【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】平成30年6月21日(2018.6.21)

【公表番号】特表2017-519412(P2017-519412A)
【公表日】平成29年7月13日(2017.7.13)
【年通号数】公開・登録公報2017-026
【出願番号】特願2016-566924(P2016-566924)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/31　(2013.01)
Ｇ０６Ｆ　21/33　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６７３Ｄ
Ｇ０６Ｆ　21/31
Ｇ０６Ｆ　21/33

【手続補正書】
【提出日】平成30年5月10日(2018.5.10)
【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】
依拠当事者側で、ユーザから認証部を登録するための要求を受信することと、
認証されたアウトオブバンド通信チャネルを介して前記ユーザから前記依拠当事者へコードを送信することと、
前記コードを使用して前記ユーザのアイデンティティを検証し、肯定的な検証に応答して前記認証部を前記依拠当事者とともに応答性良く登録することと、を含む、方法。
【請求項２】
前記コードを前記検証することが、
前記ユーザの認証部のセキュアディスプレイ内に前記コードを表示することと、前記セキュアディスプレイ上に表示された前記コードを前記認証されたアウトオブバンド通信チャネルを介して送信するよう前記ユーザに求めることと、を含む、セキュアトランザクション確認操作を遂行することを更に含む、請求項１に記載の方法。
【請求項３】
前記コードが、前記ユーザの認証部によって生成された秘密コードである、請求項１に記載の方法。
【請求項４】
前記認証部を登録するための前記要求に応答して、前記認証部に関連付けられた公開鍵を生成することと、前記公開鍵を前記依拠当事者に伝送することと、を更に含む、請求項１に記載の方法。
【請求項５】
前記公開鍵に対してハッシュ操作を遂行することによって前記コードを生成することを

更に含む、請求項４に記載の方法。
【請求項６】
前記ハッシュ操作が、ＳＨＡ－２５６、ＳＨＡ－１、又はＳＨＡ－３ハッシュ操作を含む、請求項５に記載の方法。
【請求項７】
前記アウトオブバンド通信チャネルが、郵便、電子メール、又はショートメッセージサービス（ＳＭＳ）メッセージを含む、請求項１に記載の方法。
【請求項８】
セキュアトランザクション確認操作を遂行することが、
前記依拠当事者に関連付けられた前記ユーザのアカウントに関する識別コードを表示することを更に含む、請求項２に記載の方法。
【請求項９】
前記コードが、前記ユーザの電子識別証を使用して認証／署名された電子メッセージから抽出される、請求項１に記載の方法。
【請求項１０】
前記セキュアディスプレイ内に表示される内容が、前記内容にわたってハッシュを生成すること、及び得られたハッシュ値を前記依拠当事者に提供することによって保護され、前記依拠当事者が、前記ハッシュ値を有効化することによって前記内容を有効性を確認する、請求項２に記載の方法。
【請求項１１】
依拠当事者側で、ユーザから認証部を登録するための要求を受信することと、
前記認証部によりコードを生成することと、
前記コードを前記ユーザにセキュアに提供することと、
認証されたアウトオブバンド通信チャネルを介して前記ユーザから前記依拠当事者へ前記コードを送信することと、
前記コードを使用して前記ユーザのアイデンティティを検証し、肯定的な検証に応答して前記認証部を応答性良く登録することと、を含む、方法。
【請求項１２】
前記ユーザに前記コードをセキュアに提供することが、
前記ユーザの認証部のセキュアディスプレイ内に前記コードを表示することを含むセキュアトランザクション確認操作を遂行することを含む、請求項１１に記載の方法。
【請求項１３】
前記認証部を登録するための前記要求に応答して、前記認証部に関連付けられた公開鍵を生成することと、前記公開鍵を前記依拠当事者に伝送することと、を更に含む、請求項１１に記載の方法。
【請求項１４】
前記公開鍵に対してハッシュ操作を遂行することによって前記コードを生成することを更に含む、請求項１３に記載の方法。
【請求項１５】
前記ハッシュ操作が、ＳＨＡ－２５６、ＳＨＡ－１、又はＳＨＡ－３ハッシュ操作を含む、請求項１４に記載の方法。
【請求項１６】
前記アウトオブバンド通信チャネルが、郵便、電子メール、又はショートメッセージサービス（ＳＭＳ）メッセージを含む、請求項１１に記載の方法。
【請求項１７】
セキュアトランザクション確認操作を遂行することが、
前記依拠当事者に関連付けられた前記ユーザのアカウントに関する識別コードを表示することを更に含む、請求項１２に記載の方法。
【請求項１８】
前記コードが、前記ユーザの電子識別証を使用して認証／署名された電子メッセージか

ら抽出される、請求項１１に記載の方法。
【請求項１９】
前記セキュアディスプレイ内に表示される内容が、前記内容にわたってハッシュを生成すること、及び得られたハッシュ値を前記依拠当事者に提供することによって保護され、前記依拠当事者が、前記ハッシュ値を有効化することによって前記内容を有効性を確認する、請求項１２に記載の方法。
【請求項２０】
依拠当事者側で、ユーザから認証部を登録するための要求を受信することであって、前記要求が、前記ユーザの既存の資格証明書を識別する識別情報を含む、受信することと、
前記ユーザのクライアント側で認証オブジェクトを作成することであって、前記認証オブジェクトは、前記ユーザの前記既存の資格証明書と関連付けられた公開鍵を使用して生成された署名を含む、作成することと、
前記依拠当事者側で前記署名を検証し、肯定的な検証に応答して前記認証部を応答性良く登録することと、を含む、方法。
【請求項２１】
前記認証部に関連付けられた公開鍵／秘密鍵のペアを生成することと、前記公開鍵を前記依拠当事者に送信することと、を更に含む、請求項２０に記載の方法。
【請求項２２】
前記認証オブジェクトが、前記依拠当事者における前記ユーザのアカウントに関連付けられた識別コードと、前記秘密鍵によって生成された前記公開鍵のハッシュと、前記秘密鍵によって生成された前記署名と、を含む、請求項２１に記載の方法。
【請求項２３】
前記署名を検証することが、前記オブジェクトから抽出された前記公開鍵ハッシュを、登録時に前記ユーザから受信した前記公開鍵に関して計算された前記ハッシュ値と比較することを含む、請求項２２に記載の方法。