【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5月9日(2019.5.9)

【公表番号】特表2018-517367(P2018-517367A)
【公表日】平成30年6月28日(2018.6.28)
【年通号数】公開・登録公報2018-024
【出願番号】特願2017-562730(P2017-562730)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/44　(2013.01)
Ｇ０６Ｆ　21/64　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６７５Ｄ
Ｇ０６Ｆ　21/44
Ｇ０６Ｆ　21/64

【手続補正書】
【提出日】平成31年3月22日(2019.3.22)
【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】
通信ネットワークを介するデバイスとサービスプロバイダシステムとの間の通信リンクを確立するステップと、
前記サービスプロバイダシステムにおいて、前記通信ネットワークを介して前記デバイスからデバイス公開鍵を含む通信データを含む通信を受信するステップであって、前記デバイス公開鍵は、前記通信リンクの前記確立より先に生じる、受信するステップと、
前記サービスプロバイダシステムにおいて、前記デバイスから受信された前記通信内に含まれる前記通信データを使用して取得される少なくとも1つの他のデバイスからの検証データに基づいて、前記デバイスが前記デバイスのセキュアストレージ領域内にデバイス秘密鍵を記憶することを検証するステップであって、前記デバイス秘密鍵は、前記デバイス公開鍵に対応し、前記デバイス公開鍵と前記デバイス秘密鍵とは、暗号鍵ペアである、検証するステップと、
前記デバイスから受信された前記通信内に含まれる前記通信データを使用して取得される前記少なくとも1つの他のデバイスからの前記検証データに基づいて、前記デバイスが前記デバイスの前記セキュアストレージ領域内に前記デバイス秘密鍵を記憶することの検証に応答して、前記サービスプロバイダシステムによって、サービス登録のための前記デバイスのサインアップを認証するステップと
を含む方法。
【請求項２】
前記デバイスが前記デバイスの前記セキュアストレージ領域内に前記デバイス秘密鍵を記憶することを検証するステップは、前記デバイスの製造業者に関連するホワイトリストデータベース内で前記デバイス公開鍵の表示を見つけるステップを含む、請求項1に記載の方法。
【請求項３】

前記通信は、デバイス証明書を含み、前記デバイス公開鍵は、前記デバイス証明書の一部であり、前記デバイス公開鍵は、前記デバイス証明書を受信する前記サービスプロバイダシステムによって受信され、前記デバイスが前記デバイスの前記セキュアストレージ領域内に前記デバイス秘密鍵を記憶することを検証する前記ステップは、前記デバイス証明書が信頼に値することを示すデバイスルート認証局証明書を取得するステップと、セキュアストレージが前記デバイス秘密鍵のために使用されることの表示に関して前記デバイス証明書を分析するステップとを含む、請求項1に記載の方法。

【請求項４】

分析する前記ステップは、セキュアストレージが前記デバイス秘密鍵のために使用されることの表示に関して前記デバイス証明書の拡張鍵用途部分を分析するステップを含む、請求項3に記載の方法。

【請求項５】

前記サービスプロバイダシステムによってサービスプロバイダ証明書を作成するステップであって、前記サービスプロバイダ証明書の公開鍵は、前記デバイス公開鍵である、作成するステップと、

サービスプロバイダ署名された証明書を作成するために前記サービスプロバイダシステムによって前記サービスプロバイダ証明書に署名するステップと、

前記サービスプロバイダ署名された証明書を前記サービスプロバイダシステムから前記デバイスに送るステップと

をさらに含む、請求項1に記載の方法。

【請求項６】

前記サービスプロバイダ証明書に基づいて、前記サービスプロバイダシステムのサインアップサーバから前記サービスプロバイダシステムのサービスプロバイダ認証局に証明書署名要求を送るステップであって、前記サービスプロバイダ認証局は、前記サービスプロバイダ証明書に署名する前記ステップを実行する、送るステップと、

前記サインアップサーバにおいて前記サービスプロバイダ認証局から前記サービスプロバイダ署名された証明書を受信するステップと

をさらに含み、前記サインアップサーバは、前記サービスプロバイダ署名された証明書を前記デバイスに送る前記ステップを実行する

請求項5に記載の方法。

【請求項７】

前記サービスプロバイダ証明書を作成する前記ステップは、前記サービスプロバイダ証明書のフォーマットまたはコンテンツのうちの少なくとも1つがサービスプロバイダサーバ固有、サービスプロバイダ固有、デバイスユーザ固有、デバイス固有、またはサブスクリプション固有のうちの少なくとも1つになるように実行される、請求項5に記載の方法。

【請求項８】

前記デバイスから受信された前記通信内に含まれる前記通信データを使用して取得される前記少なくとも1つの他のデバイスからの前記検証データは、前記デバイスの前記暗号鍵ペアがセキュア鍵プロビジョニングプロセスに従って作成されたかどうかの表示を含む、請求項1に記載の方法。

【請求項９】

通信ネットワークを介するデバイスとの通信リンクを確立するように構成された通信インターフェースと、

前記通信インターフェースに通信可能に結合されたハードウェアベースのプロセッサとを含み、前記ハードウェアベースのプロセッサは、

前記デバイスからデバイス公開鍵を含む通信データを含む通信を受信することであって、前記デバイス公開鍵は、前記通信リンクの前記確立より先に生じる、受信することと、

前記デバイスから受信された前記通信内に含まれる前記通信データを使用して取得される少なくとも1つの他のデバイスからの検証データに基づいて、前記デバイスが前記デ

バイスのセキュアストレージ領域内にデバイス秘密鍵を記憶することを検証することであって、前記デバイス秘密鍵および前記デバイス公開鍵は暗号鍵ペアである、検証することと、

前記デバイスから受信された前記通信内に含まれる前記通信データを使用して取得される前記少なくとも1つの他のデバイスからの前記検証データに基づいて、前記デバイスが前記デバイスの前記セキュアストレージ領域内に前記デバイス秘密鍵を記憶することの検証に応答して、サービス登録のための前記デバイスのサインアップを認証することとを行うように構成される、サービスプロバイダシステム。

【請求項１０】

前記デバイスが前記デバイスの前記セキュアストレージ領域内に前記デバイス秘密鍵を記憶することを検証するために、前記プロセッサは、前記デバイスの製造業者に関連するホワイトリストデータベース内で前記デバイス公開鍵の表示を見つけ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】

前記通信は、デバイス証明書を含み、前記デバイス公開鍵は、前記デバイス証明書の一部であり、前記プロセッサは、前記デバイス証明書を受信することによって前記デバイス公開鍵を受信するように構成され、前記デバイスが前記デバイスの前記セキュアストレージ領域内に前記デバイス秘密鍵を記憶することを検証するために、前記プロセッサは、前記デバイス証明書が信頼に値することを示すデバイスルート認証局証明書を取得し、セキュアストレージが前記デバイス秘密鍵のために使用されることの表示に関して前記デバイス証明書を分析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１２】

前記デバイス証明書を分析するために、前記プロセッサは、セキュアストレージが前記デバイス秘密鍵のために使用されることの表示に関して前記デバイス証明書の拡張鍵用途部分を分析するように構成される、請求項11に記載のシステム。

【請求項１３】

前記プロセッサは、

サービスプロバイダ証明書を作成することであって、前記サービスプロバイダ証明書の公開鍵は前記デバイス公開鍵である、作成することと、

サービスプロバイダ署名された証明書を作成するために前記サービスプロバイダ証明書に署名することと、

前記サービスプロバイダ署名された証明書を前記デバイスに送ることとを行うようにさらに構成される

請求項9に記載のシステム。

【請求項１４】

前記プロセッサは、

サインアップモジュールからサービスプロバイダ署名された証明書モジュールに証明書署名要求を送ることと、

前記デバイス証明書に基づいて、前記サービスプロバイダ署名された証明書モジュール内で前記サービスプロバイダ署名された証明書を作成することと、

前記サービスプロバイダ署名された証明書を前記サービスプロバイダ署名された証明書モジュールから前記サインアップモジュールに送ることと、

前記サインアップモジュールにおいて、前記サービスプロバイダ署名された証明書モジュールから前記サービスプロバイダ署名された証明書を受信することと

を行うようにさらに構成され、前記プロセッサは、前記サービスプロバイダ署名された証明書を前記サインアップモジュールから前記デバイスに送るように構成される

請求項11に記載のシステム。

【請求項１５】

前記プロセッサは、前記サービスプロバイダ署名された証明書のフォーマットまたはコンテンツのうちの少なくとも1つがサービスプロバイダサーバ固有、サービスプロバイダ

固有、デバイスユーザ固有、デバイス固有、またはサブスクリプション固有のうちの少なくとも1つになるように前記サービスプロバイダ証明書を作成するように構成される、請求項13に記載のシステム。