

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7564244号
(P7564244)

(45)発行日 令和6年10月8日(2024.10.8)

(24)登録日 令和6年9月30日(2024.9.30)

(51)国際特許分類		F I	
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/32 2 0 0 B
G 0 6 F	21/64 (2013.01)	G 0 6 F	21/64
G 0 6 F	21/31 (2013.01)	G 0 6 F	21/31
請求項の数 15 (全43頁)			
(21)出願番号	特願2022-570379(P2022-570379)	(73)特許権者	502208397
(86)(22)出願日	令和3年8月26日(2021.8.26)		グーグル エルエルシー
(65)公表番号	特表2023-542578(P2023-542578 A)		G o o g l e L L C
(43)公表日	令和5年10月11日(2023.10.11)		アメリカ合衆国 カリフォルニア州 9 4
(86)国際出願番号	PCT/US2021/047736		0 4 3 マウンテン ビュー アンフィシ
(87)国際公開番号	WO2023/027709		アター パークウェイ 1 6 0 0
(87)国際公開日	令和5年3月2日(2023.3.2)		1 6 0 0 Amphitheatre P
審査請求日	令和5年1月16日(2023.1.16)		arkway 9 4 0 4 3 Mounta
			in 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】 トークン償還による匿名認証

(57)【特許請求の範囲】

【請求項1】

匿名証明のための方法であって、

クライアントデバイス上で実行しているアプリケーションによって、第1のコンテンツプロバイダとは異なる第2のコンテンツプロバイダの第2のドメインからのコンテンツを受信するためにユーザを認証するための認証要求を、前記第1のコンテンツプロバイダの第1のドメイン上でホストされた第1のサーバから受信するステップと、

前記認証要求の受信に応答して、前記第2のコンテンツプロバイダに対して前記ユーザの認証を証明する匿名証明トークンを発行した証明トークン発行システムに、第2の要求とともに前記匿名証明トークンを送信することによって、前記匿名証明トークンを前記アプリケーションによって償還するステップと、

前記第2の要求に応答して、前記アプリケーションによって、前記証明トークン発行システムから、前記匿名証明トークンが正常に償還されたか否かを表し、前記証明トークン発行システムによってデジタル署名を使用して署名される、償還結果を受信するステップであって、前記償還結果が、個人を識別可能な情報を含まない、ステップと、

前記アプリケーションによって、前記第1のコンテンツプロバイダに、前記証明トークン発行システムによって署名された前記償還結果を送信するステップとを含む方法。

【請求項2】

前記第2のコンテンツプロバイダが、ニュースプロバイダであり、

前記第1のコンテンツプロバイダが、ニュースアグリゲータドメインであり、

前記アプリケーションによって、前記第1のコンテンツプロバイダに、前記証明トークン発行システムによって署名された前記償還結果を送信するステップが、前記ニュースプロバイダによってホストされたりソースへのアクセスを要求するユーザアクションに応答して実行される、請求項1に記載の方法。

【請求項3】

前記第2のコンテンツプロバイダが、メディアホスティングプラットフォームであり、

前記第1のコンテンツプロバイダが、ソーシャルメディアプラットフォームであり、

前記アプリケーションによって、前記第1のコンテンツプロバイダに、前記証明トークン発行システムによって署名された前記償還結果を送信するステップが、前記メディアホスティングプラットフォームによってホストされたりソースへのアクセスを要求するユーザアクションに応答して実行される、請求項1に記載の方法。

【請求項4】

前記クライアントデバイス上の前記アプリケーションによって、エンティティに対して前記クライアントデバイスのユーザを認証する前記ユーザのクレデンシャルへのアクセスを有する信用できるプログラムに、前記第2のコンテンツプロバイダに対して前記ユーザの認証を証明する前記匿名証明トークンのための第1の要求を送信するステップと、

前記信用できるプログラムによって、前記証明トークン発行システムに、前記匿名証明トークンのための第3の要求を送信するステップであって、前記第3の要求が、前記クライアントデバイスの前記ユーザのためのクレデンシャルのセットを含む、ステップと、

前記アプリケーションによって、前記証明トークン発行システムから、(i)前記匿名証明トークンの作成の時間を示す証明トークン作成タイムスタンプ、および(ii)前記証明トークン発行システムの第2のデジタル署名を備える、前記匿名証明トークンを受信するステップと

をさらに含む、請求項1から3のいずれか一項に記載の方法。

【請求項5】

前記第2のデジタル署名が、前記証明トークン発行システムによって維持された秘密鍵を使用して作成され、前記第2のデジタル署名が、(i)前記秘密鍵に対応し、かつ(ii)前記証明トークン発行システムによって公開された、公開鍵を使用して検証され得る、請求項4に記載の方法。

【請求項6】

前記アプリケーションによって、前記第1のコンテンツプロバイダの電子リソースを通して、前記第2のコンテンツプロバイダに、前記第2のコンテンツプロバイダからの前記コンテンツを要求するステップ

をさらに含む、請求項1から5のいずれか一項に記載の方法。

【請求項7】

前記アプリケーションによって、前記第2のコンテンツプロバイダからの前記コンテンツを受信するステップ

をさらに含む、請求項6に記載の方法。

【請求項8】

前記証明トークン発行システムの前記デジタル署名が、ブラインド署名方式に従って作成される、請求項1から7のいずれか一項に記載の方法。

【請求項9】

前記証明トークン発行システムの前記デジタル署名が、グループ署名方式、および前記クライアントデバイスに発行された匿名証明書を使用して作成され、

前記方法が、前記匿名証明書を前記クライアントデバイス上のセキュアなプライベートキーストアに記憶するステップをさらに含む、請求項1から8のいずれか一項に記載の方法。

【請求項10】

前記証明トークン発行システムによって署名された前記償還結果を送信するステップが

、(i)前記アプリケーションによって署名され、かつ(ii)前記ユーザを前記ユーザのためのクレデンシャルのセットに相関させない、追加のデータを提供するステップをさらに含む、請求項1から9のいずれか一項に記載の方法。

【請求項11】

前記第2の要求が、発行されることになる証明トークンの数を示す、請求項1から10のいずれか一項に記載の方法。

【請求項12】

前記第2の要求が、前記アプリケーションによって維持された秘密鍵を使用する第3のデジタル署名を用いて署名され、前記第3のデジタル署名が、(i)前記秘密鍵に対応し、かつ(ii)前記アプリケーションによって公開された、公開鍵を使用して検証され得る、請求項1から11のいずれか一項に記載の方法。

10

【請求項13】

前記償還結果が、前記匿名証明トークンが正常に償還されたか否かを表す単一ビットを備える、請求項1から12のいずれか一項に記載の方法。

【請求項14】

システムであって、

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13のいずれか一項に記載の方法を実行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。

20

【請求項15】

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13のいずれか一項に記載の方法の動作を実行させる命令を記憶する、非一時的コンピュータ可読記憶媒体。

【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、通信を傍受する当事者、および/または通信を受信し、それらを他の当事者に転送する仲介者など、他の当事者によって改変され得る。

30

【0002】

他の当事者は、クライアントデバイスから発生しているように見えるが、実際には他の当事者のデバイスから来る要求を送るために、クライアントデバイスをエミュレートすることができる。

【0003】

様々な認証技法が、公衆ネットワークを介してトランザクションを実行しようと試みるクライアントデバイスの識別情報を検証するために使用され得る。同時に、これらの認証技法は、プライバシーの問題を含む可能性がある。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ために使用され得る情報(不変のデバイス識別子など)を共有することを望まないことがあり、データプロバイダは、そのような情報をデータプロバイダが受信または処理することを妨げるプライバシー保護規格下で動作することがある。

40

【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の完全性/真正性を検証すると同時に、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ために使用され得る不変のデバイス識別子の使用を回避するための認証技法について説明する。

【0005】

概して、本明細書で説明する主題の第1の発明的態様は、匿名証明のための方法におい

50

て実施され得、方法は、クライアントデバイス上で実行しているアプリケーションによって、第1のコンテンツプロバイダの第1のドメイン上でホストされた第1のサーバから、第1のコンテンツプロバイダとは異なる第2のコンテンツプロバイダの第2のドメインからのコンテンツを受信するためにユーザを認証するための認証要求を受信するステップと、認証要求の受信に応答して、アプリケーションによって、および第2のコンテンツプロバイダに対してユーザの認証を証明する匿名証明トークンを発行した証明トークン発行システムに、第2の要求とともに匿名証明トークンを送信することによって、匿名証明トークンを償還する(redeem)ステップと、第2の要求に応答して、アプリケーションによって、証明トークン発行システムから、証明トークンが正常に償還されたか否かを表し、証明トークン発行システムによってデジタル署名を使用して署名される、償還(redemption)結果を受信するステップであって、償還結果が、第2のコンテンツプロバイダに対してユーザを識別することなしに、ユーザが第2のコンテンツプロバイダに対して認証されることを、第2のコンテンツプロバイダに対して検証するように動作可能である、ステップと、アプリケーションによって、第1のコンテンツプロバイダに、証明トークン発行システムによって署名された償還結果を送信するステップとを含む。

【0006】

いくつかの実装形態では、償還結果が、ユーザのためのクレデンシャルのセットを第1のコンテンツプロバイダに提供することなしに、ユーザが匿名のままであることを可能にしながら、ユーザが第2のコンテンツプロバイダに対して認証されることを、受信側に対して検証するように動作可能である。

【0007】

いくつかの実装形態では、第2のコンテンツプロバイダが、ニュースプロバイダであり、第1のコンテンツプロバイダが、ニュースアグリゲータドメインであり、アプリケーションによって、第1のコンテンツプロバイダに、証明トークン発行システムによって署名された償還結果を送信するステップが、ニュースプロバイダによってホストされたりソースへのアクセスを要求するユーザアクションに応答して実行される。

【0008】

いくつかの実装形態では、第2のコンテンツプロバイダが、メディアホスティングプラットフォームであり、第1のコンテンツプロバイダが、ソーシャルメディアプラットフォームであり、アプリケーションによって、第1のコンテンツプロバイダに、証明トークン発行システムによって署名された償還結果を送信するステップが、メディアホスティングプラットフォームによってホストされたりソースへのアクセスを要求するユーザアクションに応答して実行される。

【0009】

いくつかの実装形態では、方法は、クライアントデバイス上のアプリケーションによって、エンティティに対してクライアントデバイスのユーザを認証するユーザのクレデンシャルへのアクセスを有する信用できるプログラムに、第2のコンテンツプロバイダに対してユーザの認証を証明する匿名証明トークンのための第1の要求を送信するステップと、信用できるプログラムによって、証明トークン発行システムに、匿名証明トークンのための第3の要求を送信するステップであって、第3の要求が、クライアントデバイスのユーザのためのクレデンシャルのセットを含む、ステップと、アプリケーションによって、証明トークン発行システムから、(i)匿名証明トークンの作成の時間を示す証明トークン作成タイムスタンプ、および(ii)証明トークン発行システムの第2のデジタル署名を備える、匿名証明トークンを受信するステップとを含む。

【0010】

いくつかの実装形態では、方法は、アプリケーションによって、第1のコンテンツプロバイダの電子リソースを通して、第2のコンテンツプロバイダに、第2のコンテンツプロバイダからのコンテンツを要求するステップを含む。

【0011】

いくつかの実装形態では、方法は、アプリケーションによって、第2のコンテンツプロ

10

20

30

40

50

バイダからのコンテンツを受信するステップを含む。

【0012】

いくつかの実装形態では、証明トークン発行システムのデジタル署名が、ブラインド署名方式に従って作成される。

【0013】

いくつかの実装形態では、証明トークン発行システムのデジタル署名が、グループ署名方式、およびクライアントデバイスに発行された匿名証明書を使用して作成され、方法が、匿名証明書をクライアントデバイス上のセキュアなプライベートキーストアに記憶するステップを含む。

【0014】

いくつかの実装形態では、証明トークン発行システムによって署名された償還結果を送信するステップが、(i)アプリケーションによって署名され、かつ(ii)ユーザをクレデンシャルのセットに相関させない、追加のデータを提供するステップをさらに含む。

【0015】

いくつかの実装形態では、要求が、発行されることになる証明トークンの数を示す。

【0016】

いくつかの実装形態では、要求が、アプリケーションによって維持された秘密鍵を使用する第3のデジタル署名を用いて署名され、第3のデジタル署名が、(i)秘密鍵に対応し、かつ(ii)アプリケーションによって公開された、公開鍵を使用して検証され得る。

【0017】

いくつかの実装形態では、第2のデジタル署名が、証明トークン発行システムによって維持された秘密鍵を使用して作成され、第2のデジタル署名が、(i)秘密鍵に対応し、かつ(ii)証明トークン発行システムによって公開された、公開鍵を使用して検証され得る。

【0018】

いくつかの実装形態では、償還結果が、証明トークンが正常に償還されたか否かを表す単一ビットを備える。

【0019】

この態様の他の実施形態は、対応するシステム、装置、およびコンピュータ記憶デバイス上に符号化された、方法のアクションを実行するように構成されたコンピュータプログラムを含む。

【0020】

本明細書で説明する主題は、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で実装され得る。

【0021】

クライアントデバイスまたはユーザを認証するために、証明トークンを使用することは、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のセキュアな通信チャネルを提供する。証明トークンとともに、証明トークンに含まれるデータのデジタル署名を含めることによって、エンティティは、証明トークンが作成された後に証明トークン内のデータが変更されなかったことを検証することができる。加えて、証明トークン中にトークン作成時間を含めることによって、受信側は、要求が新しいものであるか、または潜在的に、動作を実行するために、許可されたデバイスの識別情報を不正に使用するためのサードパーティによる方式の一部であるかを決定することが可能になる。

【0022】

たとえば、証明トークンは、特定のリソースに対してクライアントデバイスを識別することなしに、クライアントデバイスがそのリソースにアクセスすることを許可されることを識別するために使用され得、リソースを保っている当事者が、クライアントデバイスが正当な許可されたユーザであることを保証されることが可能になり、クライアントデバイスが、リソースに対してその匿名性を維持することが可能になる。

【0023】

10

20

30

40

50

証明トークンシステムは、個人を識別できる情報(PII)をウェブサイトまたはプラットフォームと共有することなしに、同じプラットフォーム内の異なるウェブサイトにもわたって、および異なるプラットフォームにもわたって、デバイスおよび/またはユーザを認証するための能力を提供する。たとえば、証明トークンシステムは、サードパーティコンテンツアグリゲーティングプラットフォームおよびウェブサイトまたはプロバイダのいずれかに、PIIを提供することなしに、サードパーティコンテンツアグリゲーティングプラットフォームおよびウェブサイトを通して、認証を必要とするプラットフォームまたはプロバイダからのリソースおよびコンテンツに、ユーザがアクセスすることを可能にする。証明トークンシステムは、プライバシーを保護しており、異なるウェブサイトおよびプラットフォーム間の境界を実施し、好都合でシームレスな方法でリソースおよびコンテンツへのアクセスを提供する。サードパーティコンテンツアグリゲーティングプラットフォームに、ユーザ名およびパスワードなどのPIIを、そのようなPIIを使用してリソースにアクセスするために提供するのではなく、クライアントデバイスは、クライアントデバイスのユーザがリソースへのアクセスを有することを、サードパーティコンテンツアグリゲーティングプラットフォームに対して認証する、償還結果を提供することができる。したがって、サードパーティコンテンツアグリゲーティングプラットフォームは、通常はリソースにアクセスするために使用されるユーザのPII(たとえば、リソースに直接アクセスするために使用されるようになる、ユーザのユーザ名およびパスワード)を受信せず、リソースのパブリッシャーは、ユーザがサードパーティコンテンツアグリゲーティングプラットフォームを通してリソースにアクセスしていると決定することができない。これによって、リソースのためのユーザのPIIに関してユーザのプライバシーを保護し、サードパーティコンテンツアグリゲーティングプラットフォームを使用するユーザのプライバシーを保護する。

【0024】

証明トークンシステムは、ユーザの摩擦の原因を除去することによって、ユーザエクスペリエンスを向上させる。たとえば、証明トークンは、ユーザが追加の認証情報を提供することを必要とすることなしに、制限されたリソースへのユーザアクセスを可能にするために使用され得る。

【0025】

証明トークンはまた、証明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判定(verdict)も含むことができ、これによって、証明トークンの受信側は、データが、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来たことを検証することが可能になる。証明トークンの受信側が、クライアントデバイスが信用できるデバイスアナライザによって評価されたこと、およびデバイス完全性判定内のデータが、信用できるデバイスアナライザによって作成された後に修正されなかったことを検証することができるよう、デバイス完全性判定が、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、デジタル署名され得る。

【0026】

証明トークンは、クライアントデバイスから送信される通信の完全性を保護するが、証明トークンの使用に関連付けられた潜在的なプライバシー問題がある。第1のプライバシー問題は、コンテンツパブリッシャーまたはプラットフォームとの複数の対話内の同じ証明トークンの再使用によって、証明トークン受信側が、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相関させ、その相関に基づいてユーザデータをアグリゲートすることを潜在的に可能にし得ることである。本明細書で説明する技法は、各々がクライアントデバイスの一意の公開鍵を含む複数の証明トークンを使用することによって、そのような相関に対するプライバシーを向上させることができる。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個の対応する証明トークンのバッチを受信するために、N個の公開鍵をサードパーティデバイスアナライザに送ることができる。次いで、クライアントデバイスは、たとえば、要求ごとに新しい証明トークンを使用することができ、またはクライアントデバイスは、ある時間間隔内にすべての要

10

20

30

40

50

求のために、同じ証明トークンを使用することができ、またはクライアントデバイスは、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せられたすべての要求のために、同じ証明トークンを使用することができ、またはそれらの何らかの組合せを使用することができる。各公開鍵の使用を制限することによって、受信側が公開鍵に基づいて相関させることができる要求の量を制限し、アプリケーションサーバが償還記録(redemption record)を消費するときに有する確信の量を増すことができる。たとえば、アプリケーションサーバは、トークンが古いほど、クライアントがトークンをマルウェアに対して不注意に露出させた可能性が高いと決定することができる。このバッチ手法を使用することはまた、さもないと、証明トークンが必要とされるたびにクライアントデバイスが証明トークンのための要求を送った場合に導入されるであろう証明トークンを含むようになる要求を送信するときに、処理する要求をより少なくすることによって、デバイスアナライザの負担を低減し、ネットワーク帯域幅の消費を低減し、クライアントデバイスにおける待ち時間を低減する。

【0027】

第2のプライバシー問題は、クライアントデバイスの不変の公開鍵をデバイスアナライザと共有することによって、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、複数の別個の証明トークンの受信側は、デバイスアナライザが、同じデバイスからの同じバッチ要求においてそれらの証明トークンを受信したことを知ることができ、したがって、それらの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、その相関に基づいてユーザデータをアグリゲートすることができる。受信側は、そのようなデータを取得するために、デバイスアナライザデータストアと共謀するか、またはデバイスアナライザデータストアを侵害することが必要になる。本明細書で説明する技法は、公開鍵の生の値ではなく、公開鍵のブラインドされたバージョンをデバイスアナライザに送ることによって、そのような追跡に対するプライバシーを向上させることができる。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個のブラインドされた鍵をデバイスアナライザに送ることができ、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生の値を受信することさえなしに、N個の対応するブラインド署名のバッチを返す。

【0028】

説明する証明トークンは、トークン内の満了時間を符号化する困難を増し、トークンのセキュリティを高めるために、説明するブラインド化方式のために限られた情報量のみを符号化し得る。たとえば、限られた情報量の存在下でトークンの存続期間を制限する1つの方法は、トークンを生成するために使用される発行鍵の存続期間の間のみに有効になるように、各トークンを定義することである。

【0029】

トークン生成および償還プロセスは、制限されたコンテンツおよび/もしくはリソースを提供する、証明トークンを要求する当事者、またはそれを通してユーザが制限されたコンテンツおよび/もしくはリソースにアクセスしている当事者のいずれかと、PIIが共有されることを防止し、リソースおよび/またはコンテンツアクセスデータフローの一部として、既存のシステムと統合され得る。このプロセスは、ユーザのプライバシー、エクスペリエンス、ならびにリソースおよび/またはコンテンツへのアクセスを向上させると同時に、ユーザの側の追加の労力を必要とすることなしに、仲介者プラットフォームおよびウェブサイトの機能を拡張し、証明トークンを要求する当事者の到達範囲を増す。さらに、このプロセスは、トークンを要求する当事者が、認証されているユーザが誰であるか、またはどのようにトークンが作成されているかに関するいかなる情報を受信することも必要としない。受信する当事者は、特定のリソースおよび/もしくはコンテンツにアクセスしようとしているユーザもしくはデバイスが認証されたこと、それらの識別情報が許可された当事者として検証されたこと、またはそれらが他の方法で特定のレベルまで信用できることを示す、証明トークンを受信するにすぎない。受信する当事者はまた、要求側クライアント

デバイス/ユーザが、正しいユーザ/認証されたユーザであることを保証するために、それらの識別情報も保証される。

【0030】

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】

【0031】

【図1A】デジタルコンテンツが配信される環境のブロック図である。

【図1B】証明トークンを要求し、発行し、償還するための例示的なプロセスのデータフロー図である。

【図2】N個の証明トークンのバッチを要求し、受信するための例示的なプロセスを示すフロー図である。

【図3】証明トークンを送り、受信し、確認するための例示的なプロセスを示すフロー図である。

【図4】N個のブラインド署名された証明トークンのバッチを要求し、受信するための例示的なプロセスを示すフロー図である。

【図5】ブラインド署名された証明トークンを送り、受信し、確認するための例示的なプロセスを示すフロー図である。

【図6】例示的な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】

【0032】

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。

【0033】

概して、本明細書で説明するシステムおよび技法は、ブラウザのサンドボックス環境内でアクセスされるウェブサイトなどの隔離環境と、クライアントデバイス、およびコンテンツパブリッシャーなど、隔離環境の外部の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。セキュアなサンドボックス環境内では、コードが隔離環境内で安全に実行され得る。しかしながら、環境のセキュリティを維持するために、環境の内部で実行するコードは、環境の外部の情報へのアクセスを有していないことがある。たとえば、ウェブブラウザは、デバイスおよび/または行われている要求の真正性など、デバイスレベル情報へのアクセスを有していないことがある。いくつかの実装形態では、ウェブブラウザは、別個のオンデバイスの「デバイス完全性検証」サブシステムがアクセスすることができる同じ生の入力情報にアクセスすることが可能であり得るが、その情報をデバイス完全性判定に変換する実際のプロセスは、ブラウザ自体内で技術的に実行不可能であるか、または繰り返すために重複し得る。次のように説明するシステムおよび技法は、サンドボックス環境の外部からサンドボックス環境の内部へのパイプラインを提供する。このプロセスは、データを偽造することができないので、セキュリティを保証し、また、ユーザアクティビティを追跡するために、データを使用することができないので、プライバシーを保証する。

【0034】

クライアントデバイスおよび/または他のコンテンツパブリッシャーもしくはプロバイダなどの外部エンティティは、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ために、証明トークン(または、償還されたトークンのための償還記録)を、ネットワーク上で要求および他のデータ送信とともに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削除するための)要求、ならびに/またはコンテンツおよび/もしくはリソースへのアクセスのための要求を含み得る。証明トークンを使用して、通信チャネルをセキュアにすることは、隔離環境または証明トークンが提供される要求側の当事者のいずれかへのいかなるデータ漏洩も防止することによって、ユーザプライバシーおよびデータセキュリティを保証する。証明トークンは、クライアントデバイスの認証を偽造することができないこと、およびPIIが送信されないよ

10

20

30

40

50

うに、ユーザプライバシーが保護されることを保証する、確認のいくつかのレイヤを含む。償還プロセス、およびトークン自体ではなく、それに対するアクセスが要求されるウェブサイト、またはそこからのリソースが要求されているロケーションに提供されるセキュリティ信号としての、署名付き償還結果の使用は、クライアントデバイス/ユーザアクティビティを追跡するために、またはユーザの識別情報を決定するために、トークンを使用することができないことを保証する。

【0035】

いくつかの手法では、証明トークンは、信用できるプログラムの秘密鍵を使用してデジタル署名され得る。信用できるプログラムは、秘密鍵を秘密に維持することができる。証明トークンは、とりわけ、秘密鍵に対応する公開鍵、ペイロード、および証明トークンを含み得る。証明トークンは、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証明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決定されるような、クライアントデバイスの完全性のレベルを示す判定を含み得る。証明トークンはまた、証明トークンをクライアントデバイスにバインドするために、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)を含み得る。

【0036】

証明トークンは、証明トークン発行サーバによって、証明トークン発行サーバが秘密に保つ秘密鍵を使用してデジタル署名され得る。この秘密鍵に対応する公開鍵が、受信側システムに提供され得、受信側システムが、たとえば、公開鍵を使用して、証明トークンのデジタル署名を検証することによって、クライアントデバイスが証明トークン発行システムによって評価されたことを信用することができるようになる。2つの鍵ペアを使用するこの組合せは、受信側がクライアントデバイスの完全性およびクライアントデバイスから受信された通信の完全性を確認することを可能にし、他のデバイスが証明トークンを使用してそれらの完全性を偽造することができないように、証明トークンをクライアントデバイスにバインドする、セキュアな通信チャネルを提供する。

【0037】

いくつかの手法では、証明トークン発行システムは、証明トークンに含めるための公開鍵の生データを受信しない。代わりに、信用できるアプリケーションは、ブラインド署名方式を使用して、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、ブラインドされた公開鍵または公開鍵のブラインドされた派生物(たとえば、公開鍵のブラインドされた切捨て暗号ハッシュ)を送ることができる。ブラインド署名方式では、証明トークン発行システムは、クライアントデバイスの公開鍵の生の値を受信することなしに、クライアントデバイスの完全性を証明することができ、公開鍵を介した潜在的な追跡のリスクを低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プライバシーを向上させる。証明トークン発行システムは、受信側がブラインド署名を検証するために使用することができる、ブラインド署名検証鍵を公開することができる。

【0038】

他の手法では、グループ署名方式が、グループマネージャとして、証明トークン発行サーバとともに使用され得る。たとえば、証明トークン発行サーバは、M個の信用性グループのためのM個のグループ検証鍵を公開し、クライアントデバイスをM個の信用性グループのうちの1つに割り当て、匿名証明書をクライアントデバイスに送達することができる。クライアントデバイスは、匿名証明書を使用して、証明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用して、受信側によって検証され得る。グループ署名方式では、証明トークン発行サーバも証明トークンの受信側もクライアントデバイスの公開鍵の生の値を受信する必要がなく、公開鍵を介した潜在的な追跡のリスクを低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プライバシーをさらに向上させる。

【0039】

図1Aおよび図1Bは、証明トークンを要求し、発行し、償還するためのシステム100お

10

20

30

40

50

よびプロセス190の一例を示す。図1Aは、デジタルコンテンツが配信される環境100のブロック図である。図1Bは、たとえば、図1Aに示された環境100内で、証明トークンを要求し、発行し、償還するための例示的なプロセス190のデータフロー図である。例示的な環境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、コンテンツプラットフォーム150、証明トークン発行(ATI: attestation token issuing)サーバ170(トークン発行システムと呼ばれることもある)、およびデバイス完全性システム180(デバイス完全性コンピューティングシステムと呼ばれることもある)を接続する。例示的な環境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、コンテンツプラットフォーム150、および証明トークン発行サーバ170を含み得る。

10

【0040】

1つの特定の例では、クライアントデバイスのユーザは、ユーザおよび/またはクライアントデバイス110の認証を要求するウェブサイトからのリソースおよび/またはコンテンツにアクセスすること、またはそれを要求することを試みることができる。図1Aに示されたシステム、および図1Bに示されたプロセスは、ユーザがリソースおよび/またはコンテンツにアクセスするための、またはそれを要求するためのシームレスな方法を提供すると同時に、リソースおよび/またはコンテンツを提供するエンティティに、そのユーザおよび/またはクライアントデバイスが、リソースにアクセスすることまたはそれを要求することを許可される正当なユーザであるという、検証を提供する。

20

【0041】

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であるか、またはそれを含み得る。例示的なウェブサイトは、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むことができる、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。

【0042】

リソース145は、ネットワーク105を介して提供され得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。

30

【0043】

コンテンツプラットフォーム150は、様々な異なる関連しないリソースおよび/またはドメインへのアクセスを提供するプラットフォームである。コンテンツプラットフォーム150は、互いにまたはコンテンツプラットフォーム150に関連付けられないリソースへのアクセスを提供することができる。たとえば、コンテンツプラットフォーム150は、ビデオホスティングプラットフォーム、画像ホスティングプラットフォーム、ブログなど、様々な他のウェブサイトからのコンテンツへのアクセスを提供する、ソーシャルメディアプラットフォームであり得る。コンテンツプラットフォーム150は、様々なコンテンツパブリッシャーと通信することができ、かつ/またはそれらと統合され得る。たとえば、コンテンツパブリッシャー160は、コンテンツプラットフォーム150がそれへのアクセスを提供するリソースを含む、異なるウェブサイトであり得る。いくつかの実装形態では、コンテンツパブリッシャー160は、ウェブサイト140と同様の異なるウェブサイトであり得、リソース145と同様のリソースへのアクセスを提供することができ

40

50

る。たとえば、コンテンツパブリッシャーメイン160-3は、そのユーザによってアップロードされた画像へのアクセスを提供する、画像ホスティングウェブサイトであり得る。いくつかの実装形態では、コンテンツプラットフォーム150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に代わってデジタルコンポーネントを選択するエンティティ、コンテンツ発行パートナー152を通して、リソースへのアクセスを要求および提供することができる。

【0044】

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、ウェアラブルデバイス(たとえば、スマートウォッチなど)、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はまた、ゲームデバイスまたはストリーミングデバイスであり得る。クライアントデバイス110は、一般に、ネットワーク105を介したデータの送受信を円滑にするために、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、ネイティブ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。

【0045】

クライアントデバイス110は、1つまたは複数の秘密鍵112と、1つまたは複数の対応する公開鍵113とを含み得る。秘密鍵112および公開鍵113は、アプリケーション111、信用できるプログラム114、および/またはクライアントデバイス110上の他のプログラムによって維持され得る。クライアントデバイス110は、秘密/公開鍵ペアの1つまたは複数の異なるセットを記憶することができる。いくつかの実装形態では、秘密鍵112および公開鍵113は、セキュアなストレージ115に記憶される。

【0046】

クライアントデバイス110はまた、それに対してユーザまたはクライアントデバイス110が認証された、信用できるプログラム114も含み得る。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のネイティブアプリケーションであり得る。たとえば、信用できるプログラム114は、デバイスのオペレーティングシステム、またはそれに対してクライアントデバイス110が認証される特定のエンティティに関連付けられる、クライアントデバイス110上の実行のためのアプリケーションであり得る。

【0047】

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からの通信をセキュアにする際に使用するための他のアプリケーションに、証明トークンを発行することができる。いくつかの実装形態では、信用できるプログラム114は、それにクライアントデバイス110がリソースおよび/またはコンテンツを要求し、認証を必要とする、エンティティによって信用される。たとえば、信用できるプログラム114は、証明トークンを要求するエンティティによって信用されるプログラムであり得る。一例では、信用できるプログラム114は、アプリケーション111を通してアクセス可能であるエンティティのためのウェブベースのインターフェースであり得る。いくつかの実装形態では、信用できるプログラム114は、証明トークンを要求するエンティティに関連付けられる。たとえば、信用できるプログラム114は、例示的な報道機関によって維持されたモバイルアプリケーションであり得る。例示的な報道機関は、有料加入者によってアクセス可能であるニュースコンテンツと、すべてのビジターにとってアクセス可能であるニュースコンテンツとを作成および維持することができる。

【0048】

証明トークン発行(ATI)サーバ170は、信用できるプログラム114によって要求された証明トークンを生成する。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。一例では、信用できるプログラム114は、オペレー

10

20

30

40

50

ティングシステム、オペレーティングシステムの一部、ウェブブラウザなどであり得る。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。

【0049】

信用できるプログラム114は、クライアントデバイス110に対してローカルであってよい。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に対して完全にローカルに動作し、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に対してローカルに、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することができる。たとえば、信用できるプログラム114は、ネットワーク105を介して情報を送信および受信する、ユーザデバイス110上にインストールされたモバイルアプリケーションであり得る。

【0050】

信用できるプログラム114は、以下でより詳細に説明するように、暗号鍵(たとえば、公開/秘密鍵ペア)を生成し、暗号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、証明トークンをセキュアなストレージ115に記憶し、証明トークンを生成し、暗号鍵また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および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、デバイス完全性クライアントと対話して、デバイス完全性システムにデータを送り、デバイス完全性システムからデータを受信する。いくつかの実装形態では、信用できるプログラム114は、たとえば、ユーザプライバシー設定を変更するための要求など、指定されたタイプの要求のセットの各々について、証明トークン122のための要求を生成するように構成される。

【0051】

証明トークンは、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ためにエンティティによって使用され得る。たとえば、いくつかのエンティティは、たとえば、それらのエンティティが通常はそれへのアクセスを有していないことがあるデータへのアクセスを獲得するために、それとともにコンテンツが提供されるようになる異なるリソースを指定するために、および/またはそれに対してコンテンツが提示されるようになる異なるユーザを指定するために、リソースまたはコンテンツ要求のパラメータを偽造しようと試みることがある。加えて、一部の悪意のある当事者は、不正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ことがある。

【0052】

システム100によって実行されるプロセスでは、証明トークンが、ATIサーバ170に償還されて、署名付き償還結果(SRR:signed redemption result)が生成される。署名付き償還結果は、証明トークンが正常に償還されたか否かを示すが、ユーザ識別子、トークンが生成された時間、トークンが償還された時間、信用できるプログラム114によって提供される確認情報、またはユーザの他のPIIなどの情報を含まない。署名付き償還結果はまた、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ためにエンティティによって使用され得、証明トークンの代わりに使用され得る。トークン償還および確認プロセスを実行するのではなく、署名付き償還要求を確認として受け入れることによって、システム100によって実行されるプロセスは、要求およびユーザが認証されたことを保証しながら、ユーザのプライバシーを保護する。いくつかの実装形態では、署名付き償還結

10

20

30

40

50

果は、要求の完全性を確認するために、証明トークンに加えて使用され得る。

【0053】

このシステムの文脈では、証明トークンと署名付き償還結果の両方が、エンティティによって、ユーザが要求されたコンテンツまたは情報などの他のデータを受信するために認証されることを検証するために使用される。署名付き償還結果は、ATIサーバによって署名され、ユーザが、要求側ユーザを識別するデータ、またはユーザが認証される程度もしくはユーザの認証のレベルなどの他の情報を提供することなしに、要求されている特定のデータを受信するために認証されることを証明する。一例では、エンティティは、償還のためにリソースプロバイダに証明トークンを提供することができ、リソースプロバイダは、証明トークンを償還し、償還の結果に署名し、結果上の署名が、証明トークンが前に正常に償還されており、したがって、リソースを要求しているユーザが、要求されたリソースを受信するために認証されることを、エンティティに知らせるために使用され得る。

10

【0054】

証明トークンおよび署名付き償還結果プロセスは、他者が要求を改変することを防止し、要求が確認されたクライアントデバイス110、および代理で許可されたユーザから来たことを保証する、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仲介者を通したセキュアな通信チャネルを提供する。

【0055】

署名付き償還結果は、極めて少量のデータ(たとえば、2ビット)であり得、たとえば、ウェブサイトと、サンドボックス環境の外部で実行するアプリケーションとの間で送信されているデータの量を低減することに加えて、ウェブブラウザなどのサンドボックス環境と、サンドボックス環境の外部で実行するアプリケーションとの間のセキュアな通信チャネルを提供する。いくつかの実装形態では、署名付き償還結果は、2ビットよりも大きいものであり得る。たとえば、署名は、2ビットよりも大きいものを含み得る。いくつかの実装形態では、償還結果と、証明トークン発行サービスがそれへのアクセスを有するクライアントデバイスのデータとの間の共通のビット(すなわち、「結合可能ビット」)の数は、証明トークン発行サービスおよびSRRの受信側との同じユーザまたはデバイスの対話をリンクさせるための観測者の能力を低減するために、制限される。

20

【0056】

たとえば、証明トークンが、証明サービスと結合可能な2ビットのみを含む場合、この限られた情報量は、償還結果など、証明トークンから導出されるいかなる情報も、証明サービスと結合可能な多くとも2ビットを有するようになることを保証する。証明データは、ウェブブラウザと、ウェブブラウザの外部で実行するアプリケーションとの間で直接送信されず、その理由は、証明データの確認と償還の両方が、ATIサーバに対して行われるからである。このプロセスのために、ウェブブラウザの外部で実行するアプリケーションと、ウェブブラウザのセキュアな環境との間で送信されるデータは、証明トークンが提供するのと同じ情報(すなわち、特定のエンティティおよび/または要求が認証されており、エンティティの識別情報が正常に証明されたこと)を通信するが、露出または傍受のリスクがなく、このプロセスは、ユーザのプライバシーを保護する。

30

【0057】

ATIサーバ170は、異なる形式を有する、または異なるコンテンツを含む、異なるタイプの証明トークン122を生成することができる。いくつかの実装形態では、証明トークン122は、ATIサーバ170の公開鍵173と、証明トークン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用してデバイス完全性システムによって、または信用できるプログラム114によって生成される完全性の判定とを含む、データのセットを含む。証明トークン122はまた、証明トークン122およびデータのセット中に含まれる公開鍵173に対応する秘密鍵172を使用して、ATIサーバ170によって生成されたデジタル署名を含み得る。すなわち、ATIサーバ170は、秘密鍵172を使用して、データのセットにデジタル署名し、得られたデジタル署名をデータのセットとともに証明トークン122中に含めることができる。いくつかの実

40

50

装形態では、証明トークンは、ペイロード内でユーザのクレデンシャルを含む。

【0058】

図1Aおよび図1Bに関して説明したプロセスでは、ATIサーバ170は、証明トークンを生成および償還し、各エンティティが証明トークンシステムを作成および維持することを必要とすることなしに、証明トークンのセキュリティ上の利益を提供し、さらなるプライバシー上の利益をユーザに提供する。証明トークンが生成されるプロセスについて、以下で図2～図7に関して説明する。追加として、証明トークンシステムのみが検証データを必要とするように、要求プロセスがトークン償還プロセスを含むので、それによって、ユーザのPIIの転送およびそれへのアクセスを制限しながら、ユーザのプライバシーを保護し、証明トークンの利益を提供する。

10

【0059】

いくつかの実装形態では、証明トークンは、セキュリティ対策として、あらかじめ決定された時間期間内に満了するように設定され得る。証明トークンが満了するとき、証明トークンを必要とすることによって、ATIサーバ170は、トークンが定期的に要求されなければならないこと、およびしたがって、その識別情報が証明されているエンティティが定期的に認証されることを保証することができる。

【0060】

証明トークンが満了するとき、ATIサーバ170における対応するデータが、証明トークンを後で償還することができないことを保証するために更新され得る。いくつかの実装形態では、ATIサーバ170は、トークンを償還し、署名付き償還結果を生成するか否かを決定するより前に、証明トークンの寿命などのデータを査定する。

20

【0061】

いくつかの実装形態では、証明トークン122は、ペイロードデータを含むデータのセットと、証明トークン122が作成される時間を示す証明トークン作成時間と、データのセットのデジタル署名とを含む。この例では、ATIサーバ170は、グループ署名方式と、デバイス完全性システムまたはATIサーバ170によってクライアントデバイス110に発行された証明書とを使用して、デジタル署名を生成することができる。

【0062】

一般に、証明トークンの受信側は、次いで、証明トークンおよび/または証明トークンに含まれる完全性判定(適切な場合)を確認する。証明トークンが正常に確認される場合、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否かを決定し、それに応じて要求を処理することができる。証明トークンが正常に確認されない場合、受信側は、たとえば、要求に応答することなしに、または要求に応答してデータを変更することなしに、要求を無視または削除することができる。

30

【0063】

証明トークン作成時間は、証明トークン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が証明トークンを作成する作成時間を記録することができる。この証明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、ミリ秒、またはマイクロ秒の精度)とすることができる。証明トークン作成時間は、証明トークン122を含む要求120が新しい要求であるか、または最近の要求であるかを決定するために使用され得る。たとえば、証明トークン122を受信するエンティティは、トークン作成時間を、現在時間または証明トークン122が受信された時間と比較することができる。2つの時間の間の差がしきい値を超える場合、エンティティは、以下でより詳細に説明するように、要求が新しいものではない、または無効であると決定することができる。

40

【0064】

証明トークン作成時間は、リプレイアタックを検出するためにも使用され得る。たとえば、同じ証明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、要求が複製であること、および/または要求がリプレイアタックの一部であることを決定することができる。

【0065】

50

証明トークン作成時間は、他のデータと組み合わせて、要求のためのトランザクション識別子として働くこともできる。たとえば、トランザクション識別子は、証明トークン122が公開鍵113を含む実装形態では、証明トークン122の証明トークン作成時間および証明トークン122の公開鍵113のうちの2つ以上の組合せであり得る。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120の複数のバージョンを重複排除するために使用され得る。たとえば、ATIサーバ170は、信用できるプログラム114と関連付けられたウェブサイト140の両方から同じ要求を受信することができる。別の例では、ATIサーバ170は、コンテンツプラットフォーム150とコンテンツ発行パートナー152の両方から同じ要求を受信することができる。この例では、トランザクション識別子は、証明トークン122のトークン作成時間および証明トークン122の公開鍵113に基づくことができる。ATIサーバ170は、2つ以上の要求の中の2つのデータを比較して、要求が重複であるか否かを決定することができる。

【0066】

ペイロードは、個々の要求120のためのデータを含み得る。たとえば、ペイロードは、要求されたリソースについての情報(たとえば、リソースのトピック)、リソースのコンテキストについての情報(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)、ユーザがこの機能を有効にした場合の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)、および/または他の適切な情報を含み得る。

【0067】

いずれの例でも、証明トークンが償還され得、償還結果が、アプリケーション111がウェブサイト140に提供するコンテンツのための要求中に含まれ得、ウェブサイトが、要求が有効である、かつ/または許可されたユーザからのものであることを保証することができるようになるが、ユーザのPIIにアクセスすることができないようになる。アプリケーション111は、コンテンツプラットフォーム150、またはリソース145へのアクセスのためにウェブサイト140などの他の受信側に送られる要求中に、SRRを含めることができる。

【0068】

要求120が、パブリッシャー130、コンテンツプラットフォーム150、コンテンツ発行パートナー152、コンテンツパブリッシャードメイン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、ユーザがコンテンツパブリッシャードメイン160-2からユーザのデータのすべてを除去することを選択した場合、ペイロードは、このデータの除去およびコンテンツパブリッシャードメイン160-2を指定するデータ(たとえば、コンテンツパブリッシャードメイン160-2のため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。

【0069】

デバイス完全性システム180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さらに評価することができる。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)のレベルを決定する。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否か、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として動作しているか、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決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、証明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、これらの信号を証明トークンのための要求中に含めることができる。

【0070】

10

20

30

40

50

デバイス完全性システム180は、クライアントデバイス110の信用性(または完全性)のレベルを示す判定を発行することができる。受信側は、判定を使用して、その判定を含む要求120を信用するか否かを決定する。たとえば、判定が、クライアントデバイス110が信用できないことを示す場合、受信側は、たとえば、要求に応答しないなど、要求を無視することができる。

【0071】

いくつかの実装形態では、図1～図7に関して説明するプロセスは、信用できるプログラム114が、それに対してユーザが認証されたウェブサイトであり、ウェブサイト140が、それに対してユーザがアクセスを要求しているか、またはそこからのリソースをユーザが要求している、プログラムまたはアプリケーションであるように実行され得る。

【0072】

アプリケーション111が、特定のリソース145または他のコンテンツへのアクセスのために、ネットワーク105上で要求を送るとき、アプリケーション111は、プライバシー保護技法を使用して、ユーザの識別情報、真正性、および/または許可ステータスを証明することができる。このプライバシー保護技法は、そこからのリソースまたは他のコンテンツが要求されるアプリケーション111またはウェブサイト140のいずれかに、ユーザを識別またはさもなければ追跡するために使用され得る情報を提供することなしに、証明トークンが生成および償還されることを可能にする。プライバシー保護技法を実行するための例示的なプロセス190が、図1Bに示されている。

【0073】

ステップAにおいて、アプリケーション111は、1つまたは複数の証明トークンのための要求120を生成し、信用できるプログラム114にトークン要求120を提供することができる。たとえば、アプリケーション111は、それを通してクライアントデバイス110のユーザが、ウェブサイト140などの様々なウェブサイトアクセスしている、かつ/または、エンティティの中でも、リソース145、パブリッシャー130、およびコンテンツプラットフォーム150などの様々なリソースへのアクセス、もしくはそこからのコンテンツを要求している、ウェブブラウザであり得る。この例では、信用できるプログラム114は、そこからのリソースをアプリケーション111が要求しているか、またはそれへのアクセスをアプリケーション111が要求している、エンティティによって信用される、クライアントデバイス110上のアプリケーションであり得る。一例では、信用できるプログラム114は、スマートフォンのために例示的な報道機関によって作成およびホストされたアプリケーションであり得、ユーザは、例示的な報道機関によってホストされたウェブサイト140上のニュース記事への、ウェブブラウザ111上のニュースアグリゲータを通じたアクセスを要求中であり得る。

【0074】

クライアントデバイス110のユーザは、信用できるプログラムに対してユーザが認証されるように、信用できるプログラム114にログインクレデンシャルを提供することができる。たとえば、ユーザは、例示的な報道機関での自分のアカウントのためのユーザ名およびパスワードを使用して、例示的な報道機関にサインインすることができる。アカウントは、無料アカウントまたは有料サブスクリプションアカウントであり得、ユーザは、ログインクレデンシャルを有していないユーザが閲覧、アクセス、および/または受信するための許可を有していない、特定のコンテンツおよび/またはリソースへの追加の許可を与えられ得る。たとえば、例示的な報道機関は、いかなるログインクレデンシャルも有していないユーザに、その記事のあるサブセットへのアクセスを提供し、有料サブスクリプションなしのアカウントのためのログインクレデンシャルをもつユーザに、その記事のより大きいサブセットへのアクセスを提供し、有料サブスクリプションをもつアカウントのためのログインクレデンシャルをもつユーザに、記事およびコンテンツのその完全なアーカイブへのアクセスを提供し得る。

【0075】

アプリケーション111は、ウェブサイト140、コンテンツプラットフォーム150、およ

10

20

30

40

50

び/または他のエンティティからの証明または完全性情報のための要求を受信することなしに、ステップAを実行することができる。たとえば、アプリケーション111は、一定の間隔において、証明トークン要求120を信用できるプログラム114に送信して、証明トークンをリフレッシュすることができる。いくつかの実装形態では、証明データが正確なままであることを保証するために、およびサードパーティまたは悪人が許可なしに証明データにアクセスし、証明データを使用する可能性を低減するために、証明トークンは、あらかじめ決定された時間期間後に満了することができる。証明トークンが満了するとき、アプリケーション111は、満了した証明トークンを削除し、証明トークンのための要求120を自動的に生成し、信用できるプログラム114に要求を提供することができる。

【0076】

ステップBにおいて、信用できるプログラム114は、証明トークンのための署名付き要求を生成し、証明トークン発行(ATI)サーバ170などのトークン発行サーバが、信用できるプログラム114によって提供された情報に基づいて、ユーザの識別情報を証明する証明トークンを生成することを可能にすることができる。

【0077】

たとえば、例示的な報道機関によって作成およびホストされたスマートフォンアプリケーション114は、証明トークンのための要求121を作成し、ATIサーバ170に要求を提供することができる。この要求は、要求に関する完全性情報を示すために、例示的な報道機関アプリケーション114によって署名され得る。たとえば、要求は、要求がログインクレデンシャルを有するユーザに代わって行われているか否か、および/またはログインクレデンシャルのタイプ(すなわち、無料アカウント、最上位の有料サブスクリプションアカウント、共有ファミリープランのアカウントなど)を示すために、例示的な報道機関スマートフォンアプリケーション114によって署名され得る。いくつかの実装形態では、要求上の署名は、要求および/またはエンティティが認証されるか否かの判定を提供することができる。たとえば、例示的な報道機関アプリケーションは、要求が正当であり、かつ/またはユーザが有効なクレデンシャルを使用して、アプリケーションを通して、例示的な報道機関で認証されたと決定することができる。次いで、例示的な報道機関アプリケーション114は、要求121とともに認証の判定を含めることができる。

【0078】

いくつかの実装形態では、要求121は、要求121を作成するためのアプリケーション111からの要求120を使用して、信用できるアプリケーション114によって生成された新しい要求である。いくつかの実装形態では、要求120は、要求および/またはユーザの妥当性を示すために、信用できるアプリケーション114によって署名され、署名付き要求120が、要求121として送信される。いくつかの実装形態では、信用できるアプリケーション114によって提供された要求120および妥当性情報が、要求121として一緒に送信される。

【0079】

アプリケーション111は、証明トークンを直接要求していないので、アプリケーション111は、証明トークンのための要求中に含まれた情報へのアクセスを必要とせず、したがって、ユーザのPIIへのアクセスを有することなしに、特定のリソースへのアクセス、および/またはコンテンツの配信を容易にすることができる。これによって、証明プロセスが、ユーザのプライバシーを保護するシームレスな方法で実行されることが可能になる。アプリケーション111は、図1Aおよび図1BのステップC~Iに関して以下で説明するように、証明トークンを受信、記憶、および償還することが可能であるが、アプリケーション111は、アクセスするための許可をユーザがアプリケーション111に与えたPII以外に、ユーザが信用できるプログラム114に提供するPIIを直接受信しないか、またはそれへのアクセスを有していない。したがって、ユーザのプライバシーを保護することに加えて、説明する証明トークン生成および償還プロセスは、アプリケーション111が、ユーザからのPII情報を必要とすることなしに、コンテンツアグリゲーションなどの機能を提供することをさらに可能にする。このプロセスは、システムの機能を向上させ、情報のよりセキュアなフローを作成し、必要とされるユーザの入力の量を低減する。

10

20

30

40

50

【0080】

図1Aおよび図1Bに関して説明するプロセスは、署名の2つの異なるセットを含み、信用チェーンにおいて2つのステップを提供する。証明トークン発行者は、証明トークンおよび/または署名付き償還結果に署名し、ウェブブラウザは、ウェブサイトおよび/またはリソースの一部分にアクセスするための要求上で署名を含める。

【0081】

上記で説明したように、いくつかの手法では、信用できるプログラム114、アプリケーション111、またはクライアントデバイス110は、証明トークン要求(および、デバイス公開鍵に関連付けられたデバイス完全性判定)とともに、1つまたは複数の秘密/公開鍵ペアを含めることができる。いくつかの実装形態では、秘密/公開鍵ペアは、複数の証明トークンにわたって変更されて、証明トークン受信側による追跡に対するクライアントデバイスまたはユーザのプライバシーを向上させることができる。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、証明トークンの対応するバッチを証明トークン発行サーバから取り出すことができるので、証明トークンの再使用が低減または排除される。このバッチプロセスの例示的な例が、図2に示されている。

【0082】

ステップCにおいて、ATIサーバ170は、証明トークンを発行する。このトークン発行ステップは、多数の異なる部分を含み得る。概して、ATIサーバ170は、要求側クライアントデバイスおよび/またはユーザの識別情報を証明する極めて少数のビットを搬送する証明トークンを発行する。証明トークンを発行するより前に、ATIサーバ170は、要求が有効であることを検証し、ウェブサイト140、リソース145、コンテンツパブリッシャードメイン160、および/またはそれに対してSRRが提供される任意の他のエンティティのための追加のセキュリティレイヤを提供することができる。

【0083】

たとえば、ATIサーバ170は、要求121上の署名を検証することができる。いくつかの実装形態では、上記で説明したように、信用できるプログラム114は、要求121上でブラインド署名を提供することができる。いくつかの実装形態では、証明トークン発行サーバは、証明トークンに含めるための公開鍵の生データを受信しない。代わりに、クライアントデバイスは、ブラインド署名方式を使用して、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、ブラインドされた公開鍵または公開鍵のブラインドされた派生物(たとえば、公開鍵のブラインドされた切捨て暗号ハッシュ)を送ることができる。ブラインド署名方式では、証明トークン発行サーバは、クライアントデバイスの公開鍵の生の値を受信することなしに、クライアントデバイスの完全性を証明することができ、公開鍵を介した潜在的な追跡のリスクを低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プライバシーを向上させる。証明トークン発行サーバは、受信側がブラインド署名を検証するために使用することができる、ブラインド署名検証鍵を公開することができる。

【0084】

ATIサーバ170が要求の妥当性を検証すると、ATIサーバ170は、信用できるプログラム114および/または信用できるプログラム114に関連付けられたエンティティに対して、クライアントデバイス110および/またはユーザの識別情報を証明する、証明トークン122を発行することができる。

【0085】

ステップCにおいて発行される証明トークンの数は、ステップAおよび/またはステップBにおいて要求された証明トークンの数に直接対応し得る。たとえば、アプリケーション111は、ステップAにおいて5つの証明トークンを要求することができ、信用できるプログラム114は、ATIサーバ170に5つの証明トークンのための要求を提供することができる。要求および/または発行されることになる証明トークンの数は、アプリケーション111、信用できるプログラム114、クライアントデバイス110、および/またはATIサーバ170によって決定され得る。

【0086】

いくつかの実装形態では、ATIサーバ170は、要求される証明トークンの数から、発行される証明トークンの数を変更することができる。たとえば、ATIサーバ170は、様々なソースから要求された証明トークンの平均数に基づいて、要求に応答して発行するための証明トークンの数を自動的に決定することができる。ATIサーバ170は、セキュリティとトラフィックの低減とのバランスをとることによって、要求に応答して発行するための証明トークンの数を決定することができる。より多くのトークンを発行することによって、トークンが要求および次いで発行されなければならない回数が低減されるが、要求の妥当性およびアプリケーション111のユーザの識別情報が検証される頻度も低減される。

【0087】

いくつかの実装形態では、ステップCにおいて発行される証明トークンの数は、発行される証明トークンの最大数に依存する。たとえば、証明トークン受信側は、(1)各個々のクライアントデバイスもしくは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、選択された時間フレーム内に送られ得るトークンの数の制限(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、選択された時間フレーム内に送られ得るトークンの数の制限(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、選択された時間フレーム内に送られ得るトークンの数の制限、(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、選択された時間フレーム内に送られ得るトークンの数の制限、または(5)そのような制限のうちの2つ以上の任意の組合せを公開することができる。

【0088】

証明トークン122自体は、ベアラが認証されるか否かを示す、単一ビットの情報であり得る。たとえば、0の値は、ベアラが認証されないことを示すことができ、1の値は、ベアラが認証されることを示すことができる。

【0089】

ATIサーバ170がアプリケーション111に発行する応答は、証明トークン122自体を含み得、1または複数の暗号化されたビットの情報をさらに含み得る。いくつかの実装形態では、追加のビットの情報が証明トークン122中に含まれ得るので、証明トークン122が、ベアラが認証されるか否かを示す1ビット、および1または複数のビットの追加の情報を含むようになる。たとえば、発行の時間に、ATIサーバ170は、検証されたユーザクレデンシャルまたは他のデータなど、アプリケーション111のセキュアなサンドボックス環境の外部から、アプリケーション111のセキュアなサンドボックス環境の内部に渡されることになる、1ビットの秘密メタデータを含み得る。

【0090】

ATIサーバ170は、複数の秘密署名鍵をさらに使用して、証明トークンに署名することができる。これらの秘密署名鍵は、ATIサーバ170によって利用可能にされる対応する検証鍵を使用して検証され得、信用チェーンの一部である署名として働く。証明トークンの受信側が、ATIサーバ170によって利用可能にされた対応する検証鍵を使用して、署名鍵を検証することができるとき、受信側は、ATIサーバ170が証明トークンを発行したことを信用することができる。証明トークンに署名するこのプロセスは、たとえば、ブラインド署名方式を使用して実行され得るので、証明トークン発行サーバは、クライアントデバイスの公開鍵の生データを見ないようになる。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、証明トークン発行サーバに公開鍵を送って証明トークンの対応するバッチを取り出す前に、ブラインド署名方式を使用して、公開鍵(または、公開鍵の暗号ハッシュ、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など、ブラインド署名方式のコミットフェーズのための値として使用され得るこれらの公開鍵の好適な派生物)をブラインドすることができる。この例では、証明トークンは、公

10

20

30

40

50

開鍵を使用してブラインド署名される。このバッチプロセスの例示的な例が、図4に示されている。

【0091】

追加として、ATIサーバ170は、ATIサーバ170によって利用可能にされる対応する検証鍵とともに、複数の秘密署名鍵を使用して、ステップCにおいて証明トークンに署名することに関して上記で説明したプロセスと同様のプロセスにおいて、SRRに署名することができる。

【0092】

n個の検証鍵および単一ビットの情報の組合せは、 $n \times 2$ 個の異なる組合せを提供し、これらの組合せは、アプリケーション111によって検証可能であるトークンに、少量の情報をさらに暗号化する。暗号化された情報量は、追加の情報がトークンに暗号化されなかったことを保証するために、ウェブブラウザなどのアプリケーション111によって検証可能であり、その理由は、暗号化の結果が、暗号化されるビット数を明らかにするようになるからである。アプリケーション111が、追加のデータが証明トークンに暗号化されていると決定する場合、アプリケーション111は、トークンを記憶または償還する必要がない。たとえば、アプリケーション111が、トークンを記憶するより前に証明トークンを検証する場合、アプリケーション111は、単にトークンを破棄することができる。たとえば、アプリケーション111が、償還より前に証明トークンを検証する場合、アプリケーション111は、トークンを破棄し、トークンを償還しようとする試みを控えることができる。

【0093】

たとえば、ATIサーバ170が、予想されるビット数よりも多くを証明トークンに暗号化しようと試みる場合、証明トークンは、アプリケーション111によって実行される検査に失敗することになる。アプリケーション111は、たとえば、ATIサーバ170によって提供された公開鍵および/または検証鍵を定期的に検査することができる。次いで、アプリケーション111は、公開鍵を使用して、ATIサーバ170のデジタル署名を検証することができる。しかしながら、検証鍵のいずれも証明トークンを検証しない場合、アプリケーション111は、トークンを償還しようと試みることはなく、そして、証明トークンを破棄し得る。

【0094】

ステップDにおいて、アプリケーション111は、ATIサーバ170から受信された証明トークンを記憶する。たとえば、アプリケーション111は、ATIサーバ170から証明トークン122を受信し、次いで、セキュアなストレージにトークンを記憶する。たとえば、アプリケーション111は、アプリケーション111またはクライアントデバイス110によって維持されるセキュアなキャッシュに、証明トークン122を記憶することができる。

【0095】

ステップEにおいて、証明トークン償還のためのトリガイベントが生じる。いくつかの実装形態では、ウェブサイト140は、アクセスを提供するか、またはリソースを送信するより前に、アプリケーション111からの確認を要求することができる。たとえば、クライアントデバイス110のユーザが、例示的なソーシャルメディアウェブサイト140上で、自分のプロフィールにカスタムの背景を追加するための機能にアクセスしようと試みる場合、例示的なソーシャルメディアウェブサイト140は、その機能へのアクセスを与えるより前に、アプリケーション111からの確認を要求し得る。いくつかの実装形態では、アプリケーション111は、証明トークンを自動的に償還して、使用されることになるSRRのストアを作成することができる。たとえば、アプリケーション111のユーザは、毎日、仕事前の午前7時に例示的なニュースアグリゲーションウェブサイト140にアクセスするパターンを有し得、アプリケーション111は、そこからの記事が例示的なニュースアグリゲーションウェブサイト140上に表示される、様々な例示的なニュースウェブサイト140a、140b、および140cのための証明トークンを自動的に償還することができる。

【0096】

ユーザのプライバシーを保護するために、システム100は、証明トークンが償還される

ことを可能にするトークン償還プロセスを実施し、ATIサーバ170自体に対してトークンの詳細を秘密に保ちながら、ユーザの識別情報を証明する。トークン償還プロセスは、アプリケーション111によって、証明トークンを償還するための要求を生成することを含む。トークン償還要求および証明トークンがATIサーバ170に提供され、ATIサーバ170は、署名付き償還結果(SRR)を生成する。この署名付き償還結果は、証明トークンが正常に償還された(または正常に償還されなかった)ことを示し、ユーザのPII、または償還もしくは使用のパターンを追跡するために使用され得る情報を提供しないものであり、トークン償還要求に応答して、アプリケーション111に提供される。次いで、アプリケーション111は、ユーザの識別情報および/または要求の真正性を証明するために、ウェブサイト140からのリソースまたは他のコンテンツにアクセスするための要求中に、SRRを含めることができる。SRRがウェブサイト140に提供され、証明トークンは提供されないため、ウェブサイト140は、ユーザのPIIへのアクセスを有することなしに、ユーザがリソースにアクセスするための、および/またはコンテンツを受信するための許可を有することを確認することができる。

10

【0097】

いくつかの実装形態では、ATIサーバ170は、特定の発行者のためにいずれかの有効な証明トークンがあるか否かを決定する。所与の発行者のために利用可能なトークンがない場合、ATIサーバ170は、エラーで要求を拒否する。所与の発行者のために利用可能なトークンがある場合、ATIサーバは、要求側エンティティに証明トークンを発行する。発行者は、トークンを消費すること、および、その識別情報が証明されているエンティティのクレデンシャルまたはユーザ情報を露出させることなしに、償還証明が他の当事者に転送されることを可能にするために、SRR応答ヘッダを含む結果に基づいて行動することのいずれも行うことができる。追加として、発行者は、どのくらいの時間(たとえば、秒単位)にわたって、償還記録がキャッシュされるべきであることを示すために、証明トークンおよび/またはSRR内に情報を含め得る。いくつかの実装形態では、その情報が含まれない場合、SRRの存続期間は、償還されたトークンの発行を確認した証明トークン情報の存続期間に結び付けられることになる。いくつかの実装形態では、SRRは、発行者からのバイトの任意のプロブとして扱われる。

20

【0098】

トークン償還プロセス、ならびにSRRを使用して、要求および/またはユーザを認証するプロセスはまた、アプリケーション111のサンドボックス環境の外部からサンドボックス環境に情報を送信するためのセキュアな機構も提供する。従来、ウェブブラウザなどのアプリケーション111にとって、アプリケーションは、セキュアな環境を提供するために、サンドボックス環境の内部で実行しており、他のエンティティおよび情報から隔離される。図1～図8に関して説明するシステムおよびプロセスは、サンドボックスのセキュリティを維持する。

30

【0099】

追加として、SRRの受信側は、トークンの検証および償還を実行していないので、SRRの受信側は、証明トークン情報などの情報を要求または処理する必要がない。これによって、プロセスが、ユーザのプライバシーを保護し、送信されるデータのセキュリティを向上させることが可能になり、その理由は、ユーザが自分のクレデンシャルを信用できるプログラム114に提供しているとき、追加の情報を要求することなしに、証明トークンがアプリケーション111のユーザに発行され得るからである。

40

【0100】

いくつかの実装形態では、ATIサーバ170は、信用できるプログラム114、ウェブサイト140、コンテンツプラットフォーム150、および/または1つもしくは複数のコンテンツパブリッシャーメイン160に関連付けられる。たとえば、ATIサーバ170は、例示的な報道機関モバイルアプリケーション114および例示的な報道機関ウェブサイトを運営するエンティティ、例示的な報道機関によって維持され得る。いくつかの実装形態では、ATIサーバ170は、信用できるプログラム114、ウェブサイト140、コンテンツプラットフォ

50

ーム150、および/または1つもしくは複数のコンテンツパブリッシャーメイン160とは別個のエンティティであり、証明トークンを処理するための開発インフラストラクチャを必要としない。たとえば、ATIサーバ170は、それへのアクセスをユーザが獲得しようと試みているウェブサイト140によって、信用できる証明トークン発行システムとして指定されたサーバであり得る。ウェブサイト140は、証明トークンを処理するためのインフラストラクチャを開発または維持する必要がないようになり、代わりに、ATIサーバ170からの署名付き償還結果を受け入れる。図1Aおよび図1Bに関して説明するシステムおよび/またはプロセスは、ウェブサイト、コンテンツパブリッシャー、ならびに他のコンテンツプロバイダおよびリソースが、どのようにトークンが要求、生成、および/または償還されるかを知らなければならないし、要求が真正であること、および/またはユーザがコンテンツのアクセス/受信を許可されることを検証することを可能にする。

10

【0101】

たとえば、アプリケーション111が、別のエンティティに(たとえば、パブリッシャー130、コンテンツプラットフォーム150、コンテンツ発行パートナー152、またはコンテンツパブリッシャーメイン160に)、そのエンティティによって記憶されたデータを管理、たとえば、削除するための要求を送る場合、この要求は、SRRを含み得る。

【0102】

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とともに、SRRを自動的に送るように構成される。たとえば、証明トークンを要求し、SRRを送る各アプリケーション111は、証明トークンのアクセスおよび/または償還、ならびにSRRのアクセスおよび/または送信をアプリケーション111に行わせる、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。APIは、たとえば、ユーザデータを管理するための要求、そのためにユーザが許可を必要とするリソースおよび/またはコンテンツへのアクセスを要求するための要求など、そのためにSRRが含まれるべきである要求のセットを指定することができる。たとえば、コンテンツのための、または有料加入者のためのニュースウェブページを要求することなど、特定のリソースへのアクセスのための、いくつかのタイプの要求は、SRRを必要とし得る。

20

【0103】

ステップFにおいて、アプリケーション111は、ATIサーバ170にトークン償還要求123を送る。トークンを発行したATIサーバ170に、トークンを償還するこのステップによって、SRRが、証明トークンの代わりに提供されることが可能になる。証明トークンの発行および償還に関連付けられたデータが、ユーザアクティビティを追跡するために追跡可能信号として使用され得るのに対して、署名付き償還結果は、SRRのペアラが証明トークンを正常に償還したという情報のみを提供し、情報の中でも、トークンが償還されたコンテキスト、トークンが償還された時間、および/またはトークンが発行されるより前に提供された認証情報など、潜在的に機密、識別可能、または追跡可能な情報を提供しない。

30

【0104】

アプリケーション111は、トークン償還要求123とともに、償還のための証明トークンを示すデータを送信する。いくつかの実装形態では、トークン償還要求123は、償還のための証明トークンを含む。いくつかの実装形態では、アプリケーション111は、トークン償還要求123とともに証明トークンを送信する。いくつかの実装形態では、アプリケーション111は、クライアントデバイス110のユーザに、証明トークンの発行の成功を示すデータを送信する。

40

【0105】

償還時間に、ATIサーバ170がトークン償還要求123を受信するとき、ATIサーバ170は、証明トークンも受信する。証明トークンが正当であり、検証可能である場合、証明トークンは、ATIサーバ170が前に発行し、アプリケーション111によって記憶されたトークンである。ATIサーバ170は、トークン償還要求123とともに証明トークンを受信し、情報のビットおよび暗号鍵の可能な組合せのうちの1つを抽出する。上記で説明したビットは、証明トークンのペアラが検証されたか否かを示す。いくつかの実装形態では、利用可

50

能な複数の異なる暗号鍵が、証明トークンおよび認証のレベルに関する追加の情報を提供することができる。たとえば、異なる公開鍵は、異なるレベルの許可または異なるレベルの認証を示すことができる。いくつかの実装形態では、トークン情報は、アプリケーション111によって記憶するより前に検証され、また、ATIサーバ170によっても、トークンがATIサーバ170自体によって発行されたことを検証するために、およびアプリケーション111がトークンを修正していないことを保証するために、償還より前に検証され得る。

【0106】

ステップGにおいて、ATIサーバ170は、署名付き償還結果124を生成し、アプリケーション111に送信する。ATIサーバ170が、トークン償還要求123において示された証明トークンが有効である、かつ/またはATIサーバ170自体によって発行されたことを検証すると、ATIサーバ170は、償還結果を生成し、次いで償還結果に署名することができる。ATIサーバ170からの署名は、信用チェーンにおいて追加のリンクを追加し、署名付き償還結果の受信側が、ユーザのアクティビティまたは識別情報を追跡するために使用され得る追加の情報を受信側に提供することなしに、証明トークンがATIサーバ170に償還されたことを信用することを可能にする。

【0107】

ATIサーバ170は、たとえば、証明トークンに関連付けられた1つまたは複数のデジタル署名が偽造されていないことを検証することによって、トークン償還要求123において示された証明トークンを検証する。たとえば、ATIサーバ170は、ステップCにおいて説明したように、ATIサーバ170自体がそれを用いて証明トークンに署名した1つまたは複数のデジタル署名が、偽造されていないことを検証することができる。ATIサーバ170は、その秘密鍵を使用して、証明トークンを解読することによって、この検査を実行することができる。

【0108】

いくつかの実装形態では、ATIサーバ170は、トークン償還要求123が正当であることを保証するために、たとえば、アプリケーション111からの1つまたは複数のデジタル署名が偽造されていないことを検証することができる。たとえば、ATIサーバ170は、署名データを、アプリケーション111によって公開された1つまたは複数の公開鍵と比較することができる。いくつかの実装形態では、デジタル署名は、単に、要求がアプリケーション111によって生成されたことを示す、トークン償還要求123とともに提供されたメタデータであり得る。

【0109】

いくつかの実装形態では、ATIサーバ170は、メトリックおよび特性の中でも、償還時間、償還のためのコンテキスト、および/または証明トークンが発行された時間など、追加のトークンデータを検証することができる。いくつかの実装形態では、ATIサーバ170は、その下で特定のタイプの証明トークンが償還され得る特定のコンテキストを識別し得、現在のコンテキストが、証明トークンが償還され得る有効なコンテキストであるか否かを検証することができる。たとえば、ATIサーバ170は、特定のウェブサイト140から、加入者限定クロスワードゲームにアクセスするための証明トークンが、クロスワードゲームにアクセスしようと試みるときのみに償還され得るという、情報を受信し得る。しかしながら、トークン償還要求123は、加入者限定クロスワードゲームにアクセスするための証明トークンが、加入者限定クロスワードゲームにアクセスするための試みが行われたことを示すデータなしに、償還されていることを示し得る。次いで、ATIサーバ170は、償還のためのコンテキストが満たされないと決定し得、アクションの中でも、償還の拒否もしくは不成功の指示を送信すること、証明トークンを無効化すること、および/または単にトークン償還要求に応答しないことのいずれかによって、トークン償還要求を拒否し得る。

【0110】

いくつかの実装形態では、ATIサーバ170は、証明トークンが、トークン償還要求123が受信される時間に満了しているか否かを決定し得る。たとえば、ATIサーバ170は、証明トークンに関連付けられた作成時間に基づいて、どのくらいの時間に証明トークンが未

10

20

30

40

50

解決であるか、および証明トークンが満了したか否かを決定することができる。一例では、ATIサーバ170は、研究データベース上で検索を実行するためのアクセスのための証明トークンが、償還されるために25分未満の古さでなければならないと決定することができる。後で、ATIサーバ170が、1週間の古さである、研究データベース上で検索を実行するためのアクセスのための証明トークンを示す、トークン償還要求123を受信する場合、ATIサーバ170は、証明トークンが満了したと決定し得、アクションの中でも、償還の拒否もしくは不成功の指示を送信すること、証明トークンを無効化すること、および/または単にトークン償還要求に応答しないことのいずれかによって、トークン償還要求を拒否し得る。証明トークンのための満了期間は、10秒、15分、3時間、6日、2週間など、任意の時間量であり得る。

10

【0111】

ATIサーバ170が、証明トークンおよび/またはトークン償還要求のその検証を完了すると、ATIサーバ170は、署名付き償還結果を生成する。SRR124は、証明トークンが正常に償還されたか否かを示すデータを含み、ユーザアクティビティを追跡するために、または償還された証明トークンを生成するために使用されたクレデンシャルに関連付けられたユーザを識別するために使用され得る、追加のデータを含まない。

【0112】

証明トークンが正常に償還されたか否かの指示のみを提供する署名付き償還結果を生成するプロセスは、署名付き償還結果の受信側のためのセキュリティ、およびそのために署名付き償還結果が生成されたユーザのためのプライバシーを保証する。

20

【0113】

たとえば、証明トークンを提供するのではなく、署名付き償還結果を生成し、署名付き償還結果をウェブサイト140に提供することによって、ウェブサイト140は、証明トークンのための元の要求を追跡し、証明トークンを特定のユーザと相関させることができない。図4に関して以下で説明するように、証明トークンは、ブラインド署名方式を使用して署名されたので、トークンを発行したATIサーバ170は、ATIサーバ170自体がトークンに署名したこと、およびトークンが修正されていない、かつ/または前に償還されていないことのみを検証することができる。ATIサーバ170は、いつ証明トークンが署名されたか、または任意の追加のパラメータが証明トークンのための初期要求に関連付けられたかを知ることができず、証明トークンを要求するユーザのプライバシーを保護する。

30

【0114】

ステップHにおいて、アプリケーション111は、セキュアなストレージにSRRを記憶する。たとえば、アプリケーション111は、証明トークン122が記憶されたストレージと同様の、セキュアなキャッシュロケーションにSRR124を記憶することができる。

【0115】

ステップIにおいて、アプリケーション111は、アクセス要求125を生成し、ウェブサイト140に送信する。アクセス要求125は、SRRおよび他のパラメータを含むものなど、パラメータをさらに含み得る。アプリケーション111は、信用チェーンにおける追加のリンクとしてのデジタル署名を用いて、アクセス要求125に署名することができる。たとえば、アプリケーション111は、アクセス要求125における主要なパラメータに署名することができる。いくつかの実装形態では、すべてのパラメータが機密または重要である場合、すべてのパラメータが、アクセス要求125において署名され得る。

40

【0116】

いくつかの実装形態では、ステップIは、ウェブサイト140によってトリガされる。たとえば、アプリケーション111は、リソース145、またはウェブサイト140の特定のセクションにアクセスしようと試み得、ウェブサイト140は、アプリケーション111からの認証を要求し得る。

【0117】

いくつかの実装形態では、ステップIは、アプリケーション111がウェブサイト140から検出する情報に基づいて、アプリケーション111によって自動的に実行される。たとえば

50

、アプリケーション111は、ウェブサイト140に関連付けられたデータから、認証が必要とされ得ることを検出することができる。データは、アプリケーション111によって記憶されるか、またはウェブサイト140によって提供されるか、またはさもなければアプリケーション111にとってアクセス可能であり得る。たとえば、データは、中央データベースなど、複数の異なるデバイス上にインストールされた複数の異なるアプリケーション111がアクセスすることができる、中央の共有されたロケーションに記憶され得る。いくつかの実装形態では、アプリケーション111は、記憶されたデータに基づいて、ウェブサイト140が認証を必要とすると決定することができる。たとえば、最初にアプリケーション111がウェブサイト140にアクセスしようと試みるとき、アプリケーション111は、認証のための要求を示すデータを受信することができる。ウェブサイト140にアクセスしようとする後続の試みにおいて、アプリケーション111は、ウェブサイト140にアクセスするために認証が要求されるようになると自動的に決定し、ウェブサイト140および/またはリソース145にアクセスしようと試みるとき、SRRを提供することができる。

10

【0118】

ステップJにおいて、ウェブサイト140は、アクセス要求において提供されたSRRを検証するように試みる。ウェブサイト140がSRRを検証することができる場合、ウェブサイト140は、アクセス要求125において示されたウェブサイト140の部分へのアクセスを提供するか、または要求されたリソース145へのアクセスを提供することができる。

【0119】

図1Aおよび図1Bに関して上記で説明したプロセスは、セキュアおよび秘密である。いくつかの実装形態では、上記で説明したブラインド化方式またはグループ署名方式が、証明トークンを発行するために実施されるとき、このプロセスは、異なるプラットフォーム、コンテンツプロバイダ、およびパブリッシャーが、ユーザが特定のコンテンツにアクセスすることを許可されることを検証することを可能にすると同時に、プロセス内のどの当事者も、ユーザアクティビティを追跡すること、またはアクティビティを特定のユーザもしくはユーザの情報にリンクさせることができないように、ユーザプライバシーを保護する。

20

【0120】

いくつかの実装形態では、証明トークンが、ブラインド化またはグループ署名なしに発行される場合、トークンは、潜在的に機密の情報、または証明トークン発行サーバとコンテンツパブリッシャーとの間で共謀がある場合に、後続のウェブアクティビティを特定のデバイスにリンクさせるために使用され得る情報の中でも、高分解能タイムスタンプ、または詳細なアプリケーション情報を含み得る。

30

【0121】

1つの特定の例では、信用できるプログラム114は、クライアントデバイス110、ユーザのスマートフォン上にインストールされたモバイルアプリケーションであり、例示的な報道機関の公式の信用できるアプリケーションである。アプリケーション111は、クライアントデバイス110上にインストールされたウェブブラウザであり、ウェブサイト140は、例示的な報道機関の公式ウェブサイトである。例示的な報道機関の加入者であり、例示的な報道機関のアプリケーション114にサインオンされており、クライアントデバイス110上で例示的な報道機関の公式ウェブサイト140上のコンテンツにアクセスすることを望むユーザは、シームレスなブラウジングエクスペリエンスを有することができる。たとえば、ウェブブラウザ111は、トークン要求を生成し、要求を例示的な報道機関アプリケーション114に提供することができる。それに対してユーザが自分のログインクレデンシャルをすでに提供しており、認証される、例示的な報道機関アプリケーション114は、ATIサーバ170への署名付きトークン要求121を生成することができる。この特定の例では、ATIサーバ170は、例示的な報道機関によって維持された証明トークン発行サーバであり得る。いくつかの実装形態では、ATIサーバ170は、それに対して例示的な報道機関がトークン発行タスクを委託する、信用できるサーバであり得る。署名付きトークン要求121は、ATIサーバ170による検証のためにユーザのクレデンシャルを含み得る。ユーザのク

40

50

レデンシャルおよび/または要求121を受信および検証すると、ATIサーバ170は、ウェブブラウザ111に証明トークン122を発行することができる。証明トークン122は、ユーザのクレデンシャルおよび/または要求121が認証されたか否かを示す、少なくとも1ビットを含み得る。証明トークン122は、ウェブブラウザ111のセキュアなキャッシュに記憶され得る。次いで、アプリケーション111は、記憶された証明トークン122を示すトークン償還要求123を生成し、ATIサーバ170に送信することができる。ATIサーバ170が、トークン償還要求123において示された証明トークンを検証することができる場合、ATIサーバ170は、署名付き償還結果124を生成し、ウェブブラウザ111にSRR124を送信する。以前のステップの各々は、ユーザがウェブサイト140の特定のリソース145または部分へのアクセスを要求するより前に実行され得る。クライアントデバイス110のユーザが、例示的な報道機関のウェブサイト140上の新しいクロスワードパズルへのアクセスを要求するとき、ウェブブラウザ111は、アクセス要求125を生成し、例示的な報道機関のウェブサイト140に送信することができる。アクセス要求125は、SRR124と、ウェブサイト140によって要求された、必要とされるメタデータまたは他の情報など、他の主要なパラメータを含む。この特定の例では、例示的な報道機関ウェブサイト140は、ユーザがサブスクリプションを有すると決定することができるが、ユーザの識別情報へのアクセスを有しておらず、ユーザのアクティビティを追跡することができず、その理由は、証明トークン自体を生成するために使用される、ブラインド化または他のプライバシー保護技法が、プライバシーを保護する方法でトークンを作り出すからである。プライバシー保護技法が、証明トークンを生成するために使用されるとき、証明トークンは、コンテンツパブリッシャーが、ユーザが認証されると決定することを可能にするようになるが、発行者がトークンを署名付き償還結果に変換していなかった場合でも、コンテンツパブリッシャーは、ユーザの識別情報へのアクセスを有しておらず、ユーザのアクティビティを追跡することができない。

【0122】

別の例では、ウェブサイト140が、代わりに例示的なニュースアグリゲーションプラットフォームのためのモバイルアプリケーションまたはウェブインターフェースであり、そこで、例示的なニュースアグリゲーションプラットフォームが、例示的な報道機関とは別個であり、異なる場合、トークン自体ではなく、トークン償還プロセスおよびSRRの使用は、当事者間でユーザ情報またはアクティビティの接続または推定を行うための、例示的なニュースアグリゲーションプラットフォームまたは例示的な報道機関のいずれかの能力なしに、例示的なニュースアグリゲーションプラットフォームが、アクセスを要求するユーザが例示的な報道機関の認証されたユーザであることのみを知ることによって、例示的な報道機関によって維持された情報へのアクセスを提供することを可能にする。このようにして、例示的なニュースアグリゲーションプラットフォームは、例示的なニュースアグリゲーションプラットフォームのドメイン内のユーザのアクティビティに気づいており、例示的な報道機関は、例示的な報道機関のドメイン内のユーザのアクティビティに気づいているが、例示的なニュースアグリゲーションプラットフォームは、例示的な報道機関のドメイン内のユーザのアクティビティに気づいておらず、またはその逆も同様である。どちらのプラットフォームも、図1Aおよび図1Bに関して上記で説明したプロセスを通して、このユーザアクティビティまたはデータを決定することができない。

【0123】

プラットフォームにわたる認証の一般的に使用される方法は、異なるドメインまたはエンティティを通して、あるドメインまたはエンティティのためにユーザのクレデンシャルを提供し、異なるドメインまたはエンティティに、ユーザの情報にアクセスするための許可を与えることを、ユーザに求めることを伴う。図1Aおよび図1Bに関して説明したプロセスは、特定のウェブサイトまたはリソースにアクセスするプロセスから、サインインプロセスを除去することによって、別のエンティティのためにユーザのデータへのアクセスを要求するためのあるエンティティの能力を除去する。トークン発行および償還プロセスを使用することによって、このプロセスは、情報がすでに提供された信用できるプログラ

ム、およびユーザの認証を証明しなければならない証明トークン発行サーバを除いて、当事者のうちのいずれの者にも生の明瞭な形態でデータを提供することなしに、ユーザが認証を伝達することを可能にする。

【0124】

図1Aおよび図1Bに関して説明したプロセスは、異なるウェブサイト140および異なるプラットフォームにわたって認証を転送するための能力を提供し、ユーザの摩擦を低減し、より良いユーザエクスペリエンスを提供する。

【0125】

別の例では、例示的なビデオストリーミングサービスの有効なサブスクリプションを有するユーザは、SRRのために償還され得る証明トークンを発行され得る。SRRは、ユーザが毎回サインインすることを必要とすることなしに、ソーシャルメディア投稿中に埋め込まれる、例示的なビデオストリーミングサービスのサブスクリプションをもつユーザにとって利用可能にされたビデオのアクセスおよび/または視聴を行うために使用され得る。詳細には、説明したプロセスは、ユーザがビデオストリーミングサービスのアプリケーションにサインインしている限り、ソーシャルメディア投稿をホストするアプリケーション内でユーザがサインインすることをまったく必要とすることなしに、ユーザがコンテンツにアクセスすることを可能にすることができる。

【0126】

いくつかの方法は、ユーザがホスティングアプリケーション内で一度サインインすることを可能にし、認証がアプリケーションの存続期間の間に持続することを可能にするが、プライバシーによって動機付けられる機能的変更は、「サードパーティクッキー」などのデータに依拠するそのような手法を、将来において使用不可能にし得る。

【0127】

説明した証明トークンベースの認証プロセスは、より良いプライバシー特性を提供し、サードパーティで必要とされるサインインの数を低減し、他の手法が機能し続けない将来のシナリオにおいて、機能し続けることができる。

【0128】

別の例では、例示的な音楽ホスティングプラットフォームの有効なサブスクリプションを有するユーザは、自分のデバイス上にインストールされた例示的な音楽ホスティングプラットフォームアプリケーションを有し得る。ユーザは、例示的な音楽ホスティングプラットフォームアプリケーションに対して自分を認証し、自分の履歴に自分のアクティビティを追加することなしに、様々なウェブサイト上で、例示的な音楽ホスティングプラットフォームのサブスクリプションをもつユーザにとって利用可能にされた音楽にアクセスすることができる。

【0129】

また別の例では、例示的なビデオストリーミングサービスの有効なサブスクリプションを有するユーザは、ソーシャルメディアプラットフォーム上で友人からのチャットメッセージ内でユーザに送られた、例示的なビデオストリーミングサービスのサブスクリプションをもつユーザにとって利用可能にされたビデオにアクセスすることができる。ユーザは、ビデオにアクセスし、自分のアカウント情報を提供することなしに、自分が認証されたユーザであることを、例示的なビデオストリーミングサービスに保証することができる。

【0130】

上記で説明したように、いくつかの手法では、秘密/公開鍵ペア(および公開鍵に関連付けられた判定)は、複数の証明トークンにわたって変更されて、追跡に対するクライアントデバイスまたはユーザのプライバシーを向上させることができる。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、証明トークンの対応するバッチを証明トークン発行サーバから取り出すことができるので、証明トークンの再使用が低減または排除される。このバッチプロセスの例示的な例が、図2に示されている。

【0131】

この例では、アプリケーション200は、Nという個数の公開/秘密鍵ペアを作成する(20

10

20

30

40

50

1)。たとえば、アプリケーション200上にインストールされたウェブブラウザは、公開/秘密鍵ペアを生成することができる。公開/秘密鍵ペアは、非対称鍵ペアであり得る。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。秘密鍵を使用してデジタル署名されたデータは、対応する公開鍵を使用してのみ検証することができる。同様に、公開鍵を使用して暗号化されるデータは、対応する秘密鍵を使用してのみ解読され得る。

【0132】

アプリケーション200は、N個の証明トークンのために、証明トークン発行サーバ230に要求を送る(202)。数Nは、2以上の整数であり得る。この例では、要求は、N個の公開/秘密鍵ペアに対応するN個の証明トークンのためのものである。アプリケーション200は、アプリケーション200が署名付き償還結果を要求内で使用する頻度に基づいて、要求するための証明トークンの数Nを決定することができる。アプリケーションは、要求された証明トークンごとに公開/秘密鍵ペアを生成し、公開鍵データを要求内に含めることができる。この例では、公開鍵データは公開鍵自体であってよい。したがって、要求は、アプリケーション200のN個の公開鍵211を証明トークン発行サーバ230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の生データを含む。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。

【0133】

要求は、図1Aおよび図1Bに関して上記で説明したステップAおよびBのプロセスと同様に、アプリケーション200から信用できるプログラム220に転送され得る(221)。要求は、ユーザのクレデンシャルなどの情報を含み得る。

【0134】

証明トークン発行サーバ230は、要求を受信する(231)。信用できるプログラム220から受信されたユーザクレデンシャルに基づいて、証明トークン発行サーバ230は、クライアントデバイスの認証のレベルを決定する(232)。たとえば、証明トークン発行サーバは、M個の可能な認証レベルを有し得る。この例では、証明トークン発行サーバ230は、上記で説明したように、ユーザクレデンシャルに基づいて、これらのM個の可能な認証レベルのうちの1つを選択することができる。認証のレベルは、たとえば、特定の署名を通して符号化され得る。

【0135】

証明トークン発行サーバ230は、N個の証明トークンを生成する(233)。証明トークン発行サーバ230は、受信された公開鍵ごとに、それぞれの証明トークンを生成する。

【0136】

各証明トークンは、認証の判定と、認証の判定のためのタイムスタンプと、アプリケーション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、証明トークンが生成される時間を示す。証明トークン発行サーバは、N個の公開鍵211のうちの1つに基づいて、各証明トークンを生成することができる。たとえば、証明トークン発行サーバ230は、アプリケーション200の公開鍵と、認証判定と、タイムスタンプとを含む、データのセットをアセンブルすることができる。認証の判定がただ2つの可能な判定(認証される、または認証されない)を含む、いくつかの手法では、認証の判定は、証明トークンから省略され得る。言い換えれば、これらの手法では、証明トークン発行サーバは、認証されるユーザのための証明トークンを生成し(それらのトークンが、認証の暗示された判定を省略する)、認証されないユーザのための証明トークンを生成することを単に拒絶することができる。

【0137】

証明トークン発行サーバ230は、N個の証明トークンの各々にデジタル署名する(234)。たとえば、証明トークン発行サーバ230は、それ自体の秘密鍵を使用して、証明トークンの他のデータ(たとえば、認証判定、アプリケーション200の公開鍵、およびタイムスタンプ

10

20

30

40

50

プ)に基づいて、デジタル署名を生成することができる。

【0138】

証明トークン発行サーバ230は、アプリケーションにN個の証明トークン212を送信する(235)。アプリケーション200は、証明トークンのバッチを受信し、後の使用のために記憶する(203)。アプリケーション200は、証明トークンをローカルに、たとえば、アプリケーション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証明トークンは、たとえば、(1)証明トークン発行サーバ230によって決定される信用性の判定、(2)証明トークンの作成のためのタイムスタンプ、(3)アプリケーションの公開鍵、および(4)証明トークン発行サーバ230の秘密鍵を使用して署名された、トークンコンポーネントのデジタル署名を含み得る。

10

【0139】

図2の例に示されるように、証明トークンのバッチを取得すると、クライアントデバイスは、証明トークンを使用して、上記で説明したように、ウェブサイト、コンテンツパブリッシャードメイン、または他の証明トークン受信側に向かう様々な要求の一部として、証明トークンをアSEMBルし、送ることができる。そのような要求の例示的な例が、図3にプロセスフロー図として示されている。

【0140】

要求を準備するために、アプリケーション300は、アプリケーションのローカルストレージから証明トークンを取り出すことができる(301)。様々な手法では、アプリケーション300は、たとえば、(1)要求ごとに新しい証明トークンを使用すること、または(2)選択された時間間隔(たとえば、H連続時間)にわたって、同じ証明トークンを使用し、その間隔が経過すると、異なる証明トークンを使用すること、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せられたすべての要求のために、同じ証明トークンを使用すること(たとえば、異なる証明トークンが各アプリケーションもしくはウェブサイトのために使用される場合)、または(4)これらのトークン再使用手法のうちの2つ以上の組合せを使用すること(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せられたすべての要求のために、同じ証明トークンを使用すること)ができる。したがって、アプリケーション300は、そのための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間に基づいて、証明トークンを取り出すことができる。

20

30

【0141】

アプリケーション300は、証明トークンを償還するための要求を生成することができる(302)。要求311は、たとえば、(上記で説明したように)ペイロードデータ、要求作成タイムスタンプ、取り出された証明トークン、証明トークンに対応する公開鍵、および要求コンポーネントのデジタル署名を含み得る。いくつかの実装形態では、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コンポーネントは、ペイロードデータおよび証明トークンにアクセスすることによって、証明トークンを含み得るか、または証明トークンの形式であり得る、要求311を生成することができる。アプリケーションは、要求作成タイムスタンプとして、現在時間を決定することもできる。アプリケーションは、アプリケーションの秘密鍵(たとえば、要求中に含まれる公開鍵に対応する秘密鍵)を使用して、ペイロードデータ、公開鍵、およびタイムスタンプのデジタル署名を生成することができる。いくつかの手法では、証明トークンサイズを低減するための単純な最適化として、証明トークンは、デバイス公開鍵を省略し、その理由は、公開鍵が、証明トークンのコンポーネントとして含まれる証明トークン中にすでに存在するからである。

40

【0142】

いくつかの実装形態では、ATIサーバ170は、トークンを償還することを支援し、決定するために、それに対するアクセスが要求されるウェブサイトに関連付けられる。いくつかの実装形態では、トークンが、ブラインド化またはグループ署名などのプライバシー保護技法を使用して発行されるとき、ATIサーバ170がトークン償還を観察することによ

50

て知る唯一の情報は、この第2のコンテンツプロバイダを訪問したことがある、それに対して前にトークンを発行したユーザまたはデバイスの概数であるが、証明トークンのプライバシー保護の性質のために、いかなる特定のユーザまたはデバイスも決定することができない。

【0143】

次いで、アプリケーション300は、証明トークン発行サーバ320に要求311を送る(303)。

【0144】

証明トークン発行サーバ320は、要求を受信する(321)。証明トークン発行サーバ320は、要求を確認する(322)。たとえば、証明トークン発行サーバ320は、要求中に含まれる公開鍵を使用して、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。証明トークン発行サーバ320は、公開鍵と、たとえば、ペイロードデータ、タイムスタンプ、公開鍵、および証明トークンなど、アプリケーション300によって署名された要求のコンテンツとを使用して、デジタル署名を検証しようと試みることができる。デジタル署名が生成された後、このコンテンツのいずれかが変化した場合、検証は失敗することになる。たとえば、悪意のある当事者が、証明トークンを別の要求に挿入した場合、または認証のより高い判定を有する異なる証明トークンを要求に挿入した場合、署名検証は失敗することになる。これによって、要求のコンテンツが、たとえば仲介者による要求の送信中に変更されなかったことを保証する。

【0145】

証明トークン発行サーバ320は、証明トークンを確認する(323)。たとえば、証明トークン発行サーバ320は、証明トークン発行サーバの公開鍵を使用して、証明トークンの署名を検証することによって、証明トークンを確認することができる。これによって、同様に、証明トークンが証明トークン発行サーバによって発行されてから、証明トークンのコンテンツが変化していないことを保証する。証明トークンがデバイス公開鍵を含む場合、証明トークンの確認は、証明トークンとともに含まれるデバイス公開鍵が証明トークン内に含まれるデバイス公開鍵と一致するという確認も含み得る。

【0146】

証明トークン発行サーバ320は、証明トークンの適時性およびクライアントデバイスの認証を確認して(324)、たとえば、証明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のH時間またはD日前など、選択された時間間隔を超えて作成されなかった)ことを確認し、証明トークン内の認証判定が要求に従うのに十分な判定であることを確認する。

【0147】

これらの妥当性検査のすべてが合格である場合、証明トークン発行サーバ320は、たとえば、図1A、図1B、および図2に関して上記で説明したように、署名付き償還結果などを生成するために、証明トークンを償還することによって、要求に応答することができる(325)。妥当性検査のいずれかが不合格である場合、証明トークン発行サーバ320は、要求を無視することができる。たとえば、証明トークン発行サーバ320は、要求に応答しなくてよい、要求された動作を実行しなくてよい、などである。

【0148】

アプリケーション300は、SRRを受信する(304)。次いで、アプリケーション300は、受信側コンピューティングシステム330にアクセス要求313を送ることができる(313)。アクセス要求313は、SRR312と、ユーザデータ、コンテキストデータ、またはタイムスタンプを含む、他のパラメータとを含み得る。上記で説明したように、受信側は、エンティティの中でも、それに対するアクセスが要求されるウェブサイト、コンテンツプロバイダまたはパブリッシャーであり得る。たとえば、アプリケーション300は、コンテンツプラットフォーム150にアクセス要求およびSRRを送ることができ、コンテンツプラットフォームは、1つまたは複数のコンテンツパブリッシャードメインに要求を送ることができる。

【0149】

受信側コンピューティングシステム330は、署名付き償還結果を受信し、すべての妥当性検査が合格である場合、要求に応答することができる(331)。

【0150】

上記で説明したように、いくつかの手法では、ブラインド署名方式が、証明トークンを生成するためのプロセスにおいて使用され得るので、証明トークン発行サーバは、アプリケーションの公開鍵の生データを見ないようにする。たとえば、アプリケーションは、秘密/公開鍵ペアのバッチを生成し、次いで、証明トークン発行サーバに公開鍵を送り、証明トークンの対応するバッチを取り出す前に、ブラインド署名方式を使用して、公開鍵(または、公開鍵の暗号ハッシュ、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など、ブラインド署名方式のコミットフェーズのための値として使用され得るこれらの公開鍵の好適な派生物)をブラインドすることができる。この例では、証明トークンは、ブラインドされた公開鍵を用いてブラインド署名される。このバッチプロセスの例示的な例が、図4に示されている。

【0151】

この例では、証明トークン発行サーバ420は、アプリケーションのためのM個の異なる認証レベルを定義し、対応するM個の認証レベルのためにM個の異なるブラインド署名検証鍵411を公開することができる(421)。たとえば、M個のレベルは、認証される、および認証されない2つのレベルを含み得る。別の例では、M個のレベルは、疑わしい、満足できる、および完全に認証される3つのレベルを含み得る。他の例では、M個のレベルは、不正、疑わしい、加入者、および特別な加入者の4つのレベルを含み得る。他の量のレベルも使用され得る。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、最低の認証レベル(たとえば、「認証されない」または「不正」認証レベル)のためにブラインド署名検証鍵を割り当ててではなく、最低の認証レベルがM個の認証レベルから省略され得、証明トークン発行サーバは、最低の認証レベルをもつデバイスのためのブラインド署名を提供することを単に拒絶することができる。したがって、これらの手法では、Mは1以上の整数であり得る。

【0152】

証明トークン発行サーバ420は、ブラインド署名方式を使用して、認証レベルごとに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、インターネットエンジニアリングタスクフォース(IETF)の検証可能なオブリビアス擬似ランダム関数(VOPRF: Verifiable Oblivious Pseudorandom Function)ブラインド署名方式など、非公開で検証可能なブラインド署名方式であり得る。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、公的に検証可能なブラインド署名方式であり得る。

【0153】

証明トークン発行サーバ420は、アプリケーション400を含むアプリケーション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を公開することができる。たとえば、証明トークン発行サーバ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することができる。

【0154】

アプリケーション400は、これらのブラインド署名検証鍵を受信することができる(401)。たとえば、アプリケーション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ることができる。アプリケーション400は、以下でさらに説明するように、証明トークン発行サーバ420から後に受信される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、証明トークン発行サーバ420は、新しいブラインド署名検証鍵411を定期的に公開することができ(たとえば、毎時、毎日、毎週、または他の適切な時間期間)、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

るために使用され得る。

【0155】

N個の証明トークンのバッチを取得するために、アプリケーション400は、N個の公開/秘密鍵ペアを作成する(402)。たとえば、ウェブブラウザは、証明トークンごとにそれぞれの非対称公開/秘密鍵ペアを作成することができる。

【0156】

アプリケーション400は、ブラインド署名検証鍵を生成するために使用さ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)。すなわち、アプリケーション400は、各公開鍵のため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、公開鍵の生の値にブラインド化係数を適用することによって、公開鍵の生の値を不明瞭にすることを含み得る。このようにして、証明トークン発行サーバ420は、アプリケーション400から受信された公開鍵の生の値にアクセスすることができず、それらの値を使用して、たとえば、追加のデータとともに公開鍵の生の値を受信した別のエンティティから受信されたデータを使用して、ユーザまたはアプリケーション400を追跡することができない。

【0157】

証明トークン発行サーバ420によってブラインド署名される必要があるデータの量を低減するために、各デバイス公開鍵全体をブラインドする代わりに、アプリケーション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し得る。派生物は、公開鍵の暗号ハッシュであり得る。たとえば、アプリケーション400は、暗号ハッシュ関数を使用して、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用して、公開鍵の暗号ハッシュをブラインドすることができる。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であり得る。

【0158】

いくつかの実装形態では、証明トークン発行サーバ420は、暗号ハッシュを切り捨てることによって、ブラインドされた公開鍵データのデータサイズをさらに低減し、次いで、切捨て暗号ハッシュをブラインドすることができる。たとえば、この切捨ては、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バイトに制限することができる。この切捨ては、アプリケーション400がブラインド署名方式を使用してブラインドする、より短い暗号ハッシュをもたらす。

【0159】

このようにしてブラインド署名されるデータの量を低減することによって、データをブラインド署名する際に、証明トークン発行サーバ420にかかる負担が低減され(たとえば、CPUサイクル、データ記憶要件、メモリ消費などが低減され)、これによって、証明トークン発行サーバ420は、完全な公開鍵のブラインドされたバージョンが提供された場合よりも、ブラインド署名をより速く、より効率的に生成し、より多くの要求を処理することが可能になる。また、これによって、要求が送られるネットワークの帯域幅消費が低減され、大量のブラインドされた公開鍵データが単一の要求において送られることが可能になる。

【0160】

アプリケーション400は、N個の証明トークンのために、証明トークン発行サーバ420に要求412を送る(404)。数Nは、2以上の整数であり得る。要求は、アプリケーション400によって生成された各公開鍵411のためのブラインドされた公開鍵データを含み得る。たとえば、要求は、N個のブラインドされた公開鍵、公開鍵のN個のブラインドされた暗号ハッシュ、または公開鍵のN個のブラインドされた切捨て暗号ハッシュを含み得る。要求はまた、たとえば、アプリケーション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。いくつかの実装形態では、アプリケーション400は、図1A、図1B、図2、および図3に関して示されたプロセスと同様に、信用できるプログラム(図示せず)を通して、要求412を送信する。

【0161】

証明トークン発行サーバ420は、要求を受信する(422)。証明トークン発行サーバ420は、信用できるプログラムによって提供された可能性のある要求において示されたユーザクレデンシャルに基づいて、アプリケーション400の認証の判定を決定する(423)。いくつかの実装形態では、証明トークン発行サーバ420は、(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)M個の可能な認証判定を有し得る。証明トークン発行サーバ420は、デバイスレベル不正検出信号に基づいて、アプリケーション400をM個の可能な判定のうちの1つに割り当てることができる。

【0162】

アプリケーション400の認証の判定を決定すると、証明トークン発行サーバ420は、証明トークンのバッチを生成する(424)。たとえば、証明トークン発行サーバ420は、上記の動作402において生成された各公開鍵のための証明トークンを生成することができる。各証明トークンは、たとえば、(1)そのための証明トークンが生成されているアプリケーションの公開鍵、(2)証明トークン発行サーバによって決定される認証の判定、および(3)ブラインドされた公開鍵のブラインド解除されたブラインド署名(unblinded blind signature)、または公開鍵の暗号ハッシュ(たとえば、切り捨て後)を含み得る。いくつかの手法では、証明トークンは、認証の判定を省略することができ、その理由は、これが、ブラインド解除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的に検証可能でない場合、ブラインド署名を検証する(たとえば、以下で説明する図5の541を参照)ために、証明トークン発行サーバが呼び出されると、証明トークン発行サーバは、判定を返すこともできる。ブラインド署名が公的に検証可能である場合、ブラインド署名を検証する公開鍵は、デバイスの認証の判定も暗示する。

【0163】

アプリケーション400の認証の判定を決定し、証明トークンを生成すると、証明トークン発行サーバ420は、ブラインド署名秘密鍵を使用して、ブラインドされた公開鍵データの各部分(たとえば、各N個のブラインドされた公開鍵、または各ブラインドされた暗号ハッシュ)および証明トークンに署名する(425)。たとえば、証明トークン発行サーバ420は、アプリケーション400について決定された認証判定に対応するブラインド署名秘密鍵、たとえば、決定された認証判定のため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秘密鍵を取得することができる。このようにブラインド署名方式を使用して、証明トークン発行サーバ420は、公開鍵データの実際の値を知ることなしに、ブラインドされた公開鍵データのデジタル署名を生成することができる。

【0164】

証明トークン発行サーバ420は、クライアントデバイスに、N個のブラインド署名413および証明トークンを返す(426)。いくつかの実装形態では、証明トークンは、ブラインド署名方式を使用して署名され、N個のブラインド署名413は、ブラインド署名付き証明トークンを含む。アプリケーション400は、証明トークン発行サーバからブラインド署名を受信する。

【0165】

いくつかの実装形態では、アプリケーション400は、ブラインド署名方式を使用して、ブラインド署名をブラインド解除することができる。たとえば、アプリケーション400は、トークンの妥当性を検証するために、および、認証の判定以外に追加のユーザデータが証明トークンにおいて符号化されなかったことを保証するために、そのためにブラインド署名が生成されたブラインドされた公開鍵データと、証明トークン発行サーバ420によって公開されたブラインド署名検証鍵とを使用して、各ブラインド署名を確認することができる。これを行うために、アプリケーション400は、たとえば、各認証判定のための、複数のブラインド署名検証鍵を使用して、ブラインド署名を確認しようと試みることができる。判定が、アプリケーション400に割り当てられた判定と一致しない場合、ブラインド署名は、その判定のためのブラインド署名検証鍵を使用して確認されないことになる。アプリケーションは、ブラインド署名を正常に確認するブラインド署名検証鍵に基づいて、アプリケーション400の割り当てられた認証判定を決定することができ、たとえば、ブラ

インド検証鍵に対応する認証判定が、アプリケーション400に割り当てられた判定である。確認された場合、アプリケーションは、ブラインド署名方式を使用して、ブラインド署名をブラインド解除することができる。

【0166】

次いで、アプリケーション400は、証明トークンを記憶する(405)。たとえば、アプリケーション400の信用できるプログラムは、証明トークンを含むべき要求を送るときに後で使用するために、証明トークンをセキュアなストレージに記憶することができる。セキュアなストレージは、アプリケーション400のトークンキャッシュであり得る。上記で説明したように、いくつかの実装形態では、アプリケーション400は、記憶するより前に、証明トークンを確認しようと試みるようになる。いくつかの実装形態では、アプリケーション400は、記憶するより前に、証明トークンを確認しようと試みないようになり、受信時に証明トークンを記憶するようになる。

10

【0167】

図4の例に示されるように、証明トークンのバッチを記憶すると、アプリケーションは、次いで、証明トークン発行サーバに証明トークンを償還することができる。償還されると、証明トークン発行サーバは、証明トークンが正常に償還されたことのみを示す、署名付き償還結果を提供し、ユーザアクティビティを追跡するために使用され得る追加のユーザ情報または他の情報を提供しない。

【0168】

署名付き償還結果を受信すると、アプリケーションは、上記で説明したように、要求の中でも、コンテンツパブリッシャードメイン、ウェブサイトの特定の部分へのアクセス、および/または特定のコンテンツのために行われた様々な要求の一部として送信されることになる、署名付き償還結果を記憶することができる。そのような要求の例示的な例が、図5にプロセスフロー図として示されている。

20

【0169】

要求を準備するために、アプリケーション500は、たとえば、アプリケーションのセキュアなキャッシュから、署名付き償還結果を取り出すことができる(501)。様々な手法では、アプリケーションは、たとえば、(1)要求ごとに新しい署名付き償還結果を使用すること、または(2)選択された時間間隔(たとえば、H連続時間)にわたって、同じ署名付き償還結果を使用すること、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せられたすべての要求のために、同じ署名付き償還結果を使用すること、または(4)これらの償還結果再使用手法の組合せを使用すること(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せられたすべての要求のために、同じ署名付き償還結果を使用すること)ができる。したがって、アプリケーション500は、そのための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間に基づいて、署名付き償還結果を取り出すことができる。

30

【0170】

アプリケーション500は、(上記で説明したように)要求ペイロードと、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、署名付き償還結果と、署名付き償還結果に対応するデバイス公開鍵(たとえば、そのための公開鍵データがブラインド署名されており、ブラインド解除されたブラインド署名とともに署名付き償還結果中に含まれる、公開鍵)とを含む、コンテンツのセットを含む要求511をアSEMBLすることができる。要求はまた、アプリケーションの秘密鍵(たとえば、要求中に含まれる公開鍵に対応する秘密鍵)を使用して署名された(502)、コンテンツのセットのデジタル署名も含み得る。たとえば、アプリケーション500の信用できるプログラムは、秘密鍵を使用して、コンテンツ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、署名付き償還結果を含み得るか、または署名付き償還結果の形式であり得る。たとえば、要求は、コンテンツのセット(たとえば、署名付き償還結果を有する)およびデジタル署名を含み得る。

40

【0171】

アプリケーション500は、受信側のコンピューティングシステム520に要求511を送る(

50

503)。受信側は、たとえば、それに対するアクセスが要求されるウェブサイト、またはそれに対するアクセスが要求されるか、もしくはそこからのコンテンツが要求される、コンテンツホスティングプラットフォームであり得る。

【0172】

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、要求に含まれるデバイス公開鍵を使用して、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はまた、要求内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、その要求を確認することもできる。署名が正常に確認され、タイムスタンプが現在時間のしきい値持続時間内である場合、アプリケーション500は、要求が確認されるものと見なすことができる。

10

【0173】

受信側コンピューティングシステム520はまた、署名付き償還結果も確認する。この確認プロセスは、ブラインド署名を生成するときに証明トークン発行サーバ540によって使用さ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的に検証可能な方式(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、証明トークン発行サーバを呼び出すことなしに、署名付き償還結果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、ブラインド署名方式を使用して、署名付き償還結果中に含まれる公開鍵データのブラインド解除されたブラインド署名を検証することができる。公開鍵の暗号ハッシュが使用される場合、受信側コンピューティングシステム520は、アプリケーション500と同じ暗号ハッシュ関数を使用して、要求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、それを切り捨て)、ブラインド署名方式を使用して、暗号ハッシュのブラインド解除されたブラインド署名を検証することができる。

20

【0174】

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、証明トークン発行サーバ540を呼び出して、ブラインド解除されたブラインド署名を検証することができる(523b)。この例では、受信側コンピューティングシステム520は、ブラインド解除されたブラインド署名、および公開鍵または公開鍵の暗号ハッシュを、証明トークン発行サーバ540に送ることができる。

30

【0175】

証明トークン発行サーバ540は、ブラインド署名方式を使用して、ブラインド解除されたブラインド署名を検証しようと試みることができる(541)。応答は、検証が成功したか否か、およびブラインド解除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を示すことができる。

【0176】

受信側コンピューティングシステム520は、署名付き償還結果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、署名付き償還結果が最近作成されたことを確認し、署名付き償還結果内の信用性判定が要求に従うのに十分な判定であることを確認する。証明トークン発行サーバ540は、新しいブラインド署名検証鍵を定期的に再公開し得るので、適時性の確認は、署名付き償還結果のブラインド署名が無効な古い鍵で署名されていないことを、たとえば、署名付き償還結果が満了したブラインド署名検証鍵で検証されたと決定することによって確認することを含み得る。1つの手法では、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、公開された鍵のためのURLの一部として符号化されたので、ブラインド署名検証鍵が満了したと決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ので、ブラインド署名検証鍵が満了したと決定することができる。

40

【0177】

これらの妥当性検査のすべてが合格である場合、受信側コンピューティングシステム52

50

0は、上記で説明したように、要求に応答して(525)、たとえば、リソースへのアクセスを提供するか、またはリソースを配信することなどができる。妥当性検査のいずれかが不合格である場合、受信側コンピューティングシステム520は、要求を無視することができ、たとえば、要求に対する応答を送らないこと、設定を更新することなどを選択することができる。

【0178】

上記の説明に加えて、ユーザには、本明細書で説明するシステム、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否か、およびいつそれを可能にし得るか、サーバからのパーソナライズされたコンテンツまたは通信がユーザに送られるか否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除去されるように、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、ユーザの識別情報は、個人を識別できる情報(たとえば、電話番号、IMEI、デバイスシリアル番号)がユーザについて決定できないように扱われ得る、またはユーザの地理的ロケーションは、ユーザの具体的なロケーションが決定できないように、ロケーション情報が取得される場合に(都市、郵便番号、もしくは州のレベルなどに)一般化され得る。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、情報の保持方針、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。

【0179】

図6は、上記で説明した動作を実行するために使用され得る例示的なコンピュータシステム600のブロック図である。システム600は、プロセッサ610、メモリ620、記憶デバイス630、および入出力デバイス640を含む。構成要素610、620、630、および640の各々は、たとえば、システムバス650を使用して、相互接続され得る。プロセッサ610は、システム600内で実行するための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610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610は、マルチスレッドプロセッサである。プロセッサ610は、メモリ620または記憶デバイス630に記憶された命令を処理することが可能である。

【0180】

メモリ620は、システム600内に情報を記憶する。一実装形態では、メモリ620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620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620は、不揮発性メモリユニットである。

【0181】

記憶デバイス630は、システム600のための大容量ストレージ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630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630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、または何らかの他の大容量記憶デバイスを含み得る。

【0182】

入出力デバイス640は、システム600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640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660、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信す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の、他の実装形態も使用され得る。

【0183】

例示的な処理システムが図6で説明されているが、本明細書で説明する主題および機能的動作の実装形態は、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する構造およびそれらの構造的均等物を含む、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。

【0184】

本明細書で説明する主題および動作の実施形態は、デジタル電子回路において、または本明細書で開示する構造およびそれらの構造的均等物を含む、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。本明細書で説明す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。代替的にまたは追加として、プログラム命令は、データ処理装置による実行のために、好適な受信機装置への送信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、機械生成の電気、光、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、伝搬信号ではなく、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。

【0185】

本明細書で説明する動作は、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るか、または他のソースから受信されるデータに対して、データ処理装置によって実行される動作として実装され得る。

【0186】

「データ処理装置」という用語は、例として、プログラマブルプロセッサ、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、もしくは上記のものの組合せを含む、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)を含み得る。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、仮想機械、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、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。

【0187】

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、またはコードとも呼ばれる)は、コンパイル型言語またはインタプリタ型言語、宣言型言語または手続き型言語を含む、任意の形態のプログラミング言語で書くことができ、スタンドアロンプログラムとして、またはモジュール、コンポーネント、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いて使用するのに適した他のユニットとして含む、任意の形態で展開され得る。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、マークアップ言語ドキュメントに記憶された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実行されるか、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。

【0188】

本明細書で説明するプロセスおよび論理フローは、入力データ上で動作し、出力を生成することによってアクションを実行するために、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マブルプロセッサによって実行され得る。プロセスおよび論理フローはまた、専用論理回路構成、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)によって実行され得、装置もそれらとして実装されてよい。

【0189】

コンピュータプログラムの実行に好適なプロセッサは、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、命令およびデータを読み取り専用メモリ、もしくはランダムアクセスメモリ、またはその両方から受信することになる。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行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、携帯電話、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好適なデバイスは、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、内蔵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およびDVD-ROMディスクを含む、すべての形態の不揮発性メモリ、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、専用論理回路によって補完され得るか、または専用論理回路に組み込まれ得る。

【0190】

ユーザとの対話を提供するために、本明細書で説明した主題の実施形態は、情報をユーザに表示するためのディスプレイデバイス、たとえば、CRT(陰極線管)またはLCD(液晶ディスプレイ)モニタと、それによってユーザが入力をコンピュータに提供することができるキーボードおよびポインティングデバイス、たとえば、マウスまたはトラックボールとを有するコンピュータ上で実装され得る。他の種類のデバイスも、ユーザとの対話を提供するために使用され得、たとえば、ユーザに提供されるフィードバックは、任意の形態の感覚フィードバック、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であり得、ユーザからの入力、音響入力、音声入力、または触覚入力を含む任意の形態で受信され得る。加えて、コンピュータは、ドキュメントをユーザによって使用されるデバイスに送り、ドキュメント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回答してウェブページをそのウェブブラウザに送ることによって、ユーザと対話することができる。

【0191】

本明細書で説明する主題の実施形態は、たとえば、データサーバとして、バックエンド構成要素を含むか、また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

10

20

30

40

50

含むか、またはフロントエンド構成要素、たとえば、ユーザがそれを通じて本明細書で説明する主題の一実装形態と対話できる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を含むか、あるいは1つまたは複数のそのようなバックエンド構成要素、ミドルウェア構成要素、またはフロントエンド構成要素の任意の組合せを含む、コンピューティングシステムにおいて実装され得る。システムの構成要素は、任意の形態または媒体のデジタルデータ通信、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。

10

【0192】

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。クライアントおよびサーバは、一般に互いから離れており、典型的には通信ネットワークを通じて対話する。クライアントとサーバとの関係は、それぞれのコンピュータ上で実行され、互いに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って生じる。いくつかの実施形態では、サーバは、(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、そのユーザからユーザ入力を受信する目的で)データ(たとえば、HTMLページ)をクライアントデバイスに送信する。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。

【0193】

本明細書は多くの特定の实装形態の詳細を含んでいるが、これらは発明の範囲または特許請求され得るものの範囲に対する限定として解釈されるべきではなく、むしろ特定の発明の特定の实装形態に特有の特徴の説明として解釈されるべきである。別個の实装形態の文脈において本明細書で説明するいくつかの特徴はまた、単一の实装形態において組み合わせられて実装され得る。逆に、単一の实装形態の文脈で説明する様々な特徴はまた、複数の实装形態において別々にまたは任意の好適な部分組合せにおいて実装され得る。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、その組合せから除去される場合があり、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し得る。

20

30

【0194】

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実行されること、またはすべての例示された動作が実行されることを必要とするものとして理解されるべきではない。いくつかの状況では、マルチタスキングおよび並列処理が有利であり得る。その上、上記で説明した実装形態における様々なシステム構成要素の分離は、すべての実装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が、一般に、単一のソフトウェア製品の中に一緒に組み込まれ得るか、または複数のソフトウェア製品の中にパッケージ化され得ることを理解されたい。

40

【0195】

以上、本主題の特定の实装形態について説明した。他の实装形態は、以下の特許請求の範囲内にある。場合によっては、特許請求の範囲において列挙されるアクションは、異なる順序で実行される場合があるが、依然として望ましい結果を達成することができる。加えて、添付の図において図示されるプロセスは、望ましい結果を達成するために、必ずしも示されている特定の順序または順番を必要とするとは限らない。いくつかの实装形態では、マルチタスキングおよび並列処理が有利であり得る。

【符号の説明】

【0196】

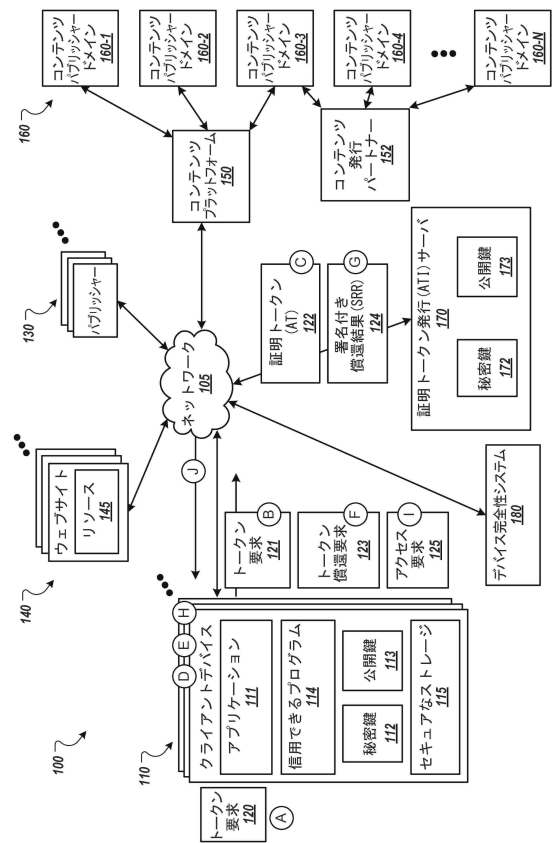
100 システム、環境、例示的な環境

50

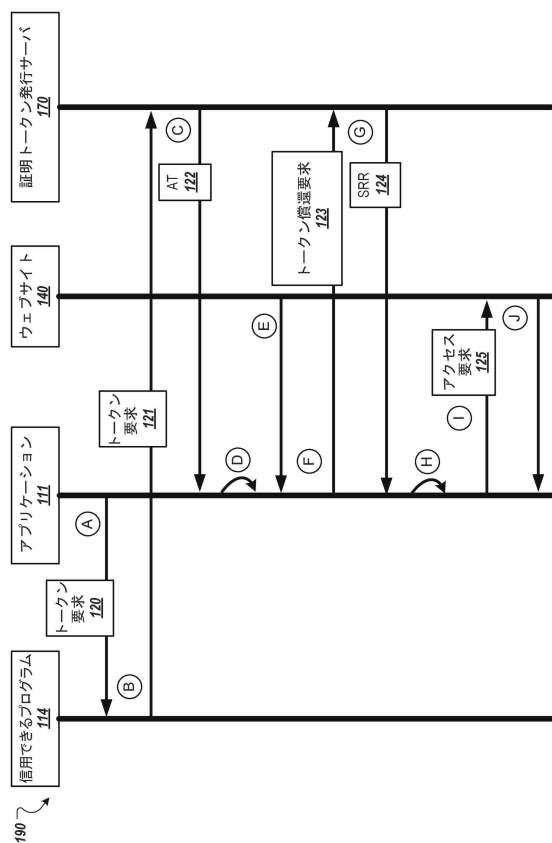
105	データ通信ネットワーク、ネットワーク	
110	クライアントデバイス、ユーザデバイス	
111	アプリケーション、ウェブブラウザ	
112、172	秘密鍵	
113、173	公開鍵	
114	信用できるプログラム、スマートフォンアプリケーション、例示的な報道機関アプリケーション、例示的な報道機関スマートフォンアプリケーション、信用できるアプリケーション、例示的な報道機関モバイルアプリケーション、例示的な報道機関のアプリケーション	
115	セキュアなストレージ	10
120	要求、トークン要求、証明トークン要求、署名付き要求	
121	要求、署名付きトークン要求	
122	証明トークン	
123	トークン償還要求	
124	署名付き償還結果、SRR	
125、313	アクセス要求	
130	パブリッシャー	
140	ウェブサイト、例示的なソーシャルメディアウェブサイト、例示的なニュースアグリゲーションウェブサイト、例示的な報道機関の公式ウェブサイト、例示的な報道機関のウェブサイト、例示的な報道機関ウェブサイト	20
140a、140b、140c	例示的なニュースウェブサイト	
145	リソース	
150	コンテンツプラットフォーム	
152	コンテンツ発行パートナー	
160、160-2、160-3	コンテンツパブリッシャードメイン	
170	証明トークン発行(ATI)サーバ、証明トークン発行サーバ、ATIサーバ	
180	デバイス完全性システム	
200、300、400、500	アプリケーション	
220	信用できるプログラム	
230、320、420、540	証明トークン発行サーバ	30
211	N個の公開鍵	
212	N個の証明トークン	
311、412、511	要求	
312	SRR	
330	受信側コンピューティングシステム	
411	ブラインド署名検証鍵、公開鍵	
413	N個のブラインド署名	
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	
600	例示的なコンピュータシステム、システム	
610	プロセッサ、構成要素	40
620	メモリ、構成要素	
630	記憶デバイス、構成要素	
640	入出力デバイス、構成要素	
650	システムバス	
660	外部デバイス	

【図面】

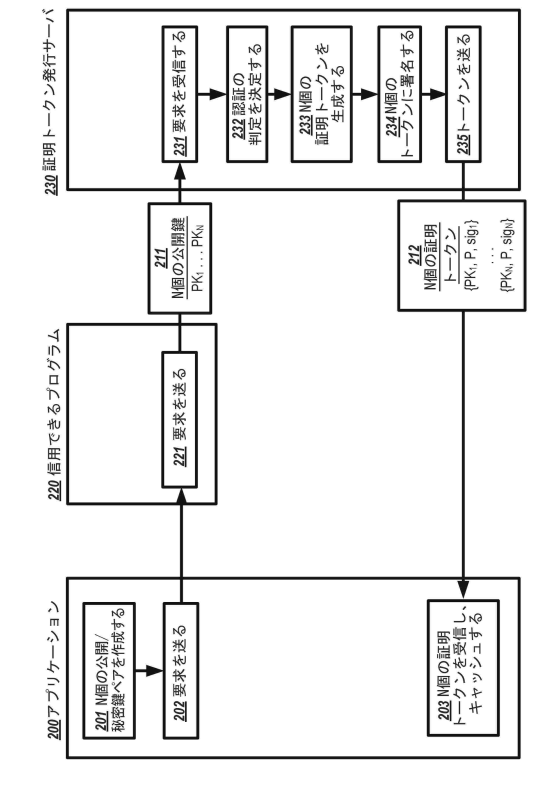
【図 1 A】



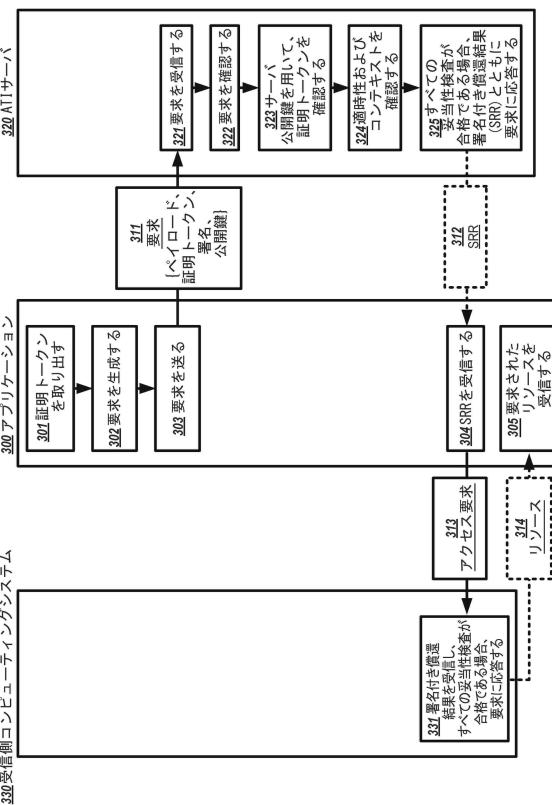
【図 1 B】



【図 2】



【図 3】



10

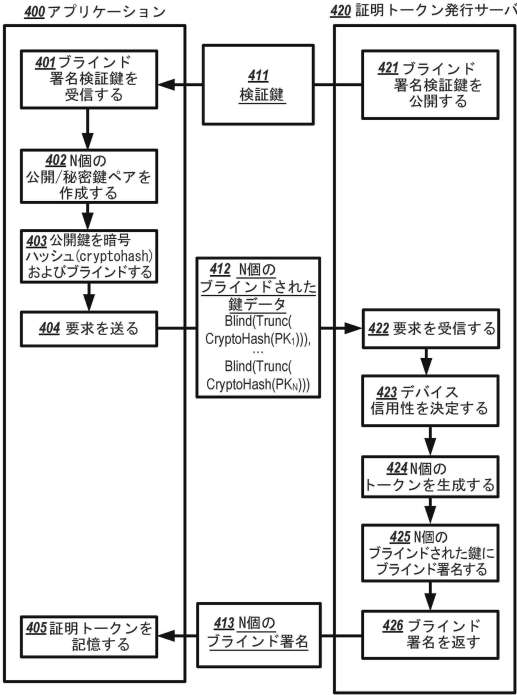
20

30

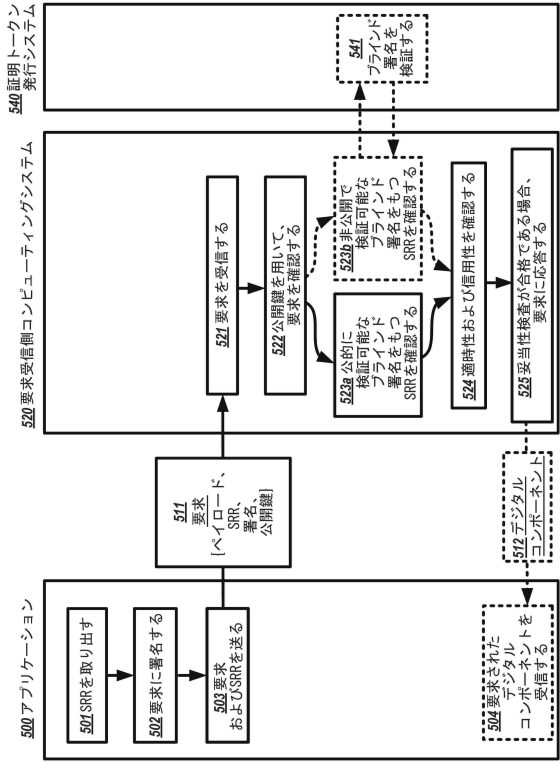
40

50

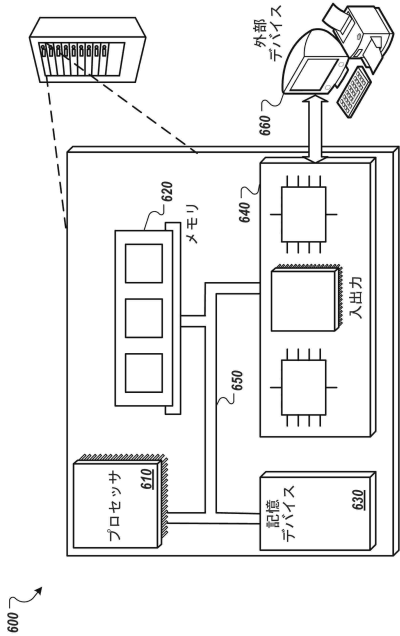
【図 4】



【図 5】



【図 6】



10

20

30

40

50

フロントページの続き

- (72)発明者 デイヴィッド・アイザック・ヴァン・クリーブ
 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 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
- 審査官 中里 裕正
- (56)参考文献 米国特許出願公開第２０１０／０３２５４４１（ＵＳ，Ａ１）
 米国特許出願公開第２０１２／０１６７１８９（ＵＳ，Ａ１）
 米国特許出願公開第２０１４／０２８２９８４（ＵＳ，Ａ１）
 米国特許出願公開第２０１５／０３４１３４０（ＵＳ，Ａ１）
 米国特許出願公開第２０１６／０１２７３４１（ＵＳ，Ａ１）
- (58)調査した分野 (Int.Cl., D B名)
 H 0 4 L 9 / 3 2
 G 0 6 F 2 1 / 6 4
 G 0 6 F 2 1 / 3 1