【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和1年8月29日(2019.8.29)

【公表番号】特表2017-530586(P2017-530586A)
【公表日】平成29年10月12日(2017.10.12)
【年通号数】公開・登録公報2017-039
【出願番号】特願2017-505504(P2017-505504)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　20/40　(2012.01)
Ｇ０６Ｑ　20/38　(2012.01)
Ｇ０６Ｆ　21/31　(2013.01)
Ｈ０４Ｌ　9/14　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０６Ｑ　20/40　３００
Ｇ０６Ｑ　20/38　３１８
Ｇ０６Ｆ　21/31
Ｈ０４Ｌ　9/00　６４１

【誤訳訂正書】
【提出日】令和1年7月16日(2019.7.16)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
方法であって、
クライアントの認証部を依拠当事者に登録することであって、前記登録によって、前記クライアントのユーザが、ネットワーク上で前記依拠当事者に対して前記ユーザを遠隔で認証することを可能にする、ことと、
前記認証部と関連付けられた第１の認証鍵と、第１の検証鍵と共に生成される署名とを少なくとも使用して、前記依拠当事者において、第１の署名付き構造を生成することと、
前記第１の署名付き構造を前記クライアント上でキャッシュすることと、
前記第１の検証鍵に対応する第２の検証鍵をトランザクションデバイスに提供することと、
前記クライアントと前記トランザクションデバイスとの間で認証トランザクションを実行することであって、前記クライアントが、前記第１の認証鍵と関連付けられた第２の認証鍵を使用して第２の署名付き構造を生成し、前記トランザクションデバイスが、前記第２の検証鍵を使用して前記第１の署名付き構造に対して前記署名を有効化し、前記第１の認証鍵を使用して前記第２の署名付き構造を有効化し、前記第１及び第２の検証鍵が同じ鍵である、並びに／あるいは前記第１及び第２の認証鍵が同じ鍵であることと、
を含む、方法。
【請求項２】
前記第１の検証鍵が、前記署名を生成するのに使用される秘密鍵であり、前記トランザクションデバイスに提供される前記第２の検証鍵が、前記署名を有効化することができる対応する公開検証鍵である、請求項１に記載の方法。

【請求項３】
前記第２の認証鍵が、前記認証部と関連付けられた秘密認証鍵を含み、前記第１の認証鍵が対応する公開認証鍵である、請求項１に記載の方法。
【請求項４】
前記第１の認証鍵が前記認証部と関連付けられた公開鍵（Ｕａｕｔｈ．ｐｕｂ）を含み、前記署名が前記第１の検証鍵を使用して少なくとも前記公開鍵に対して生成される、請求項１に記載の方法。
【請求項５】
方法であって、
クライアントの認証部を依拠当事者に登録することであって、前記登録によって、前記クライアントのユーザが、ネットワーク上で前記依拠当事者に対して前記ユーザを遠隔で認証することを可能にする、ことと、
前記認証部と関連付けられた第１の認証鍵と、第１の検証鍵と共に生成される署名とを少なくとも使用して、前記依拠当事者において、第１の署名付き構造を生成することと、
トランザクションデバイスを通したトランザクションを開始するため、ユーザ要求に応答して、前記第１の署名付き構造を前記トランザクションデバイスに格納することと、
前記第１の検証鍵に対応する第２の検証鍵を前記トランザクションデバイスに提供することと、
前記クライアントと前記トランザクションデバイスとの間で認証トランザクションを実行することであって、前記クライアントが、前記第１の認証鍵と関連付けられた第２の認証鍵を使用して第２の署名付き構造を生成し、前記トランザクションデバイスが、前記第２の検証鍵を使用して前記第１の署名付き構造に対して前記署名を有効化し、前記第１の認証鍵を使用して前記第２の署名付き構造を有効化し、前記第１及び第２の検証鍵が同じ鍵である、並びに／あるいは前記第１及び第２の認証鍵が同じ鍵である、ことと、
を含む、方法。
【請求項６】
前記第１の認証鍵が前記認証部と関連付けられた公開鍵（Ｕａｕｔｈ．ｐｕｂ）を含み、前記署名が前記第１の検証鍵を使用して少なくとも前記公開鍵に対して生成される、請求項５に記載の方法。
【請求項７】
前記第１の署名付き構造が、前記依拠当事者によって生成されるナンスと、前記公開鍵と、
前記ナンス及び前記公開鍵の組み合わせに対して生成される前記署名との組み合わせを含む、請求項６に記載の方法。
【請求項８】
前記第１の署名付き構造が、前記依拠当事者によって生成されるナンスと、前記第１の署名付き
構造を前記クライアントでキャッシュすることができる時間量を示すキャッシュタイミングデータと、前記公開鍵と、前記ナンス、前記キャッシュタイミングデータ、及び前記公開鍵の組み合わせに対して生成される前記署名との組み合わせを含む、請求項６に記載の方法。
【請求項９】
前記第２の署名付き構造が、前記トランザクションデバイスによって提供されるナンス又は値と、前記トランザクションデバイスによって提供される少なくとも前記ナンス及び／又は前記値に対して、前記第２の認証鍵を適用することによって生成される署名とを含む、
請求項６に記載の方法。
【請求項１０】
前記第２の署名付き構造が、前記トランザクションデバイスとのトランザクションの間、前記クライアントにセキュアに表示されるトランザクションテキストに対して、前記第

２の認証鍵を適用することによって生成される署名を含む、請求項６に記載の方法。
【請求項１１】
前記署名が、前記第１の認証鍵を使用して、前記トランザクションデバイス及び／又は前記依拠当事者によって検証される、請求項１０に記載の方法。
【請求項１２】
方法であって、
クライアントの認証部を依拠当事者に登録することであって、前記登録によって、前記クライアントのユーザが、ネットワーク上で前記依拠当事者に対して前記ユーザを遠隔で認証することを可能にする、ことと、
前記認証部と関連付けられた第１の認証鍵を少なくとも使用して、前記依拠当事者において、第１の署名付き構造を生成することと、
前記第１の署名付き構造を前記クライアント上でキャッシュすることと、
前記クライアントとトランザクションデバイスとの間で認証トランザクションを実行することであって、前記クライアントが、前記第１の認証鍵と関連付けられた第２の署名付き鍵を使用して第２の署名付き構造を生成し、前記トランザクションデバイスが、前記依拠当事者に対するオンライン又はアウトオブバンド接続を使用して前記第１の署名付き構造を有効化し、前記第１の認証鍵を使用して前記第２の署名付き構造を有効化し、前記第１及び第２の認証鍵は同じ鍵である、ことと、
を含む、方法。
【請求項１３】
前記第１の認証鍵が前記認証部と関連付けられた公開鍵（Ｕａｕｔｈ．ｐｕｂ）を含む、請求項１２に記載の方法。
【請求項１４】
前記第１の署名付き構造が、前記依拠当事者によって生成されるナンスと、前記公開鍵と、前記ナンス及び前記公開鍵の組み合わせに対して生成される署名との組み合わせを含む、請求項１３に記載の方法。
【請求項１５】
前記第１の署名付き構造が、前記依拠当事者によって生成されるナンスと、前記第１の署名付き構造を前記クライアントでキャッシュすることができる時間量を示すキャッシュタイミングデータと、前記公開鍵と、前記ナンス、前記キャッシュタイミングデータ、及び前記公開鍵の組み合わせに対して生成される署名との組み合わせを含む、請求項１３に記載の方法。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】００４１
【訂正方法】変更
【訂正の内容】
【００４１】
オフラインデバイス又は接続可能性が限定されているデバイスに対して、クライアントを認証するシステム及び方法
上述したように、本発明の一実施形態は、ユーザデバイス及びデバイスがオフライン（即ち、依拠当事者のバックエンド認証サーバに接続されていない）又はセミオフライン（即ち、ユーザデバイスは依拠当事者に接続されていないが、デバイスは接続されている）の状況であっても、ユーザをローカルで認証する（即ち、ユーザを検証する）ための技術を含む。図４は、依拠当事者４５１に以前に登録されている認証デバイスを伴うクライアント４００が、トランザクションデバイス４５０とセキュアなチャネルを確立してトランザクションを完了する、１つのかかる構成を図示している。限定ではなく一例として、トランザクションデバイスは、ＡＴＭ、小売場所における売場専用（ＰｏＳ）トランザクションデバイス、物のインターネット（ＩｏＴ）デバイス、又はクライアント４００とチャネルを確立し、ユーザがトランザクションを実行することを可能にすることができる、他

の任意のデバイスであってもよい。チャネルは、限定ではなく一例として、近距離無線通信（ＮＦＣ）及びブルートゥース（登録商標）（例えば、ブルートゥースコア規格バージョン４．０に記載されているようなブルートゥースローエナジー（ＢＴＬＥ））を含む、任意の無線通信プロトコルを使用して実装されてもよい。当然ながら、本発明の基本原理は、いかなる特定の通信標準にも限定されない。

【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００８１
【訂正方法】変更
【訂正の内容】
【００８１】
上述の技術を使用して、企業は、トラストアンカー（例えば、公開ＲＰＶｅｒｉｆｙＫｅｙ）を全てのデバイスに一度に（例えば、インストール時に）注入することができる。各技術者は、次に、契約当事者（例えば、技術者の雇用主であってもよい依拠当事者４５１）に登録する。上述の技術を使用して、技術者は、各デバイスを認証することができる。

【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】００８２
【訂正方法】変更
【訂正の内容】
【００８２】
上述した本発明の実施形態は、認証能力を有するクライアントを依拠当事者に登録するいずれかのシステムで実装されてもよく、認証動作は、このクライアントと、（ａ）依拠当事者の代理を果たす、及び（ｂ）トランザクションの時点でオフラインである（即ち、クライアントが登録されている依拠当事者の元のサーバに対して信頼できるネットワーク接続を有していない）、デバイスとの間で実行される。かかる例では、クライアントは、キャッシュ可能な認証要求を元のサーバから受信し、それをキャッシュする。要求されると、クライアントは認証応答を計算し、それをデバイスに送る。