

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7367212号

(P7367212)

(45)発行日 令和5年10月23日(2023.10.23)

(24)登録日 令和5年10月13日(2023.10.13)

(51)国際特許分類

F I

G 0 6 F 21/44 (2013.01)

G 0 6 F 21/44

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62 3 1 8

G 0 6 F 21/57 (2013.01)

G 0 6 F 21/57 3 2 0

請求項の数 22 (全24頁)

(21)出願番号 特願2022-528938(P2022-528938)

(86)(22)出願日 令和2年10月13日(2020.10.13)

(65)公表番号 特表2023-503028(P2023-503028 A)

(43)公表日 令和5年1月26日(2023.1.26)

(86)国際出願番号 PCT/US2020/055347

(87)国際公開番号 WO2021/101636

(87)国際公開日 令和3年5月27日(2021.5.27)

審査請求日 令和4年6月17日(2022.6.17)

(31)優先権主張番号 16/688,848

(32)優先日 令和1年11月19日(2019.11.19)

(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者 595168543

マイクロン テクノロジー, インク.

アメリカ合衆国, アイダホ州 8 3 7 1

6-9 6 3 2, ボイズ, サウス フェデ

ラル ウェイ 8 0 0 0

(74)代理人 100121083

弁理士 青木 宏義

(74)代理人 100138391

弁理士 天田 昌行

(74)代理人 100074099

弁理士 大菅 義之

(72)発明者 デュバル オリヴィエ

アメリカ合衆国 アイダホ州 8 3 7 1 6

-9 6 3 2 ボイズ サウス フェデラル

ウェイ 8 0 0 0 マイクロン テクノロ

最終頁に続く

(54)【発明の名称】 リモートホストを使用したデバイスの認証

(57)【特許請求の範囲】

【請求項1】

デバイスのソフトウェアが安全であることを認証するフィールドサーバによって行われる方法であって、

ソフトウェアのアップデートが前記デバイスへ送信されたことの通知を受信することと、

前記通知を受信することに少なくとも部分的に基づいて、前記デバイスとメモリ内の前

記ソフトウェアのアップデートとの間の関連を指し示すフラグを設定することと、

前記デバイスを認証するための第1のキーと関連付けられた証明書を含む接続リクエストを前記デバイスから受信することと、

前記接続リクエストを受信することに少なくとも部分的に基づいて、前記デバイスから受信した前記第1のキーが無効であると判定することと、

前記関連を指し示す前記フラグに少なくとも部分的に基づいて、前記第1のキーを有効であると判定することと、

前記第1のキーを有効であると判定することに少なくとも部分的に基づいて、前記デバイスとサービスとの間の接続を確立すること

を含む、方法。

【請求項2】

前記フラグに少なくとも部分的に基づいて前記第1のキーを有効であると判定すること

に少なくとも部分的に基づいて、前記メモリ内のリスト内に前記第1のキーを蓄積すること

を更に含む、請求項1に記載の方法。

【請求項 3】

前記デバイスの前記ソフトウェアがアップデートされた後、前記デバイスと関連付けられたアップデートされた証明書を受信することと、

前記アップデートされた証明書を受信することに少なくとも部分的に基づいて、前記フィールドサーバにより蓄積された前記デバイスと関連付けられた第 2 の証明書をアップデートすること

を更に含む、請求項 2 に記載の方法。

【請求項 4】

前記第 1 のキーが有効であると判定することに少なくとも部分的に基づいて、前記デバイスからの追加の接続リクエストを処理すること

を更に含む、請求項 3 に記載の方法。

【請求項 5】

前記接続リクエストを受信することに少なくとも部分的に基づいて、前記第 1 のキーと関連付けられた前記証明書と前記デバイスと関連付けられた第 2 の証明書との間の不一致を識別することと、

前記フラグに少なくとも部分的に基づいて、前記不一致に関係なく前記接続リクエストを検証することであって、前記第 1 のキーが有効であると判定することは、前記接続リクエストを検証することに少なくとも部分的に基づくこと

を更に含む、請求項 1 に記載の方法。

【請求項 6】

前記第 1 のキーと関連付けられた前記証明書を、前記フィールドサーバにより蓄積された第 2 の証明書と比較することと、

前記第 1 のキーと関連付けられた前記証明書を前記第 2 の証明書と比較することに少なくとも部分的に基づいて、アプリケーションプラットフォームへのアクセスのために前記デバイスを認証すること

を更に含む、請求項 1 に記載の方法。

【請求項 7】

前記デバイスを認証することに少なくとも部分的に基づいて、前記サービスへのサブスクリプションを検証すること

を更に含む、請求項 6 に記載の方法。

【請求項 8】

前記認証することは、前記デバイスが前記アプリケーションプラットフォームと通信し、前記サービスにサブスクライブすることを可能にする、請求項 6 に記載の方法。

【請求項 9】

前記デバイスから受信した前記第 1 のキーと関連付けられた前記証明書は、前記デバイスの前記ソフトウェアのハッシュに少なくとも部分的に基づく、請求項 1 に記載の方法。

【請求項 10】

前記接続リクエストを受信することに少なくとも部分的に基づいて、前記第 1 のキーが有効であるか否かを指し示す確認応答メッセージ又は否定確認応答メッセージを前記デバイスへ送信すること

を更に含む、請求項 1 に記載の方法。

【請求項 11】

第 1 のサーバによって行われる方法であって、

デバイスに対するソフトウェアのアップデートを識別することと、

前記ソフトウェアのアップデートを識別することに少なくとも部分的に基づいて前記ソフトウェアのアップデートが前記デバイスへ送信されることの通知を、前記デバイスのソフトウェアが安全であることを認証するための第 2 のサーバへ送信することと、

前記デバイスに対する前記ソフトウェアのアップデートを識別することに少なくとも部分的に基づいて、前記ソフトウェアのアップデートを前記デバイスへ送信すること、

前記デバイスが前記ソフトウェアのアップデートを実施したことを指し示す完了メッセ

10

20

30

40

50

ージを前記デバイスから受信することと、

前記完了メッセージを受信することに少なくとも部分的に基づいて、前記デバイスと関連付けられたアップデートされた証明書を前記第 1 のサーバから前記第 2 のサーバへ送信すること

を含む、方法。

【請求項 1 2】

前記デバイスと前記ソフトウェアのアップデートとの間の関連を指し示すフラグが、前記第 2 のサーバによって、前記通知を受信することに少なくとも部分的に基づいて、メモリ内に設定される、請求項 1 1 に記載の方法。

【請求項 1 3】

前記通知は、前記デバイスから受信したキーと関連付けられた証明書が前記ソフトウェアのアップデートに少なくとも部分的に基づいて変更されていることを識別するためのものである、請求項 1 1 に記載の方法。

【請求項 1 4】

前記ソフトウェアのアップデートを送信することに少なくとも部分的に基づいて、前記デバイスの一部分を追記書き込みモードで動作するように構成すること
を更に含む、請求項 1 1 に記載の方法。

【請求項 1 5】

前記デバイスの前記一部分を前記追記書き込みモードで動作するように構成すること
に少なくとも部分的に基づいて、前記ソフトウェアに追加情報を追記することと、

前記追加情報を追記することに少なくとも部分的に基づいて、前記ソフトウェアのアップデート前に利用可能な前記ソフトウェアのバージョンへのアクセスを防止することと、

前記追加情報を追記することに少なくとも部分的に基づいて、前記デバイスから受信したキーをアップデートすること

を更に含む、請求項 1 4 に記載の方法。

【請求項 1 6】

第 1 のサーバデバイスであって、

デバイスに対するソフトウェアのアップデートを識別することと、

前記ソフトウェアのアップデートを識別することに少なくとも部分的に基づいて、前記ソフトウェアのアップデートが前記デバイスへ送信されたことの通知を送信することと
をするように構成された前記第 1 のサーバデバイスと、

前記第 1 のサーバデバイスと電子通信し、

前記ソフトウェアのアップデートが前記デバイスへ送信されたことの前記通知を受信することと、

前記通知を受信することに少なくとも部分的に基づいて、前記デバイスとメモリ内の前記ソフトウェアのアップデートとの間の関連を指し示すフラグを設定することと、

前記デバイスを認証するための第 1 のキーと関連付けられた証明書を含む接続リクエストを受信することと、

前記関連を指し示す前記フラグに少なくとも部分的に基づいて、前記第 1 のキーを有効であるものとして受け入れること

をするように構成された第 2 のサーバデバイスと

を含む、システム。

【請求項 1 7】

前記第 1 のサーバデバイス及び前記第 2 のサーバデバイスと電子通信する前記デバイスを更に含み、前記デバイスは、

前記ソフトウェアのアップデートを受信することと、

前記ソフトウェアのアップデートを受信することに少なくとも部分的に基づいて前記ソフトウェアのアップデートを実施すること

をするように構成される、請求項 1 6 に記載のシステム。

【請求項 1 8】

10

20

30

40

50

前記デバイスは、
前記デバイスのソフトウェアをハッシュすることと、
前記ソフトウェアの前記ハッシュとデバイス固有のシークレットとに少なくとも部分的に基づいて前記第1のキーを生成すること
をするように更に構成される、請求項17に記載のシステム。

【請求項19】

前記第2のサーバデバイスは、
前記ソフトウェアのアップデートの前記実施に少なくとも部分的に基づいて、前記デバイスを認証するための前記第1のキーと関連付けられた前記証明書を含む前記接続リクエストを判定すること
をするように更に構成される、請求項17に記載のシステム。

【請求項20】

前記第2のサーバデバイスは、
前記接続リクエストを受信することに少なくとも部分的に基づいて、前記デバイスから受信した前記第1のキーが無効であることを識別すること
をするように更に構成される、請求項16に記載のシステム。

【請求項21】

前記第2のサーバデバイスは、
前記第1のキーと関連付けられた前記証明書を前記デバイスと関連付けられた第2の証明書と比較することと、
前記第1のキーと関連付けられた前記証明書を前記第2の証明書と比較することに少なくとも部分的に基づいて、前記デバイスがアプリケーションサービスにアクセスするための認証手順を実施すること
をするように更に構成される、請求項16に記載のシステム。

【請求項22】

前記第1のサーバデバイスは、
前記デバイスの前記ソフトウェアのアップデートが完了した後、前記デバイスと関連付けられたアップデートされた証明書を送信すること
をするように更に構成される、請求項16に記載のシステム。

【発明の詳細な説明】

【技術分野】

【0001】

【クロスリファレンス】

本特許出願は、2020年10月13日に出願された“AUTHENTICATING A DEVICE USING A REMOTE HOST”と題されたDuvallによる国際特許出願PCT/US2020/055347の国内段階出願であり、それは、2019年11月19日に出願された“AUTHENTICATING A DEVICE USING A REMOTE HOST”と題されたDuvallによる米国特許出願第16/688,848号の優先権を主張するものであり、それぞれは、本明細書の譲受人に割り当てられ、参照によりその全体が本明細書に明示的に組み込まれる。

【背景技術】

【0002】

以下は、一般に、少なくとも1つのメモリデバイスを含むシステムに関し、より具体的には、リモートホストを使用してデバイスを認証することに関する。

【0003】

メモリデバイスは、コンピュータ、無線通信デバイス、カメラ、及びデジタルディスプレイ等の様々な電子デバイス内に情報を蓄積するために広く使用されている。情報は、メモリデバイスの異なる状態をプログラミングすることによって蓄積される。例えば、バイナリデバイスは、論理1又は論理0でしばしば示される2つの状態の内の1つを蓄積する。他のデバイスでは、2つよりも多い状態が蓄積され得る。蓄積された情報にアクセスす

10

20

30

40

50

るために、デバイスのコンポーネントは、メモリデバイス内の少なくとも1つの蓄積された状態を読み出し得、又はセンシングし得る。情報を蓄積するために、デバイスのコンポーネントは、メモリデバイス内に状態を書き込み得、プログラミングし得る。

【0004】

磁気ハードディスク、ランダムアクセスメモリ（RAM）、リードオンリーメモリ（ROM）、ダイナミックRAM（DRAM）、同期型ダイナミックRAM（SDRAM）、強誘電体RAM（FeRAM）、磁気RAM（MRAM）、抵抗変化型RAM（RRAM）、フラッシュメモリ、及び相変化メモリ（PCM）等を含む様々なタイプのメモリデバイスが存在する。メモリデバイスは、揮発性又は不揮発性であり得る。幾つかのメモリデバイスは、サーバとの通信を実施する前に認証プロセスを実行し得る。幾つかのメモリデバイスは、ソフトウェアのアップデートを定期的の実施し得る。

10

【図面の簡単な説明】

【0005】

【図1】本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするシステムの一例を説明する。

【図2】本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするプロセスフローの一例を説明する。

【図3】本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするプロセスフローのブロック図を示す。

【図4】本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするフィールドサーバのブロック図を示す。

20

【図5】本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートする1つ以上の方法を説明するフローチャートを示す。

【図6】本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートする1つ以上の方法を説明するフローチャートを示す。

【発明を実施するための形態】

【0006】

幾つかのデバイスは、ユーザ（例えば、デバイス又はデバイスのコンポーネントの製造業者の顧客又はクライアント）によって配備及び動作され得る。一旦配備されると、サーバと通信する前にデバイスは認証され得る。認証は、セキュアなドメインにログインしようと試みる個々のプロセス又はエンティティを識別するプロセスである。認証は、認証されたデバイス（又はプロセス）のみがその保護されたリソースにアクセスすることを許可することによってネットワークを安全に保ち得、該リソースは、コンピューターシステム、ネットワーク、データベース、ウェブサイト、及びその他のネットワークベースのアプリケーション又はサービスを含み得る。サーバにおいてデータにアクセスする、又はサーバにデータを提供する前に、サーバへのアクセスをリクエストするデバイスが特定のデバイスであり、又は悪意のないデバイス（例えば、改竄されていないデバイス）であることを確認するために、デバイスはサーバとの認証手順を経り得る。

30

【0007】

サーバは、デバイスと関連付けられたキー（例えば、デバイスエイリアスキー）と、サーバに蓄積され、さもなければサーバによりアクセス可能な証明書とに基づいてデバイスを認証し得る。例えば、キー管理サーバは、証明書と、デバイスと関連付けられたキーとの生成に利用され得る。デバイス固有のシークレット及びデバイスのソフトウェアのハッシュは、証明書又はキーを生成するために使用され得る。ソフトウェアのハッシュは、デバイスのコードがエンティティによって改竄されているか否かを検出する方法として、証明書及びキーを生成する場合に使用される。ソフトウェアのハッシュが使用されるため、デバイスのソフトウェアがアップデートされた場合、証明書間の不一致が原因で認証手順は失敗し得る。

40

【0008】

本明細書に説明する技術に従えば、システムは、デバイス上でソフトウェアのアップデ

50

ートを実施することの一部として、認証手順のために使用される証明書をアップデートするように動作可能である。システムはまた、デバイスとサーバとの両方によって認識された有効なキーに基づいて、デバイスがサービスに接続することを可能にし得る。例えば、サーバはソフトウェアのアップデートをデバイスへ送信し得る。サーバは、デバイスがソフトウェアのアップデートを経験していることを指し示すフラグを設定し得る。こうした場合、デバイスが接続リクエストを送信し、キー又は証明書（例えば、ソフトウェアのハッシュが異なるためにサーバにアップロードされた証明書と一致しない無効なキー又は無効な証明書）を提示する場合、サーバは、フラグが設定されているため、キーを有効なものとして一時的に受け入れ得る。サーバは、キーを含むデバイスからの追加の接続リクエストを受け入れ得るように、キーをリストに追加し得る。こうした場合、システムは、ソフトウェアのアップデートが発生した後の認証プロセスの複雑さを軽減し得、接続遅延を軽減し得、デバイスの製造業者若しくはユーザに対するコストを軽減し得、又はそれらの組み合わせであり得る。

10

【0009】

開示の機構は、図1及び図2を参照して説明するようにシステム及びプロセスフロー図の文脈で説明される。開示のこれらの及びその他の機構は、図3～図6を参照して説明するように、リモートホストを使用してデバイスを認証することに関連する装置図及びフローチャートによって更に例証され、及びそれらを参照して説明される。

【0010】

図1は、本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするシステム100の一例を説明する。システム100は、デバイス105、キー管理サーバ150、登録ポータル165、デバイス製造ホスト175、及びフィールドサーバ185を含み得る。

20

【0011】

デバイス105は、少なくともシークレット115を安全に蓄積するように構成されたセキュアコンポーネント110を含み得る。シークレット115は、ユニークデバイスシークレット(UDS)の一例であり得る。幾つかの場合、セキュアコンポーネント110は、管理キー120を蓄積し得る。管理キー120は、サーバルートキー(SRK)の一例であり得る。SRKは、管理キー120のコピーを所有するエンティティが、セキュアコンポーネント110のセキュリティ機構をオンにすることによって、セキュアコンポーネント110を管理することを可能にし得る。デバイス105は、デバイス220全体に対する1つ以上の認証手順を実施するように動作可能なメモリデバイスと関連付けられた1つ以上のコンポーネントを含み得る。デバイス105は、車両、パーソナルコンピュータ、携帯型電子デバイス、サーバ、又は任意のその他のタイプのコンピューティングデバイスのインフォテインメントシステムの一例であり得る。

30

【0012】

セキュアコンポーネント110は、デバイス識別子構成エンジン(DICE)標準、若しくはRIOTと関付けられた標準、又はそれらの組み合わせに従って生成されたデバイス識別子125を含み得る。幾つかの場合、デバイス識別子125は、デバイスシークレット115及びソフトウェア130に基づき得る。デバイス識別子125は、第1のキーペア135及び第2のキーペア140等の非対称キーペアを生成するために使用され得る。第1のキーペアは、エイリアスキーペアの一例であり得、第2のキーペア140は、デバイス識別キーペアの一例であり得る。幾つかの例では、デバイス105は、ソフトウェア130に関連してデバイス105の機能を提供するために、セキュアコンポーネント110に接続された1つ以上の追加のコンポーネント145を含み得る。

40

【0013】

幾つかの例では、コマンドのセットは、シークレット115から及び暗号化ソフトウェアハッシュ170からデバイス識別子125を生成するために、デバイス105内で実行され得る。そうした場合、デバイス105は、デバイス製造ホスト175と通信し得る。デバイス製造ホスト175は、プロビジョニングツール180、ソフトウェア130、及

50

びソフトウェアハッシュ170を含み得る。コマンドのセットの実行は、第1のキーペア135及び第2のキーペア140等の非対称キーペアを更に生成し得る。

【0014】

システム100は、デバイス製造ホスト175と通信するキー管理サーバ150を含み得る。キー管理サーバ150は、証明書ジェネレータ155を含み得る。証明書ジェネレータ155は、非対称キーペアを生成する際にデバイス105の機構をエミュレートするように構成され得る。例えば、証明書ジェネレータ155は、キー管理サーバ150内に蓄積されたシークレット115のコピーから、及び登録ポータル165から受信したソフトウェアハッシュ170からデバイス識別子125を生成するために、デバイス105内で実行されるコマンドの同じセットを使用するように構成され得る。こうした場合、登録ポータル165は、デバイス製造ホスト175及びキー管理サーバ150と通信し得る。

10

【0015】

証明書ジェネレータ155内で実行されるコマンドのセットは、非対称キーペア（例えば、第1のキーペア135及び第2のキーペア140）を生成し得る。例えば、ソフトウェアハッシュ170及びシークレット115は、キーを創出するために組み合わせられ得る。幾つかの例では、証明書ジェネレータ155は、キーに基づいて証明書（例えば、キー証明書160）を生成し得る。例えば、証明書ジェネレータ155は、証明書ジェネレータ155又はキー管理サーバ150の秘密キーを使用して、対応する非対称キーペア内の公開キーに対する証明書（例えば、キー証明書160）にデジタル署名し得る。キー証明書160の認証は、証明書ジェネレータ155の公開キーを介して検証され得る。

20

【0016】

幾つかの場合、キー管理サーバ150は、デバイス105のキー証明書160をフィールドサーバ185に提供し得、それによって、証明書ジェネレータ155により認証された公開キーと、対応する秘密キーを使用してデバイス105により署名されたメッセージ（例えば、証明書）とに基づいてフィールドサーバ185がデバイス105を認証することを可能にする。そうした場合、フィールドサーバ185は、証明書ジェネレータ155により署名された証明書を有する公開キーの信頼性を検証し得る。

【0017】

デバイス105の公開キーが一旦証明されると、デバイス105は、フィールドサーバ185に対してそれ自体を認証するために、対応する秘密キーを使用し得る。そうした場合、デバイス105は、フィールドサーバ185と直接通信し得る。例えば、デバイス105は、秘密キーを使用してメッセージをデジタル署名し得る。デバイス105の秘密キーと関連付けられた公開キーが証明書のデジタル署名を検証するために使用される場合、デバイス105は秘密キーを所有するとみなされ得る。他の例では、デバイス105は、公開キーにより署名された証明書で指定されたアイデンティティを有するとみなされ得る。そうした場合、システム100は、セキュアコンポーネント110内のシークレット（例えば、管理キー120及びシークレット115）の実装とは異なる時間及び場所でデバイス105がソフトウェアを用いてロードされることを可能にする。システム100はまた、デバイス105が有効な公開キーに基づいてサービスに接続することを可能にし得る。

30

【0018】

フィールドサーバ185は、デバイス105のための複数の異なるサービスを含み得る。幾つかの場合、異なるサービスは、デバイス状態に依存する。例えば、デバイス105が登録ポータル165を通じて登録される場合、1つ以上のソフトウェアハッシュ170がアップロードされ得る。各ソフトウェアハッシュ170は、デバイス105の有効なバージョンを表し得る。幾つかの場合、デバイス105は、複数のステップを含み得るサプライチェーンを通過し得、各ステップは、ソフトウェア130の異なるバージョンを表し得る。フィールドサーバ185は、ソフトウェア130のバージョンを通知するために、デバイスがサプライチェーンの何れのステップにあるかをリクエストし得る。

40

【0019】

デバイス105は、（例えば、サプライチェーン内の各ステップを指し示す）あらゆる

50

ソフトウェアハッシュ170を登録ポータル165にアップロードすることによって登録され得る。証明書ジェネレータ155は、各ソフトウェアハッシュ170に対する証明書を生成し得る。そうした場合、キー管理サーバ150は、ソフトウェアハッシュ170の各バージョンをフィールドサーバ185にアップロードし得る。デバイス105がフィールドサーバ185にキーを提示する場合、フィールドサーバ185は、デバイス105をデバイス状態（例えば、ソフトウェアハッシュ170）と関連付けられたサービスに接続し得る。

【0020】

幾つかの例では、デバイス105は、登録ポータル165にアップロードされたソフトウェアハッシュ170のリストを修正し得る。例えば、デバイス105は、ソフトウェアハッシュ170のリストからソフトウェアハッシュ170を追加又は削除することをリクエストし得る。幾つかの例では、デバイス105は、登録ポータル165を介してキー管理サーバと通信するのではなく、ソフトウェアハッシュ170をキー管理サーバ150に直接追加又は削除するためのリクエストを通信し得る。証明書ジェネレータ155は、それらのソフトウェアハッシュが削除されたか、それとも追加されたか否かに基づいて証明書を再生成し得る。

【0021】

幾つかの例では、フィールドサーバ185は、接続エージェント190及び1つ以上のキー証明書160を含み得る。フィールドサーバ185がデバイス105からキーを受信した場合、フィールドサーバ185は、フィールドサーバ185内のキー証明書160の各々を受信したキーと比較し得る。他の例では、フィールドサーバ185は、デバイス状態に基づく比較のためにキー証明書160を識別し得る。例えば、デバイス105は、デバイス状態の通知をフィールドサーバ185へ送信し得る。デバイス状態に基づいて、フィールドサーバ185は、デバイス状態に対応する証明書をチェックし得る。

【0022】

幾つかの例では、デバイス105は、接続リクエストを接続エージェント190へ送信し得る。リクエストは、キー及びデバイス識別情報（例えば、デバイス識別（ID））を含み得る。接続エージェント190は、接続リクエスト（例えば、キー）をキー証明書160と照合し得る。提示されたキーが有効ではない（例えば、キー証明書160と一致しない）場合、接続エージェント190は、デバイス105がソフトウェアのアップデートを実施していること、デバイスがエラーを経験していること、又はそれら両方であることを判定し得る。幾つかの場合、エラーは、デバイス105が欠陥のある又は悪意のあるソフトウェアを含むことを識別することを指し示し得る。

【0023】

接続エージェント190は、デバイス105がソフトウェアのアップデートを経験していると接続エージェント190が判定した場合に、ローカルリストに新たなキーを追加し得る。ソフトウェアのアップデートは、キー証明書160を無効にさせ得る。例えば、キー証明書160は、ソフトウェアハッシュ170（例えば、ソフトウェアコード）をハッシュすることに基づいて生成される。そうした場合、ソフトウェアのアップデートは、ソフトウェアハッシュ170へのアップデートを含み得、それによって、キー証明書160とアップデートされたソフトウェアハッシュ170との間の不一致を指し示す。例えば、デバイスのソフトウェア130への如何なるアップデートも、フィールドサーバ185により蓄積されたキー証明書160内に反映されないことがある。幾つかの例では、キー証明書160は、ソフトウェアのアップデート（例えば、アップデートされたソフトウェアハッシュ170）に基づいて再生成され得る。幾つかの場合、ソフトウェアハッシュ170は、ソフトウェアコードが（例えば、許可されていないユーザを介して）許可なく修正されたか否かをチェックし得る。

【0024】

フィールドサーバ185は、ソフトウェアのアップデートが進行中であることを指し示すフラグを設定し得る。幾つかの例では、フィールドサーバ185は、ローカルリストへ

10

20

30

40

50

の新たなキーの追加及びフラグの設定に基づいて、無効なキーを一時的に許可し得る。他の例では、無効なキーが接続エージェント 190 に提示された場合、接続エージェント 190 は、デバイス 105 からキー証明書 160 をリクエストし得る。フィールドサーバ 185 がリクエストされた証明書を一旦受信すると、フィールドサーバ 185 は、無効なキーを検証（例えば、確認）し得る。

【0025】

デバイス 105 は、フィールドサーバ 185 と関連付けられたサービスへのサブスクリプションをデバイス 105 が含むことに基づいて接続エージェント 190 にアクセスし得る。幾つかの例では、デバイス 105 は、フィールドサーバ 185 に有効なキーを提示し得る。幾つかの場合、接続エージェント 190 は、デバイス 105 を有効なキーに対応するサービスにルーティングし得る。

10

【0026】

幾つかの例では、各キーは、別個のプロファイルを含み得る。例えば、接続エージェント 190 は、フィールドサーバ 185 に提示されたキーに基づいてデバイス 105 をプロファイルと一致させ得る。幾つかの場合、プロファイルは、デバイス 105 上に存在するソフトウェアイメージと一致させ得る。プロファイルは、シークレット 115 及びソフトウェアハッシュ 170 に加えてフィールドサーバ 185 と関連付けられ得る。幾つかの例では、プロファイルは、ソフトウェアハッシュ 170 内に埋め込まれ得、プロファイルは、サービスと関連付けられ得、又はそれらの両方であり得る。幾つかの場合、フィールドサーバ 185 は、ソフトウェアイメージと関連付けられたプロファイルを識別し得、デバイス 105 をプロファイルと関連付けられたサービスにルーティングし得る。

20

【0027】

システム 100 は、フィールドサーバ 185 にアクセスする際のデバイス 105 のセキュアな認証のための構成を備えたデバイス 105 上にソフトウェア 130 を搭載するためのプロセスを説明し得る。例えば、セキュアコンポーネント 110 は、セキュアコンポーネント 110 を使用するデバイス 105 内に後で配備又はインストールされ得るソフトウェア 130 に対する何れの知識又はアクセスもなくファクトリ内で構成され得る。セキュアコンポーネント 110 がファクトリである場合、第 1 のルートオブトラストのシークレット（例えば、管理キー 120 及びシークレット 115）は、セキュアコンポーネント 110 に導入され得る。シークレットのコピーは、ファクトリとキー管理サーバ 150 との間のセキュアな接続を介して、（例えば、セキュアコンポーネント 110 の識別と共に）キー管理サーバ 150 に蓄積され得る。

30

【0028】

幾つかの例では、デバイス製造業者は、セキュアコンポーネント 110 と追加のコンポーネント 145 とを統合するデバイス 105 の設計を開発する。デバイス 105 を動作させるためのソフトウェア 130 は、デバイス製造業者の施設（例えば、フィールドサーバ 185）で利用可能になり得る。幾つかの場合、ソフトウェア 130 をセキュアコンポーネント 110 にインストールし、ソフトウェア 130 についての情報を生成するために、プロビジョニングツール 180 が使用され得る。ソフトウェア 130 についての情報は、デバイス 105 のデバイス識別子 125 を生成するために、デバイス 105 内で使用され得る。

40

【0029】

ソフトウェア 130 についての情報は、ソフトウェア 130 のソフトウェアハッシュ 170 の一例であり得る。例えば、ソフトウェアハッシュ 170 は、ソフトウェア 130 のソースコードの暗号化関数であり得る。幾つかの場合、ソフトウェアハッシュ 170 は、デバイス製造業者と関連付けられた第 2 のルートオブトラストの情報を表し得る。他の例では、ソフトウェアハッシュ 170 は、デバイス製造業者の秘密キーを使用してデジタル署名され得る。

【0030】

デバイス 105 におけるキーの生成のために使用されるソフトウェアハッシュ 170 は

50

、セキュアコンポーネント 110 の登録中に、登録ポータル 165 を介してキー管理サーバ 150 に通信され得る。幾つかの場合、ソフトウェアハッシュ 170 は、デバイス 105 内のソフトウェア 130 のインストールプロセスの一部としてデバイス 105 に提供され得る。そうした例では、フィールドサーバ 185 上に蓄積されたキー証明書 160 は、元のソフトウェアのソフトウェアハッシュ 170 に基づき得る。デバイスのソフトウェア 130 への如何なるアップデートも、フィールドサーバ 185 により蓄積されたキー証明書 160 に反映されないことがある。ソフトウェアのアップデート後に証明書をアップデートするための技術は、本明細書に説明される。幾つかの例では、証明書ジェネレータ 155 は、デバイス 105 の動作とは無関係にデバイス 105 の公開キーを生成し、デバイス 105 の公開キーに対するキー証明書 160 に署名するためにソフトウェアハッシュ 170 を使用し得る。

10

【0031】

登録ポータル 165 は、セキュアコンポーネント 110 を管理するために管理キー 120 を使用し得、セキュアコンポーネント 110 の登録後又はキー証明書 160 の生成後にセキュアコンポーネント 110 のセキュリティ機構をアクティブにし得る。セキュアコンポーネント 110 のセキュリティ機構がアクティブにされると、デバイス 105 内にインストールされたセキュアコンポーネント 110 は、デバイス 105 のデバイス識別子 125 及びデバイス識別子 125 の暗号化キー（例えば、第 1 のキーペア 135 及び第 2 のキーペア 140）を生成する際に使用され得る。

【0032】

20

図 2 は、本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするプロセスフロー 200 の一例を説明する。プロセスフロー 200 は、管理サーバ 205、キー管理（KM）サーバ 210、フィールドサーバ 215、及びデバイス 220 を含み得、これらは、図 1 を参照して本明細書に説明した対応するデバイスの例であり得る。プロセスフロー 200 は、リモートホストを使用してデバイスを認証することを説明し得る。リモートホストは、管理サーバ 205、KM サーバ 210、フィールドサーバ 215、その他のコンポーネント、又はそれらの組み合わせを指し得る。

【0033】

225 において、管理サーバ 205 は、ソフトウェアのアップデートを識別し得る。初期化プロセスの一部として、230 において、KM サーバ 210 は、ルートキーを管理サーバ 205 へ送信し得る。235 において、KM サーバ 210 は、証明書を生成し得、該証明書をフィールドサーバ 215 にアップロードし得る。幾つかの場合、KM サーバ 210 は、KM サーバ 210 にアップロードされた各ソフトウェアハッシュに対して証明書を生成し得る。証明書は、エイリアスキー、公開キー、及びデバイス ID 秘密キーで署名された証明書を含み得る。幾つかの場合、フィールドサーバ 215 は、各証明書がエイリアスキー及び公開キーを含む複数の証明書を受信し得る。

30

【0034】

240 において、管理サーバ 205 は、ソフトウェアのアップデートを開始し得る。例えば、管理サーバ 205 は、ソフトウェアのアップデートをデバイス 220 へ送信し得る。デバイス 220 は、管理サーバ 205 からソフトウェアのアップデートを受信することに基づいてそのソフトウェアをアップデートし得る。そうした手順は、アップデートが成功したことの確認応答（ACK）又は否定確認応答（NACK）をデバイス 220 が送信することを含み得る。

40

【0035】

245 において、管理サーバ 205 は、ソフトウェアのアップデートがデバイス 220 へ送信されたことをフィールドサーバ 215 に通知し得る。そうした場合、フィールドサーバ 215 は、ソフトウェアのアップデートがデバイス 220 へ送信されたことの通知を受信し得る。通知は、デバイス 220 から受信したキーと関連付けられた証明書がソフトウェアのアップデートに基づいて変更されたことを識別するためのものであり得る。幾つかの例では、フィールドサーバ 215 は、デバイス 220 のソフトウェアを認証し得、そ

50

れによって、ソフトウェアが安全であることを指し示す。

【0036】

250において、デバイス220は、ソフトウェアのアップデートを実施し得、完了し得る。幾つかの例では、デバイス220は、デバイス220のソフトウェアをハッシュし得、ソフトウェアのハッシュ及びデバイス固有のシークレットに基づいてキーを生成し得る。ソフトウェアのアップデートは、プロセスフロー200の何時でも発生し得る。255において、デバイス220は、完了メッセージを管理サーバ205へ送信し得る。完了メッセージは、デバイス220がソフトウェアのアップデートを実施したことを指し示し得る。

【0037】

260において、フィールドサーバ215は、デバイス220と、フィールドサーバ215のメモリ内のソフトウェアのアップデートとの間の関連を指し示すフラグを設定し得る。例えば、フィールドサーバ215は、ソフトウェアのアップデートを受けているものとしてデバイス220にフラグを立てるために、データベース内に記録し得る。幾つかの場合、通知及びフラグを使用することは、アップデートされた証明書を生成するためにKMサーバ210を伴うことなく、フィールドサーバ215上に蓄積された証明書をシステムがアップデートすることを可能にし得る。こうした手順は、ソフトウェアのアップデートに遅延をもたらし得、証明書が正しいことを確認することに関連する他の問題を引き起こし得る。

【0038】

265において、フィールドサーバ215は、デバイス220を認証するためのキーと関連付けられた証明書を含む接続リクエストをデバイス220から受信し得る。例えば、デバイス220は、確立メッセージ（例えば、接続リクエスト）を送信することによって、フィールドサーバ215にエイリアスキー（例えば、第1のキー）を提示し得る。幾つかの場合、接続リクエストはデバイスID情報を含み得る。そうした場合、デバイスID情報は、キーと、235においてアップロードされた証明書とを照合するようにフィールドサーバ215に命じ得る。

【0039】

270において、フィールドサーバ215は、デバイス220から受信したキーの有効性を判定し得る。例えば、270において、フィールドサーバ215は、デバイスから受信したキーが無効であると判定し得る。幾つかの例では、フィールドサーバ215は、デバイス220とソフトウェアのアップデートとの間の関連を指し示すフラグに基づいて、キーを有効であるとして判定し（例えば、受け入れ）得る。例えば、フィールドサーバ215は、フラグに基づいてキーを有効であるものとして一時的に受け入れ得る。270において、フィールドサーバ215は、キーが有効であるとして判定することに基づいて、メモリ内のリスト内にキーを蓄積し得る。

【0040】

270において、フィールドサーバ215は、接続と関連付けられた証明書が有効であるか否かを判定し得る。幾つかの例では、フィールドサーバ215は、（例えば、接続リクエスト内に含まれる）キーと関連付けられた証明書と、デバイスと関連付けられた証明書との間の不一致を識別し得る。例えば、フィールドサーバ215は、キーと関連付けられた証明書を、（例えば、235において）フィールドサーバにより蓄積された証明書と比較し得る。不一致が識別された場合、フィールドサーバ215は、証明書を送信したデバイスを識別し得、ソフトウェアのアップデートに関連するフラグが設定されているか否かを識別し得る。フラグが設定されている場合、フィールドサーバ215は、接続リクエストを認証し得、接続リクエストの一部としてデバイス220から受信した証明書を、フィールドサーバ215により蓄積された新たな証明書として保存し得る。幾つかの実例では、フィールドサーバ215は、デバイス220に対する証明書としてソフトウェアコードのアップデートされたハッシュ値と共に、受信した証明書を蓄積することに基づいてフラグをクリアし得る。幾つかの例では、フィールドサーバ215は、キーが証明書に一致

10

20

30

40

50

することに基づいてデバイス220を認識及び認証し得る。幾つかの場合、デバイス220は、デバイス状態をフィールドサーバ215へ送信し得、それによって、キーと証明書とを比較する時間を短縮する。そうした場合、フィールドサーバ215は、デバイスを識別し得、デバイスの状態に基づいてフラグが設定されるか否かを識別し得る。他の例では、フィールドサーバ215は、フィールドサーバ215がデバイス220からキーを受信した場合に、フィールドサーバ215にアップロードされた各証明書をチェックする。

【0041】

275において、フィールドサーバ215は、キーが有効であるか否かを指し示すACKメッセージ又はNACKメッセージをデバイス220へ送信し得る。例えば、フィールドサーバ215は、キーが有効である場合にACKメッセージを送信し得、又はフィールドサーバ215は、キーが無効である場合にNACKメッセージを送信し得る。幾つかの場合、フィールドサーバ215は、エイリアスキーがフィールドサーバ215により蓄積された証明書と一致しないことを識別し得る。そうした場合、フィールドサーバ215は、デバイス220から証明書（例えば、エイリアスキーと一致するエイリアス証明書）をリクエストするメッセージを送信し得る。

【0042】

280において、フィールドサーバ215は、キーを有効であるとして判定すること（例えば、デバイス220から受信した証明書がキーを含むと判定すること）に基づいて、デバイス220とサービスとの間の接続を確立し得る。例えば、280において、フィールドサーバ215は、デバイス220とソフトウェアのアップデートとの間の関連を指し示すフラグに基づいて、不一致に関係なく接続リクエストを検証し得る。こうした場合、キーが有効であると判定することは、接続リクエストを検証することに基づく。他の例では、フィールドサーバ215は、キーと関連付けられた証明書を証明書と比較することに基づいて、アプリケーションプラットフォームへのアクセスのためにデバイス220を認証し得る。例えば、フィールドサーバ215は、サービスへのサブスクリプションを検証し得る。デバイス220を認証することは、デバイス220がアプリケーションプラットフォームと通信し、サービスにサブスクライブすることを可能にし得る。

【0043】

代替的に又は追加的に、フラグを使用して、管理サーバ205は、ソフトウェアのアップデートが完了したことの完了メッセージをデバイス220から受信することに基づいて、デバイス220と関連付けられたアップデートされた証明書を送信し得る。そうした場合、フィールドサーバ215は、デバイス220のソフトウェアがアップデートされた後、デバイス220と関連付けられたアップデートされた証明書を受信し得る。フィールドサーバ215は、フィールドサーバ215により蓄積されたデバイス220と関連付けられた証明書をアップデートし得る。代替的に又は追加的に、フラグを使用して、管理サーバ205は、ソフトウェアのアップデートをKMサーバ210へ送信し得る。KMサーバ210は、ソフトウェアのアップデートを受信し得、ソフトウェアのアップデート（例えば、ソフトウェアのアップデートされたハッシュ）に基づいてアップデートされた証明書を生成し得る。そうした場合、KMサーバ210は、アップデートされた証明書をフィールドサーバ215へ送信し得る。フィールドサーバ215は、アップデートされた証明書を受信することに基づいて、フィールドサーバ215により蓄積されたデバイス220と関連付けられた証明書をアップデートし得る。

【0044】

285において、デバイス220は、接続リクエストを送信し得る。こうした場合、フィールドサーバ215は、キーが有効であるとして判定することに基づいて、デバイス220からの接続リクエストを処理し得る。例えば、デバイス220は、接続が既に確立されている（例えば、キーが有効であると以前に認識されている）ため、フィールドサーバ215との接続の確立をバイパスし得る。

【0045】

他の例では、デバイス220を認証するための無効なキーと関連付けられた証明書を含

10

20

30

40

50

む接続リクエストをデバイス220が送信した場合に、デバイス220は、接続障害を経験し得る。290において、フィールドサーバ215は、接続リクエストを受信し得、自己署名される証明書に対する証明書リクエストを送信し得る。こうした場合、フィールドサーバ215は、接続リクエスト内の証明書が無効なキーを含むことに基づいて認証を検証するために、デバイス220が秘密キー（例えば、有効なキー）を用いて証明書に署名することをリクエストし得る。

【0046】

292において、デバイス220は、署名（例えば、署名された証明書）をフィールドサーバ215へ送信し得る。そうした場合、フィールドサーバ215は、証明書が秘密キーを用いて署名されていることに基づいて、デバイス220が秘密キーを含むと判定し得る。295において、フィールドサーバ215は、署名された証明書に起因してデバイスを識別し得る。例えば、フィールドサーバ215は、何れのデバイス220がフィールドサーバ215と接続しようと試み得るかを識別し得る。

【0047】

292において、フィールドサーバ215は、デバイス220がエラーを含むことを識別し得る。そうした場合、デバイス220は、エラーを指し示すステータスのアップデートをフィールドサーバ215がデバイス220から受信することよりも暗号的に強い（例えば、確実性が増す）ことがあり得るアラームをトリガーし得る。フィールドサーバ215は、デバイス220がアラームと関連付けられていることを検証し得、それによって、デバイス220の識別、デバイス220の位置、又はその両方を判定するためのフォレンジック分析に対する検証を使用する。

【0048】

図3は、本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするプロセスフロー300の一例を説明する。プロセスフロー300は、管理サーバ305、KMサーバ310、フィールドサーバ315、及びデバイス310を含み得、これらは、図1及び図2を参照して本明細書に説明した対応するデバイスの例であり得る。プロセスフロー300は、追記書き込みモードで動作することを説明し得る。

【0049】

325において、KMサーバ310は、ルートキーを管理サーバ205へ送信し得る。幾つかの場合、KMサーバ310は、KMサーバ310にアップロードされた各ソフトウェアハッシュに対して証明書を生成し得る。例えば、登録ポータルは、ソフトウェアの第1のバージョンに対するソフトウェアハッシュと、ソフトウェアの第2のバージョンに対するソフトウェアハッシュとをKMサーバ310にアップロードし得る。そうした場合、KMサーバ310は、あらゆるソフトウェアハッシュに対して、及びあらゆるデバイス320に対して証明書を生成し得る。330において、KMサーバ310は、第1の証明書を生成し得、第1の証明書をフィールドサーバ315にアップロードし得る。335において、KMサーバ310は、第2の証明書を生成し得、第2の証明書をフィールドサーバ315にアップロードし得る。

【0050】

340において、管理サーバ305は、デバイス320の一部分を追記書き込みモードで動作するように構成し得る。追記書き込みモードは、デバイス320内のメモリセルの1つ以上の部分に適用され得、非特権ユーザがデバイス320の1つ以上の部分内のコンテンツを消去することを防止し得る。

【0051】

345において、デバイス320は、ソフトウェアの第1のバージョンをインストールし得、それによって、デバイス320の一部分を追記書き込みモードで動作するように構成する。350において、フィールドサーバ315は、デバイス320を認証するための第1のキーと関連付けられた証明書を含む接続リクエストをデバイス320から受信し得る。355において、フィールドサーバ315は、第1のキーを第1の証明書と照合し得

10

20

30

40

50

る。例えば、フィールドサーバ315は、KMサーバ310から受信した第1の証明書に基づいて、デバイス320から受信した第1のキーの有効性を判定し得る。360において、フィールドサーバ315は、第1のキーが有効であることを指し示すACKメッセージをデバイス320へ送信し得る。

【0052】

幾つかの場合、管理サーバ305は、デバイス320の証明書を無効にするために、追記書き込みモードを使用し得る。例えば、管理サーバ305は、ソフトウェアに追加情報を追記し得る。こうしたアクションは、デバイス320により生成され接続リクエストの一部として通信される証明書が、フィールドサーバ315により蓄積された証明書と一致させないことがある。フィールドサーバ315内にフラグが設定されていない場合、フィールドサーバ315は、証明書間の不一致に基づいてデバイス320を認証することを失敗し得る。幾つかの場合、管理サーバ305は、追加情報を追記することに基づいて、デバイス320から受信したキーをアップデートし得る。そうした場合、フィールドサーバ315上のサービスへのアクセスは、キーをアップデートすることに基づいて削除され（例えば、ブロックされ）得る。

【0053】

365において、フィールドサーバ315は、第1のキーが第1の証明書と一致することに基づいて、デバイス320とフィールドサーバ315との間に接続（例えば、少なくとも第1の接続）を確立し得る。例えば、デバイス320のユーザは、1つ以上のサービス（例えば、音楽リスニングサービス、マッピングサービス、又は旅行サポートサービス等）にサブスクライブし得る。フィールドサーバ315は、1つ以上のサービスへの接続を確立し得る。

【0054】

他の例では、管理サーバ305は、サブスクリプションサービスが期限切れになることに基づいて、デバイス320の追記書き込みモード部分内に情報を書き込み得る。例えば、これらのサービスの内の幾つかは、ユーザが料金を支払うことに基づいて一時的に提供され得る。（料金の未払いを含む何らかの理由で）サブスクリプションが期限切れになった場合、ソフトウェアは、デバイス320内のセキュアなフラッシュに書き込み得る。そうした場合、デバイス320上のイメージは変更され得、それによって、証明書を生成するためのハッシュを生成するために使用された基礎となるコードを変更する。

【0055】

この方法でサービスへのサブスクリプションを無効にすることは、デバイス320がサービスに接続することを防止し得る。幾つかの場合、ソフトウェアのイメージは、外部コンピュータによってデバイス320上で修正され得る。例えば、デバイス320への直接アクセスを備えたプログラミングツールは、ソフトウェアイメージを修正し得、ソフトウェアのアップデートを送信するリモートサーバは、イメージを修正し得、又はそれら両方であり得る。

【0056】

370において、デバイス320は、追記書き込みモードを修正し得る。例えば、デバイス320は、ソフトウェアの第1のバージョンをソフトウェアの第2のバージョンに修正（例えば、アップデート）し得る。375において、フィールドサーバ315は、デバイス320を認証するための第2のキーと関連付けられた証明書を含む接続リクエストをデバイス320から受信し得る。380において、フィールドサーバ315は、第2のキーを第2の証明書と照合し得る。例えば、フィールドサーバ315は、KMサーバ310から受信した第2の証明書に基づいて、デバイス320から受信した第2のキーの有効性を判定し得る。385において、フィールドサーバ315は、第2のキーが有効であることを指し示すACKメッセージをデバイス310へ送信し得る。

【0057】

390において、フィールドサーバ315は、第2のキーが第2の証明書と一致することに基づいて、デバイス320とフィールドサーバ315との間に接続（例えば、少なく

10

20

30

40

50

とも第2の接続)を確立し得る。例えば、フィールドサーバ315は、1つ以上のサービス(例えば、音楽リスニングサービス、マッピングサービス、又は旅行サポートサービス等)への接続を確立し得る。

【0058】

デバイス320とフィールドサーバ315との間の接続を確立又は再確立するために、ソフトウェアハッシュはアップデートされ得、サービスにアクセスするために新たな証明書がリクエストされ得る。サービスは、サービスにアクセスするための支払い計画に対応する期間中にデバイス320と相互作用し得る。該期間は、サービスの購入において開始し得、サービスの有効期限まで延長し得る。有効期限後、フィールドサーバ315は、サービスへのアクセスを防止するためにコンテンツを変更し(例えば、ソフトウェアのイメージを修正し)得る。こうした場合、コンテンツを変更することが、サービスと関連付けられた各プロファイルが無効にし得るように、キーは、サービスと関連付けられたプロファイルに対応する。

【0059】

図4は、本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートするフィールドサーバ405のブロック図400を示す。フィールドサーバ405は、図1～図3を参照して説明したようなフィールドサーバの態様の一例であり得る。フィールドサーバ405は、接続コンポーネント410、ソフトウェアアップデートコンポーネント415、フラグマネージャ420、キー無効性マネージャ425、キー有効性マネージャ430、リクエストレシーバ435、及び証明書コンポーネント440を含み得る。これらのモジュールの各々は、(例えば、1つ以上のバスを介して)相互に直接的又は間接的に通信し得る。

【0060】

接続コンポーネント410は、第1のキーを有効であるとして判定することに基づいて、デバイスとサービスとの間の接続を確立し得る。幾つかの例では、接続コンポーネント410は、フラグに基づいて不一致に関係なく接続リクエストを検証し得、第1のキーが有効であると判定することは、接続リクエストを検証することに基づく。幾つかの例では、接続コンポーネント410は、第1のキーと関連付けられた証明書と証明書とを比較することに基づいて、アプリケーションプラットフォームへのアクセスのためにデバイスを認証し得る。

【0061】

幾つかの例では、接続コンポーネント410は、デバイスを認証することに基づいてサービスへのサブスクリプションを検証し得る。幾つかの例では、接続コンポーネント410は、接続リクエストを受信することに基づいて第1のキーが有効であるか否かを指し示すACKメッセージ又はNACKメッセージをデバイスへ送信し得る。幾つかの場合、認証することは、デバイスがアプリケーションプラットフォームと通信し、サービスにサブスクライブすることを可能にする。

【0062】

ソフトウェアアップデートコンポーネント415は、ソフトウェアのアップデートがデバイスへ送信されたことの通知をフィールドサーバによって受信し得、フィールドサーバは、デバイスのソフトウェアが安全であることを認証するためのものである。

【0063】

フラグマネージャ420は、通知を受信することに基づいて、デバイスとメモリ内のソフトウェアのアップデートとの間の関連を指し示すフラグをフィールドサーバによって設定し得る。

【0064】

キー無効性マネージャ425は、接続リクエストを受信することに基づいて、デバイスから受信した第1のキーが無効であると判定し得る。幾つかの例では、キー無効性マネージャ425は、接続リクエストを受信することに基づいて、第1のキーと関連付けられた証明書とデバイスと関連付けられた証明書との間の不一致を識別し得る。幾つかの例では

10

20

30

40

50

、キー無効性マネージャ 425 は、第 1 のキーと関連付けられた証明書を、フィールドサーバにより蓄積された証明書と比較し得る。

【0065】

キー有効性マネージャ 430 は、関連を指し示すフラグに基づいて、第 1 のキーを有効であるとして判定し得る。幾つかの例では、キー有効性マネージャ 430 は、フラグに基づいて第 1 のキーを有効であるとして判定することに基づいて、メモリ内のリスト内に第 1 のキーを蓄積し得る。幾つかの場合、デバイスから受信した第 1 のキーと関連付けられた証明書は、デバイスのソフトウェアのハッシュに基づく。

【0066】

リクエストレシーバ 435 は、デバイスを認証するための第 1 のキーと関連付けられた証明書を含む接続リクエストをデバイスから受信し得る。幾つかの例では、リクエストレシーバ 435 は、第 1 のキーが有効であるとして判定することに基づいて、デバイスからの追加の接続リクエストを処理し得る。

【0067】

証明書コンポーネント 440 は、デバイスのソフトウェアがアップデートされた後、デバイスと関連付けられたアップデートされた証明書を受信し得る。幾つかの例では、証明書コンポーネント 440 は、アップデートされた証明書を受信することに基づいて、フィールドサーバにより蓄積されたデバイスと関連付けられた証明書をアップデートし得る。

【0068】

図 5 は、本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートする 1 つ以上の方法 500 を説明するフローチャートを示す。方法 500 の動作は、本明細書で説明するように、フィールドサーバ又はそのコンポーネントによって実装され得る。例えば、方法 500 の動作は、図 3 を参照して説明したようなフィールドサーバによって実施され得る。幾つかの例では、フィールドサーバは、説明する機能を実施するためにフィールドサーバの機能的素子を制御するための命令のセットを実行し得る。追加的又は代替的に、フィールドサーバは、特別な目的のハードウェアを使用して、説明する機能の態様を実施し得る。

【0069】

505 において、フィールドサーバは、ソフトウェアのアップデートがデバイスへ送信されたことの通知を受信することであって、フィールドサーバは、デバイスのソフトウェアが安全であることを認証するためのものであり得る。505 の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、505 の動作の態様は、図 3 を参照して説明したようなソフトウェアアップデートコンポーネントによって実施され得る。

【0070】

510 において、フィールドサーバは、通知を受信することに基づいて、デバイスとメモリ内のソフトウェアのアップデートとの間の関連を指し示すフラグを設定し得る。510 の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、510 の動作の態様は、図 3 を参照して説明したようなフラグマネージャによって実施され得る。

【0071】

515 において、フィールドサーバは、デバイスを認証するための第 1 のキーと関連付けられた証明書を含む接続リクエストをデバイスから受信し得る。515 の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、515 の動作の態様は、図 3 を参照して説明したようなリクエストレシーバによって実施され得る。

【0072】

520 において、フィールドサーバは、接続リクエストを受信することに基づいて、デバイスから受信した第 1 のキーが無効であると判定し得る。520 の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、520 の動作の態様は、図 3 を参照して説明したようなキー無効性マネージャによって実施され得る。

【0073】

525 において、フィールドサーバは、関連を指し示すフラグに基づいて、第 1 のキー

10

20

30

40

50

を有効であると判定し得る。525の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、525の動作の態様は、図3を参照して説明したようなキー有効性マネージャによって実施され得る。

【0074】

530において、フィールドサーバは、第1のキーを有効であると判定することに基づいて、デバイスとサービスとの間の接続を確立し得る。530の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、530の動作の態様は、図3を参照して説明したような接続コンポーネントによって実施され得る。

【0075】

幾つかの例では、本明細書に説明するような装置は、方法500等の1つ以上の方法を実施し得る。装置は、ソフトウェアのアップデートがデバイスへ送信されたことの通知をフィールドサーバによって受信することであって、フィールドサーバは、デバイスのソフトウェアが安全であることを認証するためのものであることと、通知を受信することに基づいて、デバイスとメモリ内のソフトウェアのアップデートとの間の関連を指し示すフラグをフィールドサーバによって設定することと、デバイスを認証するための第1のキーと関連付けられた証明書を含む接続リクエストをデバイスから受信することと、接続リクエストを受信することに基づいて、デバイスから受信した第1のキーが無効であると判定することと、関連を指し示すフラグに基づいて、第1のキーを有効であると判定することと、第1のキーを有効であると判定することに基づいて、デバイスとサービスとの間の接続を確立することのための機構、手段、又は命令（例えば、プロセッサにより実行可能な命令を蓄積する非一時的コンピュータ可読媒体）を含み得る。

【0076】

本明細書に説明する方法500及び装置の幾つかの例は、フラグに基づいて第1のキーを有効であると判定することに基づいて、メモリ内のリスト内に第1のキーを蓄積するための動作、機構、手段、又は命令を更に含み得る。本明細書に説明する方法500及び装置の幾つかの例は、デバイスのソフトウェアがアップデートされ得る後にデバイスと関連付けられたアップデートされた証明書を受信することと、アップデートされた証明書を受信することに基づいてフィールドサーバにより蓄積されたデバイスと関連付けられた証明書をアップデートすることのための動作、機構、手段、又は命令を更に含み得る。

【0077】

本明細書に説明する方法500及び装置の幾つかの例は、第1のキーを有効であると判定することに基づいて、デバイスからの追加の接続リクエストを処理することのための動作、機構、手段、又は命令を更に含み得る。本明細書に説明する方法500及び装置の幾つかの例は、接続リクエストを受信することに基づいて、第1のキーと関連付けられた証明書とデバイスと関連付けられた証明書との間の不一致を識別することと、フラグに基づいて不一致に関わらず接続リクエストを検証することであって、第1のキーを判定することは、接続リクエストを検証することに基づき得ることのための動作、機構、手段、又は命令を更に含み得る。

【0078】

本明細書に説明する方法500及び装置の幾つかの例は、第1のキーと関連付けられた証明書をフィールドサーバにより蓄積された証明書と比較することと、第1のキーと関連付けられた証明書を証明書と比較することに基づいて、アプリケーションプラットフォームへのアクセスのためにデバイスを認証することのための動作、機構、手段、又は命令を更に含み得る。

【0079】

本明細書に説明する方法500及び装置の幾つかの例は、デバイスを認証することに基づいてサービスへのサブスクリプションを検証するための動作、機能、手段、又は命令を更に含み得る。本明細書に説明する方法500及び装置の幾つかの例では、認証することは、デバイスがアプリケーションプラットフォームと通信し、サービスにサブスクライブすることを可能にし得る。

【0080】

本明細書に説明する方法500及び装置の幾つかの例では、デバイスから受信した第1のキーと関連付けられた証明書は、デバイスのソフトウェアのハッシュに基づき得る。本明細書に説明する方法500及び装置の幾つかの例は、接続リクエストを受信することに基づいて第1のキーが有効であるか否かを指し示すACKメッセージ又はNACKメッセージをデバイスへ送信することのための動作、機構、手段、又は命令を更に含み得る。

【0081】

図6は、本明細書に開示するような例に従ったリモートホストを使用してデバイスを認証することをサポートする1つ以上の方法600を説明するフローチャートを示す。方法600の動作は、本明細書に説明するように、(第1のサーバと称され得る)管理サーバ又はそのコンポーネントによって実装され得る。例えば、方法600の動作は、図2～図3を参照して説明したような管理サーバによって実施され得る。幾つかの例では、管理サーバは、説明する機能を実行するために管理サーバの機能的素子を制御するための命令のセットを実行し得る。追加的又は代替的に、管理サーバは、特別な目的のハードウェアを使用して、説明する機能の態様を実施し得る。

【0082】

605において、管理サーバは、デバイスに対するソフトウェアのアップデートを識別し得る。605の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、605の動作の態様は、図4を参照して説明したようなソフトウェアアップデート識別子によって実施され得る。

【0083】

610において、管理サーバは、ソフトウェアのアップデートを識別することに基づいてソフトウェアのアップデートがデバイスへ送信されたことの通知を、デバイスのソフトウェアが安全であることを認証するための第2のサーバへ送信し得る。610の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、610の動作の態様は、図4を参照して説明したような通知トランシーバによって実施され得る。

【0084】

615において、管理サーバは、デバイスに対するソフトウェアのアップデートを識別することに基づいて、ソフトウェアのアップデートをデバイスへ送信し得る。615の動作は、本明細書に説明する方法に従って実施され得る。幾つかの例では、615の動作の態様は、図4を参照して説明したようなソフトウェアアップデートトランシーバによって実施され得る。

【0085】

幾つかの例では、本明細書に説明するような装置は、方法600等の1つ以上の方法を実施し得る。装置は、デバイスに対するソフトウェアのアップデートを第1のサーバによって識別することと、ソフトウェアのアップデートを識別することに基づいてソフトウェアのアップデートがデバイスへ送信されることの通知を、デバイスのソフトウェアが安全であることを認証するための第2のサーバへ送信することと、デバイスに対するソフトウェアのアップデートを識別することに基づいて、ソフトウェアのアップデートをデバイスへ送信することのための機構、手段、又は命令(例えば、プロセッサにより実行可能な命令を蓄積する非一時的コンピュータ可読媒体)を含み得る。

【0086】

本明細書に説明する方法600及び装置の幾つかの例は、デバイスがソフトウェアのアップデートを実施したことを指し示す完了メッセージをデバイスから受信することと、完了メッセージを受信することに基づいてデバイスと関連付けられたアップデートされた証明書を送信することのための動作、機構、手段、又は命令を更に含み得る。本明細書に説明する方法600及び装置の幾つかの例では、通知は、デバイスから受信したキーと関連付けられた証明書がソフトウェアのアップデートに基づいて変更され得ることを識別するためのものであり得る。

【0087】

本明細書に説明する方法 600 及び装置の幾つかの例は、ソフトウェアのアップデートを送信することに基づいて、デバイスの一部分を追記書き込みモードで動作するように構成することのための動作、機構、手段、又は命令を更に含み得る。本明細書に説明する方法 600 及び装置の幾つかの例は、デバイスの一部分を追記書き込みモードで動作するように構成することに基づいてソフトウェアに追加情報を追記することと、追加情報を追記することに基づいてソフトウェアのアップデート前に利用可能なソフトウェアのバージョンへのアクセスを防止することと、追加情報を追記することに基づいてデバイスから受信したキーをアップデートすることのための動作、機構、手段、又は命令を更に含み得る。

【0088】

本明細書に説明する方法は可能な実装であること、動作及びステップは再配され得、さもなければ修正され得ること、及びその他の実装が可能であることに留意すべきである。更に、方法の内の 2 つ以上からの部分は組み合わせられ得る。

【0089】

本明細書に説明する情報及び信号は、様々な異なる技法及び技術の内の何れかを使用して表され得る。例えば、上の説明全体通じて言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、及びチップは、電圧、電流、電磁波、磁界若しくは磁性粒子、光場若しくは光粒子、又はそれらの任意の組み合わせにより表され得る。幾つかの図面は、(複数の) 信号を単一の信号として説明し得るが、バスが様々なビット幅を有し得る場合に、信号が信号のバスを表し得ることは、当業者により理解されるであろう。

【0090】

用語“電子通信する”、“導電的に接触する”、“接続される”、及び“結合される”は、コンポーネント間の信号の流れをサポートするコンポーネント間の関係を指し得る。コンポーネント間の信号の流れを何時でもサポートし得る何らかの導電経路がコンポーネント間にある場合、コンポーネントは、相互に電子通信する(又は導電的に接触する、又は接続される、又は結合される)とみなされる。任意の所与の時間において、相互に電子通信する(又は導電的に接触する、又は接続される、又は結合される)コンポーネント間の導電経路は、接続されるコンポーネントを含むデバイスの動作に基づいて開回路又は閉回路であり得る。接続されるコンポーネント間の導電経路は、コンポーネント間の直接の導電経路であり得、又は接続されるコンポーネント間の導電経路は、スイッチ、トランジスタ、若しくはその他のコンポーネント等の介在コンポーネントを含み得る間接的な導電経路であり得る。幾つかの場合、接続されるコンポーネント間の信号の流れは、例えば、スイッチ又はトランジスタ等の 1 つ以上の介在コンポーネントを使用して一時的に中断され得る。

【0091】

メモリアレイを含む本明細書で論じるデバイスは、シリコン、ゲルマニウム、シリコン-ゲルマニウム合金、ヒ化ガリウム、窒化ガリウム等の半導体基板上に形成され得る。幾つかの例では、該基板は半導体ウエハである。その他の場合、該基板は、シリコンオンガラス(SOG)若しくはシリコンオンサファイア(SOP)等のシリコンオンインシュレータ(SOI)基板、又は別の基板上の半導体材料のエピタキシャル層であり得る。基板又は基板のサブ領域の導電性は、リン、ホウ素、又はヒ素を含むがそれらに限定されない様々な化学種を使用したドーピングを通じて制御され得る。ドーピングは、イオン注入により、又は任意のその他のドーピング手段により、基板の初期の形成又は成長の間に実施され得る。

【0092】

添付の図面に関連して本明細書に記載される説明は、例示的構成を説明し、実装され得る又は請求項の範囲内にある全ての例を表さない。本明細書で使用する用語“例示的”は、“好適”又は“その他の例よりも有利”ではなく“一例、実例、又は説明として役立つこと”を意味する。詳細な説明は、説明する技術の理解を提供するための具体的詳細を含む。これらの技術は、しかしながら、これらの具体的詳細なしに実践され得る。幾つかの実例では、説明する例の概念を不明確にすることを避けるために、周知の構造体及びデバイスはブロック図の形式で示されている。

10

20

30

40

50

【0093】

添付の図では、同様のコンポーネント又は機構は、同じ参照ラベルを有し得る。更に、同じタイプの様々なコンポーネントは、参照ラベルに続いてダッシュと、同様のコンポーネントの間で区別する第2のラベルとを付すことにより区別され得る。明細書において第1の参照ラベルのみが使用される場合、説明は、第2の参照ラベルに関係なく、同じ第1の参照ラベルを有する同様のコンポーネントの内の何れか1つに適用可能である。

【0094】

本明細書に説明する情報及び信号は、様々な異なる技法及び技術の内の何れかを使用して表され得る。例えば、上述の説明全体通じて言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、及びチップは、電圧、電流、電磁波、磁界若しくは磁性粒子、光場若しくは光粒子、又はそれらの任意の組み合わせにより表され得る。

【0095】

本明細書の開示と関連して説明する様々な説明ブロック及びコンポーネントは、本明細書に説明する機能を実施するように設計された汎用プロセッサ、digital signal processor (DSP)、application-specific integrated circuit (ASIC)、field programmable gate array (FPGA)若しくはその他のプログラマブルロジックデバイス、ディスクリートゲート若しくはトランジスタロジック、ディスクリートハードウェアコンポーネント、又はそれらの任意の組み合わせを用いて実装又は実施され得る。汎用プロセッサは、マイクロプロセッサであり得るが、代わりに、プロセッサは、任意のプロセッサ、コントローラ、マイクロコントローラ、又はステートマシンであり得る。プロセッサはまた、コンピューティングデバイスの組み合わせ（例えば、DSPとマイクロプロセッサとの組み合わせ、複数のマイクロプロセッサ、DSPコアと連携した1つ以上のマイクロプロセッサ、又は任意のその他のこうした構成）として実装され得る。

【0096】

本明細書に説明する機能は、ハードウェア、プロセッサにより実行されるソフトウェア、ファームウェア、又はそれらの任意の組み合わせで実装され得る。プロセッサにより実行されるソフトウェアで実装される場合、機能は、コンピュータ可読媒体上の1つ以上の命令又はコードとして蓄積され得、又は送信され得る。その他の例及び実装は、開示及び添付の請求項の範囲内にある。例えば、ソフトウェアの性質に起因して、本明細書で説明した機能は、プロセッサにより実行されるソフトウェア、ハードウェア、ファームウェア、配線、又はこれらの任意の組み合わせを使用して実装され得る。機能を実装する機構はまた、機能の（複数の）部分が異なる物理的場所において実装されるように分散されることを含め、様々な位置に物理的に設置され得る。また、請求項を含む本明細書で使用する時、項目のリスト（例えば、“少なくとも1つの”又は“の内の1つ以上”等の句により前置きされる項目のリスト）に使用されるような“又は”は、例えば、A、B、又はCの内の少なくとも1つのリストがA又はB又はC又はA B又はA C又はB C又はA B C（すなわち、A及びB及びC）を意味するように包含的リストを指し示す。また、本明細書で使用する時、句“に基づいて”は、条件の閉集合への言及として解釈されないであろう。例えば、“条件Aに基づいて”として説明する例示的ステップは、本開示の範囲から逸脱することなく、条件A及び条件Bの両方に基づき得る。言い換えれば、本明細書で使用する時、句“に基づいて”は、句“少なくとも部分的に基づいて”と同じ方法で解釈されるであろう。

【0097】

コンピュータ可読媒体は、非一時的コンピュータストレージ媒体と、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む通信媒体との両方を含む。非一時的ストレージ媒体は、汎用又は専用のコンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。例として、非限定的に、非一時的コンピュータ可読媒体は、RAM、ROM、電氣的消去可能プログラマブルリードオンリーメモリ（EEPROM）、コンパクトディスク（CD）ROM若しくはその他の光ディスクストレージ、磁気ディスクストレージ若しくはその他の磁気ストレージデバイス、又は命令若しくは

データ構造の形式で所望のプログラミングコード手段を搬送又は蓄積するために使用され得、汎用若しくは専用コンピュータ、若しくは汎用若しくは専用プロセッサによりアクセス可能であり得る任意のその他の非一時的媒体を含み得る。また、任意の接続はコンピュータ可読媒体と適切に呼ばれる。例えば、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線（DSL）、又は赤外線、無線、及びマイクロ波等の無線技術を使用して、ソフトウェアがウェブサイト、サーバ、又はその他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線（DSL）、又は赤外線、無線、及びマイクロ波等の無線技術は媒体の定義に含まれる。ディスク（disk）及びディスク（disc）は、本明細書で使用する時、CD、レーザーディスク（登録商標）、光ディスク、デジタル多用途ディスク（DVD）、フロッピーディスク、及びブルーレイディスクを含み、ディスク（disk）は通常、データを磁氣的に再生する一方、ディスク（disc）はレーザーを用いて光学的にデータを再生する。上記の組み合わせも、コンピュータ可読媒体の範囲に含まれる。

【0098】

本明細書の説明は、当業者が開示を製作又は使用可能なように提供されている。開示への様々な修正は当業者に分かるであろうし、本明細書で定義される包括的な原理は開示の範囲を逸脱することなくその他の変形に適用され得る。したがって、開示は、本明細書に説明した例及び設計に限定されず、本明細書に開示した原理及び新規の機構と一致する最も広い範囲に一致する。

10

20

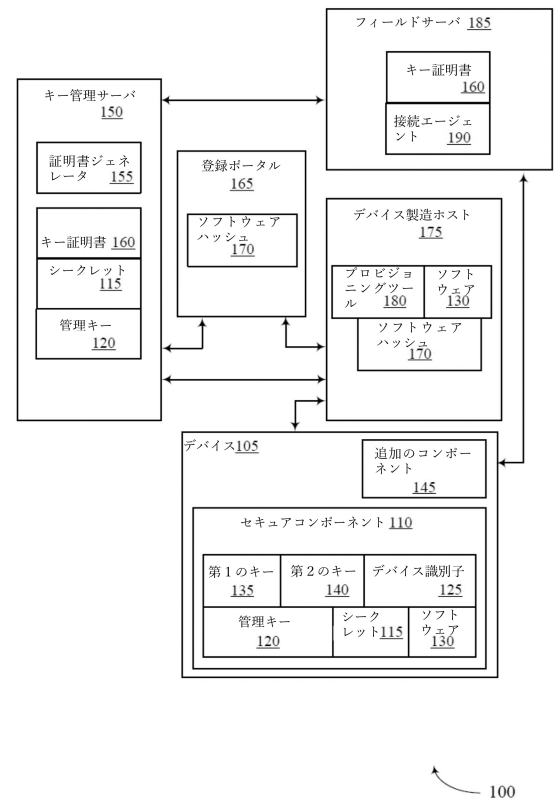
30

40

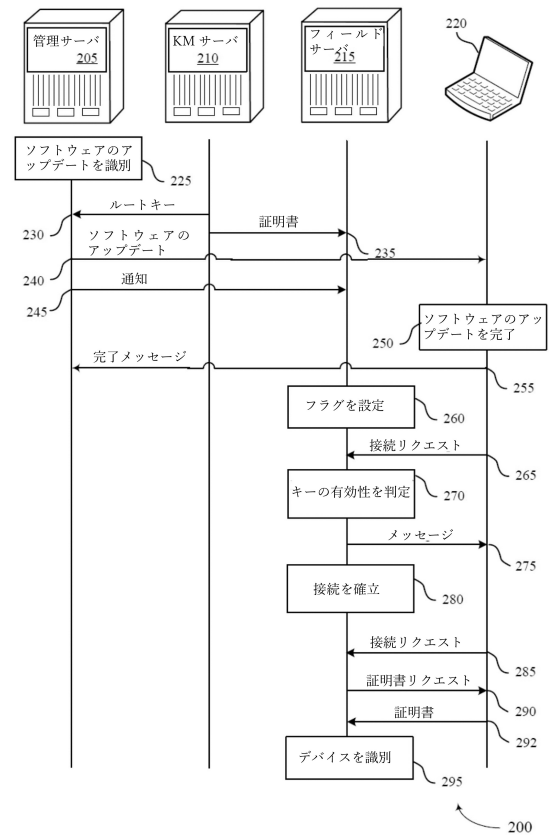
50

【図面】

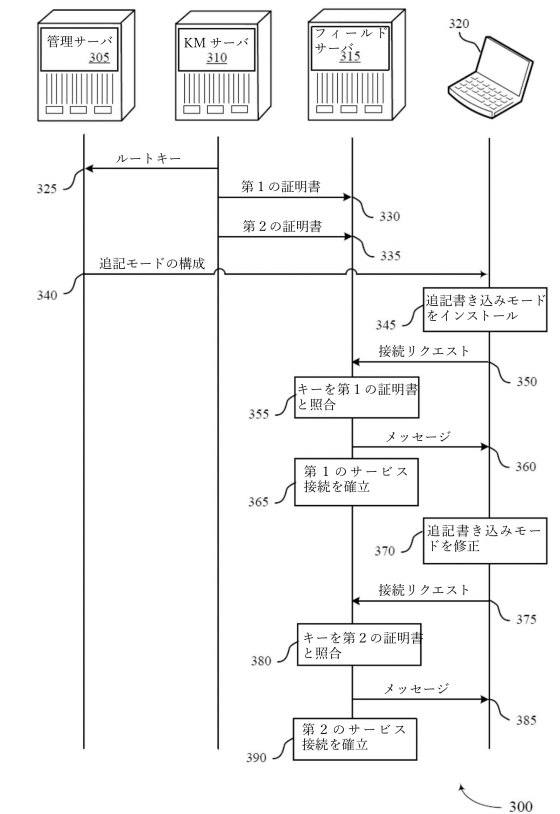
【図 1】



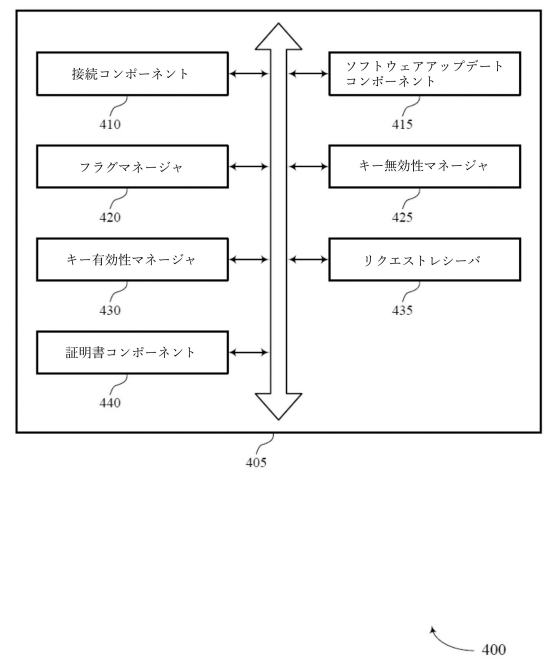
【図 2】



【図 3】



【図 4】



10

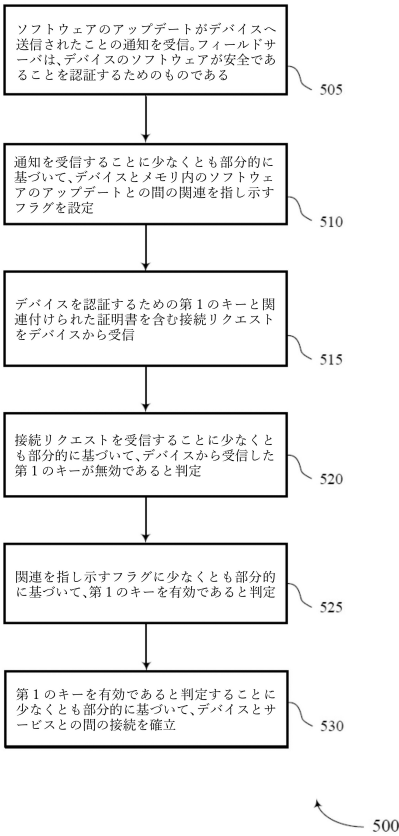
20

30

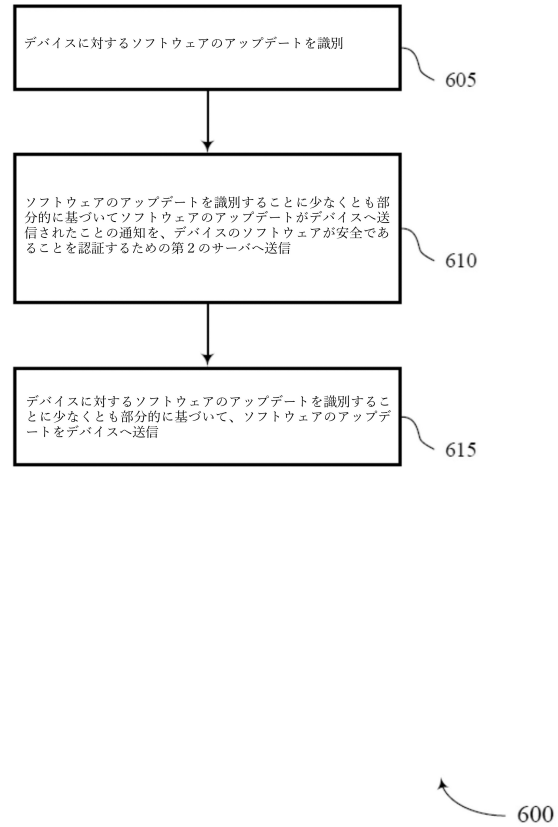
40

50

【図 5】



【図 6】



10

20

30

40

50

フロントページの続き

ジー、インク．内

審査官 岸野 徹

- (56)参考文献 特開 2019-168977 (JP, A)
特開 2011-197969 (JP, A)
特開 2017-017616 (JP, A)
特開 2016-051198 (JP, A)
米国特許出願公開第 2014/0007076 (US, A1)
米国特許出願公開第 2018/0183605 (US, A1)
- (58)調査した分野 (Int.Cl., DB名)
G06F 21/44
G06F 21/62
G06F 21/57