公開/秘密鍵ペアを作成する(402)。たとえば、クライアントデバイスの信用できるプログラムが、各デバイス完全性トークン用に、それぞれの非対称公開/秘密鍵ペアを作成してよい。

【００８０】

クライアントデバイス400は、ブラインド署名検証鍵を生成するのに使われるブラインド署名方式に従って、各公開鍵または各公開鍵の派生物をブラインドする(403)。つまり、クライアントデバイス400は、各公開鍵についての公開鍵データをブラインドし、ここで公開鍵データは、公開鍵または公開鍵の派生物のいずれかである。公開鍵をブラインド

することは、公開鍵の未加工値にブラインド化因子を適用することによって、公開鍵の未加工値を隠すことを含み得る。このようにして、デバイス完全性コンピューティングシステム420は、クライアントデバイス400から受信された公開鍵の未加工値にアクセスすること、およびそれらの値を、ユーザまたはクライアントデバイス400を追跡するのに使うこと、たとえば、公開鍵の未加工値を追加データとともに受信した別のエンティティから受信されたデータを使うことができない。

【００８１】

デバイス完全性コンピューティングシステム420によってブラインド署名される必要があるデータのボリュームを削減するために、各全体デバイス公開鍵をブラインドするのではなく、クライアントデバイス400(たとえば、その信用できるプログラム)は、公開鍵の派生物を生成し、公開鍵の派生物をブラインドすればよい。派生物は、公開鍵の暗号ハッシュであってよい。たとえば、クライアントデバイス400は、暗号ハッシュ関数を使って各公開鍵の暗号ハッシュを生成し、次いで、ブラインド署名方式を使って公開鍵の暗号ハッシュをブラインドすればよい。いくつかの実装形態では、暗号ハッシュアルゴリズムはSHA256であってよい。

【００８２】

いくつかの実装形態では、クライアントデバイス400は、暗号ハッシュを短縮することによって、ブラインド化公開鍵データのデータサイズをさらに削減し、次いで、短縮暗号ハッシュをブラインドすればよい。たとえば、この短縮は、暗号ハッシュを、より大きいデータサイズを有する元の暗号ハッシュから16バイトにまで制限し得る。この短縮の結果、クライアントデバイス400がブラインド署名方式を使ってブラインドする、より短い暗号ハッシュが得られる。

【００８３】

このようにしてブラインド署名されるデータのボリュームを削減すると、データをブラインド署名する際にデバイス完全性コンピューティングシステム420にかけられる負担が削減され(たとえば、CPU周期、データ記憶要件、メモリ消費などが削減され)、そうすることにより、デバイス完全性コンピューティングシステム420は、全公開鍵のブラインド化バージョンが与えられた場合よりも、ブラインド署名をより速く、より効率的に生成し、より多くの要求を扱うことができるようになる。また、これにより、要求が送られるためのネットワークの帯域幅消費が削減され、大量のブラインド化公開鍵データが単一の要求の中で送られることが可能になる。

【００８４】

クライアントデバイス400は、N個のデバイス完全性トークンについて、デバイス完全性コンピューティングシステム420へ要求412を送る(404)。数Nは、2以上の整数であってよい。要求は、クライアントデバイス400によって生成された各公開鍵411についてのブラインド化公開鍵データを含み得る。たとえば、要求は、N個のブラインド化公開鍵、公開鍵のN個のブラインド化暗号ハッシュ、または公開鍵のN個のブラインド化短縮暗号ハッシュを含み得る。要求は、たとえば、クライアントデバイス400の信用できるプログラムによって収集される、デバイスレベル不正検出信号も含み得る。

【００８５】

デバイス完全性コンピューティングシステム420は、要求を受信する(422)。デバイス完全性コンピューティングシステム420は、デバイスレベル不正検出信号に基づいて、クライアントデバイス400の信用性の判断を判定する(423)。たとえば、デバイス完全性コンピューティングシステム420は、M個の可能な信用性の判断(動作421において公開されたM個のブラインド署名検証鍵に対応する)を有し得る。デバイス完全性コンピューティングシステム420は、デバイスレベル不正検出信号に基づいて、M個の可能判断のうちの1つに、クライアントデバイス400を割り当てればよい。

【００８６】

クライアントデバイス400の信用性の判断を判定してから、デバイス完全性コンピューティングシステム420は、ブラインド署名用秘密鍵を使って、各ブラインド化公開鍵デー

タ(たとえば、各N個のブラインド化公開鍵または各ブラインド化暗号ハッシュ)に署名する(424)。たとえば、デバイス完全性コンピューティングシステム420は、クライアントデバイス400について判定された信用性の判断に対応するブラインド署名用秘密鍵、たとえば、判定された信用性の判断についての公開ブラインド署名検証鍵に対応するブラインド署名用秘密鍵を取得することができる(424)。ブラインド署名方式をこのように使って、デバイス完全性コンピューティングシステム420は、公開鍵データの実際の値を知ることなく、ブラインド化公開鍵データのデジタル署名を生成することができる。

【００８７】

デバイス完全性コンピューティングシステム420は、N個のブラインド署名413をクライアントデバイスに戻す(425)。クライアントデバイス400は、デバイス完全性コンピューティングシステムからブラインド署名を受信する(405)。

【００８８】

クライアントデバイス400は、ブラインド署名方式を使って、ブラインド署名を非ブラインド化する(406)。たとえば、クライアントデバイス400の信用できるプログラムは、ブラインド署名がそのために生成された、ブラインド化公開鍵データと、デバイス完全性コンピューティングシステム420によって公開されたブラインド署名検証鍵とを使って、各ブラインド署名を確認すればよい。こうするために、信用できるプログラムは、たとえば、各信用性の判断のために、複数のブラインド署名検証鍵を使ってブラインド署名を確認しようと試みてよい。判断が、クライアントデバイス400に割り当てられた判断と一致しない場合、ブラインド署名は、その判断のためのブラインド署名検証鍵を使っては確認されない。信用できるプログラムは、ブラインド署名の確認に成功するブラインド署名検証鍵に基づいて、クライアントデバイス400の信用性の、割り当てられた判断を判定することができ、たとえば、ブラインド検証鍵に対応する信用性の判断は、クライアントデバイス400に割り当てられた判断である。確認された場合、信用できるプログラムは、ブラインド署名方式を使って、ブラインド署名を非ブラインド化してよい。

【００８９】

クライアントデバイス400は、デバイス完全性トークンのバッチを生成する(408)。たとえば、クライアントデバイス400の信用できるプログラムは、上の動作402において生成された各公開鍵用のデバイス完全性トークンを生成し得る。各デバイス完全性トークンは、たとえば、(1)デバイス完全性トークンがそのために生成されているクライアントデバイスの公開鍵、(2)デバイス完全性コンピューティングシステムによって判定される信用性の判断、および(3)ブラインド化公開鍵の非ブラインド化されたブラインド署名または公開鍵の暗号ハッシュ(たとえば、短縮)を含み得る。いくつかの手法では、デバイス完全性トークンは信用性の判断を省いてよく、というのは、これは非ブラインド化されたブラインド署名から暗示され得るからである。ブラインド署名が公開検証可能でない場合、デバイス完全性コンピューティングシステムが、ブラインド署名を検証することを求められると(たとえば、以下で論じる図5の541参照)、デバイス完全性コンピューティングシステムは、判断を戻してもよい。ブラインド署名が公開検証可能な場合、ブラインド署名を検証する公開鍵も、デバイスの信用性の判断を暗示する。

【００９０】

クライアントデバイス400は、デバイス完全性トークンを記憶する(410)。たとえば、クライアントデバイス400の信用できるプログラムは、デバイス完全性トークンを、デバイス完全性トークンを含むべきである要求を送るときに後で使うために、セキュアなストレージに記憶してよい。セキュアなストレージは、クライアントデバイス400のトークンキャッシュであってよい。

【００９１】

デバイス完全性トークンのバッチを生成し、記憶してから、図4の例に示されるように、クライアントデバイスは、上述したように、デジタルコンポーネントプロバイダまたは他の認証トークン受信側向けに行われる様々な要求の一部として、認証トークンを組み立て、送るのにデバイス完全性トークンを使うことができる。そのような要求の説明のため

の例が、図5にプロセスフロー図として示される。

【００９２】

要求を準備するために、クライアントデバイス500は、たとえば、クライアントデバイスのトークンキャッシュからデバイス完全性トークンを取り出せばよい(501)。様々な手法において、クライアントは、たとえば、(1)各要求についての新しいデバイス完全性トークンを使うこと、または(2)選択された時間間隔(たとえば、H時間連続)に対して同じデバイス完全性トークンを使うこと、または(3)同じアプリケーションもしくはウェブサイトから発したすべての要求に対して同じデバイス完全性トークンを使うこと、または(4)これらのトークン再利用手法の組合せを使うこと(たとえば、選択された時間間隔内に同じアプリケーションもしくはウェブサイトから発した、すべての要求に対して同じデバイス完全性トークンを使う)を行うことができる。したがって、クライアントデバイス500は、要求が生成されるアプリケーションもしくはウェブサイトまたは要求が生成される現在時刻に基づいてデバイス完全性トークンを取り出すことができる。

【００９３】

クライアントデバイス500は、要求ペイロード(上述した)と、要求が生成される時間を示す要求作成タイムスタンプと、デバイス完全性トークンと、デバイス完全性トークンに対応するデバイス公開鍵(たとえば、公開鍵データがそのためにブラインド署名され、非ブラインド化されたブラインド署名とともにデバイス完全性トークンに含まれる公開鍵)とを含む内容のセットを含む要求511を組み立てることができる。要求は、クライアントデバイスの秘密鍵(たとえば、要求の中に含まれる公開鍵に対応する秘密鍵)を使って署名された(502)、内容のセットのデジタル署名も含み得る。たとえば、クライアントデバイス500の信用できるプログラムは、秘密鍵を使って、内容のセットに基づいてデジタル署名を生成することができる。要求は、認証トークンを含むか、または認証トークンの形であってよい。たとえば、認証トークンは、内容のセット(たとえば、認証トークン作成タイムスタンプをもつ)およびデジタル署名を含み得る。

【００９４】

クライアントデバイス500は、受信側のコンピューティングシステム520へ要求511を送る(503)。受信側がデジタルコンポーネントプロバイダである場合、クライアントデバイス500は要求をデジタルコンポーネント配信システムへ送信すればよく、このシステムは、要求を適切なデジタルコンポーネントプロバイダへフォワードする。

【００９５】

受信側コンピューティングシステム520は、要求を確認する(522)。受信側コンピューティングシステム520は、要求とともに含まれるデバイス公開鍵を使って要求のデジタル署名を検証することによって、要求を確認することができる。受信側コンピューティングシステム520は、要求の中のタイムスタンプを、要求が受信された時間と比較することによって、要求を確認することもできる。署名の確認が成功し、タイムスタンプが現在時刻の閾持続時間以内である場合、クライアントデバイス500は、要求を確認されたと見なしてよい。

【００９６】

受信側コンピューティングシステム520は、デバイス完全性トークンも確認する。この確認プロセスは、ブラインド署名を生成するときにデバイス完全性コンピューティングシステム540によって使われるブラインド署名方式に基づいて異なり得る。ブラインド署名方式が公開検証可能方式(たとえば、RSA)である場合、受信側コンピューティングシステム520は、デバイス完全性コンピューティングシステムを呼び出すことなく、デバイス完全性トークンを確認することができる(523a)。この例では、受信側コンピューティングシステム520は、デバイス完全性トークン中に含まれる公開鍵データの非ブラインド化されたブラインド署名を検証するのに、ブラインド署名方式を使うことができる。公開鍵の暗号ハッシュが使われる場合、受信側コンピューティングシステム520は、クライアントデバイス500と同じ暗号ハッシュ関数を使って、要求の中に含まれる公開鍵の暗号ハッシュを生成し(かつ、適切な場合は短縮し)、暗号ハッシュの非ブラインド化されたブラインド

署名を検証するのにブラインド署名方式を使うことができる。

【００９７】

ブラインド署名方式が非公開検証可能方式(たとえば、IETF VOPRF)である場合、受信側コンピューティングシステム520は、非ブラインド化されたブラインド署名を検証するために、デバイス完全性コンピューティングシステム540を呼び出せばよい(523b)。この例では、受信側コンピューティングシステム520は、非ブラインド化されたブラインド署名と、公開鍵または公開鍵の暗号ハッシュとを、デバイス完全性コンピューティングシステム540へ送り得る。

【００９８】

デバイス完全性コンピューティングシステム540は、ブラインド署名方式を使って、非ブラインド化されたブラインド署名を検証することを試み、デジタルコンポーネントプロバイダに応答を与えてよい(541)。応答は、検証が成功したかどうかと、非ブラインド化されたブラインド署名を検証するブラインド署名検証鍵に対応するクライアントデバイスの信用性とを示し得る。

【００９９】

受信側コンピューティングシステム520は、デバイス完全性トークンの適時性およびクライアントデバイスの信用性を確認して(524)、たとえば、デバイス完全性トークンが最近作成されたことを確かめ、デバイス完全性トークンの中の信用性判断が、要求を履行するのに十分な判断であることを確かめる。デバイス完全性コンピューティングシステム540は、新しいブラインド署名検証鍵を定期的に公開し直し得るので、適時性確認は、たとえば、デバイス完全性トークンが、満了しているブラインド署名検証鍵で検証されたと判定することによって、デバイス完全性トークンのブラインド署名が、無効な古い鍵で署名されているのではないことを確かめることを含み得る。一手法では、受信側コンピューティングシステムは、ブラインド署名検証鍵の有効日が、公開された鍵についてのURLの一部として符号化されていたという理由で、ブラインド署名検証鍵が満了したと判定することができる。別の手法では、受信側コンピューティングシステムは、検証鍵が、検証鍵の満了日を符号化するメタデータとともに公開されているという理由で、ブラインド署名検証鍵が満了したと判定することができる。

【０１００】

これらの妥当性検査すべてに通った場合、受信側コンピューティングシステム520は、上述したように、要求に応答して(525)、たとえば、設定を変更し、ユーザデータを追加または削除し、デジタルコンポーネントを送達することなどができる。デジタルコンポーネントを送達することを伴う要求に対して、応答すること525はしたがって、適切なデジタルコンポーネント512を任意選択でクライアントデバイス500へ送ることを含み得る。この例では、クライアントデバイス500はデジタルコンポーネントを提示すればよい。妥当性検査のいずれかが失敗した場合、受信側コンピューティングシステム520は要求を無視し、たとえば、要求への応答を送らず、設定を更新することなどを選べばよい。

【０１０１】

図2～図5の例に示し、上述した手法は、クライアントデバイスのデバイス公開鍵を使うことを伴うが、他の手法は、グループ署名方式のためにデバイス公開鍵の使用を控える場合がある。概して、グループ署名方式は、グループのメンバーが、グループを代表してメッセージに匿名で署名できるようにする方法である。グループ署名方式では、グループマネージャが、メッセージに証明書Cで署名するのに使われ得るグループ署名関数sign(message,C)を公開し、ここで証明書Cは、グループマネージャによってグループのメンバーに対して非公開で発行された機密証明書(匿名秘密鍵としても知られる)である。グループマネージャはまた、グループ検証鍵K(グループ公開鍵としても知られる)と、メッセージが、匿名証明書Cを使ってグループ署名関数で署名されているとともにKがCのためのグループ検証鍵である場合にのみTRUEを戻すグループ署名検証関数verify(sign(message,C),K)とを公開する。

【０１０２】

これらの技法は、デバイス完全性システムをグループマネージャとして、クライアントデバイス要求の認証のためにグループ署名方式を利用することができる。いくつかのグループ署名方式により、グループマネージャは、グループのメンバーによって作成された匿名署名を匿名化解除することができるが、秘匿性要項は、この匿名化解除能力を含まない、直接匿名認証(DAA)などのグループ署名方式を好む場合がある。たとえば、いくつかの手法では、デバイス完全性システムは、Barreto-Naehrig曲線を用いるECC DAAなどの楕円曲線暗号化(ECC)DAA方式を使うことができる。その上、いくつかのグループ署名方式により、グループマネージャはグループメンバーシップを撤回することができるようになるが、効率要項は、この撤回能力を含まないグループ署名方式を好む場合があり、したがって、これらの技法は、たとえば、数百万または数十億のグループメンバーをもつグループを有する、インターネット規模にまでスケーラブルである。

【０１０３】

クライアントデバイス要求の認証のためのグループ署名方式の説明のための例を、図6および図7のプロセスフロー図に示す。この例では、デバイス完全性コンピューティングシステム620は、クライアントデバイスについてのM個の異なるレベルの信用性を定義し、対応するM個のレベルの信用性のためのM個の異なるグループ検証鍵を公開し得る。たとえば、デバイス完全性システムは、1つ、2つ、またはより多くのグループ検証鍵、たとえば、デバイス信用性のレベルに対応するECC DAA検証鍵を公開し得る。M=1である手法の場合、グループ検証鍵はほぼ最低レベルの信用性に対応し、その最低レベルの信用性を満たさないデバイスは、信用性グループのメンバーとして加えられない。M≧2である手法の場合、異なるグループ検証鍵は、デバイス信用性のそれぞれのレベルまたは分類に対応する。いくつかの手法では、デバイス完全性コンピューティングシステムは、新しいグループ検証鍵を定期的に(たとえば、毎時間、毎日、毎週、または必要に応じて他の時間期間ごとに)公開してよく、グループ検証鍵のセットのこのリフレッシュは、以下でさらに説明するように、クライアントデバイス要求の適時性を確認するのに使われてよい。

【０１０４】

ここで図6を参照すると、クライアントデバイス600が、デバイス完全性サーバ620によって管理されるM個の信用性グループの1つについての機密証明書の形での秘密デバイス完全性証明書を要求し得る(601)。要求は、たとえば、クライアントデバイス600の信用できるプログラムによって収集された、デバイスレベル不正検出信号を含み得る。

【０１０５】

デバイス完全性コンピューティングシステムは、要求を受信する(621)。デバイス完全性コンピューティングシステム620は、デバイスレベル不正検出信号に基づいて、クライアントデバイスの信用性の判断を判定し、信用性の判断に対応する選択された信用性グループにクライアントデバイスを割り当てることができる(622)。

【０１０６】

デバイス完全性コンピューティングシステム620は次いで、選択された信用性グループに対応する匿名証明書611を生成または選択し、匿名証明書611をクライアントデバイスに戻してよい(623)。たとえば、デバイス完全性コンピューティングシステムは、デバイス完全性コンピューティングシステムによってデバイスに割り当てられたデバイス信用性レベルに関連付けられたECC DAA検証鍵に対応する資格証明を生成してよい。クライアントデバイス600は、匿名証明書611を受信し、クライアントデバイス600において、たとえば、秘密鍵ストアにローカルにセキュアに記憶してよい(602)。たとえば、クライアントデバイスは、秘密鍵ストア向けのマスター鍵を使って証明書を暗号化すればよく、そうすることによって、悪意のある関係者は、証明書を濫用すること、および異なるデバイス上で使うことができない。

【０１０７】

特定の信用性グループにおけるメンバーシップの匿名証明書を取得してから、クライアントデバイスは、この匿名証明書を、デジタルコンポーネントプロバイダまたは他の認証トークン受信側から行われる様々な要求の一部として認証トークンを組み立て、送るのに

使うことができる。この例では、認証トークンは、クライアントデバイスの公開鍵を含まないので、匿名認証トークンと呼ばれ得る。そのような要求の説明のための例が、図7にプロセスフロー図として示される。

【０１０８】

クライアントデバイス700は、デジタルコンポーネントプロバイダまたは他の認証トークン受信側から行われるべき要求を開始することができる(701)。いくつかの実装形態では、クライアントデバイスは、以下でさらに説明するように、要求が認証トークン限度を超えないことを、任意選択で確かめることができる(702)。クライアントデバイス700は、たとえば、上で、および図6において記載したデバイス完全性コンピューティングシステムから証明書をあらかじめ取得した、クライアントデバイス上の秘密鍵ストアから、匿名証明書を取り出す(703)。

【０１０９】

クライアントデバイス700は、要求711を生成し、その要求に、取り出された匿名証明書で署名する(704)。要求の生成は、たとえば、要求ペイロードと、要求作成タイムスタンプとを含む内容のセットを生成することを含み得る。要求ペイロードは、たとえば、デジタルコンポーネントを選択するのに使うことができるデータ、またはデータの削除など、認証トークン受信側によって行われるべき、要求される変更を指定するデータを含み得る。要求作成タイムスタンプは、要求が生成される時間を示し得る。いくつかの事例では、要求作成タイムスタンプは、複製された要求またはリプレイ攻撃を検出するのに十分小さい時間分解能を有する。たとえば、要求作成タイムスタンプは、約1ミリ秒未満、または約1マイクロ秒未満の時間分解能を有し得る。グループ署名方式が確率的グループ署名方式である手法では、クライアントデバイス700による、同じ要求711の2つの別個の署名行為が、異なる署名を生成する。これらの手法では、要求711の受信側が、同一の署名をもつ要求を拒絶することによって、複製された要求またはリプレイ攻撃を防ぎ得る。

【０１１０】

上で、ならびに図3および図5に記載した他の手法とは反対に、要求711は、クライアントデバイスの公開鍵を含まず、デバイス完全性トークンも含まない(図3の要求311と図5の要求511を比較されたい)。前述した手法のこれらの認証トークン特徴は、クライアントデバイスの所有および匿名証明書Cの使用が、クライアントデバイスがデバイス完全性コンピューティングシステムによって管理される信用性グループのメンバーであることを意味する、本手法のグループ署名方式には不必要である。クライアントデバイスは、公開されたグループ署名関数sign(message,C)を使う匿名証明書Cを使って要求711に署名する。たとえば、クライアントデバイス700は、匿名証明書Cを使って、内容のセットのデジタル署名を生成することができ、たとえば、クライアントデバイスは、デバイス完全性サーバによってクライアントデバイスにあらかじめ与えられたECC DAA資格証明をもつECC DAA署名方式を使って、要求に署名することができる。

【０１１１】

クライアントデバイスは、受信側のコンピューティングシステム720へ要求711を送る(705)。受信側がデジタルコンポーネントプロバイダである場合、クライアントデバイス700は要求をデジタルコンポーネント配信システムへ送信すればよく、このシステムは、要求を適切なデジタルコンポーネントプロバイダへフォワードする。

【０１１２】

受信側コンピューティングシステム720は、要求を受信する(722)。クライアントデバイス700から要求711を受信するのに先立って、受信側コンピューティングシステム720は、デバイス完全性コンピューティングシステムのM個の信用性クラスについてのM個の異なるグループ検証鍵のセットを受信する(721)。デバイス完全性コンピューティングシステム740は、これらのM個のグループ検証鍵を公開し(741)、新しいグループ検証鍵を定期的に(たとえば、毎時間、毎日、毎週、または必要に応じて他の時間期間ごとに)公開し直してよく、その場合、認証トークン受信側は、クライアントデバイスからの要求を確認するのに使うための新しいグループ検証鍵を定期的に受信する。一手法では、グループ

検証鍵は、よく知られているURLを使って、よく知られているパス上で公開され、そうすることによって、どの受信側コンピューティングシステム720も、標準HTTP要求を使ってグループ検証鍵をフェッチすることができる。パスは日付/時間情報を符号化してよく、またはグループ検証鍵に付随するメタデータが鍵満了日を符号化してよく、そうすることによって、受信側コンピューティングシステムは、以下でさらに論じるように、鍵が現行のものであるかどうかを判定することができる。

【０１１３】

受信側コンピューティングシステム720は、要求の適時性を確認する(723)。たとえば、受信側は、とりわけ、要求が複製(またはリプレイ試行)でないこと、および要求が古くないこと(たとえば、要求作成タイムスタンプと、受信側コンピューティングシステムが要求を受信する時間との間の、閾内の差)を確かめるために、要求作成タイムスタンプを精査すればよい。

【０１１４】

受信側コンピューティングシステム720は、要求の匿名署名および信用性を確認する(724)。たとえば、受信側は、M個の公開されたグループ検証鍵のセットの中の各公開されたグループ検証鍵Kについて、検証関数verify(sign(message,C),K)を評価することによって、匿名署名を確認すればよい。検証関数は、たとえば、デバイス完全性サーバによってあらかじめ公開されたECC DAA検証鍵を使って計算されるECC DAA署名検証関数であってよい。関数が、あらゆる公開されたグループ検証鍵KについてFALSEである場合、受信側は、要求が偽造されたか、またはクライアントデバイス700がどの信用性グループにも属さないと判定してよい。一方、関数が特定のグループ検証鍵KについてTRUEである場合、クライアントデバイス700は、その特定のグループ検証鍵Kに対応する信用性グループに属する。

【０１１５】

これらの妥当性検査に通った場合、認証トークン受信側は、上述したように、要求に応答して(725)、たとえば、設定を変更し、ユーザデータを追加または削除し、デジタルコンポーネントを送達することなどができる。デジタルコンポーネントを送達することを伴う要求に対して、応答すること725は次いで、適切なデジタルコンポーネント712を任意選択でクライアントデバイス700へ送ることを含み得る。クライアントデバイス700は、デジタルコンポーネントを受信する(706)。次に、クライアントデバイス700は、デジタルコンポーネントをクライアントデバイス700のユーザに対して提示すればよい。

【０１１６】

図6および図7に示し、上述したグループ署名手法は、クライアントデバイスのデバイス公開鍵に基づいて追跡を防ぐことによって、クライアントデバイスまたはユーザの秘匿性を強化するが、認証トークン受信側(デジタルコンポーネントプロバイダなど)が、認証トークン受信側へ過度の量の要求を送り得る悪用デバイスまたはアプリケーションを識別するのを妨げる場合もある。したがって、いくつかの手法では、クライアントデバイスは、クライアントデバイスが過大な量の認証トークンを送るのを抑えることができる信用できるスロットラーを含み得る。図7を再度参照すると、スロットラーは、たとえば、開始された要求を進ませる前に、要求が認証トークン限度を超えないことを検証する動作702を実施し得る。スロットラーは、たとえば、クライアントデバイスの信用できるオペレーティングシステムのスレッド、プロセス、サブルーチン、または他の構成要素であってよい。スロットラーについては、図6～図8のグループ署名手法のコンテキストにおいて以下で説明するが、スロットラーは、本明細書に記載する認証トークンコンテキストのいずれにおいても、認証トークンのボリュームを制限するのに使われ得ることが企図される。たとえば、スロットラーは、図3の要求311、または図5の要求511を制限するのに使われ得る。

【０１１７】

このスロットリング手法の説明のための例を、図8のプロセスフロー図に示す。デジタルコンポーネントプロバイダおよび認証トークンを含む要求または他の通信の他の受信側

など、様々な認証トークン受信側850が、認証トークン量限度を示す情報を公開し得る(851)。たとえば、認証トークン受信側は、(1)各個々のクライアントデバイスから、受信側の選択された宛先ドメインへ、選択された時間枠内に送られ得るトークンの数に対する限度(たとえば、Y秒、分、もしくは時間以内にX個以下の要求)、(2)個々のクライアントデバイス上の1つもしくは複数の選択されたアプリケーションから、受信側の選択された宛先ドメインへ、選択された時間枠内に送られ得るトークンの数に対する限度(たとえば、アプリケーションAから、もしくはアプリケーションA以外の任意のアプリケーションから、Y秒、分、もしくは時間以内にX個以下の要求)、(3)個々のクライアントデバイスから、受信側の選択された宛先ドメイン内の選択されたエンドポイントへ、選択された時間枠内に送られ得るトークンの数に対する限度、(4)クライアントデバイス上の1つもしくは複数の選択されたアプリケーションから、選択された宛先ドメイン内の選択されたエンドポイントへ、選択された時間枠内に送られ得るトークンの数に対する限度、または(5)そのような限度のうちの2つ以上の、任意の組合せを公開し得る。

【０１１８】

スロットラー830は、クライアントデバイス800の信用できるプログラム820(たとえば、オペレーティングシステム)の構成要素として、公開されたトークン量限度情報を受信する(821)。公開されたトークン量限度情報は、様々なやり方で受信されてよい。一手法では、各認証トークン受信側は、トークン量情報を、トークン受信側の秘密鍵で署名されたファイル中で公開する。信用できるクローラは、それらのファイルを(トークン受信側用の公開鍵と一緒に)定期的にフェッチし、それらのファイルを各クライアントデバイス800へ送達する。各クライアントデバイス上のスロットラー830は次いで、トークン受信側の署名を検証した後、スロットリング要件を履行する。たとえば、スロットラー830は、限度を超えることになる要求についての認証トークンを生成しないことによって、限度を超えないことを保証すればよい。

【０１１９】

別の手法では、各トークン受信側は、署名されたトークン量情報をデジタル配信プラットフォーム(モバイルアプリがそこからダウンロードされ得るモバイルアプリストアなど)へ提出する。デジタル配信プラットフォームは、トークン量情報を検証し、署名する。各トークン受信側は次いで、2度署名されたトークン量情報をクライアントデバイス800へ送達する。各クライアントデバイス上のスロットラー830は次いで、トークン受信側とデジタル配信プラットフォームの両方の署名を検証した後、スロットリング要件を履行する。たとえば、スロットラー830は、限度を超えることになる要求についての認証トークンを生成しないことによって、限度を超えるないことを保証すればよい。

【０１２０】

クライアントデバイス上のアプリケーション810が、認証トークンについての、信用できるプログラム820への要求を開始すると(811)、信用できるプログラム820はこの要求を受信する(822)。信用できるプログラム820は次いで、要求を履行すると、クライアントデバイスが、公開されたトークン量限度のうちの1つまたは複数を超えるかどうかを評価するために、スロットラーを呼び出せばよい(823)。要求が、公開されたトークン量限度のうちの1つまたは複数を超えることになる場合、信用できるプログラム820は認証トークン要求を拒否する(ステップ823a)。要求が、公開されたトークン量限度を超えることにならない場合、信用できるオペレーティングシステム820は、認証トークンを生成させ、適切な認証トークン受信側へ送らせる(ステップ823b)。

【０１２１】

上記の説明に加えて、ユーザには、本明細書で説明されるシステム、プログラム、または特徴がユーザ情報(たとえば、ユーザのソーシャルネットワーク、ソーシャルアクションもしくはアクティビティ、職業、ユーザの選好、またはユーザの現在のロケーションについての情報)の収集を可能にし得るかどうかおよびいつそれを可能にし得るかと、サーバからの個別化コンテンツまたは通信がユーザに送信されるかどうかの両方に関しての選択をユーザが行うことを可能にする制御が与えられ得る。加えて、いくつかのデータは、個人

を識別できる情報が削除されるように、記憶または使用される前に1つまたは複数の方法で扱われ得る。たとえば、ユーザに対して個人を識別できる情報(たとえば、電話番号、IMEI、デバイスシリアルナンバー)が判定できないように、ユーザのアイデンティティーが扱われてよく、またはユーザの具体的なロケーションが判定できないように、ユーザの地理的ロケーションはロケーション情報が取得される(都市レベル、郵便番号レベル、または州レベルなどの)場所に一般化されてよい。したがって、ユーザは、ユーザについてのどの情報が収集されるか、その情報がどのように使用されるか、情報保持ポリシー、およびどの情報がユーザに提供されるかを制御することができる。

【０１２２】

図9は、上述の動作を実施するために使うことができる例示的コンピュータシステム900のブロック図である。システム900は、プロセッサ910、メモリ920、記憶デバイス930、および入出力デバイス940を含む。構成要素910、920、930、および940の各々は、たとえば、システムバス950を使って、相互接続され得る。プロセッサ910は、システム900内での実行のために命令を処理することが可能である。いくつかの実装形態では、プロセッサ910は、シングルスレッドプロセッサである。別の実装形態では、プロセッサ910はマルチスレッドプロセッサである。プロセッサ910は、メモリ920または記憶デバイス930に記憶された命令を処理することが可能である。

【０１２３】

メモリ920は、システム900内に情報を記憶する。一実装形態では、メモリ920は、コンピュータ可読媒体である。いくつかの実装形態では、メモリ920は、揮発性メモリユニットである。別の実装形態では、メモリ920は不揮発性メモリユニットである。

【０１２４】

記憶デバイス930は、システム900に大容量記憶を提供することが可能である。いくつかの実装形態では、記憶デバイス930は、コンピュータ可読媒体である。様々な異なる実装形態では、記憶デバイス930は、たとえば、ハードディスクデバイス、光ディスクデバイス、複数のコンピューティングデバイス(たとえば、クラウド記憶デバイス)によってネットワーク上で共有される記憶デバイス、または他の何らかの大容量記憶デバイスを含むことができる。

【０１２５】

入出力デバイス940は、システム900のための入出力動作を提供する。いくつかの実装形態では、入出力デバイス940は、ネットワークインターフェースデバイス、たとえば、Ethernetカード、シリアル通信デバイス、たとえば、RS-232ポート、および/またはワイヤレスインターフェースデバイス、たとえば、802.11カードのうちの1つまたは複数を含み得る。別の実装形態では、入出力デバイスは、入力データを受信し、出力データを外部デバイス960、たとえば、キーボード、プリンタ、およびディスプレイデバイスに送るように構成されたドライバデバイスを含み得る。しかしながら、モバイルコンピューティングデバイス、モバイル通信デバイス、セットトップボックステレビクライアントデバイスなど、他の実装形態が使われてもよい。

【０１２６】

例示的な処理システムが図9で説明されているが、本明細書内で説明される主題の実装形態および機能的動作は、他のタイプのデジタル電子回路において、または本明細書で開示される構造およびその構造的等価物を含むコンピュータソフトウェア、ファームウェア、もしくはハードウェアにおいて、またはそれらのうちの1つもしくは複数の組合せにおいて実装され得る。

【０１２７】

本明細書に記載する主題および動作の実施形態は、デジタル電子回路構成において、またはコンピュータソフトウェア、ファームウェア、もしくは本明細書において開示した構造およびそれらの構造的等価物を含むハードウェアにおいて、またはそれらのうちの1つもしくは複数の組合せで実装することができる。本明細書で説明される主題の実施形態は、1つまたは複数のコンピュータプログラム、すなわち、データ処理装置による実行のた

めにまたはデータ処理装置の動作を制御するために(1つまたは複数の)コンピュータ記憶媒体上で符号化された、コンピュータプログラム命令の1つまたは複数のモジュールとして実装され得る。代替または追加として、プログラム命令は、データ処理装置による実行のために、適切な受信機装置への伝送のために情報を符号化するために生成された、人工的に生成された伝搬信号、たとえば、機械で生成された電気信号、光信号、または電磁信号上で符号化され得る。コンピュータ記憶媒体は、コンピュータ可読記憶デバイス、コンピュータ可読記憶基板、ランダムもしくはシリアルアクセスメモリアレイもしくはデバイス、またはそれらのうちの1つもしくは複数の組合せであり得るか、またはそれらに含まれ得る。さらに、コンピュータ記憶媒体は伝搬信号ではないが、コンピュータ記憶媒体は、人工的に生成された伝搬信号において符号化されたコンピュータプログラム命令のソースまたは宛先であり得る。コンピュータ記憶媒体はまた、1つまたは複数の別個の物理構成要素または媒体(たとえば、複数のCD、ディスク、または他の記憶デバイス)であり得るか、またはそれらに含まれ得る。

【０１２８】

本明細書に記載した動作は、1つもしくは複数のコンピュータ可読記憶デバイス上に記憶された、または他のソースから受信されたデータに対して、データ処理装置によって実施される動作として実装されてよい。

【０１２９】

「データ処理装置」という用語は、例として、プログラム可能プロセッサ、コンピュータ、システムオンチップ、または上記の複数のもの、もしくは組合せを含む、データを処理するための、あらゆる種類の装置、デバイス、および機械を包含する。装置は、専用論理回路、たとえば、FPGA(フィールドプログラマブルゲートアレイ)またはASIC(特定用途向け集積回路)を含むことができる。装置は、ハードウェアに加えて、当該のコンピュータプログラムのための実行環境を作成するコード、たとえば、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステム、クロスプラットフォームランタイム環境、仮想マシン、またはそれらのうちの1つもしくは複数の組合せを構成するコードも含むことができる。装置および実行環境は、ウェブサービス、分散コンピューティングインフラストラクチャおよびグリッドコンピューティングインフラストラクチャなどの様々な異なるコンピューティングモデルインフラストラクチャを実現することができる。

【０１３０】

コンピュータプログラム(プログラム、ソフトウェア、ソフトウェアアプリケーション、スクリプト、またはコードとしても知られている)は、コンパイル型またはインタープリタ型言語、宣言型または手続き型言語を含む、どの形のプログラミング言語でも書かれてよく、スタンドアロンプログラムとして、またはモジュール、構成要素、サブルーチン、オブジェクト、もしくはコンピューティング環境における使用に適した他のユニットとして、を含む、どの形でも展開することができる。コンピュータプログラムは、ファイルシステムにおけるファイルに対応し得るが、そうである必要はない。プログラムは、他のプログラムもしくはデータ(たとえば、マークアップ言語文書に記憶された1つもしくは複数のスクリプト)を保持するファイルの一部分に、当該のプログラム専用の単一のファイルに、または複数の協調ファイル(たとえば、1つもしくは複数のモジュール、サブプログラム、またはコードの部分を記憶するファイル)に記憶され得る。コンピュータプログラムは、1つのコンピュータ上で、または、1つのサイトに配置されるかもしくは複数のサイトにわたって分散され、通信ネットワークによって相互接続される複数のコンピュータ上で実行されるように展開され得る。

【０１３１】

本明細書に記載したプロセスおよび論理フローは、入力データに対して動作し、出力を生成することによってアクションを実施するための1つまたは複数のコンピュータプログラムを実行する1つまたは複数のプログラム可能プロセッサによって実施され得る。プロセスおよび論理フローは、専用論理回路、たとえば、FPGA(フィールドプログラマブルゲ

ートアレイ)またはASIC(特定用途向け集積回路)によっても実施され得、装置は、それらとしても実装され得る。

【０１３２】

コンピュータプログラムの実行に適したプロセッサは、例として、汎用マイクロプロセッサと専用マイクロプロセッサの両方を含む。一般に、プロセッサは、読取り専用メモリもしくはランダムアクセスメモリまたは両方から命令およびデータを受信する。コンピュータの必須要素は、命令に従ってアクションを実施するためのプロセッサ、ならびに命令およびデータを記憶するための1つまたは複数のメモリデバイスである。一般に、コンピュータは、データを記憶するための1つまたは複数の大容量記憶デバイス、たとえば、磁気ディスク、光磁気ディスク、または光ディスクも含むか、あるいは、それらからデータを受信することもしくはそれらにデータを転送することまたはその両方を行うために動作可能に結合される。しかしながら、コンピュータはそのようなデバイスを有する必要はない。さらに、コンピュータは、ほんの数例を挙げると、別のデバイス、たとえば、モバイル電話、携帯情報端末(PDA)、モバイルオーディオもしくはビデオプレーヤ、ゲームコンソール、全地球測位システム(GPS)受信機、またはポータブル記憶デバイス(たとえば、ユニバーサルシリアルバス(USB)フラッシュドライブ)に埋め込まれ得る。コンピュータプログラム命令およびデータを記憶するのに適したデバイスは、例として、半導体メモリデバイス、たとえば、EPROM、EEPROM、およびフラッシュメモリデバイス、磁気ディスク、たとえば、内部ハードディスクまたはリムーバブルディスク、光磁気ディスク、ならびにCD-ROMディスクおよびDVD-ROMディスクを含む、すべての形の不揮発性メモリ、媒体およびメモリデバイスを含む。プロセッサおよびメモリは、特殊目的論理回路構成によって補完されても、組み込まれてもよい。

【０１３３】

ユーザとの対話を提供するために、本明細書に記載される主題の実施形態は、ユーザに情報を表示するための、CRT(陰極線管)またはLCD(液晶ディスプレイ)モニタなどのディスプレイデバイス、ならびにキーボードおよび、ユーザがコンピュータに入力を提供することができる、たとえば、マウスまたはトラックボールなどのポインティングデバイスを有するコンピュータ上に実装することができる。他の種類のデバイスを使用して、ユーザとの対話を提供することもでき、たとえば、ユーザに提供されるフィードバックは、たとえば、視覚フィードバック、聴覚フィードバック、または触覚フィードバックなど、任意の形態の感覚フィードバックとすることができ、ユーザからの入力は、音響、音声、または触覚入力を含む任意の形で受信することができる。加えて、コンピュータは、文書をユーザによって使用されるデバイスに送信し、文書をそのデバイスから受信することによって、たとえば、ユーザのクライアントデバイス上のウェブブラウザから受信された要求に応答してウェブページをそのウェブブラウザに送信することによって、ユーザと対話することができる。

【０１３４】

本明細書に記載する主題の実施形態は、バックエンド構成要素を、たとえば、データサーバとして含む、もしくはミドルウェア構成要素、たとえば、アプリケーションサーバを含む、もしくはフロントエンド構成要素、たとえば、本明細書に記載する主題の実装形態とユーザが対話し得るためのグラフィカルユーザインターフェースもしくはウェブブラウザを有するクライアントコンピュータ、または1つもしくは複数のそのようなバックエンド、ミドルウェア、もしくはフロントエンド構成要素のどの組合せも含むコンピューティングシステムにおいて実装することができる。システムの構成要素は、デジタルデータ通信の任意の形態または媒体、たとえば、通信ネットワークによって相互接続され得る。通信ネットワークの例は、ローカルエリアネットワーク(「LAN」)およびワイドエリアネットワーク(「WAN」)、インターネットワーク(たとえば、インターネット)、ならびにピアツーピアネットワーク(たとえば、アドホックピアツーピアネットワーク)を含む。

【０１３５】

コンピューティングシステムは、クライアントおよびサーバを含み得る。クライアント

とサーバは概して、互いから離れており、通常、通信ネットワークを通して対話する。クライアントとサーバの関係は、それぞれのコンピュータ上で稼動するとともに互いとのクライアント-サーバ関係を有するコンピュータプログラムにより発生する。いくつかの実施形態では、サーバが、データ(たとえば、HTMLページ)を、クライアントデバイスへ(たとえば、クライアントデバイスと対話するユーザにデータを表示し、ユーザからユーザ入力を受信する目的のために)送信する。クライアントデバイスにおいて生成されたデータ(たとえば、ユーザ対話の結果)は、サーバにおいてクライアントデバイスから受信され得る。

【０１３６】

本明細書は、多くの具体的な実装形態詳細を含むが、これらは、任意の発明の、または特許請求され得るものの範囲において、限定と解釈されるべきではなく、特定の発明の特定の実施形態に特有な特徴の記述として解釈されるべきである。別個の実施形態の文脈において本明細書で説明されるいくつかの特徴はまた、単一の実施形態において組み合わせて実装され得る。逆に、単一の実施形態の文脈において説明される様々な特徴はまた、複数の実施形態において別々にまたは任意の適切な部分組合せで実装され得る。さらに、特徴はいくつかの組合せにおいて働くものとして上記で説明され、そのようなものとして最初に特許請求されることさえあるが、特許請求される組合せからの1つまたは複数の特徴は、場合によっては、その組合せから削除されることがあり、特許請求される組合せは、部分組合せまたは部分組合せの変形形態を対象とする場合がある。

【０１３７】

同様に、動作は、特定の順序で図面に示されるが、これは、望ましい結果を達成するために、そのような動作が図示された特定の順序でもしくは順番に行われること、または例示したすべての動作が行われることを必要とするものと理解されるべきではない。状況によっては、マルチタスキングおよび平行処理が有利であり得る。さらに、上記で説明した実施形態における様々なシステム構成要素の分離は、すべての実施形態においてそのような分離を必要とするものとして理解されるべきではなく、説明したプログラム構成要素およびシステムは一般に、単一のソフトウェア製品に一緒に組み込まれるか、または複数のソフトウェア製品にパッケージ化されることがあると理解されたい。

【０１３８】

以上、本主題の特定の実施形態について記載した。他の実施形態は、以下の特許請求の範囲の範囲内にある。いくつかのケースでは、請求項に具陳されるアクションは、異なる順序で実施され、依然として望ましい結果を達成し得る。加えて、添付の図面に示したプロセスは、所望の結果を達成するために、必ずしも示した特定の順序または順番を必要としない。いくつかの実装形態では、マルチタスキングおよび平行処理が有利であり得る。

【符号の説明】

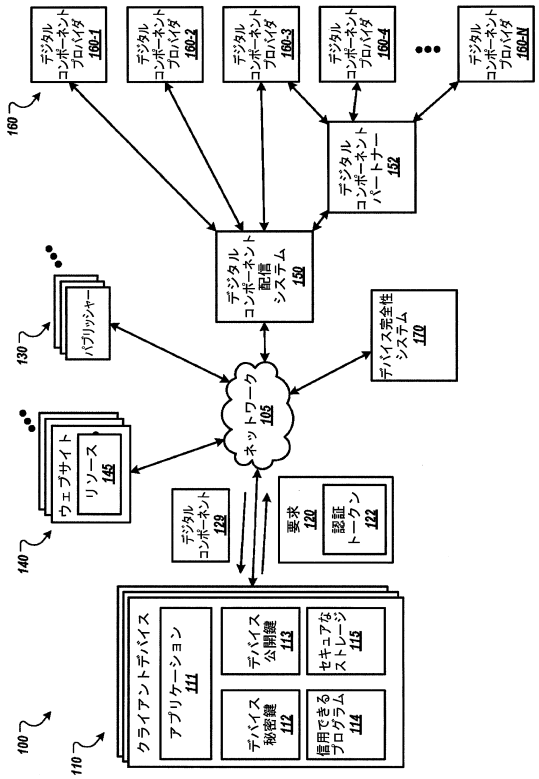
【０１３９】

105 データ通信ネットワーク、ネットワーク
110 クライアントデバイス
111 アプリケーション
112 秘密鍵
113 公開鍵
114 信用できるプログラム
115 セキュアなストレージ
120 要求
122 認証トークン
129 デジタルコンポーネント
130 パブリッシャー
140 ウェブサイト
145 リソース
150 デジタルコンポーネントシステム、デジタルコンポーネント配信システム
152 デジタルコンポーネントパートナー

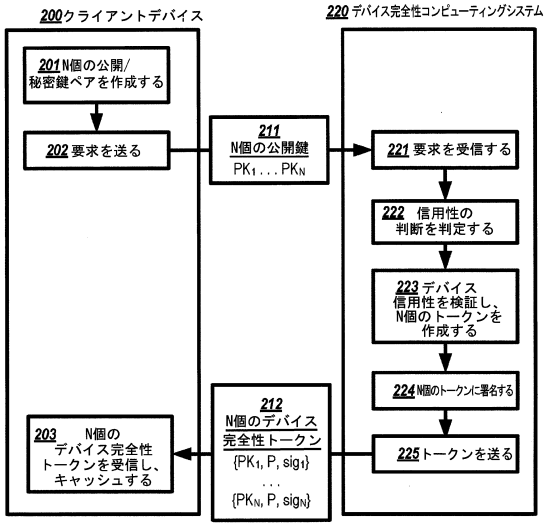
160 デジタルコンポーネントプロバイダ
170 デバイス完全性システム
200 クライアントデバイス
211 公開鍵
220 デバイス完全性コンピューティングシステム、デバイス完全性サーバ、デバイス完全性システム
300 クライアントデバイス
311 要求
312 デジタルコンポーネント
320 コンピューティングシステム、受信側コンピューティングシステム
400 クライアントデバイス
411 ブラインド署名検証鍵、公開鍵
412 要求
413 ブラインド署名
420 デバイス完全性コンピューティングシステム
500 クライアントデバイス
511 要求
512 デジタルコンポーネント
520 コンピューティングシステム、受信側コンピューティングシステム
540 デバイス完全性コンピューティングシステム
600 クライアントデバイス
611 匿名証明書
620 デバイス完全性コンピューティングシステム、デバイス完全性サーバ
700 クライアントデバイス
711 要求
712 デジタルコンポーネント
720 コンピューティングシステム、受信側コンピューティングシステム
740 デバイス完全性コンピューティングシステム
800 クライアントデバイス
810 アプリケーション
820 信用できるプログラム、信用できるオペレーティングシステム
830 スロットラー
850 認証トークン受信側
900 コンピュータシステム、システム
910 プロセッサ
920 メモリ
930 記憶デバイス
940 入出力デバイス
950 システムバス
960 外部デバイス

【図面】

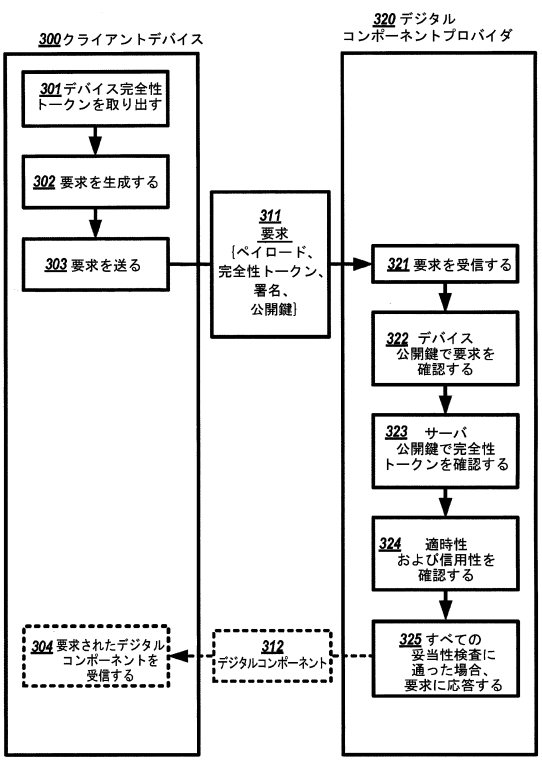
【図１】


デジタルコンポーネントプロバイダ 160-1
デジタルコンポーネントプロバイダ 160-2
デジタルコンポーネントプロバイダ 160-3
デジタルコンポーネントプロバイダ 160-4
デジタルコンポーネントプロバイダ 160-N
160
デジタルコンポーネントパートナー 152
デジタルコンポーネント配信システム 150
パブリッシャー
130
デバイス完全性システム 170
ネットワーク 105
ウェブサイトリソース 145
140
デジタルコンポーネント 129
要求 120
認証トークン 122
クライアントデバイス
アプリケーション 111
デバイス公開鍵 113
セキュアなストレージ 115
デバイス秘密鍵 112
信用できるプログラム 114
100
110

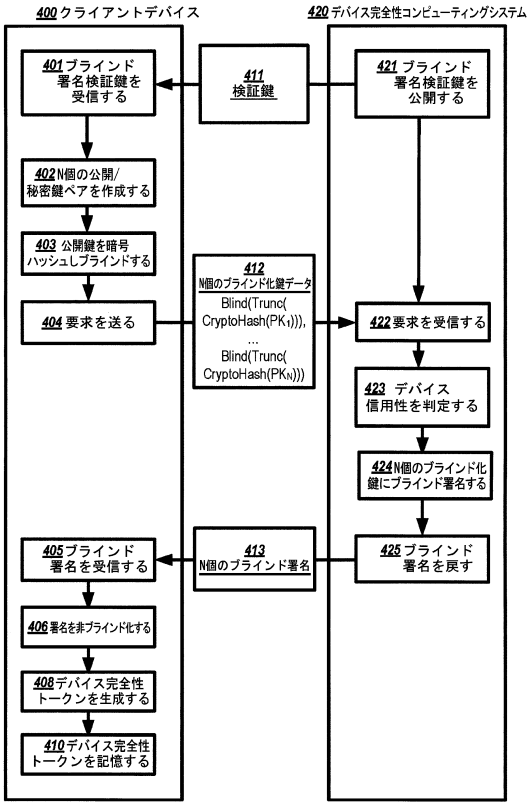
【図２】


200クライアントデバイス
220 デバイス完全性コンピューティングシステム
201 N個の公開/秘密鍵ペアを作成する
202 要求を送る
211 N個の公開鍵 PK1 . . . PKN
221 要求を受信する
222 信用性の判断を判定する
223 デバイス信用性を検証し、N個のトークンを作成する
224 N個のトークンに署名する
225 トークンを送る
212 N個のデバイス完全性トークン {PK1, P, sig1} . . . {PKN, P, sigN}
203 N個のデバイス完全性トークンを受信し、キャッシュする

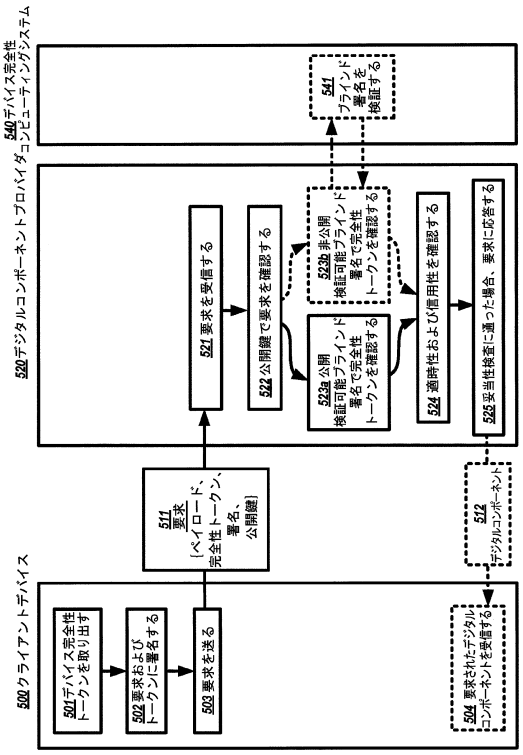
【図３】


300クライアントデバイス
320 デジタルコンポーネントプロバイダ
301 デバイス完全性トークンを取り出す
302 要求を生成する
303 要求を送る
311 要求 {ペイロード、完全性トークン、署名、公開鍵}
321 要求を受信する
322 デバイス公開鍵で要求を確認する
323 サーバ公開鍵で完全性トークンを確認する
324 適時性および信用性を確認する
325 すべての妥当性検査に通った場合、要求に応答する
304 要求されたデジタルコンポーネントを受信する
312 デジタルコンポーネント

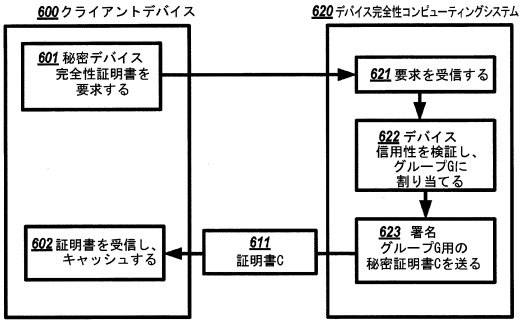
【図４】


400 クライアントデバイス
420 デバイス完全性コンピューティングシステム
401 ブラインド署名検証鍵を受信する
411 検証鍵
421 ブラインド署名検証鍵を公開する
402 N個の公開/秘密鍵ペアを作成する
403 公開鍵を暗号ハッシュしブラインドする
404 要求を送る
412 N個のブラインド化鍵データ Blind(Trunc(CryptoHash(PK1))), ... Blind(Trunc(CryptoHash(PKN)))
422 要求を受信する
423 デバイス信用性を判定する
424 N個のブラインド化鍵にブラインド署名する
425 ブラインド署名を戻す
405 ブラインド署名を受信する
413 N個のブラインド署名
406 署名を非ブラインド化する
408 デバイス完全性トークンを生成する
410 デバイス完全性トークンを記憶する

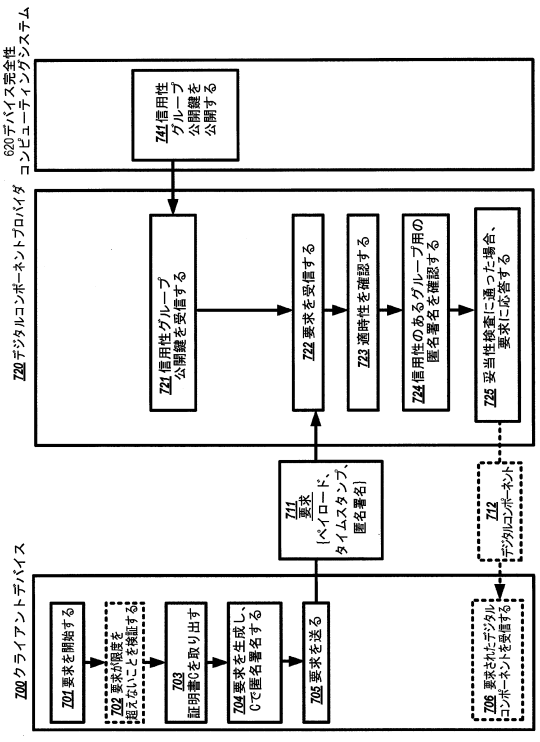
【図５】


540デバイス完全性コンピューティングシステム
541 プライバシー署名を検証する
520デジタルコンポーネントプロバイダ
521 要求を受信する
522 公開鍵で要求を確認する
522b 非公開検証可能プライバシー署名で完全性トークンを確認する
523a 公開検証可能プライバシー署名で完全性トークンを確認する
524 適時性および信用性を確認する
525 妥当性検査に通った場合、要求に応答する
511 要求（ペイロード、完全性トークン、署名、公開鍵）
512 デジタルコンポーネント
500クライアントデバイス
501デバイス完全性トークンを取り出す
502 要求およびトークンに署名する
503 要求を送る
504 要求されたデジタルコンポーネントを受信する

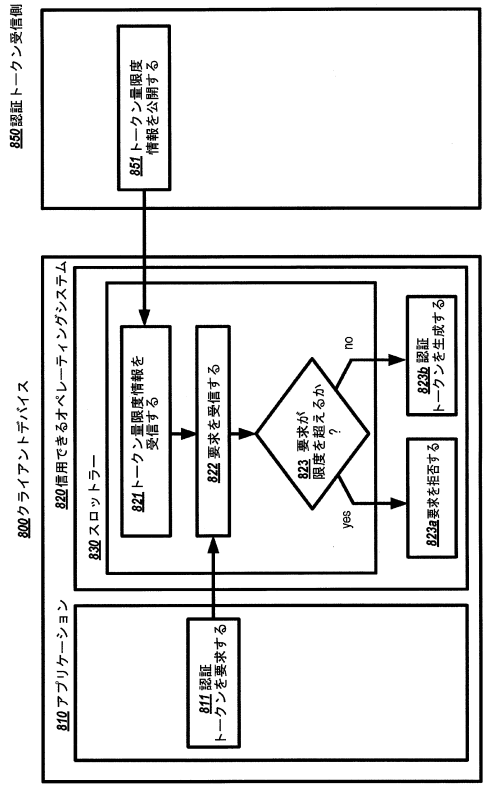
【図６】


600クライアントデバイス
620デバイス完全性コンピューティングシステム
601 秘密デバイス完全性証明書を要求する
621 要求を受信する
622 デバイス信用性を検証し、グループGに割り当てる
623 署名グループGの秘密証明書Cを送る
602 証明書を受信し、キャッシュする
611 証明書C

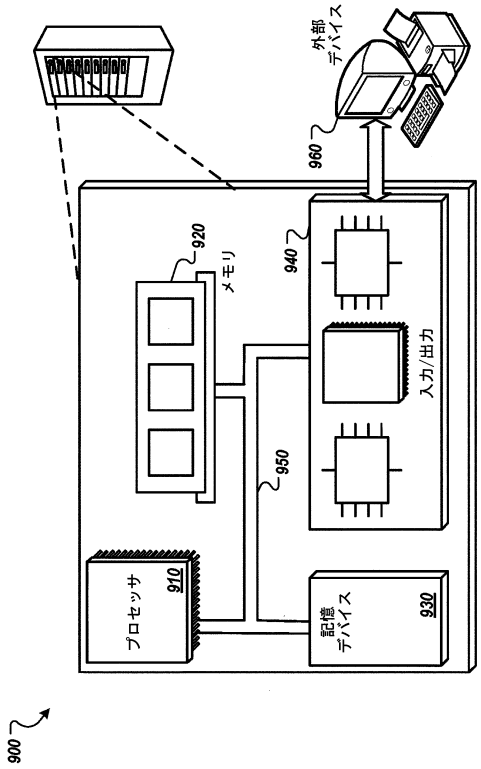
【図７】


620デバイス完全性コンピューティングシステム
741 信用性グループ公開鍵を公開する
720 デジタルコンポーネントプロバイダ
721 信用性グループ公開鍵を受信する
722 要求を受信する
723 適時性を確認する
724 信用性のあるグループ用の匿名署名を確認する
725 妥当性検査に通った場合、要求に応答する
711 要求（ペイロード、タイムスタンプ、匿名署名）
712 デジタルコンポーネント
700クライアントデバイス
704 要求を開始する
702 要求が限度を超えないことを検証する
703 証明書Cを取り出す
704 要求を生成し、Cで匿名署名する
705 要求を送る
706 要求されたデジタルコンポーネントを受信する

【図８】


850認証トークン受信側
851 トークン量限度情報を公開する
800クライアントデバイス
820信用できるオペレーティングシステム
830 スロットラー
821 トークン量限度情報を受信する
822 要求を受信する
823 要求が限度を超えるか？
no
yes
823b 認証トークンを生成する
822a 要求を拒否する
810 アプリケーション
811 認証トークンを要求する

【図９】



フロントページの続き

(72)発明者　ガン・ワン
アメリカ合衆国・カリフォルニア・９４０４３・マウンテン・ビュー・アンフィシアター・パークウェイ・１６００
(72)発明者　マルセル・エム・モティ・ユン
アメリカ合衆国・カリフォルニア・９４０４３・マウンテン・ビュー・アンフィシアター・パークウェイ・１６００

審査官　青木 重徳

(56)参考文献
特開２０２０－０４２６９１（ＪＰ，Ａ）
特開２０１３－１７５０４０（ＪＰ，Ａ）
特開２００９－０２７７０８（ＪＰ，Ａ）
特表２００９－５３９１７２（ＪＰ，Ａ）
米国特許第１０１５４０６１（ＵＳ，Ｂ１）
米国特許出願公開第２０１９／０３１２７３０（ＵＳ，Ａ１）
米国特許出願公開第２０１７／０２８９１８５（ＵＳ，Ａ１）
米国特許出願公開第２０２０／０１６２２５１（ＵＳ，Ａ１）
米国特許出願公開第２００８／０２７０７８６（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　９／０８
Ｇ０６Ｆ　２１／６４