(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号

特表2025-506640
(P2025-506640A)

(43)公表日　令和7年3月13日(2025.3.13)

(51)Int.Cl.		F I		テーマコード(参考)
H04L 9/08	(2006.01)	H04L 9/08	C	

審査請求 未請求　予備審査請求 有　(全 43 頁)

(21)出願番号　特願2024-546250(P2024-546250)
(86)(22)出願日　令和5年2月13日(2023.2.13)
(85)翻訳文提出日　令和6年8月5日(2024.8.5)
(86)国際出願番号　PCT/FI2023/050088
(87)国際公開番号　WO2023/156709
(87)国際公開日　令和5年8月24日(2023.8.24)
(31)優先権主張番号　22157019.5
(32)優先日　令和4年2月16日(2022.2.16)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(71)出願人　513156386
グルロジック　マイクロシステムズ　オーワイ
Ｇｕｒｕｌｏｇｉｃ　Ｍｉｃｒｏｓｙｓｔｅｍｓ　Ｏｙ
フィンランド共和国　２０１００　トゥルク　リンナンカツ　３４
Ｌｉｎｎａｎｋａｔｕ　３４　２０１００　Ｔｕｒｋｕ　ＦＩＮＬＡＮＤ
(74)代理人　100127188
弁理士　川守田　光紀
(72)発明者　カルッカイネン　トゥオマス
フィンランド　２０４００　トゥルク　ティッカーヤンカツ　７

最終頁に続く

(54)【発明の名称】デジタルＩＤを確立するための方法及び構成

(57)【要約】
暗号シード（１０２，ＰＵ０）を生成するように構成されたランダムデータ生成部を備え、セキュアトランスポート機構（１２０）を用いうるシステム。第１の暗号操作（１０４，２０４）を通じて暗号中間プロダクト（１０５）を生成しうる。暗号中間プロダクトは、前記暗号シードと、セキュアトランスポート機構を通じて受信したユーザの秘密（１１３，ＵＳＳ）の両方に決定論的に依存する。暗号中間プロダクトは、関係者のデジタルＩＤを構成する。そして関係者のデジタルＩＤに第２の暗号操作（１０６）を適用して、暗号化された形式の暗号シードを含む暗号出力（１０７）を生成し、その少なくとも一部をセキュアトランスポート機構を介して送信する。
【選択図】図１

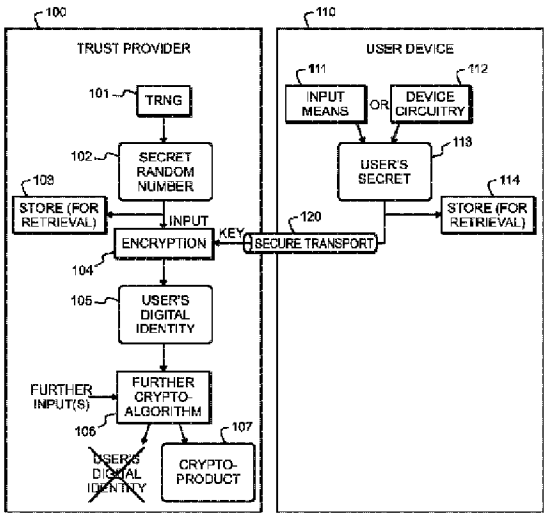


Fig. 1

【特許請求の範囲】
【請求項１】
関係者のためにデジタルＩＤを確立するためのシステムであって、
・　暗号シードを生成するように構成されたランダムデータ生成部と、
・　外部ソースと通信するための、セキュアトランスポート機構の受信側及び送信側と、
・　前記ランダムデータ生成部と前記セキュアトランスポート機構の前記受信側とに結合された第１の暗号操作部と、
・　前記第１の暗号操作部と前記セキュアトランスポート機構の前記送信側とに結合される第２の暗号操作部と、
を備え、
前記暗号シードと、前記セキュアトランスポート機構を介して外部ソースから受信したユーザの秘密との両方に決定論的に依存する暗号中間プロダクトを、前記第１の暗号操作部を通じて生成するように構成され、前記暗号中間プロダクトは前記関係者の前記デジタルＩＤを構成し、
前記関係者の前記デジタルＩＤを使用して、暗号化された形式の前記暗号シードを含む暗号出力を、前記第２の暗号操作を通じて生成するように構成され、
前記暗号出力の少なくとも一部を前記セキュアトランスポート機構を介して送信するように構成される、
システム。
【請求項２】
前記暗号出力の前記生成において前記デジタルＩＤを使用した後、前記デジタルＩＤをメモリにおいて永久的に難読化するように構成される、請求項１に記載のシステム。
【請求項３】
前記第２の暗号操作を通じて、前記暗号出力の一部として前記関係者の暗号証明書を生成するように構成される、請求項１又は２に記載のシステム。
【請求項４】
・　前記関係者の識別子及び少なくとも１つの属性を示す、受信した事前プロビジョニング要求に対して、前記関係者のための仮秘密を確立し、前記仮秘密の少なくとも一部を含む事前プロビジョニング応答を送信するように構成される、事前プロビジョニング機能と、
・　前記事前プロビジョニング応答の前記送信後に受信した登録完了要求に対して、前記登録完了再要求の内容を前記仮秘密に照らして検証することにより応答するように構成される、登録完了機能と、
を備え、
前記事前プロビジョニング機能は、前記暗号シードを使用して、前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の暫定暗号化アーカイブに格納するように構成され、
前記登録完了機能は、前記登録完了要求で受信した前記ユーザの秘密を使用して、前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の最終暗号化アーカイブに格納するように構成され、
前記システムは、前記識別子及び前記少なくとも１つの属性の前記暗号化及び前記最終暗号化アーカイブへの格納において、前記デジタルＩＤを使用するように構成される、
先行する請求項のいずれかに記載のシステム。
【請求項５】
前記事前プロビジョニング機能は、
・　前記関係者のための前記仮秘密として非対称暗号化システムの一対のエフェメラル鍵を生成し、
・　前記事前プロビジョニング応答において前記一対のエフェメラル鍵の公開鍵を送信するように構成される、
請求項４の記載のシステム。

【請求項６】
前記事前プロビジョニング機能は、
・　前記ランダムデータ生成部によって提供された乱数を前記一対のエフェメラル鍵の秘密鍵として使用し、
・　Ｃｕｒｖｅ２５５１９楕円曲線ディフィー・ヘルマン法を使用して、前記一対のエフェメラル鍵の秘密鍵から前記一対のエフェメラル鍵の公開鍵を生成するように構成される、
請求項５の記載のシステム。
【請求項７】
前記事前プロビジョニング機能は、
・　前記一対のエフェメラル鍵の前記秘密鍵と、前記システムの外部のエンティティから受信した公開鍵とを用いて、第１の数学的演算によって第１の共有秘密を生成し、
・　前記識別子と前記少なくとも１つの属性とを暗号化して前記暫定暗号化アーカイブに格納する際に、前記第１の共有秘密を使用するように構成される、
請求項５又は６の記載のシステム。
【請求項８】
前記第１の暗号処理としてＡｒｇｏｎ２ハッシュ処理を使用するように構成される、先行する請求項のいずれかに記載のシステム。
【請求項９】
・　前記デジタルＩＤを使用して、前記関係者の前記暗号出力の一部を生成するよう構成され、
・　前記システムの署名鍵で前記暗号出力の少なくとも一部分に署名することで、前記関係者の証明書を生成するように構成される、
先行する請求項のいずれかに記載のシステム。
【請求項１０】
前記暗号出力の前記一部の１つとして、非対称暗号化システムの更なる鍵ペアの公開鍵を、Ｃｕｒｖｅ２５５１９楕円曲線ディフィー・ヘルマン法を使用して前記デジタルＩＤから生成するように構成される、請求項９に記載のシステム。
【請求項１１】
前記デジタルＩＤの生成後に、登録完了応答の中で前記暗号出力を送信するように構成される、先行する請求項のいずれかに記載のシステム。
【請求項１２】
前記登録完了応答において、暗号化された形式の前記暗号シード、及び前記システムの外部のエンティティが使用するための署名された形式の暗号鍵を送信するように構成され、前記暗号鍵は、前記関係者の前記デジタルＩＤを構成する、又は前記デジタルＩＤから導出される、非対称暗号化システムの鍵ペアの片割れである、請求項１１に記載のシステム。
【請求項１３】
関係者のためにデジタルＩＤを確立する方法であって、
・　ランダムデータとして暗号シードを生成することと、
・　セキュアトランスポート機構を介して外部ソースからユーザの秘密を受信することと、
・　第１の暗号操作を適用して、前記暗号シードと前記ユーザの秘密の両方に決定論的に依存する暗号中間プロダクトであって、前記関係者の前記デジタルＩＤを構成する暗号中間プロダクトを生成することと、
・　前記関係者の前記デジタルＩＤに第２の暗号操作を適用して、暗号化された形式の前記暗号シードを含む暗号出力を生成することと、
・　前記暗号出力の少なくとも一部を、前記セキュアトランスポート機構を介して前記外部ソースに送信することと、
を含む、方法。

【請求項１４】
前記暗号出力の生成に前記デジタルＩＤを使用した後、前記デジタルＩＤを、永久にメモリから難読化することを含む、請求項１３に記載の方法。
【請求項１５】
前記第２の暗号操作を通じて、前記暗号出力の一部として前記関係者の暗号証明書を生成することを含む、請求項１３又は１４に記載の方法。
【請求項１６】
前記関係者の識別子及び少なくとも１つの属性を示す、受信した事前プロビジョニング要求に対して、前記関係者のための仮秘密を確立し、前記仮秘密の少なくとも一部を含む事前プロビジョニング応答を送信することと、
前記仮秘密を確立することの一部として、前記暗号シードを使用して前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の暫定暗号化アーカイブに格納することと、
前記事前プロビジョニング応答の前記送信後に受信した登録完了要求に対して、前記登録完了再要求の内容を前記仮秘密に照らして検証することにより応答することと、
前記登録完了機能は、前記登録完了要求で受信した前記ユーザの秘密を使用して、前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の最終暗号化アーカイブに格納することと、
前記識別子及び前記少なくとも１つの属性の前記暗号化及び前記最終暗号化アーカイブへの格納において、前記デジタルＩＤを使用することと、
を含む、請求項１３から１５のいずれかに記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、デジタルサービスを利用する際に必要とされるセキュリティの技術分野に関する。特に本発明は、関係者（Party）間で信頼（Trust）を一元的に確立する課題に関する。これらの関係者は、デジタルサービスの分散型利用において、当該一元的に確立された信頼に依存しうる。
【発明の背景】
【０００２】
デジタル通信におけるセキュリティは、機密性（Confidentiality，許可された関係者だけが情報にアクセスできる）、認証（Authentication，通信関係者は、通信相手が誰であるかを確認しなければならない）、完全性（Integrity，情報が許可されない形で変更されていないこと）、否認防止（Non-repudiation，関係者は、ある情報を送信したことを否定することができない）など、複数の側面を含む。認証については、トラストプロバイダと呼ばれる第三者に依存するのが一般的である。サービスプロバイダのウェブサイトと通信しようとするコンピュータやスマートフォンのユーザは、まずトラストプロバイダの認証サービスと連絡を取らなければならない。このとき通常、ユーザIDと使い捨てのキーが使用される。使い捨てのキーは、ユーザが所持している印刷されたリストから読み取るか、ユーザデバイスで実行されている専用アプリによって提供される。認証サービスがユーザの身元を確認すると、ユーザは、トラストプロバイダが発行したデジタル証明書とともに、通信しようとしていたウェブサイトにリダイレクトされる。
【０００３】
概念的なレベルでは、デジタル認証は、IDカード、パスポート、運転免許証、又はユーザが以前に当局から取得したその他の公的文書を物理的に提示する、よく知られた従来の慣行と比較することができる。このような公的文書の性質が十分信頼できるものであれば、ユーザは、少なくとも発行日から一定期間、好きなときに自由に再利用できることが広く合意されている。
【０００４】
デジタルの世界における既知の取り決めの欠点は、通信関係者がトラストプロバイダに継

続的に依存することである。ユーザがサービスプロバイダと連絡を取りたいときには、毎回同じ認証ルーチンを繰り返さなければならず、最終的にはユーザが支払うことになる追加コストが発生する。

【０００５】

既知の取り決めのもう一つの問題点は、ユーザがサービスプロバイダと行うことを望む通信と密接な関係を持たない可能性のある、例えば銀行、通信事業者、又はその他の中間関係者との顧客関係にユーザを縛り付けていることである。ユーザによりよい独立性を提供し、ユーザがいつ、どこで、誰と安全なデジタル通信を行うかを監視する少なくとも理論的な可能性を持つゲートキーパーとして、そのような中間関係者が機能することを排除するためには、デジタルID及び関連サービスの提供を政府又は他の信頼された当局の下で集中化（一元化）することが望ましい。

【０００６】

既知の取り決めは更なる欠点を含む。これは、印刷されたパスポート、運転免許証、IDカードなど、印刷されたID証明書を使用していた時代にさかのぼる。すなわち通常、ユーザは、サービスプロバイダと多くの情報を共有しなければならない。些細な例として、ユーザがアルコール飲料を購入する際、身分証明書の提示を求められたが、販売員は実際には、ユーザが法定年齢を上回っているか下回っているかを知る権利しかない。ところが、運転免許証を見せることで、ユーザは、正確な年齢、社会保障番号、運転が許可されている車のクラスなどを開示してしまう。同様の事態がデジタル証明書でも起こる。なぜなら通常、トラストプロバイダは、ユーザから認証要求が来た時点では、そのデジタル証明書が、後にユーザがサービスプロバイダと通信する際に何に使用されるかを知らないからである。その結果、電子証明書には、不必要に多くのユーザ情報が含まれる可能性がある。

【摘要】

【０００７】

この欄は、詳細説明において後述する概念の一部を単純化して紹介するために提供される。この欄は、特許請求される主題の重要な特徴又は本質的な特徴を特定することを意図したものではなく、特許請求される主題の範囲を限定するために使用することを意図したものでもない。

【０００８】

上記のような従来技術の欠点なしに、関係者のデジタルIDを確立し、利用し、可能にするようにする方法及び構成を提供することが目的である。特に、ユーザ、サービスプロバイダ、及びセキュアなデジタル通信及び取引を希望するその他の関係者が、信頼を提供するために第三者に継続的に依存することなく、すなわち直接的な信頼関係を介することなく、デジタルIDを確立し、利用し、可能にすることが目的である。更なる目的は、関係者が安全なデジタル通信の目的のために必要な情報のみを交換すればよいようにすることである。更に、特に重要な目的は、デジタルIDの確立と使用に関連する全てにおいて、機密性とデータ保護を確保することである。

【０００９】

第1の側面によると、関係者のデジタルIDを確立するためのシステムが提供される。このシステムは、暗号シードを生成するように構成されたランダムデータ生成部と、セキュアトランスポート機構の受信側及び送信側とを備える。第1の暗号操作が、前記ランダムデータ生成部と前記セキュアトランスポート機構の前記受信側とに結合され、第2の暗号操作が、前記第1の暗号操作と前記セキュアトランスポート機構の前記送信側とに結合される。前記システムは、前記第1の暗号操作を通じて、前記暗号シード及び前記セキュアトランスポート機構を通じて受信したユーザの秘密の両方に決定論的に依存する暗号中間プロダクトを生成するように構成される。前記暗号中間プロダクトは、前記関係者の前記デジタルIDを構成する。前記システムは、前記第2の暗号操作を通じて、前記関係者の前記デジタルIDを使用して、暗号化された形式の前記暗号シードを含む暗号出力を生成するように構成される。前記システムは、前記暗号出力の少なくとも一部を前記セキュアトランスポート機構を介して送信するように構成される。

【００１０】
実施形態によっては、前記システムは、前記暗号出力の前記生成において前記デジタルIDを使用した後、前記デジタルIDをメモリにおいて永久的に難読化するように構成される。これは少なくとも、前記デジタルIDが、少なくとも前記システムに関連するいかなる動作によっても、後で偶然に明らかになる危険性がないという利点をもたらす。
【００１１】
実施形態によっては、前記システムは、前記第2の暗号操作を通じて、前記暗号出力の一部として前記関係者の暗号証明書を生成するように構成される。これは、少なくとも、前記関係者が、前記システムに再びアクセスすることなく、後に、前記暗号証明書を認証に使用できるという利点をもたらす。
【００１２】
実施形態によっては、前記システムは、前記関係者の識別子及び少なくとも1つの属性を示す、受信した事前プロビジョニング要求に対して、前記関係者のための仮秘密を確立し、前記仮秘密の少なくとも一部を含む事前プロビジョニング応答を送信するように構成される、事前プロビジョニング機能を備える。前記システムは更に、前記事前プロビジョニング応答の前記送信後に受信した登録完了要求に対して、前記登録完了再要求の内容を前記仮秘密に照らして検証することにより応答するように構成される、登録完了機能を備えてもよい。前記事前プロビジョニング機能は、前記暗号シードを使用して、前記識別子及び前記少なくとも1つの属性を暗号化し、前記関係者に固有の暫定暗号化アーカイブに格納するように構成される場合がある。前記登録完了機能は、前記登録完了要求で受信した前記ユーザの秘密を使用して、前記識別子及び前記少なくとも1つの属性を暗号化し、前記関係者に固有の最終暗号化アーカイブに格納するように構成されてもよい。前記システムは、更に、前記識別子及び前記少なくとも1つの属性の前記暗号化及び前記最終暗号化アーカイブへの格納において、前記デジタルIDを使用するように構成されてもよい。これは、少なくとも、ユーザの登録を完了するために必要なユーザの秘密をまだ提供していない関係者に対して、特定の準備アクションが実行されることができ、また、何らかの仮の暗号化プロダクトを生成できるという利点をもたらす。
【００１３】
実施形態によっては、前記事前プロビジョニング機能は、前記関係者のための前記仮秘密として非対称暗号化システムの一対のエフェメラル鍵を生成し、前記事前プロビジョニング応答において前記一対のエフェメラル鍵の公開鍵を送信するように構成される。これは少なくとも、前記関係者のデジタルIDを後で確立するために必要なステップに追加のセキュリティを提供できるという利点をもたらす。
【００１４】
実施形態によっては、前記事前プロビジョニング機能は、前記ランダムデータ生成部によって提供された乱数を前記一対のエフェメラル鍵の秘密鍵として使用し、Curve25519楕円曲線ディフィー・ヘルマン法（Curve25519 Elliptic Curve Diffie-Hellman method）を使用して、前記一対のエフェメラル鍵の秘密鍵から前記一対のエフェメラル鍵の公開鍵を生成するように構成される。これは少なくとも、生成された鍵ペアが、デジタルIDを確立する関係者によって生成された対応する鍵ペアと数学的に一定の関係を持ちうるという利点をもたらし、これによりプロセスの更なるステップが単純化される。
【００１５】
実施形態によっては、前記事前プロビジョニング機能は、前記一対のエフェメラル鍵の前記秘密鍵と、前記システムの外部のエンティティから受信した公開鍵とを用いて、第1の数学的演算によって第1の共有秘密を生成し、前記識別子と前記少なくとも1つの属性とを暗号化して前記暫定暗号化アーカイブに格納する際に、前記第1の共有秘密を使用するように構成される。これは、上述の鍵間の数学的関係に関連する更なる利点をもたらす。
【００１６】
実施形態によっては、前記システムは、前記第1の暗号処理としてArgon2ハッシュ処理を使用するように構成される。これは少なくとも、暗号中間プロダクトを、よく知られ、広

く適用可能であり、十分なセキュリティレベルで信頼されている方法で生成できるという利点をもたらす。

【００１７】

実施形態によっては、前記システムは、前記デジタルIDを使用して、前記関係者の暗号出力の一部を生成するよう構成される。また、このシステムは、当該システムの署名鍵で暗号出力の少なくとも一部分に署名することで、当該関係者の証明書を生成するように構成されてもよい。これは少なくとも、証明書を、よく知られ、広く適用可能であり、十分なセキュリティレベルで信頼されている方法で生成できるという利点をもたらす。

【００１８】

実施形態によっては、このシステムは、暗号出力の前記一部分の1つとして、非対称暗号化システムの更なる鍵ペアの公開鍵を、Curve25519楕円曲線ディフィー・ヘルマン法を使用して前記デジタルIDから生成するように構成される。これは少なくとも、デジタルIDが確立された関係者が、後でさまざまな暗号化目的のために、このような鍵ペアを利用できるという利点をもたらす。

【００１９】

実施形態によっては、前記システムは、前記デジタルIDの生成後に、登録完了応答の中で前記暗号出力を送信するように構成される。これは少なくとも、デジタルIDが確立された関係者が、システムに再度アクセスしなくとも、システムによって確立された信用を後で利用するために十分なデジタル情報を受信しうるという利点をもたらす。

【００２０】

実施形態によっては、前記システムは、前記登録完了応答において、暗号化された形式の前記暗号シード、及び前記システムの外部のエンティティが使用するための署名された形式の暗号鍵を送信するように構成され、前記暗号鍵は、前記関係者の前記デジタルIDを構成する、又は前記デジタルIDから導出される、非対称暗号化システムの鍵ペアの片割れである。これは少なくとも、デジタルIDが確立された関係者が、システムに再度アクセスしなくとも、システムによって確立された信用を後で利用するために十分なデジタル情報を受信しうるという利点をもたらす。

【００２１】

第２の側面によると、関係者のデジタルIDを確立する方法が提供される。この方法は、ランダムデータとして暗号シードを生成することと、セキュアトランスポート機構を介して外部ソースからユーザの秘密（secret）を受信することとを含む。前記方法は、第1の暗号操作を適用して、前記暗号シードと前記ユーザの秘密の両方に決定論的に依存する暗号中間プロダクトを生成することを含む。前記暗号中間プロダクトは前記関係者の前記デジタルIDを構成する。前記方法は、前記関係者の前記デジタルIDに第2の暗号操作を適用して、暗号化された形式の前記暗号シードを含む暗号出力を生成することを含む。前記方法は、前記暗号出力の少なくとも一部を、前記セキュアトランスポート機構を介して前記外部ソースに送信することを含む。

【００２２】

実施形態によっては、前記方法は、前記暗号出力の生成に前記デジタルIDを使用した後、前記デジタルIDを、永久にメモリから難読化することを含む。これは少なくとも、前記デジタルIDが、後で偶然に明らかになる危険性がないという利点をもたらす。少なくとも、前記方法を実行する前記システムに関連するいかなる動作によっても、後で偶然に明らかになる危険性はない。

【００２３】

実施形態によっては、前記方法は、前記第2の暗号操作を通じて、前記暗号出力の一部として前記関係者の暗号証明書を生成することを含む。これは少なくとも、前記関係者が、前記方法を実行するシステムに再びアクセスすることなく、前記暗号証明書を後で認証に使用できるという利点をもたらす。

【００２４】

実施形態によっては、前記方法は、前記関係者の識別子及び少なくとも1つの属性を示す

、受信した事前プロビジョニング要求に対して、前記関係者のための仮秘密を確立し、前記仮秘密の少なくとも一部を含む事前プロビジョニング応答を送信することを含む。そして前記方法は、前記仮秘密を確立することの一部として、前記暗号シードを使用して前記識別子及び前記少なくとも1つの属性を暗号化し、前記関係者に固有の暫定暗号化アーカイブに格納することを含んでもよい。

【００２５】

前記方法は更に、前記事前プロビジョニング応答の前記送信後に受信した登録完了要求に対して、前記登録完了再要求の内容を前記仮秘密に照らして検証することにより応答することを含んでもよい。

【００２６】

前記方法は、前記登録完了要求で受信した前記ユーザの秘密を使用して、前記識別子及び前記少なくとも1つの属性を暗号化し、前記関係者に固有の最終暗号化アーカイブに格納することと、前記識別子及び前記少なくとも1つの属性の前記暗号化及び前記最終暗号化アーカイブへの格納において、前記デジタルIDを使用することと、を含んでもよい。これは、少なくとも、ユーザの登録を完了するために必要なユーザの秘密をまだ提供していない関係者に対して、特定の準備アクションが実行されることができ、また、何らかの仮の暗号化プロダクトを生成できるという利点をもたらす。

【図面の簡単な説明】

【００２７】

【図１】例示的な実施形態において、ユーザ機器とトラストプロバイダが行う動作を示す。

【図２】別の例示的実施形態で行われるいくつかの動作を示す。

【図３】図１に示した動作のより詳細な一例を示す。

【図４】図１に示した動作のより詳細な一例を示す。

【図５】図１に示した動作のより詳細な一例を示す。

【図６】図１に示した動作のより詳細な一例を示す。

【図７】図１に示した動作のより詳細な一例を示す。

【図８】図１に示した動作のより詳細な一例を示す。

【図９】例示的な実施形態において、ユーザ機器とトラストプロバイダが行う動作を示す。

【図１０】例示的な実施形態において、ユーザ機器、サービスプロバイダ、及びトラストプロバイダの間で行われる動作と交換されるメッセージを示す。

【図１１】図１０に示した動作のより詳細な一例を示す。

【図１２】図１０に示した動作のより詳細な一例を示す。

【図１３】図１０に示した動作のより詳細な一例を示す。

【図１４】図１０に示した動作のより詳細な一例を示す。

【図１５】図１０に示した動作のより詳細な一例を示す。

【図１６】図１０に示した動作のより詳細な一例を示す。

【図１７】例示的な実施形態において、ユーザ機器、サービスプロバイダ、及びトラストプロバイダの間で行われる動作と交換されるメッセージを示す。

【詳細説明】

【００２８】

以下の説明では、本開示が具現化され得る特定の形態が例示として示されている、添付図面を参照する。添付図面は本開示の一部を構成する。本開示の範囲から逸脱することなく、他の形態を利用することができ、構造的又は論理的な変更を行うことができることを理解されたい。従って、以下の詳細説明は、本開示の範囲は添付の特許請求の範囲によって定義されるため、限定的な意味で捉えられるものではない。

【００２９】

例えば、記載された方法に関連する開示は、その方法を実行するように構成された、対応する装置又はシステムにも当てはまる場合があり、その逆もまた同様であることを理解さ

れたい。例えば、特定の方法ステップが記載されている場合、対応する装置は、たとえそのようなユニットが図に明示的に記載又は図示されていなくても、記載された方法ステップを実行するユニットを備え得る。一方、例えば、特定の装置が機能ユニットに基づいて記述されている場合、対応する方法は、たとえそのようなステップが図において明示的に記述又は図示されていなくても、記述された機能を実行するステップを含み得る。更に、本明細書で説明する様々な例示的側面の特徴は、特に断りのない限り、互いに組み合わせることができることを理解されたい。

【００３０】

デジタルIDの概念は、以下の説明の中心である。デジタルIDは、暗号ID（cryptoidentity）と呼ばれることもある。概念として、デジタルID又は暗号IDは、関係者を確実に識別するのに十分な一意性を持つデジタル情報片として特徴付けられうる。例えば、数学的アルゴリズムを使用して、デジタルID又は暗号IDをシードとして使用して、暗号鍵、鍵のセット、証明書、デジタル署名などの暗号プロダクトを生成する場合、その特定のデジタルIDを知らずに同じ暗号プロダクトを取得できる可能性が、実質的に不可能といえる程度まで低くなければならない。このような暗号プロダクトを提示できる関係者は、そのデジタルIDで識別される関係者であると安全に仮定されることができる。もちろん、デジタルIDの生成及び処理に適切な注意が払われていることが前提である。

【００３１】

デジタルID又は暗号IDの真正性、ひいてはそこから生成される暗号プロダクトの信頼性は、信頼できる関係者がその生成において役割を果たすことで、大幅に向上しうる。この信頼できる関係者は、既知のトラストプロバイダに匹敵する関係者でありうる。このため、本明細書ではトラストプロバイダという用語も使用する。代替として、Vaultプロバイダ及び／又はウォレットプロバイダという用語を使用することもできる。また、CA（Certification Authority，認証局）及び/又はVA（Validation Authority，検証局）という略語を使用することもできる。

【００３２】

デジタルID又は暗号IDの性質は、従来の紙文書の世界との比較で比喩的に示すことができる。この明細書が書かれた時点では、パスポートには、使用者の生体データ（顔画像や指紋など）に由来するデジタル符号化された情報が含まれている必要がある。ユーザの顔と指紋は、ユーザの身元を表すものである。一方、パスポートは「暗号プロダクト」である。ユーザの顔がどのように見え、指の指紋がどのように形成されているかを知らなければ、全く同じパスポートを作ることは不可能である。一方、パスポートの技術的な詳細を全て適切に作成する方法を知っているのは、適切な政府当局だけである。更に当局は、顔画像と指紋を提示した人物が確かに特定されたことを適切に確認した後にのみ、パスポートの作成に同意する。このように、パスポート当局は、身元を保証する上でも、そこから「暗号プロダクト」 を製造する上でも、トラストプロバイダに匹敵する役割を担っている。

【００３３】

図1は、関係者(Party)のデジタルIDを確立するためのシステム100を左側に示す。この場合、関係者はユーザ機器110のユーザである。前記システムは、ランダムデータ生成部101を備える。「ランダムデータ生成部」の頭字語TRNGは、”True Random Number Generator”に由来する。以下の説明でより明らかになる目的のために、ランダムデータ生成部101として、この目的のために特別に作られた集積回路のような専用の装置を利用するのが有利である。最も有利な場合、ランダムデータ生成部101によって生成されるランダムデータは、最先端技術から利用可能な最大のエントロピーを含んでいる。ランダムデータ生成部101の出力の一例は、図1において、秘密乱数102として示されている。簡便かつ簡潔に表すため、秘密乱数102は暗号シードとも呼ばれる。本文中で簡潔に表すため、指定子PUOを用いて指定することもある。

【００３４】

ユーザ装置110は、入力手段111と装置回路112の少なくとも一方を備える。装置回路112は

、図1においてユーザの秘密113として示されているものを生成することができる。入力手段111が存在する場合、入力手段111は、例えば、一組のキー、タッチパッド、タッチセンサ式ディスプレイ、指紋スキャナ、虹彩スキャナ、デジタルカメラ、マイクのいずれか1つ又は複数を備えてもよい。ユーザは、そのような入力手段111のいずれかを利用して、ユーザの秘密113として一意のデジタル情報片をユーザ装置110に自由に入力してもよい。そのような一意のデジタル情報片は、例えば、記憶されたPINコード、指紋のような生体認証情報、又はユーザのバイオインプラントから読み取られたデジタル情報片であってもよい。ユーザの秘密113を生成するために使用される場合、装置回路112は、ランダムデータ生成部などを備えてもよい。ユーザ機器においてユーザの秘密113を生成することは、1つ又は複数の初期デジタルデータについての暗号に関する何らかの結果（例えばハッシュ）を計算するような、追加の操作を含んでもよい。当該初期デジタルデータは、入力手段111、装置回路112、又はその両方から受け取られてもよい。非限定的な例として、ユーザの秘密113は、例えばArgon2ハッシュなどの一方向ハッシュアルゴリズムで、1つ又は複数の初期デジタルデータから計算された256ビットハッシュであってもよい。ユーザの秘密113はまた、ユーザのシークレットソルト（User's Secret Salt）USSと呼ばれることもある。

【００３５】

以下の説明において、暗号シード又はP_{U0}102と、USS113とは、互いに完全に独立した2つの別個の環境に由来することに注意することは重要である。図1に示す実施形態では、ブロック103に示すように、暗号シード又はP_{U0}102は、システム100で後に検索できるように格納される。このような保存は、ユーザ固有の、いわゆる暫定暗号化アーカイブ（Provisional Encrypted Archive）を作成する形で行われてもよい。本明細書では、KUA(Keystore User Archive，すなわち鍵を格納するユーザアーカイブ)という略語を使用する。このため、この段階では、暗号シード又はP_{U0}102(及び場合によっては、ユーザ固有の他のデータ)を含む、暫定暗号化アーカイブを、KUA(P_{U0},...)と表すことができる。また、全ての暗号化アーカイブが、ユーザ機器110ではなく、システム100に保存されている場合、VUA(Vault User Archive，Vaultユーザアーカイブ)と呼んでもよい。

【００３６】

同様に、USS113は、ブロック114で示されるように、ユーザ機器110において後で検索可能なように記憶される。実施形態によっては、USS113をユーザ機器110に全く記憶させず、USS113が必要とされる度にユーザにUSS113を再生成することを要求することが有利である。例えば、ユーザは、PINコード又はパスワードを記憶し、それが必要とされる度に、ユーザの秘密（USS）としてそれを入力することを要求されてもよい。追加的に、又はその代わりに、ユーザは、USS113が必要とされるたびに、指紋、虹彩スキャン、バイオインプラントなどのようなバイオメトリック識別情報をユーザ機器110に読み取らせることを要求されてもよい。

【００３７】

セキュアなトランスポート機構120が、ユーザデバイス110とシステム100の間に存在する。セキュアトランスポート機構120の正確な特性は、本明細書を書いた時点でTLS（Transport Layer Security）プロトコルで得られるものと少なくとも同等の通信セキュリティを提供する限り、重要ではない。好ましい実施形態では、共有鍵又は専用鍵ペアによる暗号化など、データコンテンツの暗号化保護が関係者間で使用されてもよい。これによっても、セキュアトランスポート機構120の更なる性質はあまり重要でなくなる。一例として、セキュアトランスポート機構120は、TLSプロトコルによって保護された、1つ以上のデジタルネットワークを介した通信接続であってもよい。代替例として、ユーザが物理的に存在し、ディスプレイ、ケーブル、又はユーザ機器110の他の出力手段を利用して、システム100の対応する入力手段にユーザが情報を伝達するような、全く別のものであってもよい。

【００３８】

この例では、セキュアトランスポート機構120は双方向である。これは、システム100とユ

ーザ機器110の両方がセキュアトランスポート機構120の受信側と送信側を有することを意味する。通信のセットアップと維持の便宜のために、セキュアトランスポート機構120の2つの方向は同じ技術を利用することができる。しかし、これは要件ではなく、2つの方向は異なる技術を経由してもよい。

【００３９】

図1ではユーザ秘密113の送信のみが明示的に示されている。しかし、義務ではないが、システム100とユーザ機器110の間でセキュアトランスポート機構120を通じて複数のメッセージが交換されてもよい。一例として、ユーザ機器110は、ある公開鍵PK_{URT}をシステム100に送信してもよく、それに応答してシステム100は、例えばCurve25519楕円曲線ディフィー・ヘルマン法を使用して、対応する秘密鍵SK_{UAT}から生成した別の公開鍵PK_{UAT}をユーザ機器110に送信してもよい。添え字のURTとUATは、それぞれUser Request Token(ユーザ要求トークン）とUser Access Token（ユーザアクセストークン）に由来するものであり、簡潔に表すために用いられているが、何かを限定することを意図してはいない。

【００４０】

URT関連鍵とUAT関連鍵が前述の例のように交換された場合、ユーザの秘密113をユーザ機器110からシステム100に安全に伝送する1つの可能な方法は、AES256-GCM暗号化方式を利用することである。ここで頭字語のAESはAdvanced Encryption Standardに由来し、頭字語のGCMはGalois/Counter Mode（ガロア/カウンターモード）に由来する。上記で紹介した表記法を用いると、セキュアトランスポート機構120を介した対応する伝送は、以下のように表すことができる。

$AES256\text{-}GCM(SHA2(X25519(SK_{URT}, PK_{UAT}) \,||\, PK_{URT} \,||\, PKUAT \,||\, n), m, n, USS)$

【００４１】

ここで、SHA2()は、括弧内の引数に対して実行されるSecure Hash Algorithm 2（SHA-2，「シャーツー」と呼ばれることがある）の実行を示し、X25519()は、括弧内の引数に対してCurve25519楕円曲線ディフィー・ヘルマン法を適用することを示す。文字mは暗号化認証タグのMAC又はメッセージ認証コードを示し、文字nは暗号ノンスを示す。二重の縦線||はビットごとの論理和演算を意味する。

【００４２】

セキュアトランスポート機構120を通じてユーザの秘密113を受け取った後、システム100は、暗号化操作104を実行するように構成される。「操作」（operation）という用語は、暗号化の動作と、そのような暗号化を実行するための手段の両方を意味すると理解され得る。暗号化（encrypting）に加えて、又は暗号化の代わりに、他の暗号操作（cryptographic operation）が使用され得る。一般的に述べれば、システム100は、前記ランダムデータ生成部101と前記セキュアトランスポート機構120の前記受信端とに結合された第1の暗号操作104を備えると考えられてもよい。

【００４３】

図1の実施形態では、暗号シード又はP_{U0}102が暗号化操作104への入力を構成し、セキュアトランスポート機構120を介して受信したユーザの秘密113が暗号化操作104への暗号鍵を構成する。暗号化操作104の出力は、ユーザのデジタルID105である。言い換えると、システム100は、前記第1の暗号操作104を通じて、前記暗号シード（P_{U0}）102と、前記セキュアトランスポート機構（120）を通じて受信したユーザの秘密（USS）113との両方に決定論的に依存する暗号中間プロダクト105を生成するように構成されており、この暗号中間プロダクト（105）はユーザの前記デジタルIDを構成する。図2は、（第1の）暗号処理204がハッシュ処理であり、暗号シード（P_{U0}）102が入力、ユーザの秘密（USS）113がソルトを構成する代替案を示す。

【００４４】

第1の暗号操作104の正確な性質(暗号化、ハッシュなど)に関係なく、その出力、すなわち暗号中間プロダクト105は、数学的な操作によって生成されたものではない、一意の予測不可能なランダムエンティティである。このことは、第1の暗号操作104は数学的であるが、その入力(暗号シード又はP_{U0}102及びユーザの秘密又はUSS113)の相互独立性により、生

成オペレーションが全体として数学的でないことを意味する。

【００４５】

エントロピーの観点からは、前記一意の予測不可能なランダムエンティティのランダム性は、暗号シード又はP_{U0}102と同程度の高い品質である。このことは、暗号シード又はUSS113の生成が、外部から取得したユーザの秘密鍵又はUSS113によってソルト付け（salted）又は鍵付け（keyed）されたかどうかに関係なく当てはまる。その結果、前記ユニークで予測不可能なランダムエンティティのランダム性は、潜在的に、量子的耐性さえ有する。ただし、その2つの元の要素（暗号シード又はP_{U0}、ユーザの秘密情報又はUSS113）のみが利用可能な場合（例えばそれぞれの格納場所103及び114から取得できる場合）、完全に再現可能である。USS113の場合、先に説明したように、USS113が利用可能であるということは、ユーザがUSS113をもう一度入力する必要があることを意味する場合がある。

【００４６】

前記一意の予測不可能なランダムエンティティのビット数は、暗号シード又は P_{U0}102と、ユーザの秘密又はUSS113のビット数の合計に等しくてもよい。ただし、一度に非常に大きな結果を生成するように暗号操作104を選択することは、有利で有り得る。例えば数百万ビットの結果を生成すれば、これを後で、暗号に関する様々な目的に利用できる。

【００４７】

このような、暗号に関する更なる目的は、一般に、図1の更なる暗号アルゴリズムブロック106で表される。更なる暗号アルゴリズム又は第2の暗号操作106は、例えば鍵生成アルゴリズムでありうる。ユーザのデジタルID105は高品質な暗号ランダムデータであるため、トラストプロバイダは、それを例えば鍵生成に利用してもよい。例えば、非対称暗号化システムと対称暗号化システムのいずれか又は両方の鍵生成に利用してもよい。更に、又は代替的に、ユーザのデジタルID105は、暗号ノンス、暗号ソルト、及び／又は証明書の鍵ペアを生成するための暗号シードとして使用することができる。このような可能性のある使用は全て、一般に、更なる暗号アルゴリズムブロック106でカバーされる。

【００４８】

一般に、このシステムは、ユーザのデジタルID105を使用し、前記更なる暗号アルゴリズム又は第2の暗号操作106を通じて、暗号出力107を生成するように構成されていると言えるだろう。後で詳しく説明する理由により、暗号シード(P_{U0})102を暗号化された形式で暗号出力107の一部に含めることが有利である。

【００４９】

ユーザのデジタルID105は、更なる暗号アルゴリズム又は第2の暗号操作106の目的で直ちに使用するのに必要な期間よりも長く保存しないことが望ましい。図1の左下に模式的に示すように、システム100は、その後、デジタルID105をメモリから恒久的に難読化するように構成される。少なくとも理論的には、デジタルID105を何らかの記憶装置で利用可能な状態にしておくと、2つの元の秘密(暗号シード又はP_{U0}102と、ユーザの秘密又はUSS113)のうち少なくとも1つを後で暴露できる可能性がある。暗号化技術又はハッシュ関数104に何らかの脆弱性が発見される可能性、及び/又はユーザの秘密又はUSS113が暴露される可能性があり、その場合、当該リスクが現実のものとなる。

【００５０】

図3～図6は、図1及び図2のシステム100における第1及び第2の暗号操作の例を示す。符号102は、トラストプロバイダのシステムにおいて、高品質ランダムデータ生成部によって生成された暗号シード（上記ではP_{U0}）に対して使用されている。符号113は、セキュアトランスポート機構を介してユーザから受信したユーザの秘密（上記ではUSSとも呼ばれる）に対して使用されている。図3から図6の全ての実施形態に共通する特徴は、システムが、第1の暗号操作によって、前記暗号シードと前記（ユーザの）秘密の両方に決定論的に依存する暗号中間プロダクトを生成するように構成されていることである。暗号中間プロダクトは、ユーザのデジタルIDを構成する。また、これらの実施形態に共通するのは、前記システムが、第2の暗号操作を通じて、ユーザの前記デジタルIDを使用して、暗号化された形式の前記暗号シードを含む暗号出力を生成するように構成されていることである。

【００５１】
図3の実施形態では、第1の暗号操作304には、暗号シード102、ユーザの秘密113、及び1つ又は複数の属性301の3つの入力がある。好ましくは、属性301は、デジタルIDを生成する特定のユーザに関連するユーザ固有の属性である。ただしそれに限られるものではない。加えて、又は代替的に、前記複数の属性の少なくとも1つは、ユーザの証明書を検証したトラストプロバイダに関連する。例えば、トラストプロバイダの識別子を属性として使用してもよい。第1の暗号操作304は、例えば1つ以上の暗号操作及び／又はハッシュ操作を含んでもよく、これからユーザのデジタルID105が暗号化中間プロダクトとして得られてもよい。この入力及び可能性のある更なる入力302は、第2の暗号操作306の入力となってもよい。図3は、第2の暗号操作306からの暗号出力がどのように見えるか、又はどのように指定されるべきかについて、いかなる見解も示していない。これらの例については後に詳述する。
【００５２】
図4の実施形態が図3の実施形態と異なる点は、第1の暗号操作404の入力として属性が用いられない点である。従って、暗号中間プロダクト(ユーザのデジタルID105)は、暗号シード102とユーザの秘密113のみに依存する。ブロック402には、図3の実施形態と同様に、第2の暗号操作406への入力の1つとして、属性と可能性のある更なる入力が示されている。
【００５３】
図5の実施形態が図3及び図4の実施形態と異なるのは、いわゆる事前プロビジョニングが含まれている点である。この事前プロビジョニングは、図5では第1の暗号操作の前半501として示されている。システムはこれを、例えば、セキュアトランスポート機構を介してユーザの秘密113を受信する前に実行することができる。事前プロビジョニングの入力には、暗号シード102と、ユーザに関連する１つ又は複数の属性301が含まれる。事前プロビジョニングの結果505は、例えば、事前プロビジョニングが実行されるユーザに固有の、いわゆる暫定暗号化アーカイブを含んでもよい。
【００５４】
第1の暗号処理の後半が図5の502に示されている。入力の1つはユーザの秘密113である。事前プロビジョニング結果505又はその少なくとも一部は、第1の暗号操作の後半部502への入力として使用される。加えて、又は代替的に、暗号シード102が第1の暗号操作の後半部502への入力となる場合がある。その出力は、ユーザのデジタルID105である。他の実施形態と同様に、ユーザのデジタルID105は暗号中間プロダクトであり、本文で説明する任意の種類の第2の暗号操作に使用することができる。この際、図3及び図4のような属性及び/又は更なる入力とともに使用されてもよい。
【００５５】
図6は、事前プロビジョニングが行われる点で、図5と類似している。事前プロビジョニングは、第1の暗号操作の前半601として示されている。図5と同様に、事前プロビジョニングの入力は暗号シード102と１つ又は複数の属性301である。事前プロビジョニングはユーザの秘密鍵が受信される前に実行されてもよい。事前プロビジョニングの結果603は、ユーザに固有の暫定暗号化アーカイブを含んでもよい。
【００５６】
事前プロビジョニングの原則が有利に適用される応用として、（個人的にトラストプロバイダとコンタクトを取ったという形では）まだ「存在」していないが、特定の属性がすでに知られている関係者（Party)の電子署名証明書を、事前プロビジョニングを通じて作成する、ということがある。このような電子署名証明書は、将来の使用においても変更されないままである可能性がある。例えば、公的機関が、まだUSSを付与していない人物のためにこのような電子署名証明書を作成するかもしれない。トラスト・プロバイダ（この例では当局）は、属性に基づき、このようなユーザの公開署名鍵を再生成することができる。後にユーザから取得されるUSSは、電子署名証明書に影響を与えない。
【００５７】
第1の暗号操作の後半602は、暗号シード102とユーザの秘密113を入力とし、ユーザのデジ

タルID105を暗号中間プロダクトとして生成する操作である。ユーザのデジタルID105と事前プロビジョニング結果603は、第2の暗号操作606の入力を構成する。また、図6には示していないが、第2の暗号操作606への他の入力が存在する場合もある。図6に暗号プロダクト107として示す暗号出力には、暗号化された暗号シードが少なくとも含まれる。

【００５８】

図7は、更なる暗号アルゴリズム又は第2の暗号操作が証明書生成アルゴリズム706である例を示す。（更なる暗号アルゴリズム又は第2の暗号操作は、図1では106として示されていた。符号306、406、606も同様である。）ユーザのデジタルID105に加えて、証明書が含むべき属性、及び/又は所望の証明書プロダクト707を適切に生成するために必要な更なる鍵など、他の入力を使用してもよい。先に述べたことと同様に、属性はゼロ、1つ、又はそれ以上である可能性があり、当該属性はユーザ、トラストプロバイダ、又はその両方に関連する可能性がある。一般に、上記システムは、更なる暗号アルゴリズム又は第2の暗号操作を通じて、その暗号出力の一部としてユーザの暗号証明書を生成するように構成されてもよい。

【００５９】

図8に示す例では、図7の概念を更に少し詳しく説明する。証明書生成アルゴリズム806の特定の種類の部分として、秘密鍵生成部821、公開鍵生成部822、及び証明書生成部823がある。システムは、秘密鍵生成部821への入力としてユーザのデジタルID105を使用し、ユーザの秘密鍵831を生成するように構成される。更に、システムは、生成された秘密鍵を公開鍵生成部822への入力として使用し、ユーザの公開鍵832を生成するように構成される。証明書ジェネレータ823は、基本的に、トラストプロバイダの秘密署名鍵841を使用して、生成された公開鍵に署名する。署名操作に伴い、属性842が選択されてもよい。システムは、例えば、必要な証明書833を受領した後にユーザが利用する予定のサービスプロバイダから、属性を、好ましくは暗号化された形式で、受領している可能性がある。トラストプロバイダに関連する１つ又は複数の属性を使用してもよい。図7の概念的なレベルと比較すると、ユーザの秘密鍵831、公開鍵832、及び証明書833は、証明書生成アルゴリズム806の有用な出力である証明書プロダクト807を形成する。

【００６０】

従って、図8は、デジタルID105を使用して関係者の暗号出力を生成するようにシステムが構成されている実施形態の一例である。更に、図8の実施形態では、システムは、システムの署名鍵841を使用して暗号出力の少なくとも一部に署名することにより、前記関係者の証明書を生成するように構成されている。この実施形態では、暗号出力の一部として、前記デジタルID105から、非対称暗号化システムの鍵831及び832のペアの、公開鍵832を生成するように構成されている。このような公開鍵832を生成する例としては、まず、SKUIDと呼ばれる秘密鍵831を生成する。

【００６１】

SK_{UID}= Argon2Id(P_{U0}, USS)

【００６２】

ここで、Argon2Id()はArgon2ハッシュアルゴリズムを利用することを意味する。そして、対応する公開鍵PK_{UID}の生成に進む。

【００６３】

PK_{UID}= X25519(SK_{UID}) = X25519(Argon2Id(P_{U0}, USS)).

【００６４】

Argon2アルゴリズムは計算量が非常に多いため、SHA2アルゴリズムのような、より簡単な生成方法を使用してもよい。

【００６５】

PK_{UID}= X25519(SKUID) = X25519(SHA2(P_{U0}|| USS)).

【００６６】

公開鍵PK_{UID}をシステム100の署名鍵で署名した結果を、$SIGN_{UID}$と表してもよいだろう。

生成される可能性のある暗号プロダクトの1つは、ユーザに固有の最終暗号化アーカイブ

である。このような最終暗号化アーカイブに含まれる情報要素は、例えば暗号シードP_{UO}、公開鍵PK_{UID}、証明書$SIGN_{UID}$などである。暗号鍵として、例えばユーザの秘密USSを使用することができる。このような場合、最終暗号化アーカイブは以下のように指定される。

【００６７】

$Enc(USS, KUA(P_{UO}, PK_{UID}, SIGN_{UID}, \cdots))$.

【００６８】

図1～図8は、システムが出力、すなわち暗号プロダクト107及び/又は証明書プロダクト707又は807をその後どのように使用するかについては、いかなる見解も示していない。鍵831及び832は主にユーザ機器110が使用するものである。従って、例えば自然な可能性には、システム100が、例えば図1と同じ又は類似のセキュアトランスポート機構120を介して、少なくとも鍵831及び832を運ぶ応答をユーザ機器110に送信するように構成されており、それによってユーザ機器110が鍵831及び832を所有するようにする、というものがある。また、図8の場合のように証明書833が生成されている場合は、それも伝送される。一般に、システム100は、暗号出力107の少なくとも一部を前記セキュアトランスポート機構120を通じて伝送するように構成されている。

【００６９】

先に紹介した表記法を使用すると、暗号出力107の少なくとも一部を暗号化する1つの可能な方法は、まず暗号鍵K_{KUA}を以下のように生成することである。

【００７０】

$K_{KUA} = SHA2(X25519(SK_{UAT}, PK_{URT}) \,||\, PKUAT \,||\, PKURT \,||\, n)$

【００７１】

そして、それを使って最終暗号化アーカイブを次のようにエンコードする。

【００７２】

$Enc(K_{KUA}, KUA(P_{UO}, \cdots))$.

【００７３】

図9は、暗号出力107の少なくとも一部が、セキュアトランスポート機構120を介して受信された後、ユーザ機器110で利用される可能性のある1つの方法を示す。ユーザ機器が受信した暗号出力107の一部が、暗号化された形式の暗号シード(P_{UO})102であったと仮定すると、図9の暗号シード(P_{UO})102に関する箇所に示すように、デコーダ901が暗号シードを抽出するように構成される可能性がある。ユーザ機器は、ユーザの秘密（USS）113を安全な記憶装置から取得するか、又はユーザにもう一度入力するよう要求することができ、その後、ユーザ機器110は、図1のステップ104（又は図2のステップ204や、図3～6の対応するステップ）でシステム100が行ったのと同様の、（第1の）暗号操作904を適用することで、ユーザのデジタルID905を再現することができる。ユーザのデジタルID905を再現できるというユーザ機器110の能力は、図9のようにシステム100から応答を受信した後、ユーザのデジタルID905から導出される、又は導出できる暗号プロダクトの後の全ての使用に関して、ユーザ機器110はシステム100から独立していることを意味する。前述のパスポートの例に簡単に戻ると、ユーザは現在、トラストプロバイダが 発行した「パスポート」を受け取っている。「パスポート」の生成における暗号シード(P_{UO})102の役割と、それをユーザ機器110に配信する際に講じられた適切な暗号化対策により、ユーザ機器110が更なる暗号操作906を適用して導出した暗号プロダクト907は、ユーザがユーザ機器110を使用して通信を希望する第三者によって、十分に信頼できるレベルでデジタル検証されることが保証される。

【００７４】

図9に示すように、ユーザ機器110のデコーダ901は、受信した暗号プロダクト107の他の有用な部分も抽出することができる。このような抽出された部分は、暗号操作906の入力として使用することができる。ユーザのデジタルID905は、ユーザ機器110に保存したままにしておかないほうが有利であろう。少なくとも長期間保存しておかない方が有利である。ユーザは、ユーザの秘密113をもう一度入力しなければならないかもしれないが、ユーザ

機器110は、いずれにせよ、いつでもユーザのデジタルID905を再生成することができる。これに対応して、図9は、可能な更なる暗号操作907のいずれかを実行した直後に、ユーザ装置がメモリからユーザのデジタルID905を難読化する様子を示す。

【００７５】

図10は、例示的な実施形態において、ユーザ、サービスプロバイダ、及びトラストプロバイダの間で行われるアクション及び交換されるメッセージにおいて、上記で説明した原理がどのように適用されうるかの一例を示す。図10では実行者が関係者（Party）として名前が付けられているが、本明細書で説明する動作は、当然ながら、そのような関係者によって所有され、及び／又はそのような関係者に代わって操作される、装置及び／又は機器によって行われる動作である。従って、例えば、図10の左端の縦列を参照して本明細書で説明する動作は、図1-4の上記のようなシステムの動作である。「サービスプロバイダ」という表現は、広い意味で理解されなければならず、民間企業に加え、当局などもサービスプロバイダとみなすことができる。代替的に、サービスプロバイダとみなされている関係者（Party）は、RA（Registration Authority，登録機関）とみなすこともできる。図11～16は、図10において特定の動作がどのように有利に行われうるかの、より詳細な例を示す。

【００７６】

図10の特徴は、トラストプロバイダ側の2段階のプロセスを示していることである。この2つのステップは、前述の図5及び図6の説明と同様に、事前プロビジョニングステップと登録完了ステップと呼んでもよい。第1のステップでは、基本的にサービスプロバイダ（すなわち、図10の中央に示す関係者）が、ユーザのデジタルIDを生成するための実際の要求を行う。サービスプロバイダは、その段階ですでにサービスプロバイダが知っており、サービスプロバイダがすでに信頼関係を確立しているユーザに関してこれを行う。対応する以前の操作がどのようなものであったかはここでは重要ではないが、信頼関係の確立は、顧客サービス、登録機関、又はeIDAS認可モデルで完了したと仮定してもよいだろう。eIDASという頭字語は、欧州連合（EU）が2014年に制定した電子的な本人確認、認証、信頼サービスに関する規制を指す。

【００７７】

このように、サービスプロバイダは、何らかの方法でユーザを特定すると共に、ユーザの一意的な識別子に結びついた特定の属性を持つ保護されたアーカイブをトラストプロバイダが作成することを望む。ここでいう一意の識別子は、合理的な信頼性で正しいユーザと関連付けられる限り、秘密である必要はない。例えば、ユーザのMSIN（携帯電話加入者識別番号）、又はより馴染みのある携帯電話番号が、一意の識別子として機能することがある。本明細書では、一意な識別子をUIDという頭字語を用いて略して示す。

【００７８】

図10において、ステップ1001で、ユーザはメッセージを作成し、それを登録要求1002としてサービスプロバイダに送信する。登録要求1002は、例えばSMS（ショートメッセージサービス標準に従ったテキストメッセージ）として送信することができる。SMSにはユーザのUID（携帯電話番号）が自動的に添付され、サービスプロバイダが容易に認識できるという利点がある。

【００７９】

実施形態によっては、登録要求1002は、ペイロードとしてユーザの公開鍵を含んでもよい。ペイロードという用語はメッセージの内容を意味するが、これに加えて、1つ以上の通信プロトコルで定義されるメタデータ及び/又はヘッダ情報などがあってもよい。図11のサブステップ1101に示すように、ユーザ機器は、保護された鍵ストアなどのストレージから公開鍵PK_{URT}を読み出してもよい。あるいは、ユーザ機器は、この特定の目的のために、公開鍵PK_{URT}をオンザフライで生成してもよい。添え字の頭文字URTは、User Request Tokenを意味する。一例として、公開鍵PK_{URT}は、ユーザ機器内の乱数生成部からの256ビットの出力（RNG(256)で表される）であってもよい。図11のサブステップ1102は、ユーザ機器が図10に示す登録要求1002を作成し、送信することを表す。

【００８０】
ステップ1003で、サービスプロバイダはUIDを所望の属性と関連付け、ユーザのデジタルIDを生成するための要求となるものを準備する。図10において、当該要求は、AddUserリクエスト1004として示されている。AddUserリクエスト1004をトラストプロバイダに伝えるには、セキュアトランスポート機構を使用する必要がある。一例として、AddUserリクエスト1004は、TLSプロトコルによって保護された、1つ以上のデジタルネットワークを介した通信接続を通じて伝達されてもよい。トラストプロバイダ側で事前プロビジョニングステップをトリガするため、AddUserリクエスト1004は事前プロビジョニング要求と呼ばれることもある。
【００８１】
AddUserリクエストは、ユーザの識別子（UID）及びユーザの少なくとも1つの属性を含んでもよく、又は少なくとも高い信頼度で示すことができる。ユーザ・メタ・データ（User Meta Data）の略語であるUMDは、一般に、ユーザに関連付けられ、サービスプロバイダがトラストプロバイダに作成を要求する保護されたアーカイブに格納される1つ又は全ての属性を表すために使用することができる。要するに、AddUserリクエスト1004は、PK_{URT}、UID、及びUMDを含むか、少なくとも高い信頼度で示すべきである。ステップ1003でサービスプロバイダが取る動作の一例を図12に示す。サブステップ1201は、ユーザから登録要求1002を受信し、UIDに注目することに対応する。サブステップ1202は、登録要求1002の内容を読み取り、格納することに対応する。サブステップ1203は、所望の属性をUIDに関連付けることに対応する。サブステップ1204は、AddUserリクエスト1004を準備し、トラストプロバイダに送信することに対応する。
【００８２】
上記の説明では、公開鍵PK_{URT}は、サービスプロバイダからではなく、ユーザから発信されたものと仮定した。その当然の帰結として、対応する秘密鍵SK_{URT}はユーザのみが所有し、ユーザ機器の安全な鍵ストアに保存されていると仮定する。更なる帰結として、ある情報が公開鍵PK_{URT}で暗号化された場合、ユーザのみが秘密鍵SK_{URT}を使用してその情報を復号することができる。代替的な実施形態によれば、サービスプロバイダは、ユーザから登録要求1002を最初に受信することなく、又は少なくともユーザから公開鍵PK_{URT}を受信することなく、AddUserリクエスト1004を作成して送信してもよい。このような場合、サービスプロバイダは、対応する公開鍵をAddUserリクエストのペイロードに含め、対応する秘密鍵をサービスプロバイダの安全な鍵ストアに保存しておく。このことは、どこかの情報がサービスプロバイダの公開鍵で暗号化された場合、サービスプロバイダのみが、その秘密鍵を使用して、後でその情報を復号できることを意味する。この考察は、以下に説明する次のステップにおいて、ある重要な意味を持つ。
【００８３】
図10のステップ1005は、トラストプロバイダが実行する事前プロビジョニングステップである。一般的な特徴として、トラストプロバイダのシステム中の事前プロビジョニング機能は、関係者の識別子（UID）及び少なくとも1つの属性（UMD）を示す、受信した事前プロビジョニング要求（AddUserリクエスト1004）に対して、当該関係者のための仮秘密を確立し、前記仮秘密の少なくとも一部を含む事前プロビジョニング応答（図10のAddUser応答1006）を送信することにより、応答するように構成される。更に、前記事前プロビジョニング機能は、ランダムデータ生成部（図1の101に相当）から提供される暗号シード（図1の102に相当）を使用して、前記識別子（UID）及び前記少なくとも1つの属性（UMD）を暗号化し、前記関係者に固有の暫定暗号化アーカイブに格納するように構成される。
【００８４】
注目すべき詳細は、図10の実施形態では、ステップ1005において、トラストプロバイダは、図1を参照して先に説明したユーザの秘密113に相当するものをまだ所有していないことである。従って、このステップでは、トラストプロバイダはまだユーザの適切なデジタルIDを生成できない。これは、内部ランダムデータ生成部によって提供されるランダムデータと、ユーザから取得した更なる秘密の両方を暗号操作にかける必要があるためである。

そのために、「事前プロビジョニング」と呼ばれている。

【００８５】

図13は、図10のステップ1005に含まれる可能性のあるサブステップの例を示す。サブステップ1301で、システムはAddUserリクエスト1004を受信し、そのコンテンツ、すなわちPK_{URT}、UID、及びUMDを読み取る。サブステップ1302は、ユーザのための仮秘密を確立することを表す。この例では、仮秘密は非対称暗号化システムの鍵のペアを含む。これらの鍵は、ユーザとトラストプロバイダとの間のその後の通信で一度だけ使用されることを意図しており、そのため、ここでは非対称暗号化システムのエフェメラル鍵ペアと呼ぶ。これらはPK_{UAT}、SK_{UAT}と頭字語表記される。添え字のUATはUser Access Tokenに由来する。好都合にも、ランダムデータ生成部から得られる暗号シードは、ユーザの仮秘密を確立する際に利用される。

【００８６】

具体的かつ非限定的な例として、前記事前プロビジョニング機能は、前記ランダムデータ生成部によって提供される256ビットの乱数を前記一対のエフェメラル鍵の秘密鍵SK_{UAT}として使用し、Curve25519楕円曲線ディフィー・ヘルマン法（Curve25519 Elliptic Curve Diffie-Hellman method）を使用して、前記一対のエフェメラル鍵の秘密鍵SK_{UAT}から前記一対のエフェメラル鍵の公開鍵PK_{UAT}を生成するように構成される。

【００８７】

サブステップ1303は、ユーザに固有の暫定暗号化アーカイブを作成することを表す。暗号化のために、いわゆる共有秘密（Shared Secret）を使用することが有利であり、この共有秘密は、トラストプロバイダとユーザとの間で共有される（又は共有されることになる）。前述の公開鍵PK_{URT}がユーザからではなくサービスプロバイダから発信されたものである別のケースでは、この段階で使用される共有秘密も、トラストプロバイダとサービスプロバイダの間で共有されてもよい。

【００８８】

ここでは、サブステップ1303で暫定暗号化アーカイブを作成するために使用される共有秘密について、SS_{UST}という呼称が使用されている。添え字の頭字語USTは、User Session Token（ユーザ・セッション・トークン）に由来する。SS_{UST}を作成する有利な方法の一つは、AddUserリクエストで受信した秘密エフェメラル鍵SK_{UAT}と公開鍵PK_{URT}のスカラー倍を実行することである。言い換えれば次の通りである。

【００８９】

SS_{UST}= scalarmult(SK_{UAT}, PK_{URT}).

【００９０】

上記の”scalarmult”表記は、本質的にスカラー倍を意味するが、X25519やCurve25519のメソッドを使用すると表現することもできる。得られる利点は、鍵ペア間の数学的なつながりである。両方の関係者（Party）は、それぞれ自分の秘密鍵と相手の公開鍵を使って、同じ共有秘密を得ることができる。

【００９１】

同様の表記を用い、また保存されたペイロードにKUA(Keystore User Archive, 鍵を格納するユーザアーカイブ)という頭字語を用いると、暫定暗号化アーカイブは以下のように指定される。

【００９２】

Enc(SSUST, KUA~(UID, UMD, P_{U0},…))

【００９３】

秘密エフェメラル鍵SK_{UAT}の起源はランダムデータ生成部から取得された暗号シードにあるため、この例示的なプロセスは、先に提示した特徴に従う。すなわち、事前プロビジョニング機能は、暫定暗号化アーカイブを作成する際に暗号シードを使用するように構成される。より形式的な特徴付けによれば、事前プロビジョニング機能は、システムの外部のエンティティから受信した秘密エフェメラル鍵SK_{UAT}及び公開鍵PK_{URT}を使用して、第1の数学的演算により共有秘密SS_{UST}を生成し、前記識別子$_{UID}$及び前記少なくとも1つの属性U

MD の前記暗号化及び前記暫定暗号化アーカイブへの格納において、前記第1の共有秘密SS_{UST}を使用するように構成され得る。

【００９４】

図13のサブステップ1304は、前述した事前プロビジョニング応答1006の送信を表しており、この事前プロビジョニング応答1006には、サブステップ1302で作成された仮秘密の少なくとも一部が含まれる。特に、事前プロビジョニング応答は、生成されたエフェメラル鍵ペアの公開鍵PK_{UAT}を伝達することができる。

【００９５】

図10の実施形態では、サービスプロバイダは、AddUser応答1006を登録応答1007の形式でユーザに転送する際に、わずかな役割しか持たない。メッセージ1002及び1004の場合と同様に、トラストプロバイダとサービスプロバイダとの間にTLSで保護されたチャネルなどが存在し、サービスプロバイダとユーザとの間でテキストメッセージなどを使用できると仮定することができる。このような場合、サービスプロバイダの役割は、AddUser応答1006からペイロード（すなわちエフェメラル公開鍵PK_{UAT}）を受け取り、SMSでユーザに転送することだけである。ステップ1004のAddUserリクエストで伝達された鍵PK_{URT}が、ユーザではなくサービスプロバイダから発信された代替実施形態では、転送メッセージ1007は全く必要なく、AddUserレスポンス1006のペイロード（すなわちエフェメラル公開鍵PK_{UAT}）はサービスプロバイダに留まる可能性がある。

【００９６】

これまで説明した図10の全てのステップとサブステップは、必要であれば複数回繰り返すことができる点に注意されたい。一例として、ステップ1004のAddUserリクエストで伝達された鍵PK_{URT}が、ユーザではなくサービスプロバイダから発信された代替実施形態を考えることができる。このような実施形態は、例えば、サービスプロバイダがユーザの一意な識別子を既に知っており、ユーザとの安全な通信の可能な将来のニーズに備えているが、ユーザから適切な登録要求をまだ受け取っていないことを意味する可能性がある。

【００９７】

ある時点で、サービスプロバイダは、ユーザの一意識別子と関連付ける最初の属性（又は属性の最初のセット）を有している可能性がある。これにより、サービスプロバイダは、ユーザの一意識別子、最初の（一組の）属性、及びこの目的のために生成された鍵$PK_{URT}1$を伝える、最初のAddUserリクエストを生成して送信するよう促される可能性がある。その応答として、トラストプロバイダは、第1の共有秘密$SS_{UST}1$で暗号化された、ユーザ固有の暫定暗号化アーカイブの第1のバージョンを作成し、対応する第1のエフェメラル公開鍵$PK_{UAT}1$を送り返す。

【００９８】

その後、サービスプロバイダはユーザについて更に何かを学習し、対応する第2の（複数の）属性を生成し、第2のAddUserリクエストを送信することができる。この2回目のAddUserリクエストは、ユーザの一意識別子、2つ目の(複数の)属性、及びこの目的のために生成された鍵$PK_{URT}2$(鍵$PK_{URT}1$と同じかもしれないし、同じでないかもしれない)を運んでもよい。その応答として、トラストプロバイダは、以下の式に従って第1のバージョンをデコードする。

【００９９】

$Dec(SSUST1, KUA^{-}(\cdots))$

【０１００】

そして、ユーザに固有の暫定暗号化アーカイブの第2のバージョンを作成する。この第2のバージョンは、更新された共有秘密鍵$SS_{UST}2$で暗号化され、その計算には鍵$PK_{URT}2$が使用される。トラストプロバイダは、対応する第2のエフェメラル公開鍵$PK_{UAT}2$を送り返す。

【０１０１】

このような通信のラウンドは、必要に応じて何回でも繰り返すことができる。同じことが、例えば、登録要求1002を送信することによってこのようなラウンドの少なくともいくつかを開始することによって、ユーザが役割を有していたこのような実施形態にも適用され

る。そのような実施形態においても、図10のステップ1006及び1007に関して上述したように、トラストプロバイダからの各AddUser応答（又は少なくともそのペイロード）は、当然ながらユーザに戻る。

【０１０２】

図10のステップ1008は、図10にGetUserリクエスト1009として示す登録完了要求をユーザが準備し、送信することを表している。このような登録完了要求の目的は、原理的な図1において113として示したユーザの秘密を、トラストプロバイダに安全に伝えることである。これにより、図10に示すプロセスの第2段階として、トラストプロバイダがユーザのデジタルIDを生成して適切に利用し、ユーザの登録を完了できるようになる。

【０１０３】

図10に示す実施形態では、GetUserリクエスト1009は実際にはサービスプロバイダには全く関係なく、純粋にユーザとトラストプロバイダの間で行われるものである。メッセージを転送する際にサービスプロバイダを仲介者として利用することに反対はないが、そうする理由もないため、図10では、GetUserリクエスト1009は、TLSで保護されたネットワーク接続などの安全な通信チャネルを想定して、ユーザからトラストプロバイダに直接送信されるものとして示されている。

【０１０４】

図14は、図10のステップ1008でユーザ機器が実行する可能性のあるサブステップの例を示す。サブステップ1401では、登録応答1007を受信し、その内容、特にエフェメラル公開鍵PK_{UAT}を読む。サブステップ1402では、1つ以上のユーザ固有の秘密を生成する。そのような第1のユーザ固有の秘密は、例えばUSS（ユーザ・シークレット・ソルト）でありうる。USSはクレデンシャル・ハッシュの256ビットで構成されてもよい。このようなハッシュが計算されるクレデンシャル（credential）は、例えばユーザによってユーザ機器に入力されるPINコードである。

【０１０５】

別のユーザ固有の秘密は、鍵SK_{URT}、すなわち、公開鍵PK_{URT}が先にトラストプロバイダに送信された鍵ペアの秘密鍵である。このような場合、鍵SK_{URT}は既に生成されているが、処理の前の段階では必ずしも使用されていない。鍵SK_{URT}及びPK_{URT}を生成する有利な方法の1つは、秘密鍵SK_{URT}として256ビットの乱数RNG(256)を使用し、公開鍵PK_{URT}を関数ScalarBaseMult(SK_{URT})を適用して計算することである。また、X25519()やCurve25519()という表記も使用できる。

【０１０６】

更に別のユーザ固有の秘密は、単に文字nで指定されたノンスでありうる。ノンスnは、例えば、ユーザ機器内の乱数発生器から得られる96ビットの乱数である。

【０１０７】

上述のユーザ固有の秘密が利用可能な場合、ユーザ機器は、例えば、以下の式に従って符号化キーK_{USS}を生成してもよい。

【０１０８】

$$K_{USS} = SHA2(X25519(SK_{URT}, PK_{UAT}) \,||\, PK_{URT} \,||\, PK_{UAT} \,||\, n).$$

【０１０９】

暗号鍵K_{USS}を生成する過程でハッシュアルゴリズムを使用することは任意であるが、悪意のある者が秘密鍵を見つけ出そうとする総当たり計算攻撃に対する追加のセキュリティを提供する可能性がある。本明細書の作成時において、最適化された量子コンピューティングのアプローチとショール（Shor）のアルゴリズムを使用することで、暗号鍵のビット数を実質的に半分にすることが可能であると想定されている。つまり、例えば256ビットの鍵が128ビットにしか見えなくなり、総当たり攻撃がすでに成功している可能性がある。

【０１１０】

ユーザ機器は、生成した鍵K_{USS}を使用して、例えばAES256-GCM暗号化方式を利用することで、ユーザシークレットソルトUSSを暗号化してもよい。上記で導入された表記を使用して、GetUserリクエスト1009のペイロードは以下のように表される。

【０１１１】
AES256-GCM(SHA2(X25519(SK_{URT}, PK_{UAT}) || PK_{URT}|| PK_{UAT}|| n),m,n,USS).
【０１１２】
図14のサブステップ1403と1404は、ユーザ機器がGetUserリクエスト1009を準備して送信することを表している。
【０１１３】
図10のステップ1010は、一般的に、トラストプロバイダのシステムに含まれる、概念的に定義された登録完了機能によって実行されるアクションを表している。登録完了ステップ1010の本質的な目的は、図1を参照して先に説明した原則の適用を確実にすることである。言い換えると、登録完了ステップ1010では、生成されるユーザのデジタルIDが、互いに完全に独立した2つの別個の環境から来た暗号シードとユーザの秘密に基づいていることを保証する。
【０１１４】
鍵ペア(SK_{URT}, PK_{URT})と(SK_{UAT}, PK_{UAT})の間の数学的関係により、トラストプロバイダのシステムは、鍵K_{USS}を以下のように再生成することができる。
【０１１５】
K_{USS}= SHA2(X25519(SK_{UAT}, PK_{URT}) || PK_{URT}|| PK_{UAT}|| n)
【０１１６】
これは基本的に、ステップ1005で確立した仮の秘密鍵(PK_{UAT}, SK_{UAT})に対して、GetUserリクエスト1009のコンテンツ(K_{USS})を検証する。システムは、再生成した鍵K_{USS}を利用して、ユーザ秘密鍵USSを以下のように復号することができる。
【０１１７】
Dec(K_{USS}, USS)
【０１１８】
これらの動作は図15のサブステップ1501に含まれる。GetUserリクエスト1009を適切な、以前に作成された暫定暗号化アーカイブKUAと関連付けた後、システムはそれを以下のように復号することができる。
【０１１９】
Dec(SS_{UST}, KUA~(UID, UMD, ...).
【０１２０】
システムはまた、ユーザシークレットソルトUSSを使用して復号操作を実行してもよい。
【０１２１】
Dec(USS, KUA(P_{U0}, ...))
【０１２２】
次にシステムは、図8に示した原理を応用して、まずユーザの秘密鍵SK_{UID}を次のように生成する。
【０１２３】
SK_{UID}= Argon2Id(P_{U0}, USS)
【０１２４】
そして、対応する公開鍵PK_{UID}を生成する。
【０１２５】
PK_{UID}= X25519(SK_{UID}) = X25519(Argon2Id(P_{U0}, USS)).
【０１２６】
前述したように、Argon2アルゴリズムの代わりに、SHA2アルゴリズムのような、計算量の少ないアルゴリズムを使用してもよい。生成された公開鍵PK_{UID}は、図15のサブステップ1502において、恒久的な（パーマネントな）ユーザ公開鍵と呼ばれる。生成された鍵SK_{UID}、PK_{UID}は、それぞれECC/PCI準拠の秘密鍵、ECC/PCI準拠の公開鍵である。
【０１２７】
生成された鍵SK_{UID}及びPK_{UID}は、本実施形態における（ユーザの）デジタルIDを構成する。トラストプロバイダの観点からは、これらは、トラストプロバイダがセキュアトランス

ポート機構を通じて受信した暗号シードP_{UO}及びユーザの秘密USSの両方に決定論的に依存する、暗号中間プロダクトである。

【０１２８】

生成されたユーザ固有の公開鍵PK_{UID}は、ユーザの確定秘密と呼ばれることもある。システムは更に、確定秘密PK_{UID}をトラストプロバイダの署名鍵SK_{VID}で署名することにより、ユーザの証明書$SIGN_{UID}$を生成するように構成されてもよい。トラストプロバイダの署名鍵SK_{VID}は、好ましくはECC/PKI準拠の秘密鍵であり、署名はEd25519/EdDSAの慣行に従って行われてもよい。署名は図15のサブステップ1503として示されている。デジタル署名と署名チェックの既知の原則によれば、誰でもトラストプロバイダの対応する公開鍵を使用して、トラストプロバイダのこのようなデジタル署名をチェックすることができる。

【０１２９】

次に、システムは、GetUserリクエスト1009で受信した更なる秘密USSを使用して、ユーザ識別子UID及び全ての適切かつ利用可能な属性UMDを暗号化し、ユーザに固有の最終暗号化アーカイブに格納することに進んでもよい。暗号化は、以下のように表現され得る。

【０１３０】

$Enc(USS, KUA(UID, UMD, SIGN_{UID}, PK_{UID}, P_{UO}, ...))$

【０１３１】

これは、図15のサブステップ1504で表される。

【０１３２】

図15のサブステップ1505は、システムが、図10のGetUser応答1011である登録完了応答を送信することを表す。GetUser応答1011は、登録完了ステップの有用な最終成果物、すなわちKUA（Keystore User Archive）の更新されたコンテンツをユーザに伝えることができる。GetUser応答1011のコンテンツを暗号化するための暗号鍵は、以下のように生成される。

【０１３３】

$K_{KUA}= SHA2(X25519(SK_{UAT}, PK_{URT}) || PK_{UAT}|| PK_{URT}|| n)$

【０１３４】

そして、GetUser応答1011の暗号化されたペイロードが次のように作成される。

【０１３５】

$KUA(response) = Enc(K_{KUA}, KUA(P_{UO}, ...))$.

【０１３６】

再びAES256-GCMが有利な暗号化方法であるため、GetUser応答の1011の暗号化されたペイロードは、以下のように表すことができる。

【０１３７】

$AES256\text{-}GCM(SHA2(X25519(SK_{UAT}, PK_{URT}) || PKUAT || PKURT || n), m, n, KUA(response))$.

【０１３８】

サブステップ1504又は1505の暗号操作のいずれか又は両方は、第2の暗号操作によって暗号化された形式の暗号シードP_{UO}を含む暗号出力を生成するトラストプロバイダのシステムの一例と考えることができる。暗号出力をセキュアトランスポート機構120（図9参照）を介して送信することで、最終的にユーザは確立されたデジタルIDを安全に再現し、さまざまな通信や取引で利用できるようになる。ステップ1012におけるユーザ機器の後続の動作の例を以下に説明する。

【０１３９】

サブステップ1601は、ユーザ機器がGetUser応答1011を受信し、少なくとも部分的にデコードすることを表す。特に、ユーザ機器は鍵K_{KUA}を以下のように再生成する。

【０１４０】

$K_{KUA}= SHA2(X25519(SK_{URT}, PK_{UAT}) || PKUAT || PKURT || n)$

【０１４１】

その後、デコードに使用する。

【０１４２】
Dec(K_{KUA}, KUA(P_{U0},...)).
【０１４３】
サブステップ1602で、ユーザ機器は、デコードされた情報を利用して、例えばトラストプロバイダのシステムが先に行ったのと同様に、ユーザのデジタルIDを構成する永久鍵SK_{UID}及びPK_{UID}の独自のインスタンスを生成することができる。
【０１４４】
SK_{UID}= X25519(Argon2Id(P_{U0}, USS))
又は
SK_{UID}= X25519(SHA2(PUO || USS))
そして
pk_{UID}= x25519(sk_{UID})
【０１４５】
GetUser応答1011のペイロードに鍵PK_{UID}の署名付きフォームSIGN$_{UID}$が含まれていた場合、ユーザ機器は、SIGN$_{UID}$の署名をトラストプロバイダの対応する公開鍵で削除し、その結果がPK_{UID}の再生成されたインスタンスと一致することを確認することによって、PK_{UID}の再生成されたインスタンスを検証してもよい。これは図16のサブステップ1603で示されている。サブステップ1604は、署名済みフォームSIGN$_{UID}$をユーザのユーザ証明書として格納することを表す。
【０１４６】
図17は、例示的な実施形態において、ユーザ、サービスプロバイダ、及びトラストプロバイダの間で行われるアクション及び交換されるメッセージにおいて、上記で説明した原則がどのように適用されるかを示す別の例である。図10と図17の実施形態の違いは、事前プロビジョニング段階におけるユーザとサービスプロバイダの役割に関係する。ステップ1701で、ユーザ機器は、図17のRegUserリクエストと呼ばれる、要求メッセージのユーザ機器のバージョンを作成する。RegUserリクエスト1702は、例えばユーザの公開鍵PK_{URT}、ユーザ識別子UID、ユーザに特徴的な属性及び／又は他のメタデータUMDをトラストプロバイダに伝えてもよい。ステップ1703で、トラストプロバイダはこれらを利用して、ユーザに固有の暫定暗号化アーカイブの最初のバージョンを設定し、格納することができる。ステップ1703で格納される暫定暗号化アーカイブは、RegUserリクエストで伝達されたいずれか又は全ての情報、ならびにトラストプロバイダのシステムによって生成された高エントロピーのユーザ固有の暗号シードP_{U0}を含んでもよい。
【０１４７】
図17のステップ1704及び1705は、サービスプロバイダからトラストプロバイダへのAddUserリクエストをトリガする何かをユーザが作成し、サービスプロバイダに送信することを表す。この「何か」は、例えば、登録要求及び／又はトラストプロバイダのシステムにおける適切なユーザ固有情報へのリンクであってもよい。サービスプロバイダによるユーザの確実な識別に関して、図17のステップ1704及び1705は、先の図10のステップ1001及び1002と全く同等である。
【０１４８】
ステップ1706で、サービスプロバイダは、先の図10のステップ1003と同様に、ユーザから受信した情報を１つ又は複数の属性で補強することができる。ステップ1706の結果は、サービスプロバイダが安全なチャネルを通じてトラストプロバイダに送信するAddUserリクエスト1707である。先の図10と同様に、登録要求1705によって公開鍵PK_{URT}がサービスプロバイダの注意を引いたと仮定すると、AddUserは更に同じPK_{URT}をトラストプロバイダに伝えてもよい。UIDのようなユーザ識別子は、AddUserリクエスト1707に含まれてもよいが、必要ではない。なぜなら、トラストプロバイダがRegUserリクエスト1702で既に鍵PK_{URT}を受信していれば、同様に簡単かつ確実にユーザを識別するために使用できるからである。
【０１４９】

図17のステップ1708は、トラストプロバイダのシステムにおける事前プロビジョニングの第2ラウンドを表す。この第2ラウンドは、図10に関して先に事前プロビジョニングステップの繰り返しについて説明したものと本質的に類似している。ステップ1706でサービスプロバイダから発信された追加情報が、トラストプロバイダのシステムにおいて、ユーザに固有の暫定符号化アーカイブに追加される。追加的又は代替的に、このような追加情報は、ステップ1704でユーザから発信されたものであってもよい。しかし、トラストプロバイダはまだ図1のユーザの秘密113を所有していないため、ユーザの登録をまだ完了できない。

【０１５０】

図17の実施形態では、トラストプロバイダはRegUser応答1709を、サービスプロバイダを経由せずに直接ユーザに送信する。ただし実施形態によっては、図10のステップ1006と1007のように、サービスプロバイダを経由してもよい。RegUser応答1709は、エフェメラル公開鍵PK_{UAT}をユーザに送信し、ユーザ機器はステップ1710でこれを使用しGetUserリクエスト1711を作成する。この場合も、これら2つのステップは、図10の対応するステップ1008及び1009と同様である。GetUser要求1711を通して、トラストプロバイダは、ユーザのデジタルIDを生成するために必要なユーザの秘密を取得し、ステップ1712でユーザの登録を完了する。GetUser応答1713と、ステップ1714でのユーザ機器によるその利用は、図10の対応するステップ1011及び1012と同様である。

【０１５１】

本明細書で示される範囲又は値は、求める効果を失うことなく、拡張又は変更することができる。また、明示的に禁止されていない限り、いかなる実施形態も他の実施形態と組み合わせることができる。

【０１５２】

本願の主題は、構造的特徴及び／又は動作に特有の文言で説明されてきたが、添付の特許請求の範囲に定義される主題は、必ずしも上述の特定の特徴又は動作に限定されるものではないことを理解されたい。むしろ、上述の特定の特徴及び動作は、特許請求の範囲を実施する例として開示されており、他の同等の特徴及び動作も、特許請求の範囲に含まれることが意図されている。

【０１５３】

上述の利点及び利点は、1つの実施形態に関するものであってもよいし、複数の実施形態に関するものであってもよいことを理解されたい。これらの実施形態は、記載された問題のいずれか又は全てを解決するもの、又は記載された利点及び利点のいずれか又は全てを有するものに限定されない。また構成要素の数は、特に言及しなくとも、1つ又は複数である場合がある。

【０１５４】

本明細書に記載の方法のステップは、任意の適切な順序で、又は適切な場合には同時に実施することができる。更に、個々のブロックは、本明細書に記載される主題の精神及び範囲から逸脱することなく、いずれかの方法から削除することができる。上述した実施形態のいずれかの態様は、求める効果を失うことなく、上述した他の実施形態のいずれかの態様と組み合わせて、更なる実施形態を形成することができる。

【０１５５】

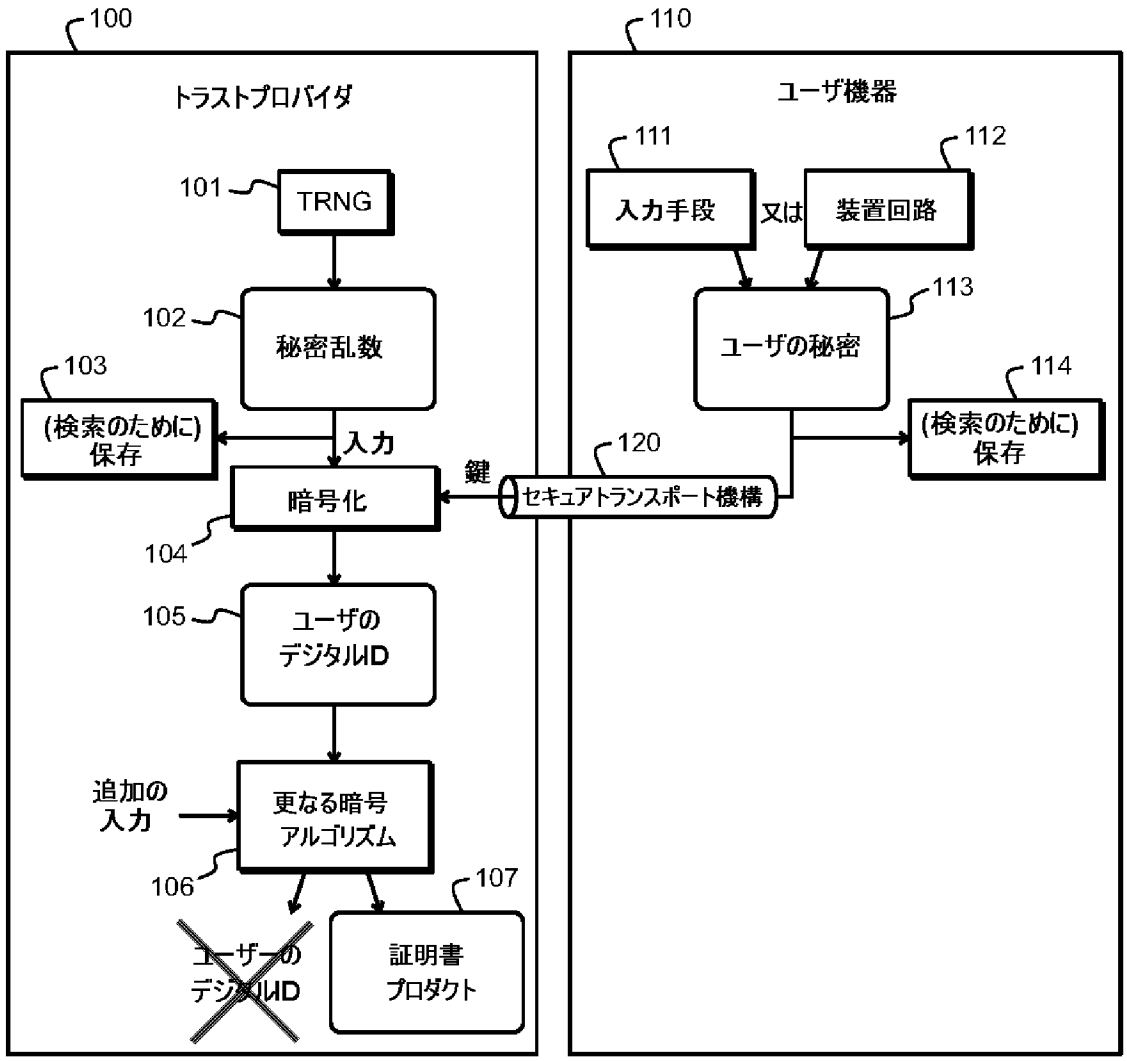
本明細書において「からなる」という用語は、特定された方法、ブロック又は要素を含むことを意味するために使用されるが、そのようなブロック又は要素は排他的なリストを構成するものではなく、方法又は装置は追加のブロック又は要素を含むことができる。

【０１５６】

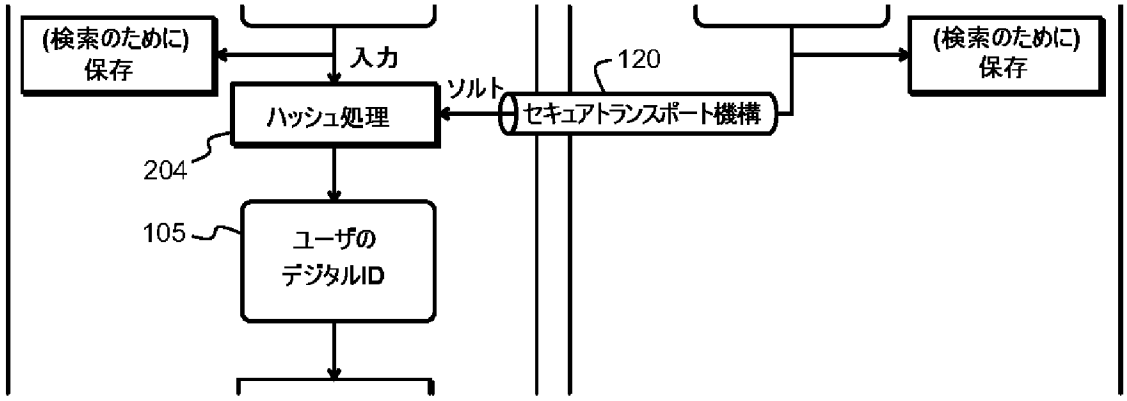
上記の説明は例示としてのみ与えられたものであり、当業者によって様々な変更がなされ得ることが理解されよう。上記の明細書、実施例及びデータは、例示的な実施形態の構造及び使用に関する完全な説明を提供する。様々な実施形態が、ある程度の特殊性をもって、又は1つ以上の個別の実施形態を参照して上記で説明されたが、当業者であれば、本明細書の精神又は範囲から逸脱することなく、開示された実施形態に多数の変更を加えるこ

とができる。

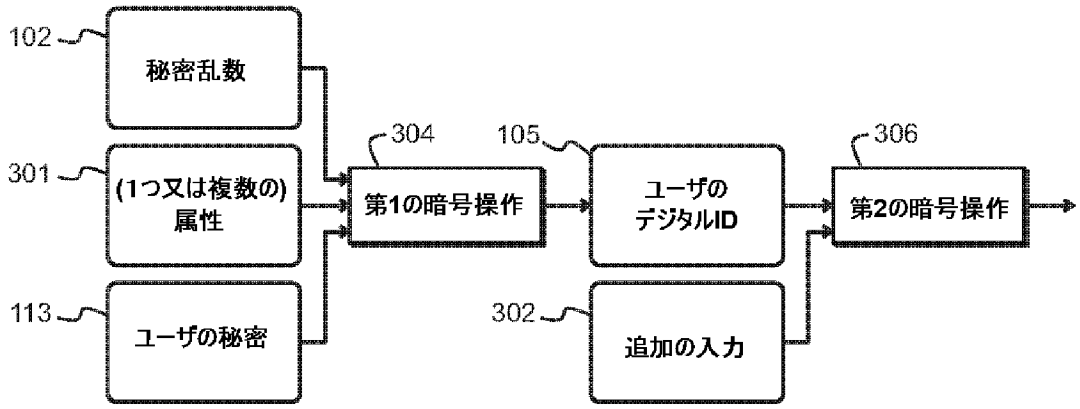
【図１】


100
トラストプロバイダ
101
TRNG
102
秘密乱数
103
(検索のために)
保存
入力
暗号化
104
105
ユーザの
デジタルID
追加の
入力
更なる暗号
アルゴリズム
106
107
ユーザーの
デジタルID
証明書
プロダクト
110
ユーザ機器
111
入力手段
又は
112
装置回路
113
ユーザの秘密
114
(検索のために)
保存
120
鍵
セキュアトランスポート機構

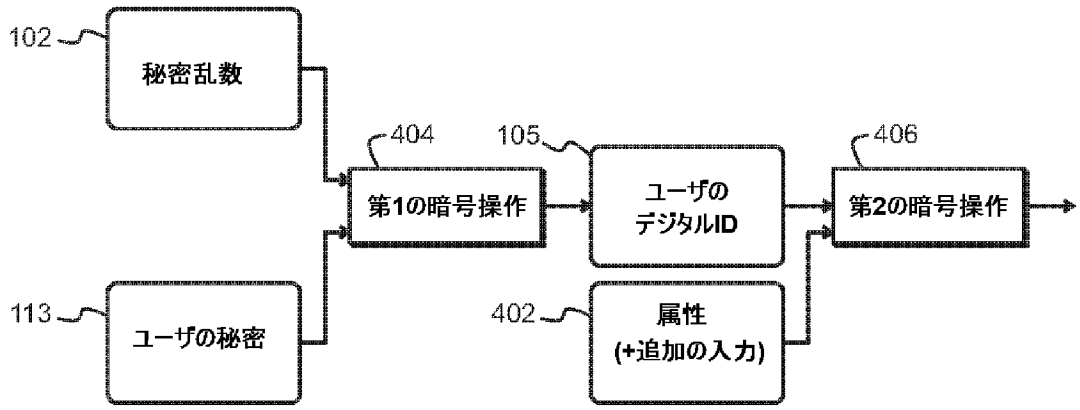
【図２】


(検索のために)
保存
入力
ハッシュ処理
204
105
ユーザの
デジタルID
ソルト
120
セキュアトランスポート機構
(検索のために)
保存

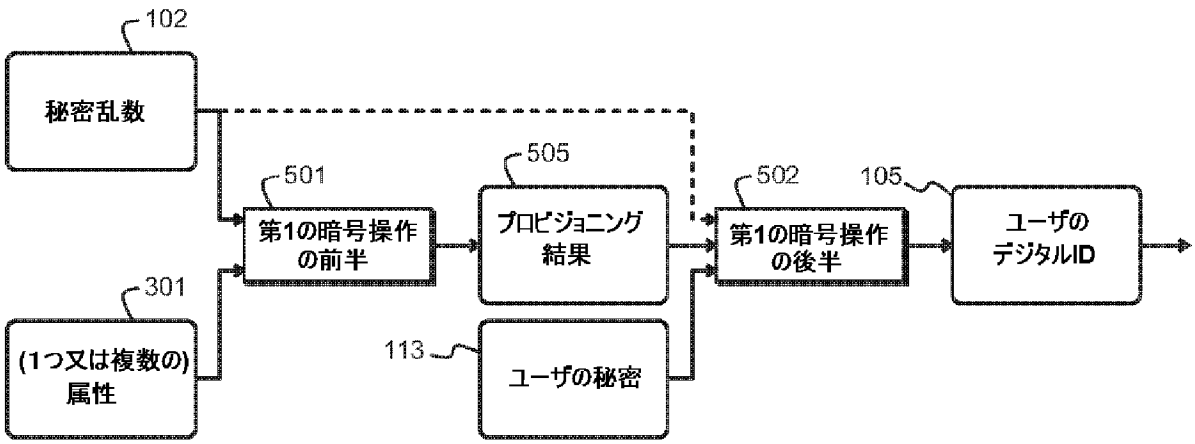
【図３】


102
秘密乱数
301
(1つ又は複数の)
属性
113
ユーザの秘密
304
第1の暗号操作
105
ユーザの
デジタルID
306
第2の暗号操作
302
追加の入力

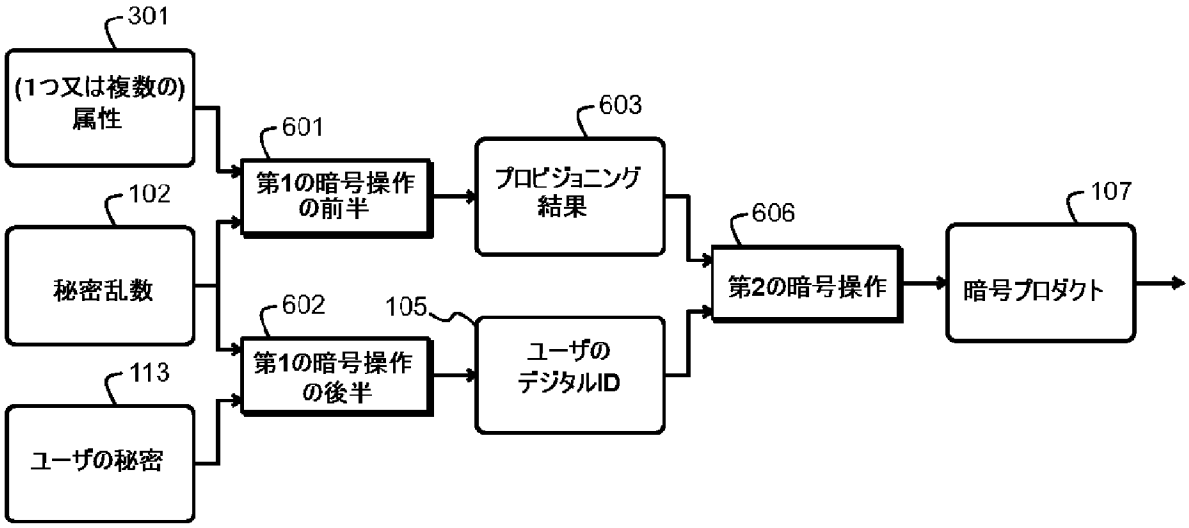
【図４】


102
秘密乱数
113
ユーザの秘密
404
第1の暗号操作
105
ユーザの
デジタルID
406
第2の暗号操作
402
属性
(+追加の入力)

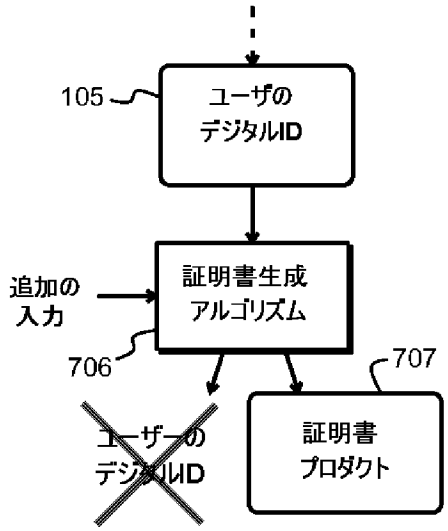
【図５】


102
秘密乱数
301
(1つ又は複数の)
属性
501
第1の暗号操作
の前半
505
プロビジョニング
結果
113
ユーザの秘密
502
第1の暗号操作
の後半
105
ユーザの
デジタルID

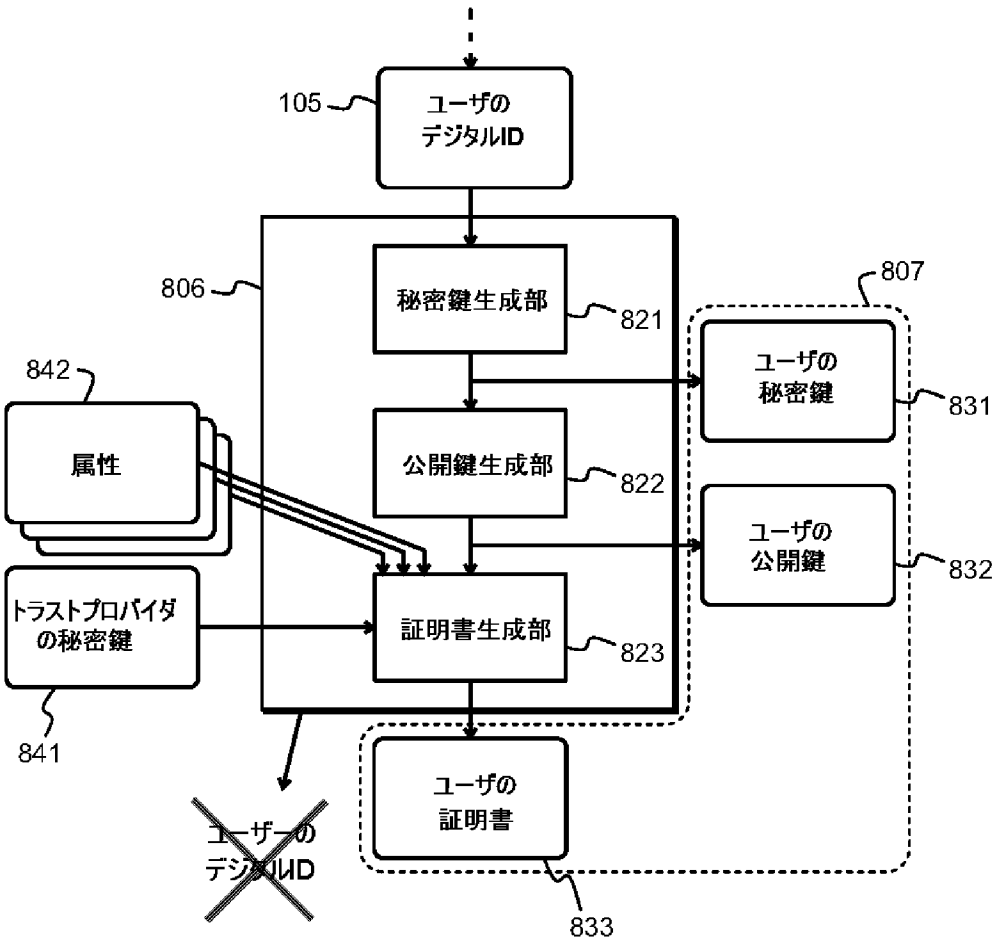
【図６】


301
(1つ又は複数の)
属性
102
秘密乱数
113
ユーザの秘密
601
第1の暗号操作
の前半
602
第1の暗号操作
の後半
603
プロビジョニング
結果
105
ユーザの
デジタルID
606
第2の暗号操作
107
暗号プロダクト

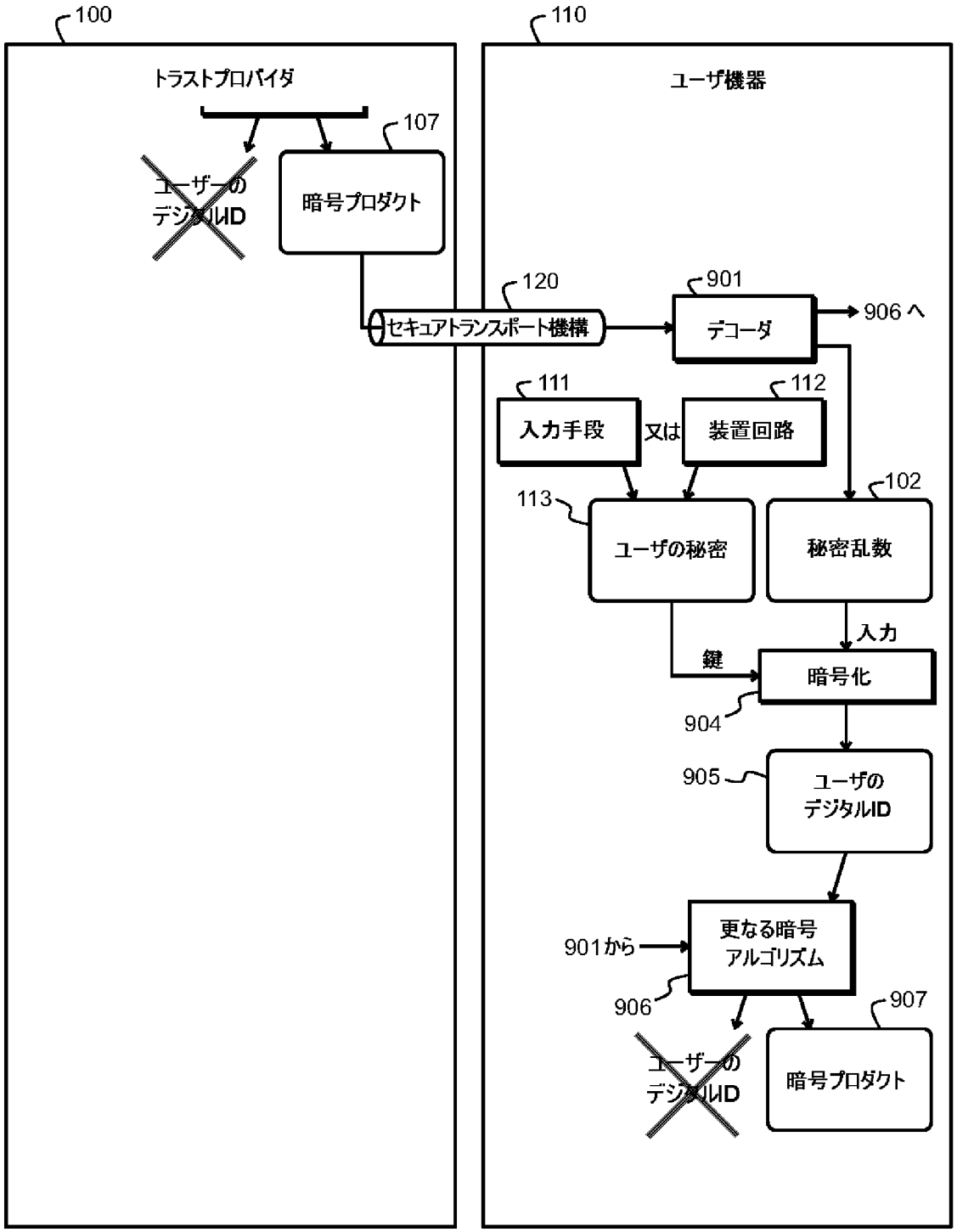
【図７】


105
ユーザの
デジタルID
追加の
入力
証明書生成
アルゴリズム
706
707
ユーザの
デジタルID
証明書
プロダクト

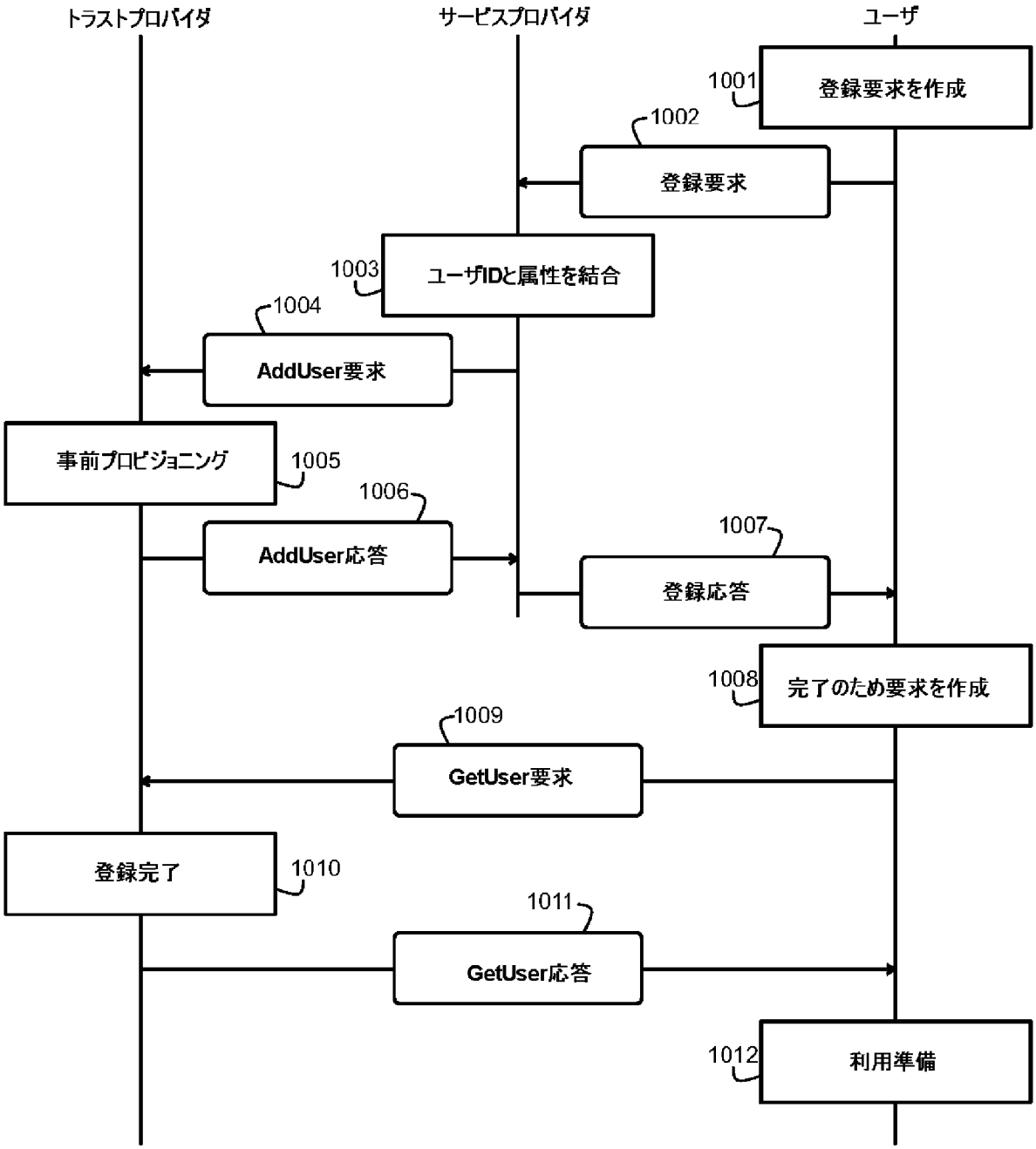
【図８】


105
ユーザの
デジタルID
806
秘密鍵生成部
821
807
ユーザの
秘密鍵
831
842
属性
公開鍵生成部
822
ユーザの
公開鍵
832
トラストプロバイダ
の秘密鍵
証明書生成部
823
841
ユーザの
証明書
ユーザーの
デジタルID
833

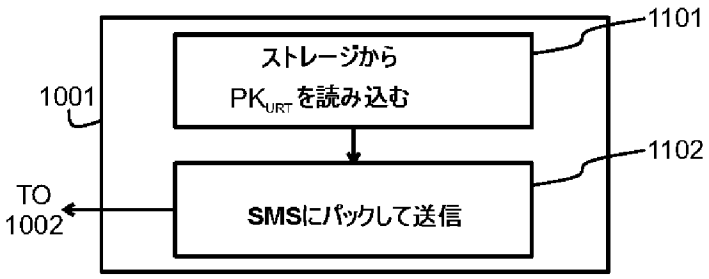
【図９】


100
トラストプロバイダ
107
ユーザーの
デジタルID
暗号プロダクト
110
ユーザ機器
120
セキュアトランスポート機構
901
デコーダ
906へ
111
入力手段
又は
112
装置回路
102
113
ユーザの秘密
秘密乱数
入力
鍵
暗号化
904
905
ユーザの
デジタルID
901から
更なる暗号
アルゴリズム
906
907
ユーザーの
デジタルID
暗号プロダクト

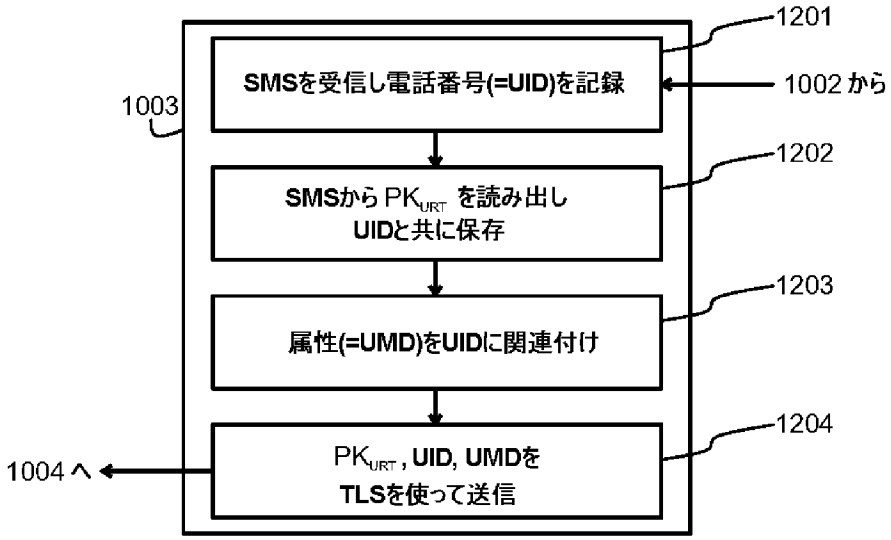
【図１０】


トラストプロバイダ
サービスプロバイダ
ユーザ
1001
登録要求を作成
1002
登録要求
1003
ユーザIDと属性を結合
1004
AddUser要求
事前プロビジョニング
1005
1006
AddUser応答
1007
登録応答
1008
完了のため要求を作成
1009
GetUser要求
登録完了
1010
1011
GetUser応答
1012
利用準備

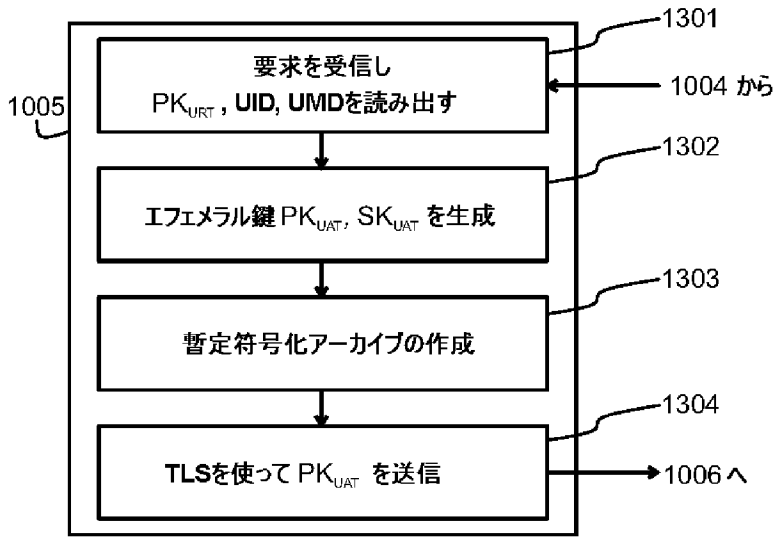
【図１１】


1101
ストレージから
PK$_{URT}$を読み込む
1001
1102
TO
1002
SMSにパックして送信

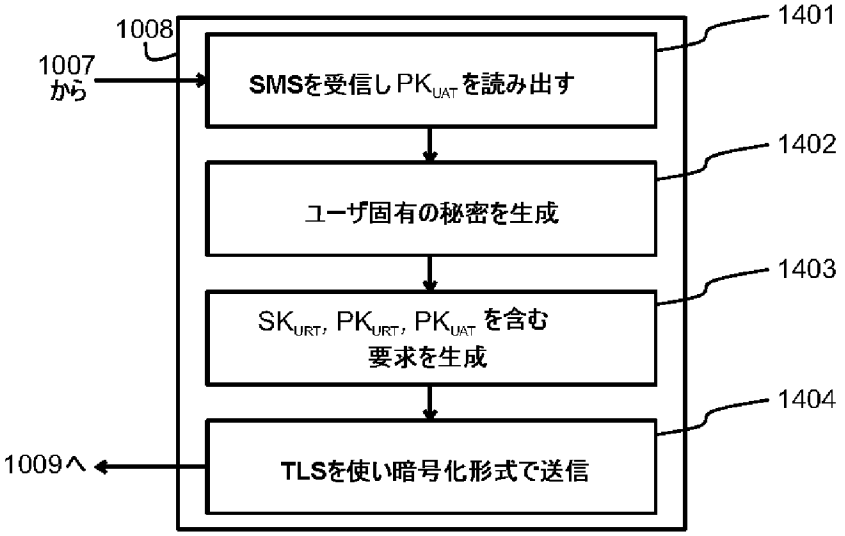
【図１２】


1201
SMSを受信し電話番号(=UID)を記録
1002から
1003
1202
SMSからPK$_{URT}$を読み出し
UIDと共に保存
1203
属性(=UMD)をUIDに関連付け
1204
PK$_{URT}$, UID, UMDを
TLSを使って送信
1004へ

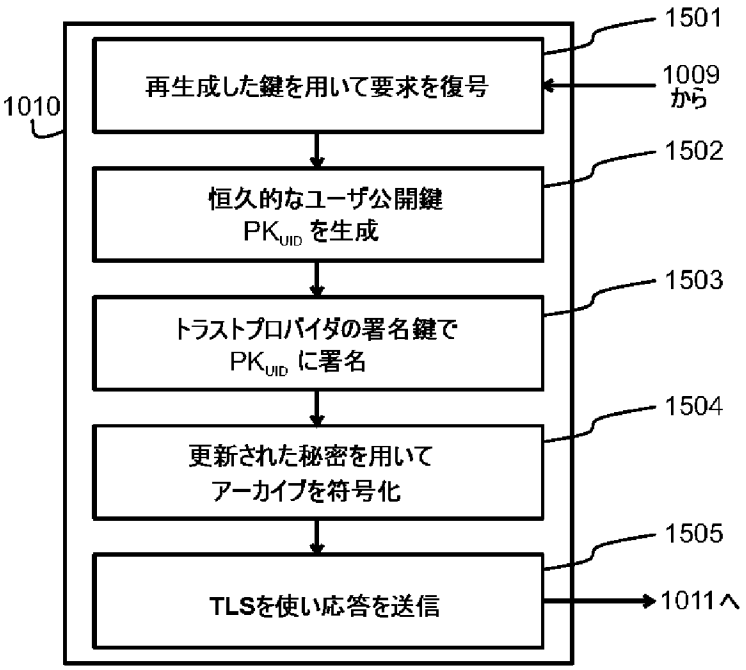
【図１３】


1301
要求を受信し
PK$_{URT}$, UID, UMDを読み出す
1004から
1005
1302
エフェメラル鍵PK$_{UAT}$, SK$_{UAT}$を生成
1303
暫定符号化アーカイブの作成
1304
TLSを使ってPK$_{UAT}$を送信
1006へ

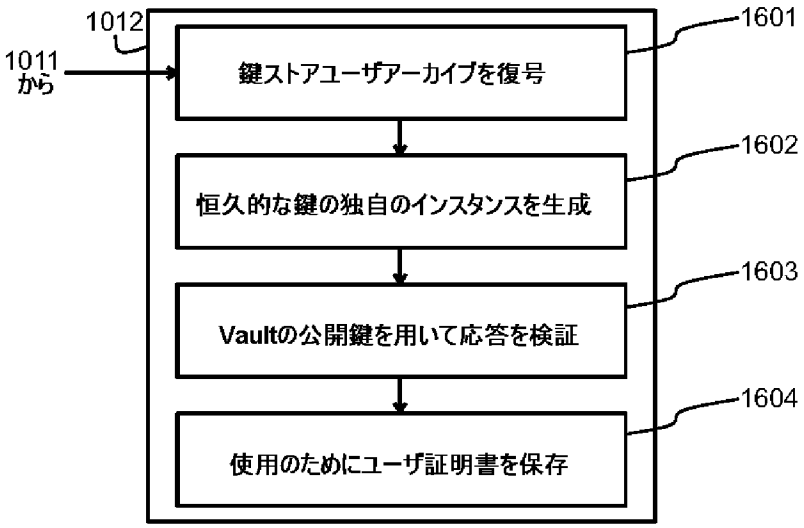
【図１４】


1008
1007
から
SMSを受信しPK$_{UAT}$を読み出す
1401
ユーザ固有の秘密を生成
1402
SK$_{URT}$, PK$_{URT}$, PK$_{UAT}$ を含む
要求を生成
1403
TLSを使い暗号化形式で送信
1404
1009へ

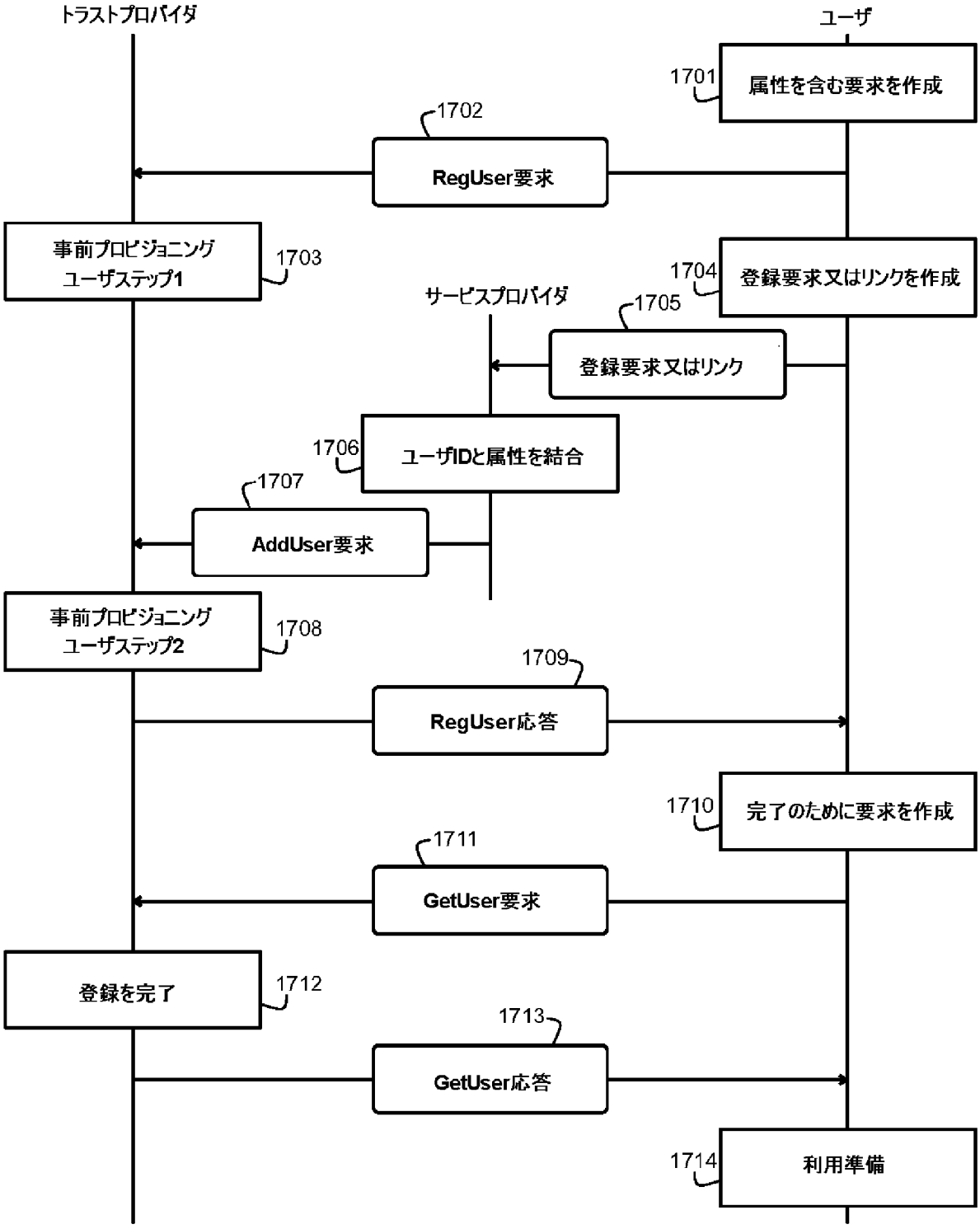
【図１５】


1010
再生成した鍵を用いて要求を復号
1501
1009
から
恒久的なユーザ公開鍵
PK$_{UID}$ を生成
1502
トラストプロバイダの署名鍵で
PK$_{UID}$ に署名
1503
更新された秘密を用いて
アーカイブを符号化
1504
TLSを使い応答を送信
1505
1011へ

【図１６】


1012
1011
から
鍵ストアユーザアーカイブを復号
1601
恒久的な鍵の独自のインスタンスを生成
1602
Vaultの公開鍵を用いて応答を検証
1603
使用のためにユーザ証明書を保存
1604

【図１７】



【手続補正書】
【提出日】令和6年4月23日(2024.4.23)
【手続補正１】
【補正対象書類名】特許請求の範囲

【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
関係者のためにデジタルＩＤを確立するためのシステムであって、
・　暗号シードを生成するように構成されたランダムデータ生成部と、
・　外部ソースと通信するための、セキュアトランスポート機構の受信側及び送信側と、
・　前記ランダムデータ生成部と前記セキュアトランスポート機構の前記受信側とに結合された第１の暗号操作部と、
・　前記第１の暗号操作部と前記セキュアトランスポート機構の前記送信側とに結合される第２の暗号操作部と、
を備え、
前記暗号シードと、前記セキュアトランスポート機構を介して外部ソースから受信したユーザの秘密との両方に決定論的に依存する暗号中間プロダクトを、前記第１の暗号操作部を通じて生成するように構成され、前記暗号中間プロダクトは前記関係者の前記デジタルＩＤを構成し、
前記関係者の前記デジタルＩＤを使用して、暗号化された形式の前記暗号シードを含む暗号出力を、前記第２の暗号操作を通じて生成するように構成され、
前記暗号出力の少なくとも一部を前記セキュアトランスポート機構を介して送信するように構成され、
前記暗号出力の前記生成において前記デジタルＩＤを使用した後、前記デジタルＩＤをメモリにおいて永久的に難読化するように構成される、
システム。
【請求項２】
前記第２の暗号操作を通じて、前記暗号出力の一部として前記関係者の暗号証明書を生成するように構成される、請求項１に記載のシステム。
【請求項３】
・　前記関係者の識別子及び少なくとも１つの属性を示す、受信した事前プロビジョニング要求に対して、前記関係者のための仮秘密を確立し、前記仮秘密の少なくとも一部を含む事前プロビジョニング応答を送信するように構成される、事前プロビジョニング機能と、
・　前記事前プロビジョニング応答の前記送信後に受信した登録完了要求に対して、前記登録完了再要求の内容を前記仮秘密に照らして検証することにより応答するように構成される、登録完了機能と、
を備え、
前記事前プロビジョニング機能は、前記暗号シードを使用して、前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の暫定暗号化アーカイブに格納するように構成され、
前記登録完了機能は、前記登録完了要求で受信した前記ユーザの秘密を使用して、前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の最終暗号化アーカイブに格納するように構成され、
前記システムは、前記識別子及び前記少なくとも１つの属性の前記暗号化及び前記最終暗号化アーカイブへの格納において、前記デジタルＩＤを使用するように構成される、
先行する請求項のいずれかに記載のシステム。
【請求項４】
前記事前プロビジョニング機能は、
・　前記関係者のための前記仮秘密として非対称暗号化システムの一対のエフェメラル鍵を生成し、
・　前記事前プロビジョニング応答において前記一対のエフェメラル鍵の公開鍵を送信す

るように構成される、
請求項３の記載のシステム。
【請求項５】
前記事前プロビジョニング機能は、
・　前記ランダムデータ生成部によって提供された乱数を前記一対のエフェメラル鍵の秘密鍵として使用し、
・　Ｃｕｒｖｅ２５５１９楕円曲線ディフィー・ヘルマン法を使用して、前記一対のエフェメラル鍵の秘密鍵から前記一対のエフェメラル鍵の公開鍵を生成するように構成される、
請求項４の記載のシステム。
【請求項６】
前記事前プロビジョニング機能は、
・　前記一対のエフェメラル鍵の前記秘密鍵と、前記システムの外部のエンティティから受信した公開鍵とを用いて、第１の数学的演算によって第１の共有秘密を生成し、
・　前記識別子と前記少なくとも１つの属性とを暗号化して前記暫定暗号化アーカイブに格納する際に、前記第１の共有秘密を使用するように構成される、
請求項４又は５の記載のシステム。
【請求項７】
前記第１の暗号処理としてＡｒｇｏｎ２ハッシュ処理を使用するように構成される、先行する請求項のいずれかに記載のシステム。
【請求項８】
・　前記デジタルＩＤを使用して、前記関係者の前記暗号出力の一部を生成するよう構成され、
・　前記システムの署名鍵で前記暗号出力の少なくとも一部分に署名することで、前記関係者の証明書を生成するように構成される、
先行する請求項のいずれかに記載のシステム。
【請求項９】
前記暗号出力の前記一部の１つとして、非対称暗号化システムの更なる鍵ペアの公開鍵を、Ｃｕｒｖｅ２５５１９楕円曲線ディフィー・ヘルマン法を使用して前記デジタルＩＤから生成するように構成される、請求項８に記載のシステム。
【請求項１０】
前記デジタルＩＤの生成後に、登録完了応答の中で前記暗号出力を送信するように構成される、先行する請求項のいずれかに記載のシステム。
【請求項１１】
前記登録完了応答において、暗号化された形式の前記暗号シード、及び前記システムの外部のエンティティが使用するための署名された形式の暗号鍵を送信するように構成され、
前記暗号鍵は、前記関係者の前記デジタルＩＤを構成する、又は前記デジタルＩＤから導出される、非対称暗号化システムの鍵ペアの片割れである、請求項１０に記載のシステム。
【請求項１２】
関係者のためにデジタルＩＤを確立する方法であって、
・　ランダムデータとして暗号シードを生成することと、
・　セキュアトランスポート機構を介して外部ソースからユーザの秘密を受信することと、
・　第１の暗号操作を適用して、前記暗号シードと前記ユーザの秘密の両方に決定論的に依存する暗号中間プロダクトであって、前記関係者の前記デジタルＩＤを構成する暗号中間プロダクトを生成することと、
・　前記関係者の前記デジタルＩＤに第２の暗号操作を適用して、暗号化された形式の前記暗号シードを含む暗号出力を生成することと、
・　前記暗号出力の少なくとも一部を、前記セキュアトランスポート機構を介して前記外

部ソースに送信することと、
前記暗号出力の生成に前記デジタルＩＤを使用した後、前記デジタルＩＤを、永久にメモリから難読化することと、
を含む、方法。
【請求項１３】
前記第２の暗号操作を通じて、前記暗号出力の一部として前記関係者の暗号証明書を生成することを含む、請求項１２に記載の方法。
【請求項１４】
前記関係者の識別子及び少なくとも１つの属性を示す、受信した事前プロビジョニング要求に対して、前記関係者のための仮秘密を確立し、前記仮秘密の少なくとも一部を含む事前プロビジョニング応答を送信することと、
前記仮秘密を確立することの一部として、前記暗号シードを使用して前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の暫定暗号化アーカイブに格納することと、
前記事前プロビジョニング応答の前記送信後に受信した登録完了要求に対して、前記登録完了再要求の内容を前記仮秘密に照らして検証することにより応答することと、
前記登録完了機能は、前記登録完了要求で受信した前記ユーザの秘密を使用して、前記識別子及び前記少なくとも１つの属性を暗号化し、前記関係者に固有の最終暗号化アーカイブに格納することと、
前記識別子及び前記少なくとも１つの属性の前記暗号化及び前記最終暗号化アーカイブへの格納において、前記デジタルＩＤを使用することと、
を含む、請求項１２又は１３に記載の方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2023/050088

A. **CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

FI, SE, NO, DK

Electronic database consulted during the international search (name of database and, where practicable, search terms used)

EPODOC, EPO-Internal full-text databases, Full-text translation databases from Asian languages, WPIAP, IPRally, XP3GPP, XPAIP, XPCPVO, XPESP, XPETSI, XPI3E, XPI3ES, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPSPRNG, XPTK, COMPDX, INSPEC, TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 10396985 B1 (NAGELBERG ALEXANDER B [US] et al.) 27 August 2019 (27.08.2019) Figs. 1-2; column 1, lines 40-46; column 6, lines 8-17, 48-54; column 8, lines 12-22; column 11, lines 55-64; column 17, lines 30-36	1-3, 8-15
A	Ibid.	4-7, 16

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"D"	document cited by the applicant in the international application	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"E"	earlier application or patent but published on or after the international filing date	"&"	document member of the same patent family
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)		
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
01 June 2023 (01.06.2023)	01 June 2023 (01.06.2023)

Name and mailing address of the ISA/ FI	Authorized officer
Finnish Patent and Registration Office FI-00091 PRH, FINLAND	Vesa-Matti Louekoski
Facsimile No. +358 29 509 5328	Telephone No. +358 29 509 5000

Form PCT/ISA/210 (second sheet) (July 2022)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2023/050088

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 10454677 B1 (NAGELBERG ALEXANDER B [US] et al.) 22 October 2019 (22.10.2019)	
X	Figs. 1-2, 5A-5B; column 3, lines 42-52; column 5, lines 4-15; column 6, lines 6-17; column 9, lines 57-67; column 15, lines 37-43	1-3, 8-15
A	Ibid.	4-7, 16
	US 2011150212 A1 (SPALKA ADRIAN [DE] et al.) 23 June 2011 (23.06.2011)	
X	Fig. 3; claim 1; paragraphs 0006-0007, 0024-0025, 0036, 0090-0091, 0094	1-2, 8, 11-14
A	Ibid.	3-7, 9-10, 15-16

Form PCT/ISA/210 (continuation of second sheet)

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2023/050088

US 10396985 B1	27/08/2019	None	
US 10454677 B1	22/10/2019	US 10880080 B1	29/12/2020
US 2011150212 A1	23/06/2011	US 2011225114 A1	15/09/2011
		EP 2365456 A2	14/09/2011
		US 8695106 B2	08/04/2014
		EP 2336933 B1	10/09/2014
		US 8677146 B2	18/03/2014
		EP 2365456 B1	20/07/2016
		US 7962761 B1	14/06/2011
		EP 2348443 B1	02/10/2013
		US 2013179176 A1	11/07/2013
		EP 2348445 B1	16/09/2015
		US 2011154055 A1	23/06/2011
		EP 2365458 A2	14/09/2011
		US 2011173455 A1	14/07/2011
		EP 2365458 B1	01/11/2017
		US 2011179286 A1	21/07/2011
		US 8522011 B2	27/08/2013
		EP 2348445 A2	27/07/2011
		EP 2348452 B1	02/07/2014
		US 8024581 B2	20/09/2011
		US 8719587 B2	06/05/2014
		US 9418242 B2	16/08/2016
		EP 2348446 A2	27/07/2011
		EP 2348452 A2	27/07/2011
		AT 554454 T	15/05/2012
		US 2011154044 A1	23/06/2011
		EP 2343665 B1	18/04/2012
		US 2011154054 A1	23/06/2011
		US 8868436 B2	21/10/2014
		US 2014189372 A1	03/07/2014
		EP 2348447 B1	16/07/2014
		US 2014181512 A1	26/06/2014
		US 2011268269 A1	03/11/2011
		EP 2336933 A2	22/06/2011
		US 2011154056 A1	23/06/2011
		EP 2348443 A2	27/07/2011
		US 2011185188 A1	28/07/2011
		EP 2343665 A1	13/07/2011
		EP 2348450 B1	06/11/2013
		EP 2348447 A2	27/07/2011

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2023/050088

US 8887254 B2	11/11/2014
US 8516267 B2	20/08/2013
US 2011154025 A1	23/06/2011
US 8699705 B2	15/04/2014
US 8661247 B2	25/02/2014
EP 2348449 A2	27/07/2011
EP 2348446 B1	15/04/2015
EP 2348450 A2	27/07/2011

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2023/050088

CLASSIFICATION OF SUBJECT MATTER

IPC
H04L 9/40 (2022.01)
H04L 9/00 (2022.01)
H04L 9/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

フロントページの続き

(81)指定国・地域　AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW