(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2020-511069
(P2020-511069A)
(43)公表日　令和2年4月9日(2020.4.9)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	
H04L	9/08	(2006.01)	H04L	9/00	601C	
G09C	1/00	(2006.01)	H04L	9/00	601E	
			G09C	1/00	640E	

審査請求 有　予備審査請求 未請求　（全 68 頁）

(21)出願番号　特願2019-547391 (P2019-547391)
(86)(22)出願日　平成30年3月1日(2018.3.1)
(85)翻訳文提出日　令和1年8月30日(2019.8.30)
(86)国際出願番号　PCT/US2018/020494
(87)国際公開番号　WO2018/160863
(87)国際公開日　平成30年9月7日(2018.9.7)
(31)優先権主張番号　62/465,806
(32)優先日　平成29年3月1日(2017.3.1)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/471,926
(32)優先日　平成29年3月15日(2017.3.15)
(33)優先権主張国・地域又は機関
米国(US)

(71)出願人　503260918
アップル　インコーポレイテッド
Ａｐｐｌｅ　Ｉｎｃ．
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
Ｏｎｅ　Ａｐｐｌｅ　Ｐａｒｋ　Ｗａｙ，Ｃｕｐｅｒｔｉｎｏ，　Ｃａｌｉｆｏｒｎｉａ　９５０１４，　Ｕ．Ｓ．Ａ．
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100112508
弁理士　高柳　司郎

最終頁に続く

(54)【発明の名称】モバイルデバイスを使用したシステムアクセス

(57)【要約】
例えば、システム機能へのアクセス（例えば、システムへの物理アクセス、エンジン／モータの始動など）を可能にするようにモバイル電子デバイスを認証するための電子セキュリティに関する技術が開示される。いくつかの実施形態では、システム及びモバイルデバイスは、ペアリングプロセス中に公開鍵ペアの公開鍵を交換する。いくつかの実施形態では、非対称トランザクションプロセスは、セキュア鍵交換（例えば、楕円曲線ディフィー・ヘルマン）を使用して確立された鍵を介して鍵導出関数を使用して共有シークレットを生成することと、システムの署名を検証してから、モバイルデバイスを識別する任意の情報を送信することと、を含む。様々な実施形態では、開示された技術により、トランザクションセキュリティ及び識別情報のプライバシーを増大させることができる。

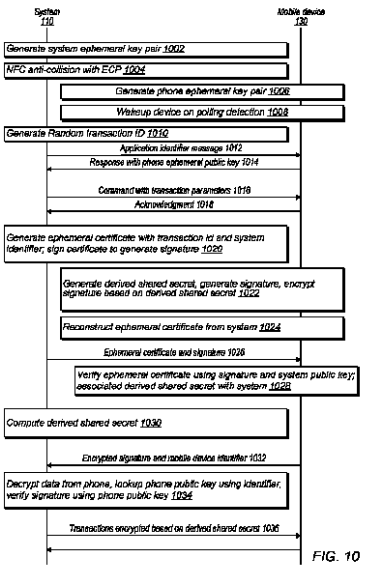


FIG. 10

【特許請求の範囲】
【請求項１】
装置であって、
第１の公開鍵及び第１の非公開鍵を含む第１の短期鍵ペアを生成し、
システムによって生成された第２の公開鍵であって、第２の短期鍵ペアに含まれる、前記第２の公開鍵を判定し、
前記第１の非公開鍵及び前記第２の公開鍵を入力として使用する鍵交換関数を使用して第１の共有シークレットを生成し、
少なくとも、前記第１の共有シークレットと、前記第１の公開鍵と、前記装置と前記システムとの間のペアリングセッション中に以前に確立された前記システムの公開鍵と、を入力に使用する鍵導出関数を使用して導出された共有シークレットを生成し、
前記ペアリングセッション中に確立された前記装置の非公開鍵でトランザクション情報に署名することによって署名を生成し、
前記導出された共有シークレットに基づいて、前記署名と、前記装置を識別する情報とを暗号化し、
前記システムの前記公開鍵を使用して前記システムから受信された署名付き証明書であって、前記ペアリングセッション中に確立された前記システムの対応する非公開鍵で署名される、前記証明書を検証し、
前記署名付き証明書の検証に応じて、前記暗号化された署名及び情報を前記システムに送信する、
ように構成される１つ以上の処理要素を備える装置。
【請求項２】
請求項１に記載の装置であって、前記署名付き証明書の検証後まで、前記装置を識別する情報を前記システムに送信しないように構成される装置。
【請求項３】
請求項１に記載の装置であって、前記鍵交換関数は楕円曲線ディフィー・ヘルマン（ＤＨ）関数である装置。
【請求項４】
請求項１に記載の装置であって、前記システムの１つ以上の機能へのアクセスを他のデバイスと共有するために、
前記他のデバイスから証明書署名要求を受信し、
前記受信された証明書を、前記他のデバイスと関連付けられた許可されたエンティティのルート証明書を使用して検証し、
前記装置のユーザを認証し、
前記システムとの前記ペアリングセッション中に確立された前記装置の前記非公開鍵を使用して前記証明書に署名し、
前記署名付き証明書を前記他のデバイスに送信する、
ように構成される装置。
【請求項５】
請求項４に記載の装置であって、前記証明書署名要求及び前記署名付き証明書は、広域ネットワークを使用することなく直接無線接続を介して送信される装置。
【請求項６】
請求項４に記載の装置であって、前記システムのセキュリティトークンを暗号化し、前記暗号化されたセキュリティトークンを前記他のデバイスに送信するように構成される装置。
【請求項７】
請求項４に記載の装置であって、前記他のデバイスからの公開鍵を使用して前記セキュリティトークンを暗号化し、前記公開鍵と関連付けられたメールボックスの場所に前記セキュリティトークンを記憶するように構成される装置。
【請求項８】

請求項４に記載の装置であって、ユーザによる前記共有アクセスの取り消しに応じて、取り消しメッセージを送信し、
前記他のデバイスのセキュア回路からの取り消し受信通知に基づいて、前記共有アクセスの取り消しを確認する、ように構成される装置。
【請求項９】
請求項１に記載の装置であって、ペアリングプロセス中に、デジタル鍵データ構造についての構成情報を埋め込む証明書を生成し、前記装置のセキュア回路の非公開鍵を使用して前記証明書に署名して、前記構成情報にしたがって前記デジタル鍵データ構造の作成を証明する、ように構成される装置。
【請求項１０】
装置であって、
モバイルデバイスとのペアリングセッション中に確立された前記装置の非公開鍵でトランザクション情報に署名することによって署名を生成し、
前記署名を前記モバイルデバイスに送信し、
前記送信された署名の応答で、前記モバイルデバイスから暗号化された署名を受信し、
第１の公開鍵及び第１の非公開鍵を含む第１の短期鍵ペアを生成し、
前記モバイルデバイスによって生成された第２の公開鍵であって、第２の短期鍵ペアに含まれる、前記第２の公開鍵を判定し、
前記第１の非公開鍵及び前記第２の公開鍵を入力として使用する鍵交換関数を使用して第１の共有シークレットを生成し、
少なくとも、前記第１の共有シークレットと、前記第１の公開鍵と、前記ペアリングセッション中に以前に確立された前記装置の公開鍵と、を入力に使用する鍵導出関数を使用して導出された共有シークレットを生成し、
前記導出された共有シークレットを使用して前記署名を復号し、
前記ペアリングセッション中に確立された前記モバイルデバイスの公開鍵を使用して前記署名を検証し、
前記検証に基づいて、１つ以上のアクションを許可する、
ように構成される１つ以上の処理要素を備える装置。
【請求項１１】
請求項１０に記載の装置であって、
非対称認証手順中のペアリングセッション中に確立された前記モバイルデバイスの非公開鍵を使用して署名された、別のデバイスから証明書を受信し、
前記証明書を検証することに基づいて、１つ以上のアクションを許可する、ように構成される装置。
【請求項１２】
請求項１１に記載の装置であって、メールボックスに記憶された暗号化されたセキュリティトークンにアクセスして、前記セキュリティトークンを検証することに基づいて、１つ以上のアクションを許可するかどうかを判定する、ように構成される装置。
【請求項１３】
コンピューティングデバイスによって実行可能である命令を記憶した非一時的コンピュータ可読媒体であって、
第１の公開鍵及び第１の非公開鍵を含む第１の短期鍵ペアを生成することと、
システムによって生成された第２の公開鍵であって、第２の短期鍵ペアに含まれる、前記第２の公開鍵を判定することと、
前記第１の非公開鍵及び前記第２の公開鍵を入力として使用する鍵交換関数を使用して第１の共有シークレットを生成することと、
少なくとも、前記第１の共有シークレットと、前記第１の公開鍵と、前記装置と前記システムとの間のペアリングセッション中に以前に確立された前記システムの公開鍵と、を入力に使用する鍵導出関数を使用して導出された共有シークレットを生成することと、
前記ペアリングセッション中に確立された前記装置の非公開鍵でトランザクション情報

に署名することによって署名を生成することと、
前記導出された共有シークレットに基づいて、前記署名と前記装置を識別する情報とを暗号化することと、
前記システムの前記公開鍵を使用して前記システムから受信された署名付き証明書であって、前記システムの対応する非公開鍵で署名される、前記証明書を検証することと、
前記署名付き証明書の検証に応じて、前記暗号化された署名及び情報を前記システムに送信することと、
を含む動作を実行する非一時的コンピュータ可読媒体。
【請求項１４】
請求項１３に記載の非一時的コンピュータ可読媒体であって、前記動作は、
前記システムの１つ以上の機能へのアクセスを他のデバイスと共有することであって、
前記他のデバイスから証明書署名要求を受信することと、
前記受信された証明書を、前記他のデバイスと関連付けられた許可されたエンティティのルート証明書を使用して検証することと、
前記装置のユーザを認証することと、
前記システムとの前記ペアリングセッション中に確立された前記装置の前記非公開鍵を使用して前記証明書に署名することと、
前記署名付き証明書を前記他のデバイスに送信することと、
を含む共有すること、を更に含む非一時的コンピュータ可読媒体。
【請求項１５】
請求項１４に記載の非一時的コンピュータ可読媒体であって、前記証明書署名要求及び前記署名付き証明書は、広域ネットワークを使用することなく直接無線接続を介して送信される非一時的コンピュータ可読媒体。
【請求項１６】
請求項１４に記載の非一時的コンピュータ可読媒体であって、前記動作は、
前記システムのセキュリティトークンを暗号化することと、前記セキュリティトークンを前記他のデバイスに送信することとを更に含む、非一時的コンピュータ可読媒体。
【請求項１７】
請求項１３に記載の非一時的コンピュータ可読媒体であって、前記動作は、
ユーザによる前記共有アクセスの取り消しに応じて、取り消しメッセージを送信することと、取り消し受信通知を検証することとを更に含む、非一時的コンピュータ可読媒体。
【請求項１８】
請求項１３に記載の非一時的コンピュータ可読媒体であって、前記動作は、前記システムにアクセス可能なセキュアメールボックスに１つ以上の設定を記憶して、１つ以上の許可されたアクションのためのパラメータを判定することを更に含む、非一時的コンピュータ可読媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概して、電子セキュリティに関し、より具体的には、モバイルデバイスを使用して別のシステムへのアクセスを得るための暗号技術に関する。
【背景技術】
【０００２】
システムの機能へのアクセス（例えば、物理アクセス、又はシステムの何らかの機能へのアクセス）を得るための従来の技術は、物理鍵又は電子鍵フォブの使用を必要とする場合がある。このような従来の鍵を持ち運ぶことは不便なことがあり、鍵を紛失したか又は盗難された場合に悪意のあるエンティティがアクセスできるようにし得る。
【図面の簡単な説明】
【０００３】

【図１Ａ】いくつかの実施形態に係る、モバイルデバイスと制御ユニットとの間の例示的なペアリング通信を示すブロック図である。
【０００４】
【図１Ｂ】いくつかの実施形態に係る、モバイルデバイスと制御ユニットとの間の例示的な要求通信及び認証通信を示すブロック図である。
【０００５】
【図１Ｃ】いくつかの実施形態に係る、制御ユニットを制御するために別のモバイルデバイスに許可を付与する例示的な通信を示すブロック図である。
【０００６】
【図２】いくつかの実施形態に係る、例示的なモバイルデバイスを示すブロック図である。
【０００７】
【図３】いくつかの実施形態に係る、ペアリングのための例示的な技術を示す通信図である。
【０００８】
【図４】いくつかの実施形態に係る、動作を許可するための例示的な技術を示す通信図である。
【０００９】
【図５】いくつかの実施形態に係る、別のデバイスを許可するための例示的な技術を示す通信図である。
【００１０】
【図６Ａ】いくつかの実施形態に係る、別のデバイスのサーバーベースの許可のための例示的な技術を示す通信図を構成する。
【図６Ｂ】いくつかの実施形態に係る、別のデバイスのサーバーベースの許可のための例示的な技術を示す通信図を構成する。
【００１１】
【図７Ａ】いくつかの実施形態に係る、モバイルデバイスとシステムの処理要素とをペアリングするための例示的な方法を示すフローチャートである。
【図７Ｂ】いくつかの実施形態に係る、モバイルデバイスとシステムの処理要素とをペアリングするための例示的な方法を示すフローチャートである。
【００１２】
【図８Ａ】いくつかの実施形態に係る、システムによる１つ以上の動作を許可するためにモバイルデバイスを認証するための例示的な方法を示すフローチャートである。
【図８Ｂ】いくつかの実施形態に係る、システムによる１つ以上の動作を許可するためにモバイルデバイスを認証するための例示的な方法を示すフローチャートである。
【００１３】
【図９Ａ】いくつかの実施形態に係る、複数のトランザクションタイプでの動作を許可するための例示的な技術を示す通信図を構成する。
【図９Ｂ】いくつかの実施形態に係る、複数のトランザクションタイプでの動作を許可するための例示的な技術を示す通信図を構成する。
【図９Ｃ】いくつかの実施形態に係る、複数のトランザクションタイプでの動作を許可するための例示的な技術を示す通信図を構成する。
【００１４】
【図１０】いくつかの実施形態に係る、標準トランザクションタイプで動作を許可するための例示的な技術を示す通信図である。
【００１５】
【図１１】いくつかの実施形態に係る、例示的なペアリング技術を示す通信図である。
【００１６】
【図１２】いくつかの実施形態に係る、例示的なシステム要素を示すブロック図である。
【００１７】

【図１３】いくつかの実施形態に係る、モバイルデバイス及びシステムの例示的な構成要素を示すブロック図である。
【００１８】
【図１４】いくつかの実施形態に係る、例示的なメールボックス構造を示す図である。
【００１９】
【図１５】いくつかの実施形態に係る、別のデバイスとの例示的なオフライン共有を示す通信図である。
【００２０】
【図１６】いくつかの実施形態に係る、別のデバイスとの例示的なオンライン共有を示す通信図である。
【００２１】
【図１７】いくつかの実施形態に係る、例示的な鍵取り消しを示す図である。
【００２２】
【図１８】いくつかの実施形態に係る、例示的なメールボックス使用を示す図である。
【００２３】
【図１９】いくつかの実施形態に係る、例示的な証明書チェーンを示すブロック図である。
【図２０】いくつかの実施形態に係る、例示的な証明書チェーンを示すブロック図である。
【図２１】いくつかの実施形態に係る、例示的な証明書チェーンを示すブロック図である。
【図２２】いくつかの実施形態に係る、例示的な証明書チェーンを示すブロック図である。
【図２３】いくつかの実施形態に係る、例示的な証明書チェーンを示すブロック図である。
【図２４】いくつかの実施形態に係る、例示的な証明書チェーンを示すブロック図である。
【００２４】
【図２５】いくつかの実施形態に係る、設計情報を記憶する例示的なコンピュータ可読媒体を示すブロック図である。
【００２５】
【図２６】いくつかの実施形態に係る、認証のための例示的なモバイル側の方法を示すフローチャートである。
【００２６】
【図２７】いくつかの実施形態に係る、認証のための例示的なシステム側の方法を示すフローチャートである。
【００２７】
【図２８】いくつかの実施形態に係る、ペアリング時のデジタル鍵構造証明のための例示的な技術を示すブロック図である。
【００２８】
本開示は、「ｏｎｅ　ｅｍｂｏｄｉｍｅｎｔ（一実施形態）」又は「ａｎ　ｅｍｂｏｄｉｍｅｎｔ（ある実施形態）」に対する参照を含む。「ｉｎ　ｏｎｅ　ｅｍｂｏｄｉｍｅｎｔ（一実施形態において）」又は「ｉｎ　ａｎ　ｅｍｂｏｄｉｍｅｎｔ（ある実施形態において）」という語句表現は、必ずしも同一の実施形態を指すわけではない。特定の機能、構造、又は特性は、本開示と一貫したいずれかの適切な方式で組み合わされてもよい。
【００２９】
本開示内で、（「ユニット」、「回路」、他の構成要素などと様々に呼ばれることがある）様々なエンティティは、１つ以上のタスク又は動作を実施するように「構成されている（configured）」ものとして記述又は主張されることがある。［１つ以上のタスクを実

施する］ように構成されている［エンティティ］というこの明確な語句は、本明細書では構造（すなわち、電子回路など、物理的なもの）を指すために使用される。より具体的には、この明確な語句は、この構造が動作中に１つ以上のタスクを実施するように配置されたことを示すために使用される。構造は、その構造が現在動作していない場合でも、何らかのタスクを実施する「ように構成されている」と述べられることがある。「認証を実行するように構成されたセキュア回路」は、例えば、対象の集積回路が現在使用されていない（例えば、電力供給装置がそれに接続されていない）場合でさえ、動作中にこの機能を実行する回路を有する集積回路を網羅することが意図される。このように、何らかのタスクを実施する「ように構成されている」ものとして記述又は説明されるエンティティは、デバイス、回路、そのタスクを実現するように実行可能なプログラム命令を記憶したメモリなど、物理的なものを指す。この語句は、本明細書では無形のものを指すためには使用されない。したがって、「～のように構成されている」との言い方は、本明細書では、アプリケーションプログラミングインタフェース（application programming interface、ＡＰＩ）などのソフトウェアエンティティを指すためには使用されない。

【００３０】

「～ように構成されている」という用語は、「～ように構成可能な」を意味することを意図していない。例えば、プログラムされていないＦＰＧＡは、何らかの特定の機能を実行する「ように構成可能」であり得るが、その機能を実施する「ように構成されている」とは見なされず、プログラミング後にその機能を実施する「ように構成されている」と言えよう。

【００３１】

添付の請求項において、ある構造が１つ以上のタスクを実行する「ように構成されている」と説明することは、その請求項要素について米国特許法第１１２条（ｆ）を援用しないことを明示的に意図している。したがって、出願された本出願中の請求項のいずれも、ミーンズプラスファンクション要素を有するものとして解釈されることを意図していない。出願人が審査過程中に１１２条（ｆ）を援用することを望む場合、それは、［機能を実行する］「ための手段」という構成体を使用して請求項要素を説明することになる。

【００３２】

本明細書で使用される用語「第１の」、「第２の」等は、名詞の前に付くラベルとして使用され、特に言及しない限りいかなるタイプの順序（例えば、空間的、時間的、論理的、等）も意味しない。例えば、モバイルデバイスは、第１のユーザ及び第２のユーザを有してもよい。「第１の」という用語は、デバイスの初期ユーザに限定されない。「第１の」という用語は、モバイルデバイスのユーザが一人だけ存在する場合にも使用されてよい。

【００３３】

本明細書で使用する「～に基づいて」という用語は、判定に影響を及ぼす１つ以上の要因を記述するために使用される。この用語は、追加の要因が判定に影響を及ぼすことがある可能性を除外しない。すなわち、判定は、特定の要因のみに基づくか、又は、特定の要因並びに他の不特定な要因に基づき得る。「Ｂに基づいて Ａを判定する」という語句を検討する。この語句により、Ｂは、Ａを判定するために使用されるか、又はＡの判定に影響を及ぼす要因であることが特定される。この語句は、Ａの判定が、Ｃなど、何らかの他の要因にも基づき得ることを除外しない。この語句は、ＡがＢのみに基づいて判定される実施形態をも網羅することを意図している。本明細書で使用する「～に基づいて」という語句はしたがって、「～に少なくとも部分的に基づいて」という語句と同義である。

【発明を実施するための形態】

【００３４】

例示的な実施形態に関する概観

本開示は、モバイルデバイスを使用して、システムの機能へのアクセスを得る実施形態について記載する。いくつかの実施形態では、非対称暗号法を使用して、モバイルデバイスとシステムとの間にセキュアチャネルを確立する。セキュアチャネルを使用して、シス

テムは、以前に記憶された公開鍵（例えば、ペアリングプロセスの一部として記憶された鍵）を使用して、モバイルデバイスのセキュア要素（secure element、ＳＥ）などのセキュア回路によって生成された署名を検証することによりデバイスを認証することができる。システムの制御ユニット（例えば、ＥＣＵ）などのプロセッサは、長期鍵ペアを記憶し、短期非対称鍵ペアを生成し、署名を検証するように構成されてもよい。モバイルデバイスは、長期非対称鍵ペアを記憶するように構成されたＳＥを含んでもよい。

【００３５】

様々な実施形態では、モバイルデバイスは、最初に、システムとのペアリング手順を実行する。この手順は、モバイルデバイスが短期公開鍵ペアをシステムと交換することと、モバイルデバイスのプロセッサが交換された鍵に基づいて（例えば、楕円曲線ディフィー・ヘルマン（elliptic curve Diffie-Hellman、ＥＣＤＨ）を使用して）システムとの共有シークレットを生成することと、を含み得る。モバイルデバイスのセキュア回路はまた、システムがモバイルデバイスを認証できるように公開鍵ペアを生成することができる。セキュア回路は、例えば、セキュア要素であってもよい。本明細書で使用する「セキュア要素」という用語は、当該技術分野におけるその理解された意味にしたがって解釈されるべきであり、これは、その情報の無許可の抽出を防止する改ざん防止法で情報を記憶するように構成されている回路（例えば、多くの場合、シングルチップマイクロコントローラ）を含む。セキュア要素のためのフォームファクタの非限定的な例としては、ＵＩＣＣ、埋め込みＳＥ、及びマイクロＳＤが挙げられる。いくつかの実施形態では、セキュア要素はまた、例えば、決済トランザクションなどの他のタイプのトランザクションにも使用される。決済トランザクションの場合、セキュア要素は、決済機器（例えば、クレジットカード）及びオーナー（例えば、カード保持者）のデータ、物理的場所又は建物への入場、送信アクセスなどを暗号化して記憶することができる。いくつかの実施形態では、セキュア要素機能のうちの少なくとも一部分は、クラウドベースであり得る。これらの実施形態では、デバイス上のセキュア要素は、サーバ上に記憶された実際の必要な情報を取り出すために使用され得る仮想情報を記憶してもよい。いくつかの実施形態では、他のタイプのセキュア回路又はセキュアプロセッサは、例えば、後述するセキュアエンクレーブプロセッサを含むセキュア要素によって実行されるものとして記載された機能を実行することができる。

【００３６】

鍵交換の後、次いで、モバイルデバイスは、非公開鍵を使用して鍵ペアの証明書を暗号化し、暗号化された証明書をシステムに送信することができる。次いで、モバイルデバイスは、公開鍵ペアに基づいて導出された値を表示し、モバイルデバイスのユーザに、証明書の公開鍵に基づいて値を導き出すことができる、システムのディスプレイ上にその値がまた表示されていることを確認するように依頼することができる。

【００３７】

モバイルデバイスが他のシステムとペアリングされると、モバイルデバイスは、他のシステムとの交換を実行して、他のシステムの機能、例えば、いくつかの実施形態では、ドアを開くこと、エンジンを始動すること又はモータを起動すること、電話をかけること、メディアを再生すること、特定の速度を上回る速度で移動することなどを有効にできる。いくつかの実施形態では、交換には、モバイルデバイスのプロセッサが、セッションのためにシステムと共有される別の暗号鍵を生成し、システムがモバイルデバイスにチャレンジを発行することが含まれる。チャレンジの受信に応じて、モバイルデバイスのセキュア要素は、以前に生成された公開鍵ペアの非公開鍵を使用して応答を生成する。他の実施形態では、セキュア要素と見なされない他のセキュア回路は、同様の機能を実行するために使用されてもよい。次いで、モバイルデバイスは、他の暗号鍵で応答を暗号化し、検証のために応答をシステムに送信する。検証の成功に応じて、システムは、要求された機能を有効にできる。

【００３８】

場合によっては、システムのオーナーは、別のユーザのモバイルデバイスがシステムに

アクセスすることを可能にしたいことがある。いくつかの実施形態では、他のユーザのモバイルデバイスのセキュア要素は、公開鍵ペア、及び公開鍵に対する対応する証明書署名要求を生成することができる。次いで、他のユーザのデバイスは、証明書署名要求をオーナーのモバイルデバイスのセキュア要素に送信してもよく、これにより、公開鍵の証明書が生成される。次いで、オーナーのモバイルデバイスは、生成された証明書を他のユーザのモバイルデバイスに送信して、モバイルデバイスがシステムの機能を有効にできるようにする。

【００３９】

モバイルデバイス及びシステムは、本明細書に記載された機能を実行するために任意の好適なハードウェアを含んでもよい。したがって、このハードウェアは、相互接続（例えば、システムバス）を介してシステムメモリ及びＩ／Ｏインタフェース（単数又は複数）又はデバイスに連結されたプロセッササブシステムを含んでもよい。モバイルデバイスとして記載されているが、このデバイスは、サーバシステム、パーソナルコンピュータシステム、デスクトップコンピュータ、ラップトップ若しくはノートブックコンピュータ、メインフレームコンピュータシステム、タブレットコンピュータ、ハンドヘルドコンピュータ、ワークステーション、ネットワークコンピュータ、モバイル電話、音楽プレーヤ、又はパーソナルデータアシスタント（personal data assistant、ＰＤＡ）などの消費者デバイスが挙げられるが、これらに限定されない、様々なタイプのデバイスのうちのいずれかであってもよい。モバイルデバイス及び／又はシステムはまた、非一時的コンピュータ可読媒体内に具現化されたプログラム命令を実行することによって、様々な機能を実行することができる。以下で更に詳細に記載された図２は、ハードウェア実施形態の更なる非限定的な例を示す。

【００４０】

いくつかの実施形態では、開示された技術は、物理鍵と同等のプライバシー、オフライン鍵共有、デバイス及びシステムにわたる相互運用性、基礎をなす無線プロトコル（単数又は複数）から独立した動作、スケーラブルシステムなどを有利に提供できる。いくつかの実施形態では、モバイルデバイス非公開鍵は、モバイルデバイスに含まれるセキュア回路（例えば、セキュア要素）を離れることはない。いくつかの実施形態では、開示された技術は、信頼されていないチャネルの上で使用することができ、能動的及び／又は受動的な盗聴者に対する保護を提供することができる。

【００４１】

本明細書で使用する「セキュアチャネル」という用語は、データを通信するための専用経路（すなわち、意図された参加者のみによって共有される経路）又は意図された参加者のみに既知の暗号鍵を使用して暗号化されたデータ若しくは署名付きデータを通信するための専用経路のいずれかを指す。本明細書で使用する「セキュア回路」という用語は、１つ以上のサービスを実行し、認証された応答を外部要求者に返すように構成された回路のクラスのうちの１つを指す。セキュア回路によって返された結果は、いかなる形態の認証もなしで単に結果を返す回路の信頼性を超える信頼性のしるしを有すると考えられる。したがって、アクセスされたデータのソースを認証しない（例えば、サードパーティアプリケーションにアクセス可能な信頼されていないメモリ領域からの）データを提供する回路は、本出願の意味においてセキュア回路と見なされないであろう。本明細書で開示する実施形態では、セキュア要素及びセキュアエンクレーブプロセッサは、セキュア回路の例として提供される。例えば、検証可能な暗号署名で署名することなどによって、返される結果を認証することによって、セキュア回路は、なりすまし防止機能を提供することができる。同様に、非公開鍵（private key）又は秘密鍵（secret key）を使用して結果を暗号化することによって、セキュア回路は、暗号化されたデータのソースを認証することができる（様々な実施形態では、暗号化は、単独で、又は署名と組み合わせて使用されてもよい）。更に、場合によっては、セキュア回路は、「改ざん防止性」であると言われることがあり、この用語は、１つ以上のサービスを実行するセキュア回路の部分の危殆化を防止する機構を指す、当該技術分野の用語である。例えば、セキュアメールボックスは、セキ

ュア回路の一部分のみ（例えば、予め定義されたメモリ領域）が他の回路に直接アクセス可能であるように実装されてもよい。同様に、セキュア回路によって実行されるファームウェアは、暗号化され得、署名され得、及び／又は他の処理要素にアクセス不可能な領域に記憶され得る。

【００４２】

図１Ａは、いくつかの実施形態に係る、システムの制御ユニットなどの回路とモバイルデバイスとの間の例示的なペアリング通信１４５を示すブロック図である。例示的な目的のために、単一の制御ユニットが様々な例で論じられているが、同様の技術が、複数の異なる制御ユニット又はプロセッサ（例えば、マイクロコントローラ）及び異なる車両機能を制御する様々なタイプの制御ユニット又はプロセッサと共に使用されてもよい。「ＥＣＵ」という用語は、制御ユニットの一例であり、車両の１つ以上の動作を制御するように構成された回路を含む、その十分に理解された意味にしたがって解釈されることが意図される当該技術分野の用語である。

【００４３】

例示された実施形態では、システム１１０は、制御ユニット１３７を含み、ユーザからペアリング要求１４０を受信する。いくつかの実施形態では、システム１１０は、車両、又はＥＣＵなどのその構成要素である。車両の例としては、航空機、船舶、ＲＶ、自動車、バス、鉄道車両、宇宙船、ロボット装置などが挙げられるが、これらに限定されない。車両でない場合のシステムの例としては、建物などの物理的場所、交通機関アクセス制御、及びモノのインターネット又はホームオートメーションデバイス若しくはコントローラを更に含む。システム１１０によって実行されるように記載された様々なアクションは、システム１１０に含まれるプロセッサ、構成要素、又はデバイスによって実行されてもよいことに留意されたい。ペアリング要求は、例えば、システム１１０内のタッチスクリーンを使用して入力された入力を介してシステム１１０にて開始されてもよく、例えば、ユーザを識別する情報及び／又はユーザの初期認証に関する情報、例えば、個人識別番号（personal identification number、ＰＩＮ）、パスワード、バイオメトリック認証などを含んでもよい。様々な実施形態では、情報は、本明細書で論じられる無線通信に関して帯域外で送信されてもよい。いくつかの実施形態では、システムの製造業者又はプロバイダは、システム１１０の販売時に初期ＰＩＮをユーザに提供し、初期ＰＩＮは、その後、ペアリング要求１４０で使用される。

【００４４】

例示された実施形態では、モバイルデバイス１３０は、アプリケーションプロセッサ（application processor、ＡＰ）１３６及び無線インタフェース１３２（例えば、ＮＦＣインタフェース、Ｂｌｕｅｔｏｏｔｈインタフェース、Ｗｉ－Ｆｉダイレクトインタフェースなど）を含み、無線インタフェース１３２は更に、ＳＥ１３４を含む。いくつかの実施形態では、ＳＥ１３４は、モバイルデバイス１３０とシステム１１０との間のセキュア通信を容易にするために、様々な暗号化動作を実行するように構成されている。本明細書ではＮＦＣ通信について論じているが、これは、本開示の範囲を限定することを意図するものではないことに留意されたい。他の実施形態では、様々な適切なインタフェースのいずれかは、Ｗｉ－Ｆｉダイレクト、Ｂｌｕｅｔｏｏｔｈなどの開示された技術と共に使用されてもよい。更に、様々な実施形態では、特定のタイプの要素（例えば、アプリケーションプロセッサ、セキュア要素、ＥＣＵなど）に関して本明細書で論じられる様々な機能は、他のタイプの要素によって実行されてもよい。

【００４５】

モバイルデバイス１３０とシステム１１０とのペアリングは、共有シークレット（共有鍵とも称され得る）の確立と、システム１１０によってＳＥ１３４からの長期公開鍵を記憶することと、を伴い得る。例示的なペアリング手順の詳細な説明については、図３を参照して以下で論じる。ペアリングされると、ＳＥ１３４はまた、例えば、図４を参照して以下で論じるように、モバイルデバイス１３０が様々な動作を実行するようにシステム１１０に命令するトランザクションを容易にし得る。

【００４６】
図１Ｂは、いくつかの実施形態に係る、動作を実行するためのシステムとモバイルデバイスとの間の例示的な通信を示すブロック図である。動作の例としては、ドアロックを開くこと、エンジンを始動すること、機能を有効化又は無効化すること、再生されているメディアを変更すること、システムを広域ネットワークに接続又は接続解除すること、追加ユーザを許可又は除去すること、鍵チェーンデータへのアクセス、購入の実行能力などが挙げられる。例示された実施形態では、ＳＥ１３４は、ＡＰ１３６によって開始された要求１５０について認証通信１５５を実行するように構成されている。
【００４７】
図１Ｃは、別のモバイルデバイス１６０に制御ユニット１３７に許可を付与する例示的な通信を示すブロック図である。これにより、ペアリングされたデバイスのユーザが、例えば、友人又は家族の１つ以上の他のデバイスへのアクセスを許可することができ得る。例示された実施形態では、ＳＥ１３４は、（例えば、署名付き証明書を含み得る）許可付与１６５をモバイルデバイス１６０に送信し、この許可付与１６５により、システム１１０が、モバイルデバイス１６０が認証通信１７０に基づいてモバイルデバイス１３０から許可を受信したことを確認できる。例示された実施形態では、モバイルデバイス１６０は、ＳＥ１３４によって署名されるべき鍵を含み得る許可要求１６２を送信する。
例示的なモバイルデバイスの実装
【００４８】
次に図２を参照すると、いくつかの実施形態に係る、モバイルデバイス１３０のブロック図が示されている。モバイルデバイス１３０は、無線インタフェース１３２、ＳＥ１３４、及びバイオセンサ１３８を含み得る。例示された実施形態では、モバイルデバイス１３０は、通信ファブリック２６０を介して連結された、セキュアエンクレーブプロセッサ（secure enclave processor、ＳＥＰ）２１０、セルラインタフェース２２０、ＣＰＵ２３０、メモリ２４０、周辺装置２５０を更に含む。図示のように、ＳＥＰ２１０は、１つ以上のプロセッサＰ２１２、セキュアメモリ２１４、及び１つ以上のセキュリティ周辺装置２１６を含み得る。ＳＥ１３４は、１つ以上のプロセッサＰ２２２及びメモリ２２４を含み得る。ＣＰＵ３２０は、１つ以上のプロセッサＰ２３２を含み得る。メモリ２４０は、インタフェースアプリケーション２４２を記憶し得る。いくつかの実施形態では、モバイルデバイス１３０は、図に示すものとは異なるように実装されてもよい。
【００４９】
いくつかの実施形態では、ＳＥＰ２１０は、１人以上の許可されたユーザの以前にキャプチャされたバイオメトリックテンプレートデータ２１８を維持し、ユーザを認証するためにバイオセンサ１３８によってキャプチャされた新たに受信されたデータと比較するように構成されている。（別の実施形態では、バイオセンサ１３８又はＳＥ１３４が比較を実行し得る。）例示された実施形態では、ＳＥＰ２１０は、バイオメトリックテンプレート２１８内の指紋、顔バイオメトリックデータ（例えば、虹彩データ、音声データ、顔又は身体特性）などから収集されたバイオメトリックデータを記憶するように構成されている。指紋の実施形態では、各テンプレート２１８は、特定の登録されたユーザに対応してもよく、固有のインデックス値を割り当てられてもよい。いくつかの実施形態では、バイオセンサ１３８から受信したバイオメトリックデータがテンプレート２１８に記憶されたバイオメトリックデータと一致する場合、ＳＥＰ２１０は、照合テンプレート２１８と関連付けられた固有のインデックス値をＳＥ１３４に提供するように構成されており、これは次に、インデックス値を使用して、認証されている既知のユーザの対応する識別情報を検索する。いくつかの実施形態では、ＳＥＰ２１０は、複数のテンプレート２１８を記憶してもよい。様々な実施形態では、ＳＥＰ２１０、ＳＥ１３４、及び／又はバイオセンサ１３８間の通信は、ＣＰＵ２３０などの別のエンティティがそれらの通信を閲覧できないように暗号化される。
【００５０】
様々な実施形態では、ＳＥＰ２１０は、バイオメトリックデータを安全に記憶するよう

に構成されている。したがって、様々な実施形態では、ＳＥＰ２１０は、慎重に制御されたインタフェースを除いて、モバイルデバイス１３０の残りの部分から分離される（したがって、ＳＥＰプロセッサ２１２、セキュアメモリ２１４、及びセキュリティ周辺装置２１６のためのセキュアエンクレーブを形成する）。ＳＥＰ２１０へのインタフェースが慎重に制御されるので、ＳＥＰプロセッサ２１２、セキュアメモリ２１４、及びセキュリティ周辺装置２１６への直接アクセスを防止することができる。一実施形態では、セキュアメールボックス機構が実行されてもよい。セキュアメールボックス機構では、外部デバイスは、メッセージをインボックスに送信することができる。ＳＥＰプロセッサ２１２は、メッセージを読み取り、解釈し、メッセージに応じて行われるアクションを決定することができる。ＳＥＰプロセッサ２１２からの応答メッセージは、セキュアメールボックス機構の一部でもあるアウトボックスを介して送信されてもよい。他の回路は、メールボックス機構を介する以外に、ＳＥＰ２１０の内部リソースにアクセスすることができない場合がある。外部構成要素からのコマンド／要求及び外部構成要素への結果の受け渡しのみを許可する他のインタフェースを使用してもよい。外部デバイスからＳＥＰ２１０への他のアクセスが許可されていない場合があり、これにより、ＳＥＰ２１０は、「アクセスから保護」され得る。より具体的には、ＳＥＰ２１０の外側の任意の場所で実行されるソフトウェアは、ＳＥＰ２１０を用いてセキュア構成要素への直接アクセスを妨げられ得る。ＳＥＰプロセッサ２１２は、コマンドが実行されるかどうかを判定することができる。場合によっては、コマンドを実行するか否かの判定は、コマンドのソースによって影響を受ける場合がある。すなわち、コマンドは、あるソースからは許可され得るが、別のソースから許可されない場合がある。

【００５１】

様々な実施形態では、ＳＥＰ２１０は、ＳＥ１３４に関して記載された機能を実行するように構成されてもよく、及び／又はその逆であってもよい。いくつかの実施形態では、ＳＥ１３４は、デバイス１３０の識別情報を認証するように構成され、一方、ＳＥＰ２１０は、デバイス１３０の現在のユーザの識別情報を認証するように構成されている（この識別情報は、いくつかの実施形態では、システムアクセスにも必要となる場合がある）。

【００５２】

いくつかの実施形態では、ＳＥＰプロセッサ２１２は、ＳＥＰ２１０に関して記載された（descried）機能の実施を容易にする安全にロードされたソフトウェアを実行することができる。例えば、セキュアメモリ２１４は、ＳＥＰプロセッサ２１２によって実行可能なソフトウェアを含み得る。セキュリティ周辺装置２１６のうちの１つ以上は、ソフトウェアのソース（例えば、フラッシュメモリなどの不揮発性メモリ）に接続され得る外部インタフェースを有してもよい。別の実施形態では、ソフトウェアのソースは、別の周辺装置２１６に連結された不揮発性メモリであってもよく、ソフトウェアは、サードパーティによる観察を回避するために暗号化されてもよい。ソースからのソフトウェアは、認証されるか、又は別の方法でセキュアであると検証されてもよく、ＳＥＰプロセッサ２１２によって実行可能であってもよい。いくつかの実施形態では、ソフトウェアは、ＳＥＰ２１０に割り当てられたメモリ２１４内のトラストゾーンにロードされてもよく、ＳＥＰプロセッサ２１２は、実行のためにトラストゾーンからソフトウェアをフェッチしてもよい。ソフトウェアは、観察を回避するために、暗号化された形態でメモリ２４０に記憶されてもよい。セキュアソフトウェアのセキュリティを確実するために講じられたステップにもかかわらず、セキュアソフトウェアは、記憶された非公開鍵に直接アクセスする／取得することを依然として妨げられ得る。一実施形態では、ハードウェアのみが非公開鍵へのアクセスを有し得る。

【００５３】

セキュリティ周辺装置２１６は、ＳＥＰ２１０によって実行されるセキュアサービスを手助けするように構成されたハードウェアであってもよい。したがって、セキュリティ周辺装置２１６は、様々な認証アルゴリズムを実行／高速化する認証ハードウェア、暗号化を実行／高速化するように構成された暗号化ハードウェア、セキュアインターフェースを

介して外部（モバイルデバイス１３０に）デバイスと通信するように構成されたセキュアインタフェースコントローラなどを含み得る。

【００５４】

いくつかの実施形態では、ＳＥ１３４は、公開鍵情報２２８などのメモリ２２４に記憶された機密情報へのアクセスを制限するために、ＳＥＰ２１０と同様の機能を実行してもよい。例えば、ＳＥ１３４は、メールボックスを実行して、プロセッサ２２２及びメモリ２２４へのアクセスを制限し得る。様々な実施形態では、ＳＥプロセッサ２２２はまた、メモリ２２４に記憶されたアプレット２２６など、本明細書に記載された機能を実行するために、安全にロードされたソフトウェアを実行する。

【００５５】

一実施形態では、アプレット２２６は、モバイルデバイス１３０の登録及び読取機による認証を実行するように実行可能である。登録に関して、アプレット２２６は、公開鍵ペアを生成し、対応する証明書を取得するために実行可能であり得、これは、公開鍵情報２２８としてメモリ２２４に記憶されてもよい。

【００５６】

いくつかの実施形態では、インタフェースアプリケーション２４２は、登録及び認証が実行されるときに、ＳＥＰ２１０、ＳＥ１３４とモバイルデバイス１３０のユーザとの間のインタフェースを容易にするように実行可能である。したがって、アプリケーション２４２は、これらのプロセス中に様々なアクションを実行するようにユーザに指示する様々なプロンプトをユーザに提供することができる。アプリケーション２４２はまた、これらのプロセス中に適切な場合に、バイオセンサ１３８、ＳＥＰ２１０、及び／又はＳＥ１３４をアクティブ化してもよい。アプリケーション２４２によって実行される様々なアクションは、以下で更に詳細に記載される。

【００５７】

いくつかの実施形態では、セルラインタフェース２２０は、モバイルデバイス１３０とシステム１２０及び１４０などの１つ以上の外部システムとの間の双方向作用を容易にするように構成された長距離無線機である。セルラリンク２２０は、ベースバンドプロセッサ、アナログＲＦ信号処理回路（例えば、フィルタ、ミキサ、発振器、増幅器などを含む）、デジタル処理回路（例えば、デジタル変調及び他のデジタル処理用）、１つ以上のアンテナなどの長距離ネットワークとインタフェースするための好適な回路を含み得る。セルラインタフェース２２０は、ＧＳＭ、ＵＭＴＳ、ＣＤＭＡ２０００、ＬＴＥ、ＬＴＥ－Ａなどの複数の無線アクセス技術／無線通信プロトコルのいずれかを使用して通信するように構成されてもよい。

【００５８】

前述のように、ＣＰＵ２３０は、１つ以上のプロセッサ２３２を含み得る。概して、プロセッサは、プロセッサにより実行される命令セットアーキテクチャ内に定義された命令を実行するように構成された回路を含み得る。プロセッサ２３２は、集積回路上に他の構成要素と共にシステムオンチップ（system on a chip、ＳＯＣ）又は他の一体化レベルとして実装されるプロセッサコアを含み得る（又はそれに対応し得る）。プロセッサ２３２は、別個のマイクロプロセッサ、マルチチップモジュール実装内に集積化されるプロセッサコア及び／又はマイクロプロセッサ、複数の集積回路として実装されるプロセッサなどを更に含み得る。

【００５９】

プロセッサ２３２は、オペレーティングシステムなどのシステムの主制御ソフトウェアを実行してもよい。概して、使用中にＣＰＵ２３０により実行されるソフトウェアは、システムの所望の機能を実現するために、システムの他の構成要素を制御し得る。プロセッサはまた、他のソフトウェアを実行してもよい。これらのアプリケーションは、ユーザ機能を提供し得、低レベルデバイス制御、スケジューリング、メモリ管理などについてオペレーティングシステムに依存し得る。したがって、プロセッサ２３２（又はＣＰＵ２３０）は、アプリケーションプロセッサとも称され得る。ＣＰＵ２３０は、Ｌ２キャッシュ及

び／又はシステムの他の構成要素に対するインタフェース（例えば、通信ファブリック２６０に対するインタフェース）などの他のハードウェアを更に含み得る。

【００６０】

メモリ２４０は、概して、データを記憶するための回路を含み得る。例えば、メモリ２４０は、スタティックランダムアクセスメモリ（static random access memory、ＳＲＡＭ）、ダブルデータレート（ＤＤＲ、ＤＤＲ２、ＤＤＲ３、ＤＤＲ４など）ＤＲＡＭを含むシンクロナスＤＲＡＭ（synchronous DRAM、ＳＤＲＡＭ）などのダイナミックＲＡＭ（dynamic RAM、ＤＲＡＭ）であり得る。ＤＤＲ　ＤＲＡＭの低電力／モバイルバージョン（例えば、ＬＰＤＤＲ、ｍＤＤＲなど）がサポートされ得る。デバイス１３０は、動作を順序付けし（及び場合によっては再順序付けし）、メモリ２４０へ動作を提示するための、メモリ動作用の待ち行列を含み得るメモリコントローラ（図示せず）を含み得る。メモリコントローラは、メモリへの書き込みを待っている書き込みデータ、及びメモリ動作の送信元への返送を待っている読み出しデータを記憶するためのデータバッファを更に含んでもよい。いくつかの実施形態では、メモリコントローラは、最近アクセスされたメモリデータを記憶するためのメモリキャッシュを含み得る。いくつかの実施形態では、メモリ３３０は、デバイス１３０に、デバイス１３０に関して本明細書に記載された様々な機能を実行させるための、１つ以上のプロセッサ２３２によって実行可能なアプリケーション２４２の命令などのプログラム命令を含み得る。

【００６１】

周辺装置２５０は、デバイス１３０内に含まれる追加ハードウェア機能の任意のセットであり得る。例えば、周辺装置３４０は、カメラ又は他の画像センサからの画像キャプチャデータを処理するように構成された画像信号プロセッサなどの映像周辺装置、１つ以上の表示デバイスに映像データを表示するように構成されたディスプレイコントローラ、グラフィックス処理ユニット（graphics processing units、ＧＰＵ）、映像エンコーダ／デコーダ、スケーラ、ローテータ、ブレンダなどを含み得る。周辺装置２５０は、マイクロフォン、スピーカ、マイクロフォン及びスピーカに対するインタフェース、オーディオプロセッサ、デジタル信号プロセッサ、ミキサなどの音声周辺装置を含み得る。周辺装置２５０は、ユニバーサルシリアルバス（Universal Serial Bus、ＵＳＢ）、ＰＣＩエクスプレス（PCI Express、ＰＣＩｅ）を含む周辺構成要素相互接続（peripheral component interconnect、ＰＣＩ）、シリアルポート及びパラレルポートなどのインタフェースを含む、各種のインタフェースのためのインタフェースコントローラを含み得る。周辺装置２５０は、メディアアクセスコントローラ（media access controllers、ＭＡＣ）などのネットワーク用周辺装置を含み得る。ハードウェアの任意のセットが含まれてもよい。

【００６２】

通信ファブリック２６０は、デバイス１３０の構成要素間で通信するための任意の通信相互接続及び通信プロトコルであり得る。通信ファブリック２６０は、共有バス構成、クロスバー構成、及びブリッジを有する階層化バス、を含むバスベースであり得る。通信ファブリック２６０はまた、パケットベースとすることもでき、ブリッジを有する階層構造、クロスバー、ポイントツーポイント、又は他の相互接続とすることもできる。

【００６３】

図２は、モバイルデバイス１３０内の構成要素を描写しているが、同様の構成要素は、システム１１０又はモバイルデバイス１６０に関して記載された機能などの本明細書に記載された他の機能を実行するために使用されるコンピュータシステム内に存在し得ることに留意されたい。したがって、これらのシステムはまた、前述したもののようなＣＰＵ、メモリ、様々なネットワークインタフェース、及び周辺装置を含んでもよい。

例示的なペアリング技術

【００６４】

図３は、ペアリング手順のためのユーザ３１０、システム１１０（例えば、制御ユニット１３７を使用する）、アプリケーションプロセッサ１３６、及びＳＥ１３４の間の例示的なメッセージを示す通信図である。いくつかの実施形態では、ペアリング手順は、モバ

イルデバイス１３０によって記憶されている長期公開鍵ｓｙｓｔｅｍ．ＰＫと、システム１１０によって記憶されている長期公開鍵ｓｅ．ＰＫと、をもたらす。次いで、これらの鍵は、例えば、図４を参照して後述するように、様々なトランザクションに使用されてもよい。

【００６５】

図３の手順では、ユーザ３１０は、３０２で、例えば、システムのコンソールインタフェース又は何らかの他の入力デバイスを使用して、システム１１０とのペアリングを開始する。例示された実施形態では、システム１１０は、次いで、３０４で、現在の状態が非ペアリングであること（例えば、システムが別のモバイルデバイスと現在ペアリングされていないこと）をチェックする。他の実施形態では、システム１１０が別のデバイスと既にペアリングされている場合であっても、ペアリングを可能とすることができる。１つのモバイルデバイスのみが一度にペアリングできるようにすると、セキュリティが向上するが、柔軟性を制限し得る（但し、以下で更に詳細に論じられるように、これは、ペアリングされたモバイルデバイスが他のモバイルデバイスを許可できるようにすることによって緩和され得る）。

【００６６】

例示された実施形態では、ユーザ３１０は、システム１１０に認証情報を提出する。これは、ユーザＰＩＮ、パスワード、システムのためのフォブ又は鍵の存在、バイオメトリックなどを含んでもよい。いくつかの実施形態では、複数のタイプの認証情報が必要とされ得る。これにより、無許可の個人がペアリング手順を開始することを防止することができる。一般的に言って、システム１１０は、オーナー鍵をシステムに追加する前にペアリング状態に入る必要があり得、この状態に入る前にユーザがシステムの所有権を証明することを必要とし得る。所有権を証明するための技術は、システム１１０の製造業者によって定義され得る。

【００６７】

例示された実施形態では、３０６で、システム１１０は、認証情報を検証し、それに応じて、短期鍵ペアを生成する。例示された実施形態では、システム１１０は、この時点で「進行状態でのペアリング」に切り替える。他の実施形態では、他の状態が使用されてもよく、その状態は、図に示すものとは異なる時点で入出してもよいことに留意されたい。

【００６８】

例示された実施形態では、鍵ペアは、短期公開鍵ｓｙｓｔｅｍ．ｅＰＫ及び短期秘密鍵ｓｙｓｔｅｍ．ｅＳＫを含む。鍵は、使用が制限されているという意味で「短期」であってもよく、例えば、特定の使用回数だけ有効であり得るか（単一使用のみに有効である実施形態を含む）、又は特定の時間インターバルで有効であり得る。短期鍵は、各トランザクションの終わりに削除されてもよい。短期鍵は、失効後は無効であるので、これは、鍵が何らかの形で傍受された場合に、無許可の個人によって鍵が再使用されることを防止することができる。

【００６９】

例示された実施形態では、ユーザ３１０はまた、３０８で、ＡＰ１３６を介してモバイルデバイス１３０とのペアリング手順を開始する。これは、例えば、タッチスクリーンなどのモバイルデバイス１３０の入力デバイスを使用して実行されてもよい。ユーザは、例えば、アプリケーションを開始し、ペアオプションを選択することによって、ペアリング手順を開始することができる。いくつかの実施形態では、ユーザがペアリングアプリケーションにナビゲートすることを要求する代わりに、モバイルデバイス１３０は、例えば、システム１１０による通信に応じて、ペアリング動作が所望されることを確認するために、ユーザに入力を自動的に促すように構成されている。他の実施形態では、ペアリングプロセスのユーザ開始は、ペアリングが行われるというインジケーションのブロードキャストを回避するために、両方のデバイス上で必要とされ得る。モバイルデバイス１３０はまた、パスワード、バイオメトリックスキャン、ＰＩＮなどの認証情報をユーザに促すことができる。

【００７０】
ペアリング手順の開始に応じて、例示された実施形態では、３１２で、ＡＰ１３６はまた、短期鍵ペアｐｈｏｎｅ．ｅＰＫ及びｐｈｏｎｅ．ｅＳＫを生成する。例示された実施形態では、システム１１０及びＡＰ１３５は、次いで、３１４及び３１６で、これらのそれぞれの生成された短期公開鍵、ｓｙｓｔｅｍ．ｅＰＫ及びｐｈｏｎｅ．ｅＰＫ、を交換する。次いで、各デバイスは、３１８で、交換された公開鍵及びこれらのそれぞれの秘密鍵に基づいて、共有シークレットを導出する。上述のように、ＥＣＤＨを使用して共有シークレットを導出することができる。このプロセスのこの時点で、例示された実施形態では、短期鍵を使用して、システム１１０とモバイルデバイス１３０との間に認証されていないセキュアチャネルが確立されている。他の実施形態では、共有シークレット又は共有鍵を確立するために、他の技術が使用されてもよい。共有シークレットを取得するために開示された技術は、例示的な目的で開示されるが、本開示の範囲を限定することを意図するものではない。

【００７１】
例示された実施形態では、システム１１０は、次いで、３２２で、共有シークレットを使用して暗号化された証明書（ｓｙｓｔｅｍ．Ｃｅｒｔ）を送信する。特定の例示された実施形態では、共有シークレットは、暗号鍵（ＫＥＮＣ）及びメッセージ許可コード（ＫＭＡＣ）を含む。これらは、システム側のｓｙｓｔｅｍ．ｅＳＫ／ｐｈｏｎｅ．ｅＰＫ及びモバイルデバイス側のｐｈｏｎｅ．ｅＳＫ／ｓｙｓｔｅｍ．ｅＰＫから導出された共有対称鍵であってもよい。これらの鍵は、ＡＰ１３６及びシステム１１０のＥＣＵに記憶されてもよく、各トランザクション後に削除されてもよい。例示された実施形態では、表記（ＫＥＮＣ、ＫＭＡＣ）（データ）は、ＫＥＮＣを使用する暗号化動作及びＫＭＡＣを使用するハッシング動作（このハッシュ出力は、鍵交換の完全性を保護するために使用され得る）を意味する。ＡＰ１３６は、例示された実施形態では、３２４で、共有シークレットを使用して、暗号化された証明書ｓｙｓｔｅｍ．Ｃｅｒｔからシステム公開鍵ｓｙｓｔｅｍ．ＰＫを抽出する。

【００７２】
例示された実施形態では、３２６で、ＡＰ１３６は、次いで、新しい鍵ペアをＳＥ１３４から生成するように要求する。例示された実施形態では、ＳＥ１３４は、３２８で、公開鍵／非公開鍵ペアｓｅ．ＳＫ及びｓｅ．ＰＫ並びに対応する証明書ｓｅ．Ｃｅｒｔを生成する。例示された実施形態では、証明書は、公開鍵のためのラッパーであり、これは、公開鍵を記載し、ＳＥ１３４がこのような公開鍵を発行することを許可されていることを示し得る。証明書は、自己署名されていたものでもよく、又は認証局からの証明書に基づいているものでもよい（例えば、ＳＥ１３４が中間機関である場合）。ＳＥ１３５は、３３２で、証明書ｓｅ．ＣｅｒｔをＡＰ１３６に送信し、これは、次いで、共有シークレットを使用して（例示された実施形態では、ＫＥＮＣ及びＫＭＡＣ技術を使用して）証明書を暗号化し、３３４で、セキュアチャネルを介して暗号化された証明書をシステム１１０に送信する。

【００７３】
例示された実施形態では、システム１１０は、次いで、３３６で、ＭＡＣを検証し、証明書ｓｅ．Ｃｅｒｔを復号する。システム１１０は、次いで、モバイルデバイスと関連付けられた許可されたエンティティからのルート証明書（例えば、モバイルデバイス１３０の製造業者又はＯＥＭから取得される）を使用してｓｅ．Ｃｅｒｔを検証し、ｓｅ．Ｃｅｒｔから公開鍵ｓｅ．ＰＫを抽出する。いくつかの実施形態では、モバイルデバイス１３０の製造業者は、そのルート証明書を様々なシステム製造業者に提供して、この手順を容易にすることができる。

【００７４】
例示された実施形態では、次いで、３３８で、テキスト確認が実行され（他の実施形態では、このステップは、省略されてもよい）、モバイルデバイス１３０及びシステム１１０の両方が共有シークレットに基づいてテキスト情報を生成し、テキスト情報をユーザに

表示する。例示された実施形態では、ユーザは、次いで、テキストが両方のデバイス上で同一であることをシステム１１０に示す。これは、ペアリング手順中に、（例えば、表示されたテキストを一致させなくする、）無許可のエンティティによる改ざんを検出及び回避するために使用されてもよい。

【００７５】

例示された実施形態では、システム１１０は、次いで、３４２で、オーナー資格（例えば、モバイルデバイス１３０がどの動作を実行することを許可されているかを指定する情報）と共にｓｅ．ＰＫを記憶する。この長期ＳＥ公開鍵は、モバイルデバイス１３０からの今後の要求を認証するために使用され得る。モバイルデバイス１３０のオーナー資格の例としては、ドアを開く、エンジンを始動する、システム１１０から鍵（例えば、オーナー鍵及び友人鍵）を追加／削除する、別の関係者に鍵共有を委任する、資格を変更する、システムをペアリングされていない状態に設定する、鍵チェーンデータ（例えば、ウェブサイトユーザ名、パスワード、ＷＬＡＮネットワーク情報、決済情報など）にアクセスする、システム１１０内で購入を実行する、他の暗号動作を実行するなどが含まれ得るが、これらに限定されない。例示された実施形態では、システム１１０はまた、ペアリングされた状態に切り替えられ、これにより、後続のペアリングを防止し得る（例えば、モバイルデバイス１３０がペアリングされなくなるまで）。いくつかの実施形態では、所有権の移転は、（例えば、図５の手順を使用して）オーナー資格を新しいユーザに付与し、次いで、ペアリングされていない状態に遷移することなく、以前のオーナーの鍵を取り消すことによって実行されてもよい。他の実施形態では、ペアリングされていない状態への遷移は、所有権を別のモバイルデバイスに移転するために必要とされ得る。

【００７６】

いくつかの実施形態では、システム１１０とのペアリングのために回転ＰＩＮが使用される。例えば、システム１１０は、ペアリングに成功した際に新しいＰＩＮをユーザに表示することができ、新しいＰＩＮは、別のモバイルデバイスとの別のペアリングの前にユーザによって入力される必要がある。これにより、無許可のユーザによって開始されたペアリングを防止することができる。

【００７７】

様々な動作は、ＡＰ１３６、ＳＥ１３４、又はＳＥＰ２１０のうちのものによって実行されるものとして本明細書で論じられる。これらの実施形態は、説明の目的で議論されるが、本開示の範囲を限定することを意図するものではない。他の実施形態では、これらのプロセッサのうちの１つによって実行されるように記載されたアクションは、これらのプロセッサ及び／又は他の処理要素のうちの他のもの又は組み合わせによって実行されてもよい。一例として、追加のセキュリティが所望される場合、ＳＥＰ２１０を使用して、ＳＥ１３４によって実行されるように記載された様々な動作のために、バイオメトリック認証を要求する場合がある。更に、本明細書で開示する様々な通信図でのメッセージの順序及びタイプは、本開示の範囲を限定することを意図するものではない。様々な実施形態では、同様のメッセージが異なる順序で送信されてもよく、開示されたメッセージが省略されてもよく、及び／又は追加のメッセージが利用されてもよい。

【００７８】

いくつかの実施形態では、ユーザはまた、システム１１０をペアリングされていない状態に遷移させることができる、ペアリング解除動作を開始し得る。これを使用して、例えば、システムの所有権を移転するために、又はユーザが新しいモバイルデバイスを購入した場合に、新しいデバイスをシステム１１０のオーナーデバイスとして登録することができる。このプロセスのために、モバイルデバイス１３０は、非公開鍵ｓｅ．ＳＫで認証しながら特定のコマンドを送信することができる。いくつかの実施形態では、ペアリング解除はまた、システム１１０のインタフェースを介して、例えば、最後のペアリング動作から新しいＰＩＮを入力することによって、実行され得る。

【００７９】

いくつかの実施形態では、システム１１０は、図３の動作中に「ペアリング」状態で動

作し、この状態でペアリング要求を拒否するように構成されている。いくつかの実施形態では、システム１１０は、多数のペアリング試行が失敗した後に（数は、設定可能であり得る）、ブロックされた状態に遷移するように構成されている。ブロックされた状態では、ユーザは、製造業者に連絡して、リカバリＰＩＮを取得する必要があり得、リカバリＰＩＮは、所有権の証明を示した後にのみ提供され得る。

【００８０】

いくつかの実施形態では、帯域外通信を使用して、セキュアチャネルを確立することができる。例えば、システム１１０は、例えば、モバイルデバイス１３０のカメラを使用して、画像、テキスト、又はアニメーションをスキャンすることによって、パスワードを動的に生成し、パスワードを帯域外のモバイルデバイス１３０に転送することができる。画像、テキスト、又は情報は、例えば、システム１１０のマルチメディアシステム上に表示され得る。この帯域外共有シークレットは、認証されていないセキュアチャネルを確立するために、セキュアリモートパスワード（secure remote password、ＳＲＰ）などのパスワード認証鍵交換（password authenticated key exchange、ＰＡＫＥ）技術と共に使用され得る。これらの実施形態では、システム１１０によって表示されたテキストとモバイルデバイス１３０によって表示されたテキストとの間のユーザによるテキストマッチングは、例えば、帯域外通信が中間者攻撃を防止し得るため、省略され得る。

【００８１】

いくつかの実施形態では、ＢＬＵＥＴＯＯＴＨペアリングなどの既存のペアリングを使用して、モバイルデバイス１３０からシステム１１０にｓｅ．Ｃｅｒｔを転送することができる。

例示的な動作許可技術

【００８２】

図４は、システム１１０によって動作を許可するためのシステム１１０（例えば、制御ユニット１３７を介して）、アプリケーションプロセッサ１３６、及びＳＥ１３４の間の例示的なメッセージを示す通信図である。例示された実施形態では、通信を使用して、システム１１０によって実行されるべき動作を指定するモバイルデバイス１３０からのコマンドを認証する。

【００８３】

例示された実施形態では、４０２で、システム１１０は、ＡＰ１３６との通信を開始する。いくつかの実施形態では、これは、ポーリングメッセージ（例えば、ＮＦＣ衝突防止拡張非接触ポーリング（enhanced contactless polling、ＥＣＰ）メッセージ）を送信することを含む。他の実施形態では、他の通信開始技術が使用されてもよい。それに応じて、例示された実施形態では、ＡＰ１３６は、４０４で、短期鍵ペアｐｈｏｎｅ．ｅＳＫ及びｐｈｏｎｅ．ｅＰＫを生成する（但し、他の実施形態では、ＳＥ１３４などの他の処理要素が短期鍵ペアを生成し得る）。鍵ペアの例としては、楕円曲線暗号法（elliptic curve cryptography、ＥＣＣ）ペア、ＡＥＳ暗号化を使用して生成されたペアなどが挙げられる。例示された実施形態では、ＡＰ１３６は、４０６で、この鍵ペア及びチャネルネゴシエーションオプションをシステム１１０に送信する。いくつかの実施形態では、システム１１０と通信距離内にあると判定したことに応じて、モバイルデバイス１３０は、システム１１０に対する１つ以上のコマンドの入力をユーザに自動的に促すことができる。

【００８４】

例示された実施形態では、４０８で、システム１１０はまた、短期鍵ペア（ｓｙｓｔｅｍ．ｅＳＫ及びｓｙｓｔｅｍ．ｅＰＫ）を生成し、システム１１０とのセキュア通信に使用するためのＫＥＮＣ及びＫＭＡＣを導出する。（いくつかの実施形態では、この鍵ペアのためにＥＣＣを使用してもよい）。例示された実施形態では、システム１１０はまた、ｓｙｓｔｅｍ．ｅＰＫ及びｐｈｏｎｅ．ｅＰＫ短期公開鍵を含み、ｓｙｓｔｅｍ．ＳＫで署名された、ｓｙｓｔｅｍ．ｅＣｅｒｔ証明書を生成する。

【００８５】

例示された実施形態では、４１２で、システム１１０はまた、次の情報を生成する。要

求された動作、理由、及びチャレンジを含むデータ構造である動作辞書（operation dictionary、ＯＤ）。この場合、動作は、チャレンジの署名であり得る（例えば、システム１１０は、チャレンジがＳＥ１３４の秘密鍵を使用してＳＥ１３４によって署名されることを要求している）。この理由は、システムによって実行されるべき動作を指定することができる（例えば、物理アクセスを可能にするか、又はシステムの駆動を可能にする）。システム１１０は、次いで、ＫＥＮＣ及びＫＭＡＣを使用して、ＯＤを暗号化及びＭＡＣし、また、４２４で、公開鍵ｓｙｓｔｅｍ．ＰＫの証明書ｓｙｓｔｅｍ．ｅＣｅｒｔを送信する。ＡＰ１３６は、公開鍵ｓｙｓｔｅｍ．ＰＫを使用して、（例えば、ペアリングプロセス中に記憶されるように）ｓｙｓｔｅｍ．ｅＣｅｒｔを検証し、ｓｙｓｔｅｍ．ｅＣｅｒｔから短期公開鍵ｓｙｓｔｅｍ．ｅＰＫを抽出する。ＡＰ１３６はまた、ｓｙｓｔｅｍ．ｅＰＫ及びｐｈｏｎｅ．ｅＳＫを使用して、共有シークレット（本実施形態では、ＫＥＮＣ及びＫＭＡＣ）を導出する。ＡＰ１３６は、次いで、４２６で、ＫＥＮＣを使用して、ＭＡＣを検証し、ＯＤを復号する。図４のセキュアチャネルは、プライバシー目的のために使用されてもよいことに留意されたい。

【００８６】

例示された実施形態では、ＡＰ１３６は、次いで、４２８で、ＳＥ１３４からのＯＤの署名を要求する。ＳＥ１３４は、４３２で、秘密鍵ｓｅ．ＳＫを用いてＯＤに署名することにより、ＯＤＳｉｇｎａｔｕｒｅを計算し、４３４で、ＯＤＳｉｇｎａｔｕｒｅをＡＰ１３６に返す。例示された実施形態では、署名は、ＯＤにおけるチャレンジであり得る。長期秘密鍵ｓｅ．ＳＫを使用する暗号化により、プライバシー保護が必要なデータが中間者攻撃で漏洩するのを防ぐことができ、盗聴者への漏洩なしで、電話が固有の識別子又は証明書をシステム１１０と共有することを可能にし得る。いくつかの実施形態では、モバイルデバイス１３０は、署名ステップのためのユーザ認証、例えば、署名のためのＳＥＰ２１０を使用するバイオメトリック認証を要求するように更に構成されている。概して、モバイルデバイス１３０は、いくつかの実施形態では、このステップでｔｏｕｃｈ　ＩＤ又は他のユーザ検証を要求するように構成されてもよい。

【００８７】

例示された実施形態では、ＡＰ１３６は、次いで、コマンド（いくつかの実施形態では、これは、システム１１０によって実行されるはずの所望の動作（単数又は複数）を示す）を設定し、４３６で、システム１１０への応答をＭＡＣ及び暗号化する。例示された実施形態では、４３８で、応答は、ＯＤＳｉｇｎａｔｕｒｅ、公開鍵ｓｅ．ＰＫのハッシュ、及びコマンドを含む。これは、確立されたセキュアチャネルを利用することができ、システム１１０がモバイルデバイス１３０を認証することを可能にし得る。様々な実施形態では、暗号化すること及びＭＡＣすることの両方が論じられているが、他の実施形態では、ＭＡＣを使用せずに秘密鍵を使用して暗号化することが使用され得ることに留意されたい。

【００８８】

例示された実施形態では、４４２で、システム１１０は、共有シークレットのＫＭＡＣ部分を使用してＭＡＣを検証し、共有シークレットのＫＥＮＣ部分を使用してＯＤＳｉｇｎａｔｕｒｅを復号し、（ペアリング手順中に受信及び記憶されたままの）ｓｅ．ＰＫを使用してＯＤＳｉｇｎａｔｕｒｅを検証する。例示された実施形態では、システム１１０は、関連付けられたアクセスポリシーを適用する（例えば、ユーザが要求された動作（単数又は複数）を実行することを許可されているかどうかを判定し、ユーザが許可されている場合にコマンドを実行する。例えば、システム１１０は、ドアをロック解除して内部へのアクセスを可能にし、システムが駆動されることを可能にし、アラームを無効にすることなどを可能にし得る。

【００８９】

いくつかの実施形態では、開示された技術は、モバイルデバイス１３０が、ユーザの同意なしで、（例えば、モバイルデバイスを不正な無線機を使用して追跡することを可能にし得る）固有の識別子又はデータを解放するのを防止する。特に、公開鍵証明書、公開鍵

ハッシュ、又は他の種類の鍵／デバイス固有の識別子を使用して、ユーザデバイスを追跡することができるが、開示された技術は、この情報を交換する前にセキュアチャネルを確立することによって、及び／又はこの情報を送信する前にシステムを認証することによって、この情報が傍受されるのを防止することができる。

【００９０】

いくつかの実施形態では、開示された技術は、前方秘匿特性を有し、これにより、長期鍵の取得に成功した攻撃者が過去の通信を復号することができなくなる。いくつかの実施形態では、この特性は、各側に短期鍵を使用することによって達成される。他の実施形態では、より緩和した前方秘匿特性が、システム側で長期鍵及びモバイルデバイス側で短期鍵を使用して実施されてもよい。これにより、システム側での実施を簡略化することができる。

【００９１】

いくつかの実施形態では、ＡＰ１３６によって実行されるものとして記載された動作（例えば、セキュアチャネルの確立）は、ＳＥ１３４によって実行されてもよく、これにより、システム１１０の制御に関して柔軟性が低減し得るが、全体的なセキュリティを改善することができる。

【００９２】

様々な実施形態では、デバイス１３０の認証に加えて、ユーザ認証が実行されてもよい。認証は、無許可のユーザがモバイルデバイス１３０を使用して、システム１１０に許可を付与するのを防止することができる。認証は、例えば、ＳＥＰ２１０によって少なくとも部分的に実行されてもよく、これにより、認証が完了するまで、ＳＥ１３４がペアリング又は認可セッションのための更なる通信を実行するのを防止することができる。いくつかの実施形態では、バイオメトリックテンプレートは、システムに含まれるセキュア回路に記憶されてもよく、バイオメトリック認証の少なくとも一部分を実行するように構成されてもよい。他の実施形態では、バイオメトリック認証は、モバイルデバイスによって完全に処理されてもよい。他の実施形態では、モバイルデバイス１６０の認証は、例えば、システムアクセスの目的で、ユーザが自身のモバイルデバイスを別のユーザに物理的に貸すことを可能にするために、モバイルデバイス１６０のユーザを認証することなく実行されてもよい。

別のモバイルデバイスへの例示的な許可

【００９３】

図５は、別のモバイルデバイス１６０に許可を付与するためのシステム１１０、アプリケーションプロセッサ１３６、及びＳＥ１３４の間の例示的なメッセージを示す通信図である。ｓｈａｒｅｅデバイス（許可が共有されているデバイス）に許可を付与するための追加の実施形態について、図１５を参照して以下で論じる。

【００９４】

例示された実施形態では、５０２で、システム１１０のオーナーのＡＰ１３６は、別のモバイルデバイスに対して許可されるべき資格のセットを選択する。例えば、オーナーは、他のモバイルデバイスで利用可能な制限速度、他のモバイルデバイスがシステム１１０にアクセスする時間帯などを制限することができる。「オーナー」という用語は、便宜上本明細書で使用されるが、モバイルデバイスがシステム１１０と以前にペアリングされている限り、ＡＰ１３６及びＳＥ１３４は、実際にシステム１１０を所有しないユーザのモバイルデバイスに含まれてもよいことに留意されたい。

【００９５】

例示された実施形態では、オーナーＡＰ１３６は、５０４で、鍵共有が所望されるという通知と、他のＡＰ５３６に資格を指定する情報とを送信する（例示された実施形態では、他のＡＰ５３６及び他のＳＥ５３４は、別のモバイルデバイス１６０に含まれる）。ＡＰ５３６は、５０６で、資格情報及び鍵ペア生成要求をＳＥ５３４に送信し、これにより、５０８で、公開鍵／非公開鍵（ｓｅ＿ｏｔｈｅｒ．ＳＫ及びｓｅ＿ｏｔｈｅｒ．ＰＫのペア）並びに対応する証明書ｓｅ＿ｏｔｈｅｒ．Ｃｅｒｔを生成する。例示された実施形

態では、ＳＥ５３４はまた、資格を証明書に埋め込む（これにより、資格への無許可の変更を防止することができる）。ＳＥ５３４は、次いで、５１２で、ｓｅ＿ｏｔｈｅｒ．ＣｅｒｔをＡＰ５３６に返送し、５１４で、それを署名要求と共にＡＰ１３６へ転送する。

【００９６】

例示された実施形態では、５１６で、ＡＰ１３６は、（例えば、モバイルデバイス１６０の電話製造業者からの）ルート証明書を使用してｓｅ＿ｏｔｈｅｒ．Ｃｅｒｔをチェックし、（例えば、変更されていないことを確実するために）資格をチェックし、ユーザを認証する。認証としては、バイオメトリック認証、ＰＩＮ、ユーザ名／パスワードの組み合わせなどを挙げてもよい。ＡＰ１３６は、次いで、５１８で、署名要求及びｓｅ＿ｏｔｈｅｒ．ＣｅｒｔをＳＥ１３４に送信し、これにより、５２２で、証明書をｓｅ．ＳＫで署名し、５２４で、署名付き証明書ｓｅ＿ｏｔｈｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅをＡＰ１３６に返送する。モバイルデバイス間の通信は、ローカルに（例えば、ＮＦＣ若しくはＢｌｕｅｔｏｏｔｈなどの直接無線接続を介して）又はネットワークを介して実行されてもよい。一般的に言って、本明細書で論じられるデバイス間の様々な通信は、リモートで、又は例えば、ローカル直接無線接続を介してごく近接して実行されてもよい。

【００９７】

例示された実施形態では、ＡＰ１３６は、５２６で、署名をＡＰ５３６に送信し、これは、次いで、５２８で、システム１１０とのアクセストランザクションにおいて鍵識別子として署名を使用する。システム１１０は、署名内の資格をチェックして、資格を強化することができる。モバイルデバイス１６０によるトランザクションは、例えば、図４のトランザクションと同様に実行されてもよい。このようにして、モバイルデバイス１３０のユーザは、モバイルデバイス１６０を安全に許可して、システム１１０を使用して特定の動作のセットを実行させることができる。これは、友人、家族、借り主などがシステム１１０にアクセスできるようにするために使用され得る。ライドシェアリングコンテキストでは、モバイルデバイス１６０は、システム１１０へのアクセスを借りる又は共有する個人又はエンティティであり得る。

【００９８】

いくつかの実施形態では、鍵共有は、共有ネットワークの管理会社などのサードパーティに委任されてもよい。このシナリオでは、サーバは、（例えば、モバイルデバイスの１６０によって生成される代わりに）鍵ペアを生成することができ、これにより、オーナーデバイスは、共有ネットワークのルート証明書を使用して公開鍵の発信元を検証することができる。管理会社には、次の資格が与えられ得る。例えば、ドアを開く、エンジンを始動する、システム１１０へ／から友人公開鍵を追加／削除する、及び失効日。

【００９９】

更に、いくつかの実施形態では、モバイルデバイス１３０は、ユーザ入力に応じて、他のモバイルデバイス（単数又は複数）のための特定の鍵を取り消すように構成されている。これらの実施形態では、システム１１０は、対応する証明書を除去するか、又は取り消されたものとしてマークする（これにより、証明書は、所望であれば、後で再有効化することができる）。一度取り消されると、他のモバイルデバイスが動作を実行するようにシステム１１０に命令しようと試みても、トランザクションは、承認されないだろう。いくつかの実施形態では、オーナーモバイルデバイスがシステム１１０からペアリングされていない場合、システム１１０はまた、許可された任意の友人鍵を取り消すように構成されている。

【０１００】

いくつかの実施形態では、許可された友人の資格としては、ドアを開く、エンジンを始動する、システムから公開鍵を除去する、鍵失効日、制限速度、場所制限、時間制限などが含まれ得るが、これらに限定されない。

【０１０１】

いくつかの実施形態では、システム製造業者などの別の関係者は、どの動作がシステムによって許可されているかに関する入力（例えば、新しい鍵又は新しいオーナーペアリン

グを追加する）を望み得る。これにより、製造業者は、例えば、保証目的のための所有権の変更をより良好に追跡できるようになる。これらの実施形態では、特定の動作のためにユーザのデバイスによって実行される署名に加えて、他の関係者のサーバからの署名もまた、特定の動作を実行する前にシステム１１０によって要求されてもよい。

【０１０２】

様々な開示された実施形態では、ペアリング及び鍵共有は、オフラインで実行されてもよい（例えば、システムが広域ネットワークに接続されていない場合）。非公開鍵は、モバイルデバイスに埋め込まれたセキュア要素又はＳＥＰから離れることはできず、これにより、改ざんを防止することができる。更に、開示された技術は、従来の技術に対するアクセストランザクションに必要とされる交換数を低減することができる。開示された技術は、信頼されていないチャネルを介してでもセキュリティを提供することができる。また、開示された技術は、能動的及び受動的な盗聴者の両方に対する保護を提供することができる。

【０１０３】

以下の表は、いくつかの実施形態に係る、本明細書で開示する様々な動作に使用され得る非限定的な例示的な暗号法アルゴリズムを提供する。

【表１】

システム上での短期鍵ペア生成 （system. ePK、system. eSK） 電話上での短期鍵ペア生成 （phone. ePK、phone. eSK） システム上での長期鍵ペア生成 （system. PK、system. SK） 電話上での長期鍵ペア生成 （phone. PK、phone. SK） SE上での長期鍵ペア生成 （se. PK、se. SK）	NIST Ｐ－256を用いるECC （コンパクト又は圧縮表現をサポートし得る）
対称セッション鍵（KENC. KMAC）	AES 256 GCM AES 256 CCM AES 128 GCM AES 128 CCM
KDF鍵導出関数	SHA 256 AES 256 CBC
対称セッション鍵生成	TR－03111、X9. 63 KDFに定義されるECKA
オーナーペアリングのためのPAKE	SRP
イモビライザートークン共有	NIST Ｐ－256を用いるECIES
DHディフィー・ヘルマン	NIST Ｐ－256を用いるECDH
ペアリングのための表示可能なテキスト導出	共有シークレットを介するSHA－512

例示的なオンライン動作

【０１０４】

前述の様々な実施形態は、互いに近くにあるデバイス間で、オフラインで（例えば、広域ネットワーク接続なしで）実行されてもよい。いくつかの実施形態では、システム製造業者はまた、遠隔動作の実行のために、広域ネットワーク（例えば、インターネット）を介した通信を可能にし得る。いくつかの実施形態では、製造業者又はいくつかの他のエンティティは、ネットワークアクセスを提供するプロキシとして機能してもよく、これにより、システムはネットワークに直接公開されない。エンティティは、システム認証をエンティティのサーバに要求することができる。友人鍵をシステムに追加するためのオンライン技術について、以下で論じる（友人鍵はまた、本明細書では、ｓｈａｒｅｅ鍵とも称され得、「友人」という用語は、便宜上使用されるが、ｓｈａｒｅｅ／友人とオーナーとの間の任意の特定の関係を暗示することを意図するものではない）。他の実施形態では、同

様のオンライン技術が、とりわけ、本明細書で論じられる様々な他の動作のいずれかに使用され得る。

【０１０５】

いくつかの実施形態では、制御ユニット１３７に記憶された公開鍵は、例えば、ベストエフォート基準でサーバと同期される。例えば、新しいオーナーがペアリングされるたびに、及び新しい友人鍵が追加されるたびに、システム１１０は、その記憶された公開鍵をサーバと同期するよう試みるように構成されてもよい。いくつかの実施形態では、システム１１０は、インターネットを介してシステム１１０に到達する方法として使用される、非秘密の固有の識別子及び統一資源識別子（uniform resource identifier、ＵＲＩ）を提供するように構成されている。これにより、（例えば、デバイス１３０がサーバを認証できるようにするために、トランスポートレイヤセキュリティ（transport layer security、ＴＬＳ）などのプロトコルを使用して）モバイルデバイス１３０がサーバとのセキュアセッションを確立できるようにし得る。セッションが確立されると、デバイス１３０は、ＳＥ１３４を使用して、システム１１０によって提供されたチャレンジ及び／又はシステム１１０によって実行されるべきコマンドに署名することができる。サーバは、パケットフォーマット及び署名をチェックするプロキシとして機能してから、システム１１０に要求を送信することができる。サーバはまた、サービス妨害攻撃又は不正な形式のパケットに対するファイアウォールタイプの保護を提供してもよい。いくつかの実施形態では、デバイス１３０のサーバ認証は、デバイス１３０がサーバチャレンジに有効な鍵で正常に署名した後にクライアント認証を含んでもよい。

【０１０６】

いくつかの実施形態では、システム製造業者などのエンティティは、例えば、新しい鍵又はオーナーペアリングの発行など、本明細書に記載された様々な動作の監視を望む場合がある。これらの実施形態では、オーナーデバイス又は友人デバイスによって提供された署名に加えて、システム１１０はまた、特定の動作を実行する前に、エンティティのサーバ（単数又は複数）からの署名を要求し得る。しかしながら、この監視は、これらの動作がオフラインで実行されるのを防止することができる。

【０１０７】

例えば、サーバは、新しい鍵が発行されたことをモバイルデバイス１３０、デバイス１６０、及び／又はシステム１１０によって通知される場合があり、これにより、サーバ署名を取り出すために、関与する関係者のうちの少なくとも１つがオンライン（サーバと接続される）である必要がある。関与するデバイスのいずれもサーバに到達できない場合、これらの実施形態では、システム１１０は、署名がエンティティから取り出せるまで、新しい鍵を限定された機能で使用できるようにし得る。例えば、新しい友人ユーザは、システムにアクセスできるが、オンライン許可が完了するまでは、閾値速度まで、かつ指定された場所の閾値距離内でのみ駆動でき得る。いくつかの実施形態では、サーバは、例えば、サーバが利用不可能になった場合に、サーバ署名に関する要件をリモートで無効にするように構成されている。

【０１０８】

図６Ａ～図６Ｂは、いくつかの実施形態に係る、サーバ６１０の関与を伴う例示的な通信を示す。図６Ｂは、図６Ａにおける通信の続きであることに留意されたい。

【０１０９】

例示された実施形態では、ＡＰ１３６が６２０でｓｅ＿ｏｔｈｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅを受信するまで、図５を参照して前述したように通信を進める。その時点で、例示された実施形態では、６２２で、サーバ６１０への（例えば、インターネットを介した）ネットワーク接続が利用可能である場合、ＡＰ１３６は、ｓｅ＿ｏｔｈｅｒ．Ｃｅｒｔ及びｓｅ＿ｏｔｈｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅのサーバ署名を要求する。そうである場合、サーバ６１０は、ｓｅ＿ｏｔｈｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅをチェックし、６２４で、ｓｅ＿ｏｔｈｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅが有効である場合、ｓｅ＿ｏｔｈｅｒ．Ｃｅｒｔに署名する。例示された実施形態では、サーバ６１０はまた、失

効時間までｓｅ＿ｏｔｈｅｒ．Ｃｅｒｔを記憶する。サーバ６１０は、次いで、６２６で、ｓｅ＿ｏｔｈｅｒＳｅｒｖｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅをＡＰ１３６に送信する。

【０１１０】

例示された実施形態では、ＡＰ１３６は、６２８で、ｓｅ＿ｏｔｈｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅ及びｓｅ＿ｏｔｈｅｒＳｅｒｖｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅを他のＡＰ５３６に送信する（サーバ署名が受信された場合、そうでなければＡＰ１３６がサーバ署名なしで第１の署名を送信する）。ｓｅ＿ｏｔｈｅｒＳｅｒｖｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅが提供されない場合、例示された実施形態では、６３２で、ＡＰ５３６がサーバ６１０からの署名を要求するように構成されている。

【０１１１】

次に図６Ｂを参照すると、サーバ６１０は、６３４で、ＡＰ１３６からの要求と同様に、ＡＰ５３６からの要求を処理し得る。例示された実施形態では、ＡＰ５３６は、次いで、６３８で、システム１１０とのトランザクションを開始し、ｓｅ＿ｏｔｈｅｒ．Ｃｅｒｔ、ｓｅ＿ｏｔｈｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅ、及びｓｅ＿ｏｔｈｅｒＳｅｒｖｅｒＣｅｒｔＳｉｇｎａｔｕｒｅを送信する（サーバ署名が受信された場合、そうでなければ省略されてもよい）。

【０１１２】

例示された実施形態では、システム１１０は、受信されなかった場合、６４４で、サーバ署名を要求し、接続が利用可能である場合、６４８で、サーバ６１０からの応答を受信する。システム１１０は、次いで、６５２で、存在する場合に、ｓｅ＿ｏｔｈｅｒＳｅｒｖｅｒ．ＣｅｒｔＳｉｇｎａｔｕｒｅをチェックし、またｓｅ＿ｏｔｈｅｒＣｅｒｔＳｉｇｎａｔｕｒｅもチェックする。両方の署名が検証される場合、システム１１０は、トランザクションに対してｓｅ＿ｏｔｈｅｒ．Ｃｅｒｔの資格を適用するように構成されている。サーバ署名が取得できなかった場合、システム１１０は、トランザクションに対してより制限された資格のセットを許可するように構成されてもよい（又はトランザクションを完全に拒否してもよい）。

【０１１３】

図６Ａ～図６Ｂの実施例のトランザクションに関与する各デバイスは、サーバ６１０からの署名を要求するように構成されているが、他の実施形態では、そうでない場合がある。更に、サーバ署名を要求するために、他のデバイスによって同様の技術が使用されてもよい。様々な実施形態では、開示された技術は、サーバ６１０がシステム１１０とのトランザクションをセキュアな方法で監視できるようにし得る。

【０１１４】

いくつかの実施形態では、大規模なペアリングにより、エンティティは一連のシステムを管理することができる。例えば、オーナー鍵は、エンティティのサーバ（単数又は複数）上に生成されてもよく、公開鍵は、製造中にシステムプロセッサ（例えば、ＥＣＵ）に個別に記憶されてもよい。いくつかの実施形態では、同一の公開鍵が全システムにプッシュされ、その後、本明細書に記載された所有権移転技術を使用して転送され得る。

【０１１５】

システム製造業者は、生産中にシステムプロセッサ（例えば、ＥＣＵ）内にルート証明書をプロビジョニングすることができる。製造業者はまた、例えば、他の電話製造業者をサポートするために、生産後に新しい証明書をプッシュしてもよい。これらの証明書は、セキュア要素製造業者、電話製造業者、及び／又はシステム製造業者のためのルート証明書を含んでもよい。

例示的な方法

【０１１６】

図７Ａは、いくつかの実施形態に係る、モバイルデバイスによってシステムとペアリングする方法を示すフローチャートである。図７Ａに示す方法は、とりわけ、本明細書で開示するコンピュータ回路、システム、デバイス、要素又は構成要素のいずれかと共に使用

することができる。様々な実施形態では、図示の方法要素の一部は、同時に実行してもよく、図示のものとは異なる順序で実行してもよく、又は省略してもよい。必要に応じて、追加の方法要素をも実行してもよい。

【０１１７】

７１０で、例示された実施形態では、システムとのペアリング動作を実行するための第１の要求を受信したことに応じて、モバイルデバイスは、システムとの第１の共有暗号鍵を確立する。これは、短期鍵ペアを確立することと、短期鍵ペアに基づいて共有シークレットを導出することと、を含み得る。共有シークレットを導出することは、ＥＣＤＨ又はいくつかの他の非対称暗号化技術を使用し得る。ペアリング動作を実行する要求は、システムから又はユーザから（例えば、入力構成要素を介して）受信され得る。車両及びモバイル電話電話に関して、様々な実施形態が本明細書に記載されることに留意されたい。これらのデバイスは、例示的な目的で含まれるが、本開示の範囲を限定することを意図するものではない。様々な実施形態では、開示された技術は、様々なタイプのデバイスのうちの２つ以上の間での相互認証のために使用され得る。例えば、同様の技術を使用して、ペアリングされたウェアラブルデバイス、分散センサ、モノのインターネットのデバイスなどを用いてデバイスを認証することができる。

【０１１８】

７２０で、例示された実施形態では、セキュア回路（例えば、ＳＥ１３４又はＳＥＰ２１０）は、公開鍵ペアと、公開鍵ペアの公開鍵を含む、公開鍵ペアに対応する証明書（例えば、ｓｅ．Ｃｅｒｔ）と、を生成する。いくつかの実施形態では、これは、セキュア回路によって実行される。

【０１１９】

７３０で、例示された実施形態では、モバイルデバイスは、第１の共有鍵を使用して証明書を暗号化する。

【０１２０】

７４０で、例示された実施形態では、モバイルデバイスは、暗号化された証明書をシステムに送信する。これは、モバイルデバイス側からのペアリングプロセスを終了することができる。他の実施形態では、モバイルデバイスは、成功したペアリングのインジケーションを受信することができる。

【０１２１】

いくつかの実施形態では、モバイルデバイスは、公開鍵ペアに基づいて生成された値を表示し、モバイルデバイスのユーザに、システムもまた値を表示していることを確認するように要求するように構成されている。これにより、いくつかの実施形態では、意図されない又は悪意のあるペアリングを回避することができる。

【０１２２】

いくつかの実施形態では、別のモバイルデバイスがシステムにアクセスできるようにする第２の要求に応じて、モバイルデバイスは、公開鍵ペアの非公開鍵を使用して、他のモバイルデバイスのセキュア回路によって生成された別の公開鍵ペアの証明書に署名する。いくつかの実施形態では、モバイルデバイスは、広域ネットワークを介して、セキュア回路によって署名された証明書のサーバ署名を要求し、サーバ署名は、他のモバイルデバイスによって要求された動作を許可するかどうかを判定するために、システムによって使用可能である。

【０１２３】

いくつかの実施形態では、モバイルデバイスは、モバイルデバイスがモバイルデバイスのユーザによって指定された資格のセットのうちのものに許可されているかどうかを示す。

【０１２４】

図７Ｂは、いくつかの実施形態に係る、システムによってモバイルデバイスとペアリングする方法を示すフローチャートである。図７Ｂに示す方法は、とりわけ、本明細書で開示するコンピュータ回路、システム、デバイス、要素又は構成要素のいずれかと共に使用

することができる。様々な実施形態では、図示の方法要素の一部は、同時に実行してもよく、図示のものとは異なる順序で実行してもよく、又は省略してもよい。必要に応じて、追加の方法要素をも実行してもよい。

【０１２５】

７５０で、例示された実施形態では、システムの処理要素は、モバイルデバイスとの第１の共有暗号鍵（これは、例えば、図７Ａの要素７１０の鍵であり得る）を確立する。

【０１２６】

７６０で、例示された実施形態では、システムの処理要素は、第１の公開鍵ペアに対応し、そのペアの公開鍵を含むモバイルデバイスから暗号化された証明書を受信する。公開鍵ペアは、例えば、モバイルデバイスのセキュア回路によって生成されてもよい。

【０１２７】

７７０で、例示された実施形態では、システムの処理要素は、第１の共有暗号鍵を使用して暗号化された証明書を復号し、復号された証明書を記憶する。

【０１２８】

図８Ａは、いくつかの実施形態に係る、モバイルデバイスによって認証する方法を示すフローチャートである。図８Ａに示す方法は、とりわけ、本明細書で開示するコンピュータ回路、システム、デバイス、要素又は構成要素のいずれかと共に使用することができる。様々な実施形態では、図示の方法要素の一部は、同時に実行してもよく、図示のものとは異なる順序で実行してもよく、又は省略してもよい。必要に応じて、追加の方法要素をも実行してもよい。

【０１２９】

８１０で、例示された実施形態では、モバイルデバイスは、システムとの第２の共有暗号鍵（これは、例えば、ペアリングに使用される第１の共有暗号鍵とは異なり得る）を確立する。これは、システムからの通信に基づいて、システムの近接を検出することに基づいて、などで実行されてもよい。これは、例えば、短期鍵ペア及びＥＣＤＨの使用を含んでもよい。

【０１３０】

８２０で、例示された実施形態では、モバイルデバイスは、システムからチャレンジを受信し、システムとのペアリングセッション中に確立された公開鍵ペアの非公開鍵（例えば、ｓｅ．ＳＫ）を使用して、システムから受信したチャレンジに対する応答を生成する。例えば、セキュア回路は、秘密鍵を使用してチャレンジに署名することができる。

【０１３１】

８３０で、例示された実施形態では、モバイルデバイスは、第２の共有暗号鍵を使用して応答を暗号化する。

【０１３２】

８４０で、例示された実施形態では、モバイルデバイスは、暗号化された応答をシステムに送信する。

【０１３３】

図８Ｂは、いくつかの実施形態に係る、システムによってモバイルデバイスを認証する方法を示すフローチャートである。図８Ｂに示す方法は、とりわけ、本明細書で開示するコンピュータ回路、システム、デバイス、要素又は構成要素のいずれかと共に使用することができる。様々な実施形態では、図示の方法要素の一部は、同時に実行してもよく、図示のものとは異なる順序で実行してもよく、又は省略してもよい。必要に応じて、追加の方法要素をも実行してもよい。

【０１３４】

８５０で、例示された実施形態では、システムの処理要素は、モバイルデバイスとの第２の共有暗号鍵（例えば、図８Ａの要素８１０の鍵）を確立する。

【０１３５】

８６０で、例示された実施形態では、処理要素は、要求された動作に応じてモバイルデバイスにチャレンジを発行する。動作は、（例えば、システムへの近接に基づいて、）モ

バイルデバイスへの使用入力に基づいて、システムから受信した情報に基づいて、などで、モバイルデバイスによって自動的に要求され得る。チャレンジは、例えば、動作辞書に含まれ得る。チャレンジは、共有暗号鍵を使用して暗号化されてもよい。いくつかの実施形態では、要求された動作を示す情報がチャレンジに含まれ、これは、モバイルデバイスが、要求された動作が実際に所望されているかどうかを確認できるようにし得る。

【０１３６】

８７０で、例示された実施形態では、処理要素は、チャレンジに対する応答を受信し、第２の共有暗号鍵を使用して応答を復号する。

【０１３７】

８８０で、例示された実施形態では、処理要素は、要求された動作を許可する前に、ペアリングセッション中に確立された公開鍵ペアの非公開鍵を使用して、応答がモバイルデバイスによって署名されていることを検証する。例えば、処理要素は、ｓｅ．ＰＫを使用して、応答がｓｅ．ＳＫを使用して署名されたかを検証することができる。いくつかの実施形態では、処理要素は、図８Ｂの１つ以上の要素が失敗した場合に要求された動作を拒否する（例えば、共有暗号鍵が正常に確立されていない、チャレンジに対する応答が不正確である、チャレンジに対する応答が適切に署名されていない、など。

例示的なマルチトランザクションタイプの実施形態

【０１３８】

いくつかの実施形態では、複数のタイプの認証トランザクションがサポートされる。図９Ａ～図９Ｃは、２つのタイプのトランザクション（これらは、本明細書では、「標準」及び「高速」トランザクションと称され得る）を用いる例示的なトランザクションフローを示す通信図である。いくつかの実施形態では、標準トランザクションは、予め確立された対称鍵を伴わないが、１つ以上の後続の高速対称トランザクションで使用するために記憶され利用可能なこのような鍵を生成するために使用されてもよい。図９Ｂ及び図９Ｃは、図９Ａで開始された通信の続きであることに留意されたい。

【０１３９】

図９Ａで、システム１１０及びモバイルデバイス１３０は、それぞれの短期鍵ペアを生成し、要素９０２～９０６で通信を開始する。短期鍵ペアは、通信の開始前及び／又は開始後に生成され得ることに留意されたい。このプロセスは時間を要するため、様々な実施形態では、ユーザに可視のトランザクション時間を低減するために、トランザクションが開始する前に、鍵を生成することが望ましい場合がある。通信の開始には、例えば、通信を開始するために、ＥＣＰによるＮＦＣ衝突防止を使用するシステム１１０を含み得る。９０８で、システム１１０は、次いで、現在のトランザクションのためにランダムな（又は疑似ランダムな）ｔｒａｎｓａｃｔｉｏｎ．ＩＤを生成し、メッセージ９１０を送信する（例示された実施形態では、これは、ＳＥＬＥＣＴ　ＡＣＣＥＳＳメッセージであるが、他の実施形態では、様々なタイプのメッセージが使用され得る）。いくつかの実施形態では、このメッセージは、トランザクションを実行するためにモバイルデバイス１３０上で（例えば、ＳＥ１３４によって）実行可能なアプレットのアプレットＩＤを示す。

【０１４０】

以下の用語及び表記が本明細書で使用され得る。

【０１４１】

ＡＰは、いくつかの実施形態では、例えば、モバイルデバイスのアプリケーションプロセッサである。

【０１４２】

ＣＡＳＤは、いくつかの実施形態では、制御機関セキュリティドメイン（Controlling Authority Security Domain）であり、その中に記憶された証明書は、「ＳＥ証明書」と称され得る。

【０１４３】

ＤｏＳは、サービス妨害（denial of service）を指す。

【０１４４】

ＥＣＰは、拡張非接触ポーリング（enhanced contactless polling）を指す。

【０１４５】

ＨＣＩは、ホスト通信インタフェース（host communications interface）を指す。

【０１４６】

ＩＶｅは、いくつかの実施形態では、対称暗号法のための初期ベクトル（initial vector）である。このベクトルは、例えば、ｔｒａｎｓａｃｔｉｏｎ．ＩＤが変化するため、トランザクション毎に変化し得る。

【０１４７】

ＫＡＥｓｅｅｄは、いくつかの実施形態では、暗号化鍵及びＭＡＣセッション鍵を導出するために使用される対称長期鍵である。これは、両側のＮＶＭに記憶されてもよく、高速トランザクションのためのルート鍵として使用されてもよい。その寿命は、システム側に実施されたセキュリティポリシーによって決定され得る（例えば、更新まで最大１０トランザクション、エンジン始動時は常に更新、など）。

【０１４８】

ＫＡＥｅは、いくつかの実施形態では、ｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒ及び機密ペイロードを暗号化するために使用される導出された対称鍵である。

【０１４９】

ＫＡＥｍは、いくつかの実施形態では、ｐｈｏｎｅＴａｇを計算するために使用される導出された対称鍵である。

【０１５０】

ＫＤＦは、いくつかの実施形態では、鍵導出関数（key derivation function）である。様々な実施形態では、異なる導出定数を使用して、同一の入力シークレットから導出することができる。

【０１５１】

ＫＴＳは、いくつかの実施形態では、鍵追跡サーバ（key tracking server）である。

【０１５２】

ＬＰＭは、低出力モード（low power mode）を指す。

【０１５３】

ＰＡＫＥは、パスワード認証鍵交換（password authenticated key exchange）を指す。

【０１５４】

ｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍは、いくつかの実施形態では、固有の公開トランザクションデータに対して計算されたＭＡＣ値である。デバイスがシステムと同一の対称鍵を所有していることを示し得る。いくつかの実施形態では、高速トランザクションのみで使用される。

【０１５５】

ｓｙｓｔｅｍ．Ｓｉｇは、いくつかの実施形態では、システムがｓｙｓｔｅｍ．ＳＫを所有していることを示すために使用される。両短期鍵、ｓｙｓｔｅｍ　Ｉｄｅｎｔｉｆｉｅｒ、及びｔｒａｎｓａｃｔｉｏｎ．ＩＤに署名されてもよい。

【０１５６】

ＤＨは、いくつかの実施形態では、ディフィー・ヘルマン鍵交換関数である。

【０１５７】

ｔｒａｎｓａｃｔｉｏｎ．ＩＤは、いくつかの実施形態では、対称鍵導出及びＭＡＣ／署名生成のために両側の可変要素として使用されるトランザクションの固有の識別子である。

【０１５８】

ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒは、いくつかの実施形態では、システムの固有の識別子である。ＮＦＣトランザクションの場合、ＲＦフィールドの到達範囲によって保護されてもよい。ＢＴトランザクションの場合、ＢＴチャネルのプライバシー保護に依存し得る。デバイス側では、システムの長期公開鍵を決定するために使用されてもよい。

【０１５９】
ｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒは、いくつかの実施形態では、デバイスの固有の識別子である。いくつかの実施形態では、それは、電話がシステム識別情報を検証した後、セキュアチャネルで送信することによって、トランザクション中のプライバシーのために保護される。システム側で使用して、高速又は標準／フルのどのフローが取られるべきかを示す署名ｔｒａｎｓａｃｔｉｏｎ．Ｔｙｐｅ読取機判定値を検証するためにデバイス公開鍵を選択することができる。
【０１６０】
ｔｒａｎｓａｃｔｉｏｎ．Ｔｙｐｅは、いくつかの実施形態では、（他の可能なタイプのトランザクションの中でも）例えば、高速又は標準／フルのどのフローが取られるべきかを示す読取機判定値である。
【０１６１】
ｐｈｏｎｅＤａｔａは、いくつかの実施形態では、暗号化された電話識別子及び任意選択のメールボックスデータである。
【０１６２】
ｐｈｏｎｅＴａｇは、いくつかの実施形態では、トランザクション関連データに対して計算されたＭＡＣである。
【０１６３】
ｐｈｏｎｅＡｕｔｈｅｎｔｉｃａｔｅｄＤａｔａは、いくつかの実施形態では、電話識別子及び電話署名を含む。
【０１６４】
表記ＫＡＥｅ：ＫＡＥｍ：ＩＶｅ＝ＫＤＦ（．．．）は、３つの値すべてが、異なる導出定数を使用して同一ＫＤＦから導出されることを意味する。定数は、本明細書において指定されていない。
【０１６５】
表記ｐｈｏｎｅＤａｔａ：ｐｈｏｎｅＴａｇ＝ＥｎｃＭａｃ（ＫＡＥｅ：ＫＡＥｍ）（ＩＶ＝ＩＶｅ，ＡＤ＝．．．，ＡＥ＝．．．）は、ｐｈｏｎｅＤａｔａがＫＡＥｅで暗号化されたデータＡＥであり、ｐｈｏｎｅＴａｇがＫＡＥｍを使用したＡＤに対するＭＡＣ値であることを意味する。
【０１６６】
９１２で、例示された実施形態では、モバイルデバイス１３０は、示されたアプレットを実行して、短期電話公開鍵ｐｈｏｎｅ．ｅＰＫと共にＳＥＬＥＣＴ応答を送信する。いくつかの実施形態では、システム１１０は、ＢＵＳ－Ｓ１転送を使用して、ｐｈｏｎｅ．ｅＰＫを、開示された動作実行するように構成されたプロセッサに送信することができる。様々な実施形態では、システム１１０は、セキュア要素読取機として動作することができ、暗号動作を実行するように構成された１つ以上のプロセッサと通信することができる、１つ以上のＮＦＣデバイスを（例えば、ドアハンドル内、点火機付近などに）含んでもよい。いくつかの実施形態では、これらの通信に使用されるバスは、比較的遅い場合があり、つまり高速トランザクション技術は、標準トランザクション技術と比較して、これらのバス上で送信されるデータの量を低減し得る。
【０１６７】
９１４で、システム１１０は、次いで、システム公開鍵ｓｙｓｔｅｍ．ｅＰＫ、「ｓｙｓｔｅｍ　Ｉｄｅｎｔｉｆｉｅｒ」値（システム１１０に固有であり得る）、及びトランザクションＩＤを含むＡＵＴＨ０コマンドを送信する。ＡＵＴＨ０コマンドはまた、どのタイプのトランザクション、例えば、標準又は高速、が実行されるべきかを示し得る。それに応じて、モバイルデバイス１３０は、トランザクションのために、ランダム共有シークレットＫＡＥｓｅｅｄを生成するか、又は以前にネゴシエーションされたＫＡＥｓｅｅｄを選択する。いくつかの実施形態では、生成／選択は、システム識別子についての情報の伝達を回避するために（例えば、システム識別子が既にデバイスに知られているかどうかを示すことを回避するために）、一定時間インターバルを使用して実行される。例示さ

れた実施形態では、システム識別子が既知であり、対応するＫＡＥｓｅｅｄが存在する場合、既存のＫＡＥｓｅｅｄが選択されてもよい。これは、以下で更に詳細に論じられるように、高速経路トランザクションに使用されてもよい。そうでなければ、生成されたランダムＫＡＥｓｅｅｄが選択されてもよい。

【０１６８】

９１６で、モバイルデバイス１３０は、例示された実施形態では、次いで、同一のＫＤＦを使用して、選択されたＫＡＥｓｅｅｄ、ｔｒａｎｓａｃｔｉｏｎ．ＩＤ、及び文字列「ａｕｔｈ１」（この文字列は、例示的な目的のために使用されるが、様々な実施形態では、両側で既知の様々な値のいずれかが実施されてもよいことに留意されたい）を使用して、ＫＡＥｅ及びＫＡＥｍを計算する。（モバイルデバイス１３０は、高速トランザクションタイプためのＫＡＥｅを生成しない場合があることに留意されたい）。モバイルデバイス１３０は、（「ＡＵＴＨ０　ｃｍｄ」｜ｐｈｏｎｅ．ｅＰＫ｜ｓｙｓｔｅｍ．ｅＰＫ｜ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒ｜ｓｙｓｔｅｍ．ＰＫ｜ｔｒａｎｓａｃｔｉｏｎ．ＩＤ｜ｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒ｜ｐｈｏｎｅ．ＰＫ）のＭＡＣ（ＫＡＥｍ）としてｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍを更に決定し、ｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍと共にＡＵＴＨ０応答を送信する。ｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍは、システム１１０による別のバス転送ＢＵＳ－Ｓ２を伴い得る。いくつかの実施形態では、モバイルデバイスは、ＫＡＥ値を計算しないか、又は標準トランザクションの暗号文を生成しない。

【０１６９】

９２０で、ＡＵＴＨ０応答に基づいて、システム１１０は、標準技術と高速技術とでは異なるように進み得る。標準技術では（例えば、ポリシー若しくはコンテキストが標準認証を必要とする場合、又はｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍが検証されない場合）、システム１１０は、ｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍを無視し（又は暗号文を有さない肯定応答メッセージを単に受信し）、図９Ｂの要素に進む。高速技術では、システム１１０は、対応するｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍが見つかるまで既知の電話を捜索する。システム１１０は、次いで、そのモバイルデバイスのために以前にネゴシエーションされたｓｅｅｄ（例えば、以前の標準トランザクションからのＫＡＥｓｅｅｄ［ｉ］）並びにｔｒａｎｓａｃｔｉｏｎ．ＩＤのＫＤＦとして、ＫＡＥｍ（及び標準トランザクションのためのＫＡＥｅ）を計算する。既知のモバイルデバイスを捜索するこの技術は、モバイルデバイス１３０の識別子を公開するのを回避することができ、これにより、例えば、プライバシーを高め、モバイルデバイス１３０の追跡を回避することができる。一般的に言って、開示された技術は、公開鍵証明書、公開鍵ハッシュ、又はデバイスを追跡するために使用され得る他の鍵／デバイス固有の識別子の解放を回避することができる。

【０１７０】

システム１１０は、次いで、ｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍ　ＭＡＣを検証しようと試み、検証の成功に応じて、要求されたアクションを直ちに認証及び許可することができる（これにより高速トランザクションが終了し得る）。ｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍの検証が成功しない場合、標準トランザクション技術が進み得る。

【０１７１】

次に図９Ｂを参照すると、９３０で、システム１１０は、ｐｈｏｎｅ．Ｃｒｙｐｔｏｇｒａｍを破棄し（これは、高速トランザクションではないため）、ｓｙｓｔｅｍ．ｅＰＫを含むｓｙｓｔｅｍ．ｅＣｅｒｔ、ｐｈｏｎｅ．ｅＰＫ、ｓｙｓｔｅｍ　Ｉｄｅｎｔｉｆｉｅｒ、ｓｙｓｔｅｍ．ＳＫで署名されたｔｒａｎｓａｃｔｉｏｎ．ＩＤを生成して、ｓｙｓｔｅｍ．Ｓｉｇを生成する。システム１１０は、例示された実施形態では、次いで、ｓｙｓｔｅｍ．Ｓｉｇを含むＡＵＴＨ１コマンド９３４を送信する。これは、システム１１０によるｓｙｓｔｅｍ．Ｓｉｇの別のバス転送ＢＵＳ－Ｓ３を伴い得る。

【０１７２】

システム１１０は、例示された実施形態では、次いで、ｓｙｓｔｅｍ．ｅＳＫ及びｐｈｏｎｅ．ｅＰＫ、ｓｙｓｔｅｍ．ｅＰＫ、ｐｈｏｎｅ．ｅＰＫ、並びにｓｙｓｔｅｍ．ＰＫのＤＨ鍵交換のＫＤＦを使用してＫＡＥｓｅｅｄを計算する。このＫＡＥｓｅｅｄは、

共有対称鍵として記憶され、いくつかの実施形態では、後続の高速トランザクションに使用され得る。この共有シークレットは、無期限に使用されてもよく、又は使用が制限されていてもよい（例えば、特定の時間インターバル又は使用回数の後に失効する場合がある）。一般的に言って、ＫＡＥｓｅｅｄは、短期鍵に対する楕円曲線暗号法、及びシステム公開鍵（例えば、ｓｙｓｔｅｍ．ＰＫ）を含むＫＤＦを使用して計算された共有シークレットの例である。システム１１０は、次いで、ＫＡＥｓｅｅｄ及びｔｒａｎｓａｃｔｉｏｎ．ＩＤのＫＤＦを使用してＫＡＥｅ、ＫＡＥｍ、及びＩＶｅを計算する。

【０１７３】

モバイルデバイス１３０は、例示された実施形態では、９３２で、公開鍵ｓｙｓｔｅｍ．ＰＫ及び受信されたｓｙｓｔｅｍ．Ｓｉｇを使用してｓｙｓｔｅｍ．ｅＣｅｒｔを検証する。モバイルデバイス１３０は、次いで、システム１１０のｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒのために不揮発性メモリにＫＡＥｓｅｅｄを記憶する。モバイルデバイス１３０は、次いで、検証が成功した場合、以前に計算されたｐｈｏｎｅ　ｄａｔａ及びｐｈｏｎｅＳｉｇとしてｐｈｏｎｅＡｕｔｈｅｎｔｉｃａｔｅｄＤａｔａを生成し、ｐｈｏｎｅＡｕｔｈｅｎｔｉｃａｔｅｄＤａｔａを有するＡＵＴＨ１応答９４０を送信する。いくつかの実施形態では、システム１１０によるｐｈｏｎｅＡｕｔｈｅｎｔｉｃａｔｅｄＤａｔａの別のバス転送を伴い得る。

【０１７４】

システム１１０は、例示された実施形態では、次いで、９４２で、ＫＡＥｍを使用してｐｈｏｎｅＡｕｔｈｅｎｔｉｃａｔｅｄＤａｔａをＭＡＣすることによりｐｈｏｎｅＴａｇ’を生成し、ｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒを復号し、ｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒを使用してｐｈｏｎｅ．ＰＫを検索及び検証し、公開鍵ｐｈｏｎｅ．ＰＫを使用してｐｈｏｎｅ．Ｓｉｇを検証し、任意のパケットデータを復号し、モバイルデバイス１３０のｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒのために不揮発性メモリにＫＡＥｓｅｅｄを記憶する。検証が成功した時点で、システム１１０は、モータ又はエンジンを始動することなどの要求されたアクションを許可し得る。

【０１７５】

いくつかの実施形態では、エンジンを始動すること、又はシステム１１０をパークの外に移動することなどの特定のタイプのアクションには標準トランザクションタイプが必要とされる。いくつかの実施形態では、高速トランザクションタイプは、システム１１０内の他の読取機と比較して、より遅いバスを有するＮＦＣ読取機（例えば、内部コンソールではなくドア内に位置する読取機）に使用されてもよい。

【０１７６】

次に図９Ｃを参照すると、システム１１０及びモバイルデバイス１３０は、９４４及び９４６に示すように、ＫＡＥｓｅｅｄ、ｔｒａｎｓａｃｔｉｏｎ．ＩＤ、ｐｈｏｎｅ．ｅＰＫ、及び１つ以上の既知の値又は文字列のＫＤＦを使用して、ＫＳ１、ＫＳ２、ＩＶ１、及びＩＶ２を計算し得る。いくつかの実施形態では、これらの値は、システム１１０とモバイルデバイス１３０との間で追加の情報を転送するためのセッションに使用されてもよい。

【０１７７】

いくつかの実施形態では、モバイルデバイス１３０は、システム１１０からのデータを記憶するために使用される１つ以上のメールボックスを含む。例示的なメールボックス実装形態は、図１８を参照して以下で論じる。いくつかの実施形態では、プライバシー保護されたメールボックスは、暗号化なしでＡＰ１３６にアクセス可能であり、一方、機密メールボックスは、セキュアＮＦＣを介してシステム１１０のみにアクセス可能である。一般的に言って、メールボックス（単数又は複数）は、様々な情報を記憶するために使用されてもよく、この情報は、システム１１０の製造業者又は設計者によって定義されるフォーマットであってもよい。いくつかの実施形態では、この情報は、イモビライザートークンを含んでもよい。いくつかの実施形態では、この情報は、１つ以上のアクションを実行するためのパラメータを示す設定（例えば、座席及び鏡位置に関する快適性設定など）を

含んでもよい。したがって、モバイルデバイス１３０の開示された技術は、様々な異なるタイプのシステムとの通信を可能にし得る。

【０１７８】

いくつかの実施形態では、システム１１０は、モバイルデバイス１３０とのペアリング中に、機密メールボックスを使用して、固定化鍵を記憶する。特定のアクションを実行する（例えば、エンジンを始動するなどの）前に、システム１１０は、機密メールボックスから１つ以上の固定化鍵を取り出し、検査することができる。システム１１０は、要求されたアクションを許可するために使用されるとすぐに鍵を破棄し得る。

【０１７９】

いくつかの実施形態では、プライベートメールボックスを使用して、例えば、サードパーティアプリケーション、診断、コマンド、無線ペアリング情報などのためのユーザ設定を記憶する。いくつかの実施形態では、プライベートメールボックスは、ランダムアクセスをサポートする。

【０１８０】

いくつかの実施形態では、ＫＡＥｓｅｅｄはまた、超広帯域（ultra-wideband、ＵＷＢ）通信のための対称鍵として使用されてもよい。これらの通信は、飛行時間を利用して、モバイルデバイス１３０及びシステム１１０の近接を検証することができる。本明細書で論じられる共有シークレット技術を使用して、このような通信が実際に許可されたデバイスで実行されていることを認証することができる。

【０１８１】

いくつかの実施形態では、他のモバイルデバイスと共有される鍵の有効性は、システム１１０が完全なアクセスリストを受信するときに自動的にインクリメントされる生成カウンタによって管理される（但し、例えば、既存のエントリが有効なままであることを可能にする、リストへのインクリメンタルな追加が実行される場合には、カウンタは変更されないままであり得る）。カウンタは、単調であってもよく、ロールオーバーを回避するようにサイズ決めされてもよい。これらの実施形態では、カウンタの値よりも低い生成カウンタで署名された任意の以前の又は保留中の要求は、システム１１０によって拒否され得る。これにより、ユーザが自身のアクセスが失効すること意図していたときに、ユーザが誤って友人のモバイルデバイスからシステム１１０へのアクセスを離れることを回避することができる。

ＫＤＦによる例示的な標準トランザクション

【０１８２】

図１０は、いくつかの実施形態に係る、非対称トランザクション示す。いくつかの実施形態では、このようなトランザクション中に確立された共有シークレット（例えば、以下で論じるＫＡＥｓｅｅｄ）は、後続の高速経路（例えば、対称）技術のためにデバイスによって保存されてもよい。いくつかの実施形態では、図１０に示す技術は、図９Ａ～図９Ｃに示す技術と類似しているが、標準技術のみに焦点を当てている（高速経路技術に関する詳細を省略している）。いくつかの実施形態では、非対称暗号法は、比較的より強力な認証及び前方秘匿性を提供し、一方、高速トランザクションは、向上した性能を提供し得る（例えば、処理リソースが制限されている場合）。いくつかの実施形態では、標準トランザクションは、友人デバイス（本明細書では、「ｓｈａｒｅｅ」とも称され得る）がシステム１１０に初めて接触するときに常に初めて使用される。標準トランザクションは、高速トランザクションが要求されても、モバイルデバイス１３０によって（例えば、初めての接触若しくは未知のシステムのために）又はシステム１１０によって（例えば、対称鍵が確立されていない場合）強制され得る。

【０１８３】

一般的に言って、例示された実施形態では、短期鍵ペア及び以前に決定された長期鍵（ペアリングから）を使用して、共有シークレット（ＫＡＥｓｅｅｄ）をネゴシエーションする。共有シークレットは、モバイルデバイスによって、署名を生成する（長期秘密鍵を使用して署名される）ために使用され、署名は、電話ＩＤなどの他の電話データと共に暗

号化される。モバイルデバイスは、システムからの署名付き証明書を検証した後に、データをシステムに送信する。システムは、電話データを検証し、それを復号し、電話ＩＤを使用してｐｈｏｎｅ．ＰＫを検索し、次いで、ｐｈｏｎｅ．ＰＫを使用して署名を検証する。例示された実施形態では、システム及びモバイルデバイスは、次いで、標準トランザクション中に確立された値を使用して、メールボックスデータを転送し、このメールボックスデータは、様々な通信及び目的に使用され得る。

【０１８４】

更により一般的には、図１０は、認証材料を生成して、その材料を、材料を認証するモバイルデバイス１３０に送信するシステムを伴い、プライベートチャネルを作成し、エンドポイント認証材料を生成する。システム１１０は、次いで、モバイルデバイスを認証し、セキュアチャネルを作成することができる。認証は、１つ以上のアクションを許可するために使用されてもよく、プライベート及び／又はセキュアチャネルは、様々なタイプの情報を交換するために使用されてもよい。開示された技術は、モバイルデバイス１３０が任意の識別情報を提供する前にシステム１１０の認証を可能にすることができ、また、セキュアチャネルを使用してモバイルデバイス１３０に関する情報を識別するための暗号化を提供してもよい。

【０１８５】

より具体的には、１００２で、例示された実施形態では、システム１１０は、システム短期鍵ペア（例えば、ｓｙｓｔｅｍ．ｅＳＫ及びｓｙｓｔｅｍ．ｅＰＫ）を生成する。１００４で、システム１１０は、拡張非接触ポーリングを用いてＮＦＣ衝突防止を実行する（但し、他の実施形態では、他の技術が使用され得る）。１００６で、モバイルデバイス１３０は、電話短期鍵ペア（例えば、ｐｈｏｎｅ．ｅＳＫ及びｐｈｏｎｅ．ｅＰＫ）を生成し、１００８で、ポーリング検出を起動する。

【０１８６】

１０１０で、例示された実施形態では、システム１１０は、ランダムトランザクションｉｄを生成し、アプリケーション識別子メッセージ１０１２をモバイルデバイス１３０に送信する。例えば、メッセージは、ＳＥＬＥＣＴ　ＡＣＣＥＳＳ　ＡＩＤメッセージであり得、このメッセージは、モバイルデバイス１３０上の適切なアプリケーションを選択するためのアプリケーション識別子を示す。１０１４で、モバイルデバイス１３０は、電話短期公開鍵ｐｈｏｎｅ．ｅＰＫと共に応答する。いくつかの実施形態では、トランザクションは、ＳＥＬＥＣＴコマンド／応答、ＡＵＴＨ０コマンド／応答、ＡＵＴＨ１コマンド／応答、及び所望により、１つ以上のＳＥＴ／ＧＥＴコマンド／応答を含む（ＡＵＴＨ及びＳＥＴ／ＧＥＴメッセージについては、以下で更に詳細に論じられる）。

【０１８７】

１０１６で、例示された実施形態では、システム１１０は、トランザクションパラメータを有するコマンドを送信する。いくつかの実施形態では、これは、ＡＵＴＨ０コマンドと称され得る。いくつかの実施形態では、このコマンドは、次を含む：ｓｙｓｔｅｍ．ｅＰＫ｜ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒ｜ｔｒａｎｓａｃｔｉｏｎ．ＩＤ｜ｔｒａｎｓａｃｔｉｏｎ．Ｔｙｐｅ＝標準。他の実施例では、ｔｒａｎｓａｃｔｉｏｎ．Ｔｙｐｅは、高速トランザクション又は何らかの他のタイプのトランザクションを示し得る。したがって、ＡＵＴＨ０コマンドは、デバイスによって必要とされるシステム公開情報（静的識別子及びランダムセッション情報）を提供して、適用可能であれば、高速トランザクションのための既に確立された対称シークレットに基づいて暗号文を計算することができる。例示された標準トランザクションでは、応答は、１０１８で、データなしの肯定応答のみであり得る。

【０１８８】

１０２０で、例示された実施形態では、システム１１０は、トランザクションｉｄ及びシステム識別子を有する短期証明書を生成し、証明書に署名して署名を生成する。これは、例えば、ｓｙｓｔｅｍ．ｅＰＫ｜ｐｈｏｎｅ．ｅＰＫ｜ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒ｜ｔｒａｎｓａｃｔｉｏｎ．ＩＤを含む短期証明書ｓｙｓｔｅｍ．ｅＣｅｒｔを生成

することを含み得る。これは、ペアリングからの秘密鍵（例えば、ｓｙｓｔｅｍ．ＳＫ）で署名され、署名ｓｙｓｔｅｍ．Ｓｉｇを取得し得る。

【０１８９】

１０２２で、例示された実施形態では、モバイルデバイス１３０は、導出された共有シークレットを生成し、署名を生成し、導出された共有シークレットに基づいて署名を暗号化する。いくつかの実施形態では、これは、ＫＡＥｓｅｅｄ＝ＫＤＦ（ＤＨ（ｓｙｓｔｅｍ．ｅＰＫ、ｐｈｏｎｅ．ｅＳＫ），ｓｙｓｔｅｍ．ｅＰＫ｜ｐｈｏｎｅ．ｅＰＫ｜ｓｙｓｔｅｍ．ＰＫ）を生成することを含む。本実施例では、Ｄｉｆｆｉｅ Ｈｅｌｌｍａｎ関数ＤＨは、共有シークレットを生成するために使用される鍵交換関数の一例であり、鍵導出関数ＫＤＦは、鍵交換関数の出力に基づいて、導出された共有シークレット並びに公開鍵ｓｙｓｔｅｍ．ｅＰＫ、ｐｈｏｎｅ．ｅＰＫ、及びｓｙｓｔｅｍ．ＰＫを生成する。いくつかの実施形態では、モバイルデバイス１３０はまた、ｄｉｖｅｒｓｉｆｉｅｒ＝ｔｒａｎｓａｃｔｉｏｎ．ｉｄｅｎｔｉｆｉｅｒ｜ｐｈｏｎｅ．ｅＰＫ｜ｓｙｓｔｅｍ．ｅＰＫ｜ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒ｜ｓｙｓｔｅｍ．ＰＫを定義する。いくつかの実施形態では、モバイルデバイス１３０は、ＫＡＥｅ１：ＫＡＥｍ１：ＩＶｅ１＝ＫＤＦ（ＫＡＥｓｅｅｄ，ｄｉｖｅｒｓｉｆｉｅｒ｜「電話からシステムへ」）を計算し、ＫＡＥｅ２：ＫＡＥｍ２：ＩＶｅ２＝ＫＤＦ（ＫＡＥｓｅｅｄ，ｄｉｖｅｒｓｉｆｉｅｒ｜「システムから電話へ」）を計算する。これらの導出された対称鍵は、電話及び／又は機密ペイロードを識別する情報を暗号化するために使用されてもよく、これにより、このような情報のセキュリティを高めることができる。

【０１９０】

いくつかの実施形態では、モバイルデバイス１３０は、署名ｐｈｏｎｅ．Ｓｉｇ＝Ｓｉｇｎ（ｐｈｏｎｅ．ＳＫ，ｔｒａｎｓａｃｔｉｏｎ．ｉｄｅｎｔｉｆｉｅｒ｜ｐｈｏｎｅ．ｅＰＫ｜ｓｙｓｔｅｍ．ｅＰＫ）を生成する。いくつかの実施形態では、モバイルデバイス１３０は、ｐｈｏｎｅ．Ｄａｔａ：ｐｈｏｎｅ．Ｔａｇ＝ＥｎｃｒｙｐｔＭａｃ（ＫＡＥｅ１：ＫＡＥｍ１：ＩＶｅ１：カウンタ＝０）（ｐｈｏｎｅ．Ｉｄｅｎｔｉｆｉｅｒ｜ｐｈｏｎｅ．Ｓｉｇ｜［ｍａｉｌｂｏｘ ｄａｔａ］）を計算する。

【０１９１】

１０２４で、例示された実施形態では、モバイルデバイス１３０は、ｓｙｓｔｅｍ．ｅＰＫ｜ｐｈｏｎｅ．ｅＰＫ｜ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒ｜ｔｒａｎｓａｃｔｉｏｎ．ｉｄｅｎｔｉｆｉｅｒを使用して、システムｓｙｓｔｅｍ．ｅＣｅｒｔからの短期証明書を再構築する。これは、以下で論じるように、システムからの短期証明書の検証を容易にすることができる。

【０１９２】

１０２６で、例示された実施形態では、システム１１０は、１０２０で生成された短期証明書及び署名を送信する。このメッセージは、ＡＵＴＨ１コマンドと称され得る。いくつかの実施形態では、システム１１０は、署名を送信することによって、このメッセージ内でデバイスに対してそれ自体を認証する。

【０１９３】

１０２８で、例示された実施形態では、モバイルデバイス１３０は、署名ｓｙｓｔｅｍ．Ｓｉｇ及びシステム公開鍵ｓｙｓｔｅｍ．ＰＫを使用して、短期証明書ｓｙｓｔｅｍ．ｅＣｅｒｔを検証する。デバイスが署名を検証することができる場合、それは、新しい対称共有シークレットＫＡＥｓｅｅｄをシステム１１０の検証された識別子と関連付けることができる。

【０１９４】

並行して、例示された実施形態では、システム１１０は、同一の対称共有シークレットを計算する。特に、１０３０で、例示された実施形態では、システム１１０は、導出された共有シークレットＫＡＥ ｓｅｅｄ＝ＫＤＦ（ＤＨ（ｓｙｓｔｅｍ．ｅＳＫ，ｐｈｏｎｅ．ｅＰＫ），ｓｙｓｔｅｍ．ｅＰＫ｜ｐｈｏｎｅ．ｅＰＫ｜ｓｙｓｔｅｍ．ＰＫ）を計算する。システム１１０はまた、ＫＡＥｅ１：ＫＡＥｍ１：ＩＶｅ１＝ＫＤＦ（ＫＡＥｓ

ｅｅｄ，ｄｉｖｅｒｓｉｆｉｅｒ｜「電話からシステムへ」）を計算し得る。

【０１９５】

１０３２で、モバイルデバイス１３０は、暗号化された署名及びモバイルデバイス識別子を有する応答（これは、ＡＵＴＨ１応答と称され得る）を送信する。より具体的には、モバイルデバイス１３０は、このメッセージでｐｈｏｎｅ．Ｄａｔａ及びｐｈｏｎｅ．Ｔａｇを送信することができ、このメッセージは、上述のように、様々な予め計算された暗号化された及びＭＡＣされたデータを含み得る。

【０１９６】

１０３４で、システム１１０は、モバイルデバイス１３０からのデータを復号し、識別子を使用して電話の公開鍵を検索し、公開鍵を使用して署名ｐｈｏｎｅ．Ｓｉｇを検証する。特に、これは、ｐｈｏｎｅ．Ｔａｇを検証することと、ｐｈｏｎｅ．Ｄａｔａを復号することと、ｐｈｏｎｅ．Ｉｄｅｎｔｉｆｉｅｒを使用してｐｈｏｎｅ．ＰＫを検索することと、ｐｈｏｎｅ．ＰＫを使用してｐｈｏｎｅ．Ｓｉｇを検証することと、ｐｈｏｎｅ．Ｉｄｅｎｔｉｆｉｅｒと関連してＫＡＥｓｅｅｄを記憶することとを含み得る。したがって、システム１１０がデバイス署名（ｐｈｏｎｅ．Ｓｉｇ）を正常に検査することができる場合、対称シークレットをデバイスと関連付ける。追加のメールボックスデータは、復号され、システム側で使用され得る。

【０１９７】

様々なトランザクションでは、デバイス１３０は、セキュアチャネルを作成するために、例えば、導出された鍵（ＫＡＥｍ、ＫＡＥｅ）を使用して、トランザクションの終了時にプライベート及び／又は機密メールボックスのコンテンツを要求し得る。

【０１９８】

したがって、例示された実施形態では、デバイス１３０は、短期鍵を介するＤＨ及び長期システム鍵ｓｙｓｔｅｍ．ＰＫを含むＫＤＦを使用して、共有シークレット（ＫＡＥｓｅｅｄ）を計算する。また、ｐｈｏｎｅ．ＳＫを使用して、デバイス署名（ｐｈｏｎｅＳｉｇ）も計算する。一方で、システムは、長期システム鍵ｓｙｓｔｅｍ．ＳＫによって署名された短期証明書を生成し、その署名をデバイスに送信する。同一の短期証明書を再構築したデバイスは、署名を検証し、成功した場合、システム識別子に関する共有シークレット（ＫＡＥｓｅｅｄ）を記憶する。ＫＡＥｓｅｅｄは、次いで、次の高速トランザクションに使用され得るだけでなく、導出された対称鍵（ＫＡＥｅ、ＫＡＥｍ）を使用して最終ペイロード転送をセキュアにするためにも使用され得る。ＡＵＴＨ１応答を受信すると、システムは、デバイスの公開鍵を検索して、ｐｈｏｎｅＡｕｔｈｅｎｔｉｃａｔｅｄＤａｔａの一部として受信された復号された電話識別子を使用して、電話署名を検証する。成功した場合、システムは、任意選択のペイロード（例えば、イモビライザートークン）を復号し、このデバイスのＫＡＥｓｅｅｄを永続的メモリに記憶する。所望により、次いで、導出されたセッション鍵を使用して、デバイスからシステムにペイロード（例えば、イモビライザートークン）を転送することができる。ＵＷＢシステムでは、セキュアレンジングマスター鍵（secure ranging master key、ＳＡＳＫ）は、ＫＡＥｓｅｅｄから導出することができる。

【０１９９】

いくつかの実施形態では、このトランザクションによって解決されるプライバシー問題は、電話がｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒを無許可の読取機に解放することを防止することである。公開鍵証明書、公開鍵ハッシュ、又は任意の種類の鍵／デバイス固有の識別子を解放することは、ユーザの同意なしにデバイスを追跡するための潜在的な方法と見なすことができる。デバイス側のＫＡＥｓｅｅｄの選択は、ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒがデバイスによって攻撃者に知られているかどうかに関する任意の知識を開示しないように、定時間設計で実施されてもよい。いくつかの実施形態では、前方秘匿性は、例えば、短期鍵の使用により、本明細書で論じられる様々なトランザクションに提供される。

【０２００】

いくつかの実施形態では、性能を向上させるために、図１０のトランザクションに様々

な修正を行うことができる。例えば、公開鍵サイズを低減するために、例えば、コンパクトな又は圧縮された形態をＥＣＣポイントに使用してもよい。いくつかの実施形態では、（例えば、フィルｅＣｅｒｔの代わりに）ｓｙｓｔｅｍ．ｅＣｅｒｔを再構築するために必要な最小量のデータを転送することができる。いくつかの実施形態では、短期鍵、ｓｙｓｔｅｍＩｄｅｎｔｉｆｉｅｒ、ｔｒａｎｓａｃｔｉｏｎ．ＩＤなどのデータは、プリフェッチされ得る。更に、効率的なＥＣ曲線の選択もまた、性能を向上させることができる。

例示的なペアリング実施形態

【０２０１】

図１１は、いくつかの実施形態に係る、ＰＡＫＥを使用してセッション鍵を生成するペアリングトランザクションを示す通信図である。

【０２０２】

いくつかの実施形態では、ペアリング前に、システム１１０は、それが受信する公開鍵の発信元を検証するために、デバイス製造業者のルート証明書を記憶する。いくつかの実施形態では、システムは、ＯＥＭバックエンドに記憶されたルート証明書を使用する（及びこれらの実施形態では、ペアリング中にオンラインであるべきである）。他の実施形態では、証明書は、デバイスによって提供されてもよい。この場合、システムによって検証され得る権限によって署名されるべきである。いくつかの実施形態では、ペアリング前に、システムは、１１０２で、テレマティクスを介してシステム製造業者のバックエンドからシークレット（ｐａｉｒｉｎｇＰａｓｓｗｏｒｄ）を受信し、ユーザは、システム製造業者のウェブポータル／ａｐｐ／ディーラー／ユーザマニュアルからシークレット（ｐａｉｒｉｎｇＰａｓｓｗｏｒｄ）を取得して、１１０４で、それを使用する。例示された実施形態では、Ｋは、ＰＡＫＥアルゴリズムによって、両側に生成された対称セッション鍵である。

【０２０３】

いくつかの実施形態では、１１１６及び１１２０で、ＰＡＫＥプロトコルを使用して、セッション鍵Ｋに基づいてセキュアチャネルが確立される。例示された実施形態では、短期鍵は、（１１０６及び１１０８で）両側に生成され、ペアリング要求１１１０及び肯定応答１１１２は、セキュアチャネルを確立する前に交換される。メッセージ１１２１及び１１２４では、証明書ｓｙｓｔｅｍ．Ｃｅｒｔ及びｐｈｏｎｅ．Ｃｅｒｔは、このチャネルを通じて安全に交換される。証明書交換及び検証の後、システムは、次いで、データをプロビジョニングするために、本明細書に（例えば、図１０に）記載された標準トランザクションを実行してもよい。

【０２０４】

いくつかの実施形態では、ペアリングモードになると、システムは、バックエンドに達し、ｐａｉｒｉｎｇＰａｓｓｗｏｒｄ値を要求する。ペアリングモードに入る条件は、システムＯＥＭによって定義され得る。バックエンドは、次いで、ｐａｉｒｉｎｇＰａｓｓｗｏｒｄを生成し、それをシステムに送信し、ＯＥＭユーザアカウントを通じてユーザと並行してそれを提供する。ユーザは、（例えば、ウェブブラウザで又はインストールされたＯＥＭ　ａｐｐを通じて）ｐａｉｒｉｎｇＰａｓｓｗｏｒｄを取り出す。ユーザは、次いで、ＯＥＭ　ａｐｐ内又はＯＳ内のいずれかでモバイルデバイス上でペアリングモードを開始し、ｐａｉｒｉｎｇＰａｓｓｗｏｒｄを入力する。ｐａｉｒｉｎｇＰａｓｓｗｏｒｄはまた、本明細書では、ＰＩＮとも称され得ることに留意されたい。ＯＥＭ　ａｐｐは、適切なＯＳ　ＡＰＩを通じて、ｐａｉｒｉｎｇＰａｓｓｗｏｒｄをアプレットに直接送信することができる。デバイス及びシステムが両方とも、ペアリングパスワードに基づいて短期鍵ペアを生成した場合、いくつかの実施形態では、両ＵＩは、ＮＦＣコンソール読取機上でデバイスをタップするようにユーザを促す。いくつかの実施形態では、システム１１０は、例えば、許可されたペアリング試行の失敗回数、ペアリングの成功後の挙動、非常に多く試行を失敗した後の挙動、非常に多く試行を失敗した後のリカバリ手順、システムへのシークレット配信、及び／又はオーナーへのシークレット配信を含む、ｐａｉｒ

ｉｎｇＰａｓｓｗｏｒｄに対する１つ以上のポリシーを実行してもよい。

【０２０５】

いくつかの実施形態では、車両は、ペアリング中に、どのようにデジタル鍵をモバイルデバイスによって設定すべきかを指定する構成情報を送信する。この構成情報は、例えば、どのタイプのトランザクションが許可されているか、システムメタデータ、開始日、失効日などを示す様々なフィールドを含み得る。モバイルデバイスのオペレーティングシステムは、セキュア要素上の１つ以上のアプレットに命令して、構成にしたがってデジタル鍵を作成することができる。ＳＥはまた、長期公開鍵ペアｐｈｏｎｅ．ＰＫ及びｐｈｏｎｅ．ＳＫを生成してもよい。いくつかの実施形態では、ＳＥは、（デジタル鍵が構成にしたがって作成された証明として）構成情報を有する証明書を生成し、ｐｈｏｎｅ．ＳＫを使用してそれに署名する。これらの実施形態では、システム１１０は、証明書を検証すること及び構成情報が正しいことを確認することによって、デジタル鍵が適切に作成されたことを検証できる。証明を伴うより詳細な例が図２８に示されており、以下で詳細に論じられる。

例示的なシステム及び構成要素の概観

【０２０６】

図１２は、いくつかの実施形態に係る、例示的な分配システムを示すブロック図である。例示された実施形態では、システムは、モバイルデバイス製造業者バックエンド１２３０、鍵追跡サーバ１２５０、ＯＥＭビジネスバックエンド１２７０、及び他のバックエンド１２１０を含む。例示された実施形態では、これらのバックエンドシステムのうちのものは、オーナーデバイス１３０、システム１１０、友人デバイス１６０、及びサービスデバイス１２２０と通信する。

【０２０７】

いくつかの実施形態では、システム１１０は、テレマティクスリンクを介してＯＥＭビジネスバックエンドにリンクされる。このリンクは、セキュア通信チャネルを提供することができ、システムＯＥＭによって完全に制御され得る。いくつかの実施形態では、システムは、オーナーペアリング、システムロック／ロック解除、エンジン始動などのアクションのためにモバイルデバイスと通信するためのＮＦＣ読取機を装備する。例示された実施形態では、デバイスはまた、鍵追跡サーバ１２５０と通信して、発行されたデジタル鍵を追跡、署名、及び取り消しすることができる。いくつかの実施形態では、オーナーデバイスは、ＯＥＭ　Ａｐｐを通じてＯＥＭビジネスバックエンド（例えば、これは、オーナーアカウントをホストし得る）と通信する。いくつかの実施形態では、友人及びサービスデバイスは、メインサービスのために、ＯＥＭビジネスバックエンドにリンクする必要はない。いくつかの実施形態では、これらのデバイスは、ＯＥＭ　Ａｐｐを使用して任意選択のアカウントにアクセスすることができる。デバイスは、様々な製造業者によって製造されてもよく、複数のそれぞれのモバイルデバイス製造業者バックエンドと通信することができる。

【０２０８】

いくつかの実施形態では、ＫＴＳ１２５０は、ビジネスバックエンドを信頼し、車両と関連付けられた鍵の変化を記録しながら、チェック機能及び署名機能を提供することができる。いくつかの実施形態では、鍵共有のために、ＫＴＳ１２５０は、友人の公開鍵、友人のアクセス権、友人の生成カウンタ、開始日及び失効日、鍵識別子、ＳＥ署名、オーナー署名、並びにＫＴＳ署名を記録する。

【０２０９】

製造業者バックエンド１２３０は、いくつかの実施形態では、デバイス上のシステム鍵アプリケーション（又はアプレット）のライフサイクルを管理し、ルートＡｐｐｌｅ　ＯＥＭ証明書をアプリケーションにプロビジョニングする責任がある。また、デバイスを一時停止、復元、及びワイプするためのサービスを提供してもよい。いくつかの実施形態では、デバイスＯＥＭバックエンド（単数又は複数）は、システムＯＥＭビジネスバックエンド１２７０と強く統合されていない場合がある。いくつかの実施形態では、いくつかの

接続は、オーナーへのＯＥＭに基づく取り消し又はデバイス紛失／盗難の通知に使用され得る。いくつかの実施形態では、バックエンド１２３０は、他のバックエンドにリアルタイムで接続されていない。いくつかの実施形態では、デバイスＯＥＭ　ＳＥルート証明書の交換は、すべての所有されていないルート証明書を検証及び署名し、それらをモバイルデバイスにプロビジョニングするために、すべてのデバイスＯＥＭ間で一度だけ行われる。いくつかの実施形態では、開示された技術を使用するすべてのデバイスは、システムと通信することができるセキュア回路（証明されたセキュア要素など）及び近距離無線（例えば、ＮＦＣ）機能を含むべきである。デバイスのホワイトリスト登録は、各システムＯＥＭによって実行されてもよい。

【０２１０】

図１３は、いくつかの実施形態に係る、例示的な近距離無線（例えば、ＮＦＣ）接続性を示すブロック図である。例示された実施形態では、モバイルデバイス１３０は、アプリケーションプロセッサ１３６を含み、これは、ＮＦＣコントローラ１３３２に接続されている。ＮＦＣコントローラは、例示された実施形態では、セキュアエレメント１３４に接続し、ＮＦＣアンテナからセキュア要素又はアプリケーションプロセッサ１３６のいずれかへのルーティングを制御する。アプリケーションプロセッサ１３６は、いくつかの実施形態では、ＮＦＣトランザクションのために起動している必要はない。いくつかの実施形態では、システムは、少なくとも２つのＮＦＣ読取機、例えば、例示されたドアハンドル読取機１３３０及びコンソール読取機１３３５を装備する。いくつかの実施形態では、１つのＥＣＵ１３７Ｃは、すべての読取機を制御し、本明細書で論じられる様々な暗号動作を含む、ＮＦＣ通じて通信プロトコルを実行するソフトウェアを含む。例示された実施形態では、別のＥＣＵ１３７Ｂは、スクリーン出力及び１つ以上のユーザ入力デバイス１３２５を制御する。別のＥＣＵ１３７Ａはまた、テレマティクスリンク１３２０を介してシステムＯＥＭバックエンドへのセキュアチャネル確立することができる。様々な実施形態では、ＥＣＵの配置は、異なるＯＥＭで異なり得ることに留意されたい。

【０２１１】

いくつかの実施形態では、ＮＦＣ構成要素は、カードエミュレーションモード及びサポートされたＥＣＰ（例えば、ＥＣＰ２．０）及びフィールド検出モードを使用する。いくつかの実施形態では、ＳＥ１３４は、対称及び非対称暗号法をサポートし、識別及び公開鍵署名のためのローカル認証局（certificate authority、ＣＡ）を記憶し、システム鍵アプリケーションを含み、並びに／又はカードコンテンツアプリケーションを含む。いくつかの実施形態では、システム鍵アプリケーションは、高速及び標準トランザクションを実行するように構成されており、イモビライザートークンを記憶及び管理し、オーナーペアリング、共有、及び取り消しを管理する。いくつかの実施形態では、アプリケーションは、オペレーティングシステムが、共有／イモビライザートークンのために利用可能な鍵の数、既に共有されている鍵の数、既に共有されている鍵についての情報、及び／又は別のオーナーから受信された鍵に関する情報をクエリできるようにする。アプリケーションは、共有鍵を追跡することができ、他の製造業者のＳＥからの署名を検証することができる。アプリケーションは、指定された鍵の使用を一時的に無効にするように構成することができる。いくつかの実施形態では、アプリケーションは、ＳＥ１３４にロードされる前に検査されてもよい。

【０２１２】

オペレーティングシステムは、いくつかの実施形態では、オーナーペアリング、トランザクション、鍵共有、及び取り消しなどの主な機能をネイティブに実行する。いくつかの実施形態では、それは、近接共有（例えば、ａｉｒ－ｄｒｏｐ）を通じて鍵を送受信し、リモート共有（例えば、ｉＭｅｓｓａｇｅ）を通じて鍵を送受信し、他の電話ＯＥＭデバイスとの間で鍵を送受信し、発行された友人鍵のリストを示し、共有のために利用可能な鍵の数を示し、鍵がシステム上でいつ使用されかを示す、他の製造業者ＳＥの製造業者署名付きルート証明書を記憶して、鍵共有に使用される公開鍵のＳＥ署名を検証し、システムＯＥＭサーバにセキュアセッションを開いて、（ＯＥＭユーザアカウント資格証明書を

使用せずに）システムと遠隔通信するように構成されている。いくつかの実施形態では、オペレーティングシステムは、ペアリングプロセス中にバックエンドからデバイスＳＥにオーナーＰＩＮを受け渡すことと、各関連付けられたシステムのデジタル鍵毎にプライベートメールボックススロットへの読み出し及び書き込みを個々に行うことと、各関連付けられたシステムのデジタル鍵毎に機密メールボックススロットに個々に書き込むことと、リモートコマンド実行のためのアプリケーションにアクセスすることと、（例えば、プロフェッショナルサービスのために）デバイスの代わりにサーバと友人鍵を共有することと、友人鍵又はアドホック鍵を（例えば、共有又はプロフェッショナルサービスのために）デバイスの代わりにサーバから受信することと、デバイス上の共有鍵についての非機密情報を取り出すことと、並びに／又は鍵を取り消すこととをできるようにするＡＰＩをシステムＯＥＭアプリケーションに提供する。

【０２１３】

いくつかの実施形態では、オペレーティングシステムは、特定のタイプのアクションの認証（又はバイオメトリック認証などの特定の認証タイプ）を要求するように構成されている。これらのアクションとしては、（オーナーによって要求されたオーナーデバイス上、友人によって要求された友人デバイス上、オーナーによって要求された友人デバイス上、友人に送信された要求を有するオーナーデバイス上を含む）例えば、オーナーペアリング、完全鍵共有、サービス鍵共有、鍵取り消しが挙げられ得る。いくつかの実施形態では、すべての要求は、バックエンドを介して、システム１１０にも進む。いくつかの実施形態では、（例えば、デバイス上でユーザによって明示的に構成されない限り）認証を必要としないアクションの例としては、ドアロック／ロック解除トランザクション、エンジン始動トランザクション、特定の状況における友人の最初のトランザクション、及びＫＴＳ１２５０又はオーナー／友人デバイスからの鍵取り消し要求の受信（例えば、サイレント取り消しのため）が挙げられ得る。

【０２１４】

特定のプロセッサ、ソフトウェアコンポーネント、又はハードウェアコンポーネントによって実行されるものとして本明細書に記載された様々な機能は、例示的な目的のために論じられているが、本開示の範囲を限定することを意図するものではないことに留意されたい。他の実施形態では、様々な機能は、本明細書に記載されるもの以外の要素によって実行されてもよい。

【０２１５】

いくつかの実施形態では、モバイルデバイス１３０は、時計などのウェアラブルデバイスであり、これは、例えば、携帯電話とペアリングされ得る。いくつかの実施形態では、デバイス１３０に関して、本明細書に記載された機能は、このようなデバイス間で分割されてもよい。

【０２１６】

いくつかの実施形態では、システム１１０は、オーナー公開鍵及び／又はデバイス情報などのオーナーペアリング情報をＫＴＳ１２５０に提供するように構成されている。いくつかの実施形態では、システム１１０は、非機密鍵共有情報のバックアップを介してオーナーデバイスを変更することをサポートし得る。

【０２１７】

いくつかの実施形態では、クラウドサービスシステムは、（オンラインの場合）紛失若しくは盗難デバイス上のデジタル鍵機能を一時的に無効にし、（オンラインの場合）紛失若しくは盗難デバイス上のデジタル鍵をリモートでワイプし、ユーザ識別情報とデバイス識別情報とを安全に結合し、及び／又は新しいデバイス上の共有鍵の復元を容易にするために、デジタル鍵共有情報をバックアップするように構成されてもよい。

【０２１８】

鍵追跡サーバ１２５０は、いくつかの実施形態では、記憶されたデータに対するプライバシー保護を提供するように構成されている。いくつかの実施形態では、ＫＴＳ１２５０は、システムが盗難され、オーナーがアクセスを許可している場合にのみ、データクエリ

にアクセスされる。いくつかの実施形態では、ＫＴＳ１２５０は、システムＯＥＭビジネスバックエンドからプライバシーを分離しており、鍵を記憶及び署名し、署名前にサービス有効性及び鍵ポリシーをチェックし、（例えば、サービスが失効している、デジタル鍵がないなどの特定の理由で、署名及びａｂエラーコードの送信をすることはできず、サービスサブスクリプションをチェックし、サービスの署名付き鍵の数をチェックし、（例えば、ペアリング中にシステム１１０から受信されたｏｗｎｅｒ．ＰＫを使用して）オーナー署名の有効性をチェックし、並びに／又は（例えば、製造業者ＯＥＭルート証明書へのアクセスを使用して）ＳＥ署名の有効性をチェックする。ＫＴＳ１２５０はまた、鍵がシステム内若しくはシステムＯＥＭバックエンド内で削除されたときにデバイス上の鍵を取り消すことができ、デバイス上の鍵が削除されたときにシステムＯＥＭバックエンドを通じてシステム内の鍵を取り消すことができ、及び／又は最初の友人トランザクションの前に共有された友人鍵情報が既にシステムにプロビジョニングされていることを友人デバイスに通知することができる。

【０２１９】

いくつかの実施形態では、提案されるシステムは、非対称暗号法を使用して、システム及びデバイスを相互に認証する。デバイスは、いくつかの実施形態では、既知のシステムにのみその識別情報を明らかにする。より高速なトランザクションが必要とされる状況では、追従するトランザクションは、非対称トランザクションにおいて合意された共有シークレットを使用して、対称暗号法を通じてデバイスを認証することができる。鍵をデバイスにプロビジョニングするためにＴＳＭは必要ではない。公開鍵は、オーナーデバイスとシステムとのペアリングを通じて相互に交換されてもよい。オーナーは、次いで、デジタル鍵を友人及び家族に分配することができる。システムは、すべての関連する機能について完全にオフライン（すなわち、サーバ接続は不要）で機能すると考えられる。規制又はビジネス上の制約がある状況でオンライン接続を必要とする場合、それらの追加は、システム設計によってサポートされる。

【０２２０】

いくつかの実施形態では、複数のタイプの鍵が実施され、所与のデバイスは、複数のシステムの鍵を保持することができる（及びこれらのシステムのために異なる行を有し得る）。いくつかの実施形態では、次の鍵タイプが実施される。オーナー、友人、プロフェッショナルサービスプロバイダ、システム共有、及びアドホックサービス。

【０２２１】

いくつかの実施形態では、システムは、１つのみのオーナーデバイスを承認する。ペアリングされていない状態では、システムと関連付けられたデバイスは、オーナーデバイスと見なされる。オーナーデバイスがシステムと関連付けられた後、システムは、ペアリングされていない状態からペアリングされた状態に切り替わる。オーナーデバイス鍵は、オーナーペアリングプロセスを通じて、鍵追跡サーバによって追跡される。適切な資格を定義し、割り当てるのは、システムＯＥＭ次第である（以下を参照されたい）。システムは、いくつかの友人デバイスを承認することができる。友人デバイスは、システム上に制限された資格を有してもよい。それらは、鍵を発行する際にオーナーによって割り当てられ、友人鍵のためのシステムＯＥＭポリシーにしたがってシステムによってチェックされる。それらはまた、システムによって承認されるために、追跡サーバに登録される必要もあり得る。プロフェッショナルサービスプロバイダ鍵の発行は、ネイティブに管理されず、ａｐｐを通じて管理される。ａｐｐは、オーナーが鍵をプロフェッショナルサービスプロバイダ（professional service provider、ＰＳＰ）と共有する方法を提供する。サーバで代表されるＰＳＰは、友人と類似しているが、その使用のためにイモビライザートークンを必要としない。ＰＳＰが常にオンラインであると仮定されるため、イモビライザートークンを含み、ＫＴＳによって追跡される鍵を従業員に発行する。従業員デバイスは、鍵を共有することができない。システム共有モデルでは、オーナーは、システム共有会社のサーバである。それは、友人鍵をシステム共有ユーザに発行し、鍵が追跡されるシステムｅを取る。システム共有ユーザは、自身のデバイスからアドホックサービス鍵を発行する

ことができる。システムオンライン／オフライン状況では、システムとの最初のトランザクションに関して、友人鍵と同一のルールが適用される。アドホック実行のために、システムは、同時にアクティブな単一のサービスデバイスを承認する。いくつかの実施形態では、サービスデバイスは、更なる鍵を他のエンティティに発行することができない。それらは、他の制限された資格を有してもよい。

【０２２２】

いくつかの実施形態では、デジタル鍵は、鍵識別子、鍵フレンドリー名、ＶＩＮ、システム公開鍵、鍵イモビライザートークン、スペアイモビライザートークン、オーナー資格、デバイス公開鍵、デバイス情報及びＯＳ情報、鍵タイプ、受信者アカウント識別子、鍵追跡サービスＵＲＬ、システムメタデータ、開始日、失効日、受信者資格、ＳＥ署名、鍵追跡署名などの様々なフィールドのうちの１つ以上を（例えば、そのタイプに応じて）含むデータ構造で表される。いくつかの実施形態では、デジタル鍵は、データ構造のあるインスタンスで表される。異なるタイプの鍵はまた、異なるフィールドのセットを有してもよい。

【０２２３】

いくつかの実施形態では、資格は、システムと関連付けられた各デバイスの対応する公開鍵と共にシステムによって記憶される。接続が利用可能である場合、システムＯＥＭポリシーに応じて、資格は、ネットワークを介してオーナーによって変更され得る。資格の変化が許容されない場合、現在の鍵を取り消すことができ、新しい鍵を発行して、資格の変更を反映しなければならない。

共有鍵の例示的な最初の使用

【０２２４】

いくつかの実施形態では、鍵が友人又は家族と共有されている場合、システム１１０は、検証された要求された署名を有した後に、友人の新しい公開鍵を記憶するべきである（以下で更に詳細に論じられる）。いくつかの実施形態では、標準トランザクションフローがこの状況で使用される。いくつかの実施形態では、次の追加の暗号要素がオーナーの標準トランザクションフローに対して使用される。ＳＥ．ｓｉｇ、ｏｗｎｅｒ．ＳＫ、ｏｗｎｅｒ．Ｓｉｇ、ｆｒｉｅｎｄ．ｅＰＫ／ｆｒｉｅｎｄ．ｅＳＫ、ｆｒｉｅｎｄ．ＰＫ／ｆｒｉｅｎｄ．ＳＫ、ｆｒｉｅｎｄ．Ｃｅｒｔ、及びＫＴＳ．ｓｉｇ。いくつかの実施形態では、ＳＥ．Ｓｉｇは、その鍵が信頼できるセキュア要素によって生成されたことを証明する公開鍵の署名である。いくつかの実施形態では、ｏｗｎｅｒ．ＳＫは、オーナーのシステムへのアクセスを共有するときに、友人の公開鍵に署名するために使用されるオーナーのデバイス内の長期非公開鍵である。この鍵は、標準トランザクションフローで使用されるもの（ｐｈｏｎｅ．ＳＫと名付けられている）と同一の鍵であってもよい。いくつかの実施形態では、ｏｗｎｅｒ．Ｓｉｇは、識別情報及び資格が正しく、かつ鍵が信頼できるセキュア要素上で生成されたことをオーナーが検証したときに、オーナーが友人の公開鍵に署名すると生成される。いくつかの実施形態では、ｆｒｉｅｎｄ．ｅＰＫ／ｆｒｉｅｎｄ．ｅＳＫは、各トランザクション上に生成される短期鍵ペアであり、各トランザクション後に削除されてもよい。いくつかの実施形態では、ｆｒｉｅｎｄ．ＰＫ／ｆｒｉｅｎｄ．ＳＫは、デバイスペアリング中に友人の電話によって生成される長期鍵ペアである。１つの鍵ペアは、関連付けられたシステム毎に生成されてもよい。いくつかの実施形態では、ｆｒｉｅｎｄ．Ｃｅｒｔは、証明書埋め込みｆｒｉｅｎｄ．ＰＫである。いくつかの実施形態では、ｓｅ＿ｆｒｉｅｎｄ．ＳＫ、ｏｗｎｅｒ．ＳＫ、及び（任意選択で）ｔｒａｃｋｉｎｇ．ＳＫによって署名される。いくつかの実施形態では、ｆｒｉｅｎｄ．ＰＫがシステム内に正常に記憶されると、証明書は、廃止になる。いくつかの実施形態では、ＫＴＳ．Ｓｉｇは、新しい鍵が記録されたことをシステムに通知する鍵追跡サーバによって追加される任意選択の署名である。

【０２２５】

このトランザクション変形例では、友人が初めてシステムに近づく前は、友人の公開鍵は、バックエンドによってシステムにプッシュされていないと仮定することができる。ペ

イロードは、ＡＵＴＨ１応答又はＳＥＳＳＩＯＮメッセージのうちの１つで、［ｍａｉｌｂｏｘ－ｄａｔａ］として、デバイス側に送信され得る。例えば、ｍａｉｌｂｏｘ＿ｄａｔａ＝ＳＥ署名、オーナー署名、及び鍵追跡署名を含むｆｒｉｅｎｄ．Ｃｅｒｔであり得る。データを送信するとき、デバイス１３０は、受信されたシステム識別子に基づいてデータを準備することができる。最初の友人トランザクションの前に、バックエンドがすべてのデータを既にシステムにプロビジョニングするように管理した場合、デバイスは、ＫＴＳリンクを通じて通知を取得し、データを送信することを控えることがあり得る。いくつかの実施形態では、ペイロードは、鍵共有プロセスにおける友人によって取得されたデータ要素からなり、このデータ要素は、友人の公開鍵、セキュア要素よる友人の公開鍵の署名、オーナーによる友人の公開鍵の署名、鍵追跡サーバによる友人の公開鍵の任意選択の署名、署名前にオーナーが公開鍵に添付した資格、友人のＳＥ署名の検証を可能にする友人ＳＥ証明書、及び／又はオーナーのＳＥ署名の検証を可能にするオーナーのＳＥ証明書を含み得る。

例示的なイモビライザートークン技術

【０２２６】

いくつかの実施形態では、イモビライザートークンを使用して、セキュリティを高めることができる。いくつかの実施形態では、モバイルデバイス１３０は、システム１１０とのすべてのエンジン始動トランザクションにおいて、イモビライザートークンと呼ばれるシークレットデータを記憶及び解放することができる。イモビライザートークンは、エンジンを始動できるようにするために、様々なＥＣＵによって検査されてもよいが、例えば、盗難防止対策としてシステム内に永続的に記憶されていなくてもよい。その結果、いくつかの実施形態では、イモビライザートークンが鍵フォブ又は関連付けられたモバイルデバイスによって分配されるまで、システムを開始することができない。いくつかの実施形態では、イモビライザートークンは、決して複製されるべきではない。いくつかの実施形態では、システム１１０は、モバイルデバイス１３０によって計算された署名の検証の際に、イモビライザートークンをローカルに記憶し、それをＥＣＵに解放することができるセキュア要素を埋め込むことができる。その場合、デバイスは、例えば、システムが単にデジタル署名検証及びそのセキュア要素のセキュリティに依存し得るため、このトークンを記憶及び解放する必要がない場合がある。

【０２２７】

イモビライザートークンが例示的な目的で、本明細書で論じられるが、この議論は、本開示の範囲を限定することを意図するものではないことに留意されたい。むしろ、イモビライザートークンは、開示された技術を使用して処理することができるセキュリティトークン又は第２レベルのセキュリティトークンの一例である。

【０２２８】

様々な技術を使用して、イモビライザートークンをモバイルデバイスのセキュア要素内に記憶することができ、この技術は、システム製造業者間で様々であってもよい。いくつかの実施形態では、１つの（又は１セットの）イモビライザートークン（単数又は複数）は、オーナーペアリングステップ中にシステム１１０によって生成され、標準トランザクションで開かれたセキュアチャネルを通じてデバイス１３０にプッシュされる。いくつかの実施形態では、１つの（又は１セットの）イモビライザートークン（単数又は複数）は、オーナーペアリングステップ中にシステム製造業者バックエンドによって生成され、ネットワークを通じてデバイスにプッシュされる。いくつかの実施形態では、イモビライザートークンは、オーナーによって友人に提供され、鍵共有中に友人の公開鍵で暗号化される。いくつかの実施形態では、友人がサービス鍵を作成するとき、その友人は、自身のイモビライザートークンをサービス鍵オーナーに提供する。システムとの次のトランザクションにおいて、又はネットワークを通じて、友人は、新しいイモビライザートークンを受け取り、このイモビライザートークンは、自分の公開鍵で登録されている。オーナーが取り消すか、又は友人が自分のモバイル鍵を削除すると、イモビライザートークンも削除される。その場合、オーナーは、新しい友人鍵を共有できるように、新しいイモビライザー

トークンを取得できる。オーナーへの新しいイモビライザートークンの発行は、友人のデバイスからの取り消し受信通知を生成するオーナー、並びに／又は友人の公開鍵及び対応するイモビライザートークンが削除されたことを確認するシステムに関連し得る。いくつかの実施形態では、デバイスは、イモビライザートークンを機密メールボックス内に記憶する。メールボックスは、スロットに編成されてもよい。これにより、１つのイモビライザートークンパッケージ（例えば、友人＋アドホック）を含むスロットを、有効なＳＥ署名を有する検証された友人デバイスから受信した公開鍵と（例えば、鍵共有を通じて）関連付けることができ得る。

【０２２９】

図１４は、いくつかの実施形態に係る、例示的なメールボックス編成を示すブロック図である。例示された実施形態では、オーナーの機密メールボックスには４つのスロットが存在し、３つのスロットが満たされている（但し、他の実施形態では、任意の数のスロットが実装されてもよい）。例示された実施形態では、各スロットは、最大で２つのイモビライザートークンを記憶するように構成されている。各スロットは、公開鍵（例えば、友人ＰＫ１４３０又はオーナーＰＫ１４４０）に割り当てることができる。例示的な実施例では、第１のスロット１４１０は、プロビジョニングされておらず、オーナーＰＫ１４４０を有する第４のスロットは、オーナーのために確保される。第２のスロット１４２０は、例示された実施形態では、例えば、オーナーペアリング中に、割り当てられていないイモビライザートークン１４２２及び１４２４を受信している。友人ＰＫ１４３０を有する第３のスロットは、友人公開鍵、及び共有の証拠としてイモビライザートークンのハッシュを含む。システムの友人デバイス上で鍵が取り消されると、同期プロセスは、取り消し受信通知をオーナーへ提供することができる。受信通知は、友人デバイスのセキュア要素によって署名されるか、又は別の方法で認証されてもよい。受信通知を受信したことに応じて、オーナーデバイスアプリケーションは、受信通知の公開鍵及び取り消された公開鍵自体に対応するメールボックススロットのすべてのコンテンツを削除することができる。

【０２３０】

いくつかの実施形態では、プライベートメールボックスは、例えば、モバイルデバイス１３０のメインプロセッサを関与させることなくシステム１１０で利用可能なデータを作成することによって、低出力モード（ＬＰＭ）動作を容易にすることができる。いくつかの実施形態では、セキュア要素は、例えば、デバイスがＬＰＭにある間に、プライベートメールボックスデータへのアクセスを提供することができ得る。

追加の鍵共有及び追跡の実施形態

【０２３１】

様々な実施形態では、オーナーは、別の人物又はエンティティと鍵を共有したいと考えている。オーナーは、個人又は会社であり得る。いくつかの実施形態では、オーナーは、友人によって生成された公開鍵に署名し、それを何らかの特定の資格と関連付ける。オフライン技術は、（例えば、図１５に示すように）ネットワークを介してシステム１１０に到達できない場合に使用してもよく、一方、オンライン技術は、（例えば、図１６に示すように）システム１１０に到達できる場合に使用してもよい。

【０２３２】

例示された実施形態では、１５０２で、システムは最初に、カウンタｓｙｓｔｅｍ．ＧｅｎＣｏｕｎｔ（共有鍵の数と関連付けられた）、オーナー公開鍵ｏｗｎｅｒ．ＰＫ、ｓｈａｒｅｅ証明書（共有が既に発生している場合）、及びシステム証明書ｓｙｓｔｅｍ．Ｃｅｒｔを記憶する。オーナーデバイス１３０は、カウンタＣｏｐｙＧｅｎＣｏｕｎｔ、ｏｗｎｅｒ．ＰＫ、及び任意の現在のｓｈａｒｅｅ証明書のコピーを記憶する。いくつかの実施形態では、鍵共有は、現在のカウンタ値を維持し、共有鍵を取り消すとカウンタ値が増加する。１５０６で、オーナーデバイス１３０は、資格のセットを選択し、次いで、１５０８で、ｓｈａｒｅｅデバイス１６０に鍵共有試行及び資格を通知する。

【０２３３】

１５１０で、例示された実施形態では、友人のデバイスは、長期公開鍵ペア（例えば、

ｎｅｗＳｈａｒｅｅ．ＳＫ及びｎｅｗＳｈａｒｅｅ．ＰＫと称され得る）を生成する。例示された実施形態では、ｓｈａｒｅｅデバイス１６０はまた、暗号化のための公開鍵及び非公開鍵ペア（例えば、ｎｅｗＳｈａｒｅｅ．ｅｎｃＳＫ及びｎｅｗＳｈａｒｅｅ．ｅｎｃＰＫ）を生成する。ｓｈａｒｅｅデバイス１６０はまた、示された資格を埋め込む証明書を生成する。

【０２３４】

１５１２で、ｓｈａｒｅｅ１６０は、署名要求で証明書ｎｅｗＳｈａｒｅｅ．Ｃｅｒｔをオーナーデバイス１３０に送信する。デジタル鍵を友人と共有するようにオーナーデバイス１３０に要求すると、友人のＳＥは、公開鍵を含む証明書ｎｅｗＳｈａｒｅｅ．Ｃｅｒｔを作成することができ、その公開鍵は、ＳＥ上でローカルＣＡによって署名される。証明書は、オーナーが友人の公開鍵の信頼性を検証できるようにするデータ要素を含んでもよい。署名検証のための証明書チェーンの詳細技術については、以下で論じる。

【０２３５】

１５１４で、オーナーデバイス１３０は、（例えば、ｓｈａｒｅｅデバイス１６０の電話製造業者（manufactuer）又は電話ＯＥＭの）ルート証明書を使用して、ｎｅｗＳｈａｒｅｅ．Ｃｅｒｔをチェックし、埋め込み型資格がオーナーによって選択されたものと一致することをチェックし、（例えば、バイオメトリック認証、パスコードなどを使用して）ユーザを認証する。認証が失敗した場合、いくつかの実施形態では、オーナーデバイス１３０は、共有を進めないように構成されている。これは、例えば、盗難オーナーデバイスによる共有を防止することができる。

【０２３６】

１５１６で、オーナーデバイス１３０は、資格及び生成カウンタなどの１つ以上のデータ要素をデジタル鍵構造に追加し、オーナー非公開鍵ｏｗｎｅｒ．ＳＫでそれに署名し、完全なデータを友人にｗｒａｐｐｅｄＤａｔａとして送信し返してもよい。いくつかの実施形態では、これは、ｎｅｗＳｈａｒｅｅ．ＧｅｎＣｏｕｎｔ＝ＣｏｐｙＧｅｎＣｏｕｎｔ；ｎｅｗＳｈａｒｅｅ．Ｓｉｇ＝ｓｉｇｎ（ｎｅｗＳｈａｒｅｅ．Ｃｅｒｔ｜ｎｅｗＳｈａｒｅｅ．ＧｅｎＣｏｕｎｔ）ｗｉｔｈ　ｏｗｎｅｒ．ＳＫ；及びｗｒａｐｐｅｄ　ｄａｔａ＝ｅｎｃｒｙｐｔイモビライザートークン［＋データ］ｗｉｔｈ　ｎｅｗＳｈａｒｅｅ．ｅｎｃＰＫを決定することを含む。これにより、システム１１０は、例えば、オーナーデバイス１３０が資格を確認したことを検証できるようにし得る。

【０２３７】

１５１８で、オーナーデバイス１３０は、署名、カウンタ、及び暗号化されたデータをｓｈａｒｅｅデバイス１６０に送信する。これは、例えば、ｎｅｗＳｈａｒｅｅ．ＧｅｎＣｏｕｎｔ、ｎｅｗＳｈａｒｅｅ．Ｓｉｇ、及びｗｒａｐｐｅｄＤａｔａを含んでもよい。

【０２３８】

１５２０で、例示された実施形態では、ｓｈａｒｅｅ１６０は、署名及びカウンタをシステム１１０に送信する。１５２２で、システムは、署名及び証明書を検査し、カウンタをチェックし、ｓｈａｒｅｅを許可されたリストに追加する。例えば、これは、ｎｅｗＳｈａｒｅｅ．Ｓｉｇを検査し、ｎｅｗＳｈａｒｅｅ．Ｃｅｒｔを検査し、ｎｅｗＳｈａｒｅｅ．ＧｅｎＣｏｕｎｔ＝＝ｓｙｓｔｅｍ．ＧｅｎＣｏｕｎｔを検査し、成功した場合、ｓｈａｒｅｅを許可されたリストに追加することを含み得る。

【０２３９】

いくつかの実施形態では、開示されたオフライン技術は、様々な状況において、例えば、広域ネットワーク接続又はサーバへの任意の接続なしに、分散鍵共有を可能にすることができる。

【０２４０】

いくつかの実施形態では、生成カウンタは、取り消された鍵の再使用を保護する。いくつかの実施形態では、オーナー又は友人のいずれかが、鍵追跡サーバに到達して署名を取得することができる。いくつかの実施形態では、システムＯＥＭビジネスバックエンドに

到達する鍵追跡サーバ又はオーナーデバイスのいずれかが、共有されたデジタル鍵構造の１つ以上の関連要素、例えば、友人の公開鍵、資格、生成カウンタ、開始日及び失効日、鍵識別子、鍵フレンドリー名、ＳＥ署名、オーナー署名、並びに／又はＫＴＳ署名など、をシステムに提供する。

【０２４１】

図１６は、例示的なオンライン通信を示す詳細な通信図である。例示された実施形態では、いくつかの要素は、図１５の要素と類似している。例示された実施形態では、オーナーデバイスはまた、現在のｓｈａｒｅｅデバイスのセットの新しいアクセスリストを生成し、新しいアクセスリストの署名されたコピーをシステム１１０に送信する。

【０２４２】

いくつかの実施形態では、システム製造業者は、遠隔動作を実行するためのデバイスによって、システム１１０がインターネットなどの広域ネットワークに到達することを所望により可能にし得る。システムがインターネット上で直接公開され、攻撃に対してより脆弱になることを回避するために、システム製造業者サーバは、システム製造業者のサーバへのデバイスの認証時にシステムへのアクセスを提供するプロキシとして機能し得る。いくつかの実施形態では、システムＥＣＵに記憶された公開鍵は、ベストエフォート基準でシステム製造業者のサーバと同期される。いくつかの実施形態では、新しいオーナーがペアリングされるたびに、及び新しい友人鍵が追加されるたびに、システムは、その記憶された公開鍵及び取り消しリストを、システム製造業者のサーバと同期することを試みる。デバイスとのペアリングの間、システムは、デバイスに、インターネットを介してシステムに到達する方法としてシステム製造業者のサーバと共に使用される非秘密の固有の識別子及びＵＲＩを提供することができる。このＵＲＩ及び固有の識別子を使用して、デバイスは、システム製造業者のサーバとのセキュアセッションを確立することができる。セキュアセッションは、デバイスがサーバを認証できるようにＴＬＳのような標準プロトコルを使用することができる。セッションが確立されると、デバイスは、セキュア要素を使用して、システムによって提供されたチャレンジ及び／又はシステムによって実行されるべきコマンドに署名することができる。プロキシとして機能するシステム製造業者のサーバは、パケットフォーマット及び署名が正しいことをチェックしてから、要求をシステムに送信することができる。サービス又は不正な形式のパケットの妨害に対するファイアウォールタイプの保護もまた、システム製造業者のサーバによって処理されてもよい。いくつかの実施形態では、ＴＬＳサーバ認証は、デバイスが有効な鍵でサーバチャレンジに正常に署名した後に、クライアント認証でアップグレードされてもよく、これは、複雑性が増大することを犠牲にして、ＤＯＳ攻撃をフィルタするのに役立ち得る。

【０２４３】

いくつかの実施形態では、次のオンライン遠隔動作が、ＯＥＭサーバとのセキュアセッション内で利用可能である。ドアロック／ロック解除、トランクロック解除、友人鍵取り消し、オーナーデバイス除去、オーナーデバイスのアンペアリング、及び／又は空調若しくは加熱などの快適性アクション。

【０２４４】

システム製造業者は、新しい鍵の発行若しくはオーナーペアリングなどの、本明細書における動作の一部を追跡及び／又は制御することを望み得る。本文脈中、友人／オーナーデバイスによって実行される署名に加えて、システム製造業者のサーバによって生成される署名は、特定の動作を可能にするためにシステムによって必要とされ得る。しかしながら、このような要件は、これらの動作に関するオフライン機能を妨害し得る。システム製造業者のサーバは、オーナーのデバイス、友人のデバイス、又は新しい鍵が発行されたシステムによって通知されてもよく、それにより、関与する３つの関係者のうちの少なくとも１つは、サーバから署名を取り出すためにオンラインであるべきである。関係者のいずれもサーバに到達できない場合、システムは、署名がシステム製造業者のサーバから取り出され得るまで、例えば、制限された機能で、鍵を一時的に使用することを依然として可能にすることができる。いくつかの実施形態では、システム製造業者は、例えば、そのサ

ーバがいくつかのポイントで利用不可能になる場合に、追加のサーバ署名の必要性を遠隔で無効にすることができる。

【０２４５】

いくつかの実施形態では、システムがオフラインである場合、友人のデバイスは、前述したように、最初のトランザクションにおいてデータ要素をシステムに提示する。イモビライザートークンの転送は、このトランザクションの一部として実行され得る。いくつかの実施形態では、この転送にはメールボックスが使用されてもよい。オーナー及び友人が異なる製造業者からのデバイスを使用する場合、送信者は、受信者の公開鍵に署名するために、ＳＥによって使用される制御機関セキュリティドメイン（ＣＡＳＤ）証明書などの証明書を提供することができる。

【０２４６】

いくつかの実施形態では、鍵追跡のために、ＳＥは、一時的なセキュア要素識別情報（ローカルＣＡ）を提供し、これは、ＳＥがワイプされるまで不変である。この識別情報は、デバイス製造業者によって制御されてもよく、製造業者のローカルのＣＡルート証明書を使用してシステムＯＥＭによって検証することができる。識別情報は、製造業者バックエンドによってＳＥ－ＩＤにリンクされてもよく、これは、外部識別情報に公開されない。鍵追跡サーバ１２５０は、いくつかの実施形態では、デジタル鍵に署名する前に、デバイス適格性を検証する責任がある。検証は、セキュア要素の署名を検証できるようにする、デバイス製造業者の一時的なルート証明書を使用して実行されてもよい。加えて、デバイスは、次の情報を配信してもよい。デバイス製造業者、デバイスハードウェア、デバイスＯＳバージョン、及び／又はＪＣＯＰプラットフォーム識別子。

【０２４７】

いくつかの実施形態では、ＫＴＳ１２５０は、記憶されたデータに対してプライバシー保護を提供するために、ＯＥＭビジネスバックエンドから物理的及び論理的に分離される。いくつかの実施形態では、ＫＴＳ１２５０は、システムが盗難され、オーナーがアクセスを許可している場合にのみ、データクエリにアクセスされるため、ビジネス目的に利用されない場合がある。いくつかの実施形態では、モバイル鍵を有する任意のデバイスは、ＵＲＬがシステムからオーナーデバイスに、並びにオーナーデバイスから友人デバイス及びサービスデバイスにモバイル鍵で配信されるため、ＫＴＳと交信することができる。いくつかの実施形態では、ＫＴＳは、次の通信インタフェースを有する。ＫＴＳ－デバイス、ＫＴＳ－ＯＥＭビジネスバックエンド／システム、ＫＴＳ－デバイス。

【０２４８】

いくつかの実施形態では、ＫＴＳ－デバイスインタフェースは、両方の関係者が通信を開始できるようにするが、最初のステップは、モバイル鍵を受信した後に、デバイスによって行われるべきである。このインタフェースは、友人デバイスが新しいモバイル鍵をサーバに提供するときに、次の動作に使用することができる：サービス有効性をチェックする、サービスの署名付き鍵の数をチェックする、（例えば、電話ＯＥＭルート証明書へのアクセスを用いて）ＳＥ署名の有効性をチェックする、（例えば、システムＰＫのコピーを使用して）オーナー署名の有効性をチェックする、モバイル鍵及びデバイス情報を登録する、最初のトランザクションでシステムに提示されたモバイル鍵データに署名する、システムにプロビジョニングするためにモバイル鍵データをシステムＯＥＭバックエンドに提供する（システムがオンラインの場合）、署名付きモバイル鍵をデバイスに送信し返すか、又はエラー及び理由コードを提供する。理由コードの例としては、無効なＳＥ署名／ホワイトリストに登録されていないＳＥ、無効／未知のオーナー署名、有効ではないサービスサブスクリプション、及び／又は発行されたモバイル鍵が最大数に到達、が挙げられ得る。いくつかの実施形態では、このインタフェースは、友人が友人のデバイス上の鍵を削除して、取り消し要求をサーバに送信するときに使用されてもよい。いくつかの実施形態では、このインタフェースは、ＫＴＳ１２５０が成功した取り消しに関してオーナーデバイスに通知するときに使用されてもよい。例えば、モバイル鍵状態の変化が発生すると、ＫＴＳ１２５０は、オーナーデバイスに接触してアプレット状態を更新してもよい（友

人公開鍵及び関連付けられた追跡データを除去する（例えば、図１４に示すように、友人モバイル鍵データのハッシュ）。

【０２４９】

いくつかの実施形態では、ＫＴＳ－ＯＥＭビジネスバックエンド／システムインタフェースを使用して、システム内の取り消し要求のＯＥＭビジネスバックエンドを通知するか、及び／又は削除がＯＥＭオーナー若しくは友人アカウントを通じて、若しくはシステム内で開始されたときに、デバイス上の鍵の取り消しを要求する。

例示的な鍵取り消し技術

【０２５０】

鍵は、システム１１０及びモバイルデバイス１３０を含む様々な場所で取り消すことができる。いくつかの実施形態では、鍵の有効性は、システムが完全なアクセスリストを受信するときにインクリメントされる生成カウンタを使用して管理される。鍵を除去するために、新たなアクセスリストは、取り消されるはずの鍵を含まず、現在のアクセスリストに対して少なくとも１ずつインクリメントされた生成されたカウンタを含む。いくつかの実施形態では、システム１１０は、新しい現在の値よりも小さい生成カウンタで署名された、任意の以前の又は保留中の要求を拒否するように構成されている。いくつかの実施形態では、生成カウンタは、リストへの増分追加が実行されるときは変化しないので、既存のエントリが有効なままであることができる。いくつかの実施形態では、カウンタは、単調であり、ロールオーバーを回避するのに十分な大きさの値までカウントするように構成されている。

【０２５１】

図１７は、モバイルデバイス１３０による例示的な鍵取り消しを示す通信図である。例示された実施形態では、モバイルデバイス１３０は、１７０２で作成されたセキュアチャネルを介して、１７０４で鍵取り消し要求を受信する。１７０６で、モバイルデバイス１３０は、次いで、セキュア要素（又はいくつかの他のセキュア回路）に命令して、取り消されたものとして鍵をマークする。この状態では、鍵は、トランザクションに使用することはできないが、取り消し証明に署名するためにのみ使用できる。いくつかの実施形態では、モバイルデバイス１３０は、取り消された鍵上の取り消し証明をＳＥから要求するように構成されており、この取り消し証明は、１７０６に示すように、ｐｈｏｎｅ．ＳＫによって署名され得る。例示された実施形態では、モバイルデバイスは、取り消し証明１７０８を返し、サーバ１４６は、１７１０で、ｐｈｏｎｅ．ＰＫを使用して、取り消し証明の信頼性を検証する。いくつかの実施形態では、モバイルデバイス１３０は、要素１７１２～１７１６に示すように、取り消された状態の鍵を削除するように、ＳＥに命令するように構成されている。他の実施形態では、本明細書で論じられる様々な要素のうちのいずれかは、取り消し証明を検証するように構成されてもよい。いくつかの実施形態では、取り消しフローは、ＯＥＭバックエンドに到達し、鍵状態を同期することを要求する、デバイスへのプッシュ通知によって開始する。

【０２５２】

様々な実施形態では、開示された技術により、取り消された鍵がｓｈａｒｅｅデバイス上で実際に除去されたか又は凍結されたことの証明を用いて、システム、オーナーデバイス、及び／又はインターネットベースの取り消しを可能にし得る。例えば、別のオーナーデバイスとのペアリングの前に、取り消し技術もまた、オーナーデバイス上で使用され得る。いくつかの実施形態では、図１７の開示された取り消し技術は、例えば、サーバを伴わずに、友人モバイルデバイスとオーナーモバイルデバイスとの間で直接使用されてもよい。例えば、友人デバイスは、取り消し受信通知をオーナーデバイス１３０に直接送信してもよい。

例示的なメールボックス技術

【０２５３】

図１８は、いくつかの実施形態に係る、例示的なメールボックス技術を示すブロック図である。例示された実施形態では、アプリケーションプロセッサ１３６は、プライベート

メールボックス１８３０への読み書きアクセス、及び機密メールボックス１８４０への書き込みアクセスを有する、ＯＳ及びアプリケーション１８１０を実行する。セキュア要素１３４はまた、例示された実施形態では、長期システム公開鍵及び電話秘密鍵のための記憶装置１８２０を含む。システム１１０は、例示された実施形態では、システム秘密鍵及び電話非公開鍵のための記憶装置１８２５を含み、また、ユーザ設定のための記憶装置１８３５及びイモビライザートークンのための記憶装置１８４５を含む。

【０２５４】

いくつかの実施形態では、メールボックス機構は、セキュア要素が、アプリケーションプロセッサ１３６によって及びシステム１１０によってアクセス可能な小さいデータバッファを記憶できるようにする。これらのデータバッファは、セキュア要素揮発性又は不揮発性メモリ内に記憶され得、トランザクション又はプロビジョニング中に読み出し／書き込みされてもよい。いくつかの実施形態では、デバイス１３０上に作成された各鍵は、異なるセキュリティ特性を有する２つのメールボックスと関連付けられ、異なる使用状況をターゲットにしている。

【０２５５】

プライベートメールボックス１８３０は、いくつかの実施形態では、例えば、デバイス内部有線リンクを使用して、アプリケーションプロセッサ１３６に読み書きアクセス可能である。また、いくつかの実施形態では、前述のセキュアチャネルが登録されたｓｙｓｔｅｍ．ＰＫを用いて確立されると、例えば、ＲＦインタフェースを使用して、システム１１０によっても読み書きアクセス可能である。交換されたデータは、電話追跡を防止するために確立されたセキュアチャネルによって保護され得る。いくつかの実施形態では、このメールボックスは、ユーザ設定をＡＰ１３６からシステムに送信し、診断情報をシステムからＡＰ１３６に送信し、特定のコマンドをシステムに送信し、及び／又はＢｌｕｅｔｏｏｔｈペアリング情報をシステムに送信するために使用されてもよい。いくつかの実施形態では、このメールボックスは、ランダムアクセスをサポートし、そのコンテンツを、オフセット／長さパラメータを使用して読み出し／書き込みすることができる。

【０２５６】

機密メールボックス１８４０は、いくつかの実施形態では、システムに読み書きアクセス可能であり、アプリケーションプロセッサ１３６によって書き込みアクセス可能である。いくつかの実施形態では、また、データがｎｅｗＳｈａｒｅｅ．ｅｎｃＰＫで暗号化されたときに、アプリケーションプロセッサ１３６によって、例えば、内部有線リンクを介して書き込みされ得る。いくつかの実施形態では、鍵オブジェクト構成によって許可された場合、及びユーザの同意がある場合に、機密メールボックスのコンテンツは、別の信頼されたセキュア要素の証明書／公開鍵（pubkey）で暗号化されてエクスポートされ得る。いくつかの実施形態では、ＲＦ上で交換された任意のデータは、確立されたセキュアチャネルによって保護されて、ユーザ追跡を防止する。いくつかの実施形態では、このメールボックスは、イモビライザートークンをオーナーデバイスから友人デバイスにプロビジョニングするため、イモビライザートークンをシステムからデバイスにプロビジョニングするため、及び／又はイモビライザートークンをデバイスからシステムに解放するために使用され得る。いくつかの実施形態では、このメールボックスは、ランダムアクセスをサポートし、そのコンテンツを、オフセット／長さパラメータを使用して読み出し／書き込みすることができる。例えば、図１４を参照して上述したように、１組のイモビライザートークンは、機密メールボックス内で異なるオフセットで書き込み／読み出しすることができる。

例示的な証明書チェーン

【０２５７】

いくつかの実施形態では、公開鍵基盤（public key infrastructure、ＰＫＩ）機構を使用して、特定のデジタル鍵まで信頼のチェーンを構築する。いくつかの実施形態では、これらのチェーンは、デバイス証明書チェーン、システム証明書チェーン、オーナーペアリング鍵証明、及び鍵共有鍵証明を含む。

【０２５８】
いくつかの実施形態では、デバイス製造業者は、他のデバイス製造業者からの証明書署名要求（certificate signing request、ＣＳＲ）を処理するためのセキュアサービスを提供するべきである。ルート証明書のクロス署名は、所与のシステム製造業者のホワイトリストに登録されたすべてのデバイス製造業者に必要とされ得る。署名付き証明書は、所有しているデバイス製造業者のみによって又はすべての他のデバイス製造業者によって、デバイスＯＳに埋め込まれてもよい。後者の選択肢は、鍵共有中の証明書のデータ転送を低減することができるが、すべての他のデバイスがデバイスＯＥＭの証明書を記憶することを必要とする。いくつかの実施形態では、システム製造業者は、すべてのホワイトリストに登録されたデバイス製造業者からのＣＳＲを尊重するために、セキュアサービスを提供するべきである。いくつかの実施形態では、署名付き証明書は、デバイスのＯＳに記憶され、検証のためのオーナーペアリング中に提供される。
【０２５９】
図１９は、いくつかの実施形態に係る、例示的なデバイス証明書チェーンを示すブロック図である。例示された実施形態では、製造業者ルート証明書２１０２は、フット（foot）非公開鍵２１０８を使用して自己署名され、セキュア要素１３４のセキュアプロビジョニングに使用される（ルート非公開鍵はまた、ローカルＣＡ証明書１２３２及びローカルＣＡ非公開鍵１２３４の生産プロビジョニング（production provisioning）にも使用される。
【０２６０】
例示された実施形態では、ＯＥＭ１ルート証明書２１１２は、ＯＥＭルート非公開鍵２１１８を使用して自己署名され、これはまた、製品プロビジョニング（product provisioning）中にＳＥ２１１０に提供されるＣＡＳＤ証明書２１１４を署名するためにも使用される。例示された実施形態では、ＯＥＭ１ルート証明書２１１２はまた、信頼された交換を使用して、電話ＯＥＭバックエンド２１７２から電話製造業者バックエンド１２３０に提供される。バックエンド１２３０は、署名２１０６でルート証明書２１１２に署名し、署名付き証明書をＯＳ２１２０にプロビジョニングする。
【０２６１】
したがって、いくつかの実施形態では、各適格なセキュア要素は、生産プロビジョニングされた公開鍵ペア（例えば、ＣＡＳＤ）を含み、それにより、ＳＥは、本物のＳＥ上に公開鍵が作成されたことを証明することができる。例示された実施形態では（I the illustrated embodiment）、ＣＡＳＤ公開鍵は、ＯＥＭバックエンド内に安全に保持されたルート鍵によって署名される証明書に埋め込まれる。製造業者は、ＣＡＳＤ署名に基づいて、インスタンス鍵ペアの信頼性を証明するアプレットインスタンス内に記憶されたローカルＣＡ証明書に署名することができる。これにより、証明書チェーンからのＳＥＩＤなどの静的識別子の排除を可能にし得る。デバイスが受信された鍵のＳＥ署名を検証できるようにするために、すべての適格なデバイスＯＥＭのルート証明書は、それぞれのバックエンド間で交換され、いくつかの実施形態では、次いで、受信デバイスＯＥＭルート非公開鍵２１１８で署名される。対応するルート証明書は、すべてのＯＥＭデバイスのＳＥに安全にプロビジョニングされる。署名付きＯＥＭルート証明書は、すべてのＯＥＭデバイスに記憶される。証明書の信頼性は、ＳＥ内での各使用前に検証されるため、セキュアな記憶は必要ではない。
【０２６２】
様々な技術では、開示された技術は、本明細書で開示する技術を実装するために、様々な製造業者からのモバイルデバイスの使用を容易にし得る。
【０２６３】
図２０は、いくつかの実施形態に係る、例示的なデバイス証明書チェーンを示すブロック図である。例示された実施形態では、製造業者ルート証明書２１０２は、システムＯＥＭバックエンド１２７０のルート非公開鍵２２１８を使用して（例えば、信頼された交換を介して）、署名される（ＯＥＭ署名２２１９）。いくつかの実施形態では、デバイスＯ

ＥＭがシステム製造業者によってホワイトリストに登録されるか、又はシステムＯＥＭがデバイス製造業者によってサポートされると、デバイスルート証明書は、システムＯＥＭルート非公開鍵によって署名される。いくつかの実施形態では、ＯＥＭ１ルート証明書２２１２は、各システム１１０に安全に記憶される。例示された実施形態では、署名付き製造業者ルート証明書２１０２は、デバイスオペレーティングシステム２１２０に記憶される。

【０２６４】

いくつかの実施形態では、例えば、システムがデバイスルート証明書を記憶するように構成されている場合、オーナーペアリング交換を簡略化することができる。その場合、デバイスＯＥＭは、システムＯＥＭ署名付きルート証明書２１０２をデバイスＯＳ内に記憶する必要がない場合がある。

【０２６５】

図２１は、いくつかの実施形態に係る、システムＯＥＭ署名付きローカルＣＡを用いる例示的な技術を示すブロック図である。いくつかの実施形態では、ローカルＣＡ証明書が設定時にシステムＯＥＭによって署名されると、システム１１０は、次いで、その埋め込まれたシステムＯＥＭルート証明書を使用して、オーナー公開鍵証明書を直接検証することができる。例示された実施形態では、製造業者ローカルＣＡ証明書２１３２は、デバイスＯＳ２１２０に記憶され、デバイス製造業者バックエンド１２３０及びシステムＯＥＭバックエンド１２７０の両方によって署名される。

【０２６６】

図２２は、いくつかの実施形態に係る、例示的なオーナーペアリング証明書チェーンを示すブロック図である。いくつかの実施形態では、オーナーペアリングセッション中、オーナーデバイス１３０は、長期鍵ペアを作成する。公開鍵は、オーナーデバイスＳＥによって署名されて、システム１１０に転送されるデバイス公開鍵証明書２４３２を、ＳＥ証明書２１３２及びシステムＯＥＭ－署名付きデバイスルート証明書２１０２と一緒に生成する。次いで、システムは、システムＯＥＭルート証明書２１１２を使用してデバイスＯＥＭルート証明書２１０２を検証し、デバイスＯＥＭルート証明書２１０２を使用してＳＥ証明書２１３２を検証し、ＳＥ証明書２１３２を使用してデバイス公開鍵を検証することができる。いくつかの実施形態では、すべての検証が成功すると、デバイス公開鍵は、オーナー公開鍵としてシステムに記憶される。

【０２６７】

図２３は、いくつかの実施形態に係る、システムＯＥＭ－署名付きローカルＣＡを使用する例示的なオーナーペアリングを示すブロック図である。システムが各ホワイトリストに登録されたデバイスＯＥＭの（システムＯＥＭ署名付き）ルート証明書を記憶するように構成されているいくつかの実施形態では、デバイスＯＥＭルート証明書がセキュアなメモリに記憶されているならば、オーナーペアリングの一部として、デバイスＯＥＭルート証明書を提供する必要性及びデバイスＯＥＭルート証明書の検査が排除され得る。システム内にすべてのデバイスＯＥＭ証明書を記憶する必要性は、オーナーデバイスが図示のようにシステムＯＥＭによって署名されたローカルＣＡ証明書を提供する場合には排除され得る。

【０２６８】

例示された実施形態では、製造業者ローカルＣＡ証明書２１３２は、製造業者（署名２３０７）によって及びＯＥＭ（署名２５１９）によって署名され、ＯＥＭ１ルート証明書２１１２を使用して検証され、次いで、デバイス公開鍵証明書２４４２を検証するために使用される。

【０２６９】

図２４は、いくつかの実施形態に係る、例示的な鍵共有証明書チェーンを示すブロック図である。いくつかの実施形態では、署名付き公開鍵が鍵共有プロセス中に友人デバイスからオーナーデバイスに送信されると、オーナーデバイスのセキュア要素は、ＣＡ識別子フィールドを通じてＳＥ証明書を識別し、ＡＰから対応するＯＥＭルート証明書を取り出

すことができる。例示された実施形態では、ＳＥ１３４は、製造業者ルート証明書を使用して、ＯＥＭ証明書２１１２を検証し、次いで、ＯＥＭ証明書を使用して、ＯＥＭ　ＳＥ２１１０から受信されたＯＥＭ　ＣＡＳＤ証明書（これはまた、ＳＥ証明書とも称され得る）を検証する。次いで、そのＯＥＭ　ＣＡＳＤ証明書を使用して、友人の公開鍵証明書を検証する。いくつかの実施形態では、検証が成功した場合、オーナーデバイスは、オーナー公開鍵と関連付けられた非公開鍵を使用して、友人の公開鍵に署名し、この非公開鍵はまた、（オーナーペアリングで）システムに記憶される。

【０２７０】

いくつかの実施形態では、ＯＥＭ　ＣＡＳＤ証明書は、例えば、デバイスＯＥＭ署名によってＳＥ製造業者署名を置き換えるローカルＣＡスキームによって置き換えられ得る。

付加的な実施形態

【０２７１】

いくつかの実施形態では、装置は、セキュア回路と、システムとのペアリング動作を実行するための第１の要求を受信したことに応じて、システムとの第１の共有暗号鍵を確立するように構成されている１つ以上の処理要素と、を備え、セキュア回路は、公開鍵ペアと、公開鍵ペアに対応する証明書であって、この証明書は、公開鍵ペアの公開鍵を含む、証明書と、を生成するように構成されており、装置は、第１の共有鍵を使用して証明書を暗号化し、暗号化された証明書をシステムに送信するように構成されている。

【０２７２】

いくつかの実施形態では、セキュア回路は、決済トランザクションのための決済データを記憶するように更に構成されているセキュア要素である。いくつかの実施形態では、装置は、公開鍵ペアに基づいて生成された値を表示し、装置のユーザに、システムもまた値を表示していることを確認するように要求するように更に構成されている。いくつかの実施形態では、装置は、システムに動作を実行させるための第２の要求を受信することに応じて、第２の共有暗号鍵を確立し、公開鍵ペアの非公開鍵を使用して、システムから受信したチャレンジに対する応答を生成し、第２の共有暗号鍵を使用して応答を暗号化し、暗号化された応答をシステムに送信するように構成されている。いくつかの実施形態では、動作は、システムのドアを開けることと、システムのナビゲーションシステムを有効化することと、又はシステムのエンジンを始動することとを含む。いくつかの実施形態では、装置は、別のモバイルデバイスがシステムにアクセスできるようにする第２の要求を受信することに応じて、公開鍵ペアの非公開鍵を使用して、他のモバイルデバイスのセキュア回路によって生成された別の公開鍵ペアの証明書に署名するように構成されている。いくつかの実施形態では、装置は、広域ネットワークを介して、セキュア回路によって署名された証明書のサーバ署名を要求するように更に構成されており、サーバ署名は、他のモバイルデバイスによって要求された動作を許可するかどうかを判定するために、システムによって使用可能である。いくつかの実施形態では、装置は、他のモバイルデバイスがモバイルデバイスのユーザによって指定された資格のセットのうちのものを実行することが許可されているかどうかを示すように更に構成されている。

【０２７３】

いくつかの実施形態では、非一時的コンピュータ可読媒体は、動作を引き起こすようにコンピューティングデバイスによって実行可能な命令をその上に記憶しており、その動作には、システムとのペアリング動作を実行するための第１の要求を受信することと、第１の要求に応じて、システムとの第１の共有暗号鍵を確立することと、デバイスのセキュア回路を使用して、公開鍵ペアと、公開鍵ペアに対応する証明書であって、この証明書は、公開鍵ペアの公開鍵を含む、証明書と、を生成することと、第１の共有鍵を使用して証明書を暗号化することと、暗号化された証明書をシステムに送信することと、が含まれる。

【０２７４】

いくつかの実施形態では、動作は、公開鍵ペアに基づいて生成された値を表示することと、コンピューティングデバイスのユーザに、システムが値を表示していることを確認するように要求することと、を更に含む。いくつかの実施形態では、動作は、システムに動

作を実行させるための第２の要求を受信することと、第２の要求に応じて、第２の共有暗号鍵を確立することと、セキュア回路及び公開鍵ペアの非公開鍵を使用して、システムから受信したチャレンジに対する応答を生成することと、第２の共有暗号鍵を用いて応答を暗号化することと、応答をシステムに送信することと、を更に含む。

【０２７５】

いくつかの実施形態では、動作は、別のモバイルデバイスがシステムにアクセスできるようにする第２の要求を受信することと、第２の要求に応じて、セキュア回路及び公開鍵ペアの非公開鍵を使用して、他のモバイルデバイスのセキュア回路によって生成された別の公開鍵ペアの証明書に署名することと、を更に含む。

【０２７６】

いくつかの実施形態では、装置は、システムに含まれるか又はシステムに連結するように構成されており、その装置は、１つ以上の処理要素を備え、この１つ以上の処理要素は、モバイルデバイスとの第１の共有暗号鍵を確立し、暗号化された証明書であって、この証明書は、第１の公開鍵ペアに対応し、かつ第１の公開鍵ペアの公開鍵を含み、この証明書は、第１の共有された暗号化された鍵を使用して暗号化されている、証明書をモバイルデバイスから受信し、暗号化された証明書を復号し、復号された証明書を記憶するように構成されている。

【０２７７】

いくつかの実施形態では、１つ以上の処理要素は、第１の公開鍵ペアに基づいて値を生成し、ユーザによってモバイルデバイス上に表示された対応する値と比較するために、システムのディスプレイ上に値を表示させるように更に構成されている。いくつかの実施形態では、１つ以上の処理要素は、システムによる１つ以上の動作のうちのどれにモバイルデバイスがアクセスする資格を有するかを示す情報を記憶するように更に構成されている。いくつかの実施形態では、１つ以上の処理要素は、システムに動作を実行させる要求に対して、モバイルデバイスにチャレンジを発行し、モバイルデバイスとの第２の共有暗号鍵をネゴシエーションし、チャレンジに対する応答を受信し、第２の共有暗号鍵を使用して応答を復号し、動作を許可する前に、第１の公開鍵ペアの非公開鍵を使用して、応答がモバイルデバイスによって署名されていることを検証するように更に構成されている。いくつかの実施形態では、１つ以上の処理要素は、別のモバイルデバイスによって生成された公開鍵ペアの証明書を受信し、証明書がモバイルデバイスによって第１の公開鍵ペアの非公開鍵によって署名されていると判定したことに応じて、他のモバイルデバイスに対する証明書を記憶し、他のモバイルデバイスのための記憶された証明書に基づいて、他のモバイルデバイスの動作を許可するかどうかを判定するように更に構成されている。

【０２７８】

いくつかの実施形態では、非一時的コンピュータ可読媒体は、動作を引き起こすようにシステムのコンピューティングデバイスによって実行可能な命令をその上に記憶しており、その動作には、モバイルデバイスとの第１の共有暗号鍵を確立することと、暗号化された証明書であって、この証明書は、第１の公開鍵ペアに対応し、かつ第１の公開鍵ペアの公開鍵を含み、この証明書は、第１の共有された暗号化された鍵を使用して暗号化されている、証明書をモバイルデバイスから受信することと、暗号化された証明書を復号し、復号された証明書を記憶することと、を含む。

【０２７９】

いくつかの実施形態では、動作は、システムに動作を実行させる要求に対して、モバイルデバイスにチャレンジを発行することと、モバイルデバイスとの第２の共有暗号鍵をネゴシエーションすることと、チャレンジに対する応答を受信し、第２の共有暗号鍵を使用して応答を復号することと、動作を許可する前に、第１の公開鍵ペアの非公開鍵を使用して、応答がモバイルデバイスによって署名されていることを検証することと、を更に含む。いくつかの実施形態では、動作は、別のモバイルデバイスによって生成された公開鍵ペアの証明書を受信することと、証明書がモバイルデバイスによって第１の公開鍵ペアの非公開鍵によって署名されていると判定したことに応じて、他のモバイルデバイスに対する

証明書を記憶することと、他のモバイルデバイスのための記憶された証明書に基づいて、他のモバイルデバイスの動作を許可するかどうかを判定することと、を更に含む。

例示的なコンピュータ可読媒体

【０２８０】

本開示は、上で詳細に様々な例示的な回路について説明している。本開示は、そのような回路を含む実施形態だけでなく、そのような回路を指定する設計情報を含むコンピュータ可読記憶媒体もまた網羅することが意図される。したがって、本開示は、開示された回路を含む装置だけでなく、開示された回路を含むハードウェア（例えば、集積回路）を製造するように構成された作製システムによって認識されるフォーマットで回路を指定する記憶媒体も網羅する特許請求の範囲を支持することを意図する。そのような記憶媒体に対する特許請求の範囲は、例えば、回路設計を行うが、それ自体が設計を作製しないエンティティを網羅することを意図する。

【０２８１】

図２５は、いくつかの実施形態に係る、回路設計情報を記憶する例示的な非一時的コンピュータ可読記憶媒体を示すブロック図である。例示された実施形態では、半導体製造システム２７２０は、非一時的コンピュータ可読媒体２７１０に記憶された設計情報２７１５を処理し、設計情報２７１５に基づいて集積回路２７３０を作製するように構成されている。

【０２８２】

非一時的コンピュータ可読媒体２７１０は、様々な適切なタイプのメモリデバイス又は記憶装置デバイスのいずれかを含んでもよい。媒体２７１０は、インストール媒体、例えば、ＣＤ－ＲＯＭ、フロッピーディスク又はテープデバイス、ＤＲＡＭ、ＤＤＲ　ＲＡＭ、ＳＲＡＭ、ＥＤＯ　ＲＡＭ、Ｒａｍｂｕｓ　ＲＡＭなどの、コンピュータシステムメモリ又はランダムアクセスメモリ、フラッシュ、磁気媒体、例えばハードドライブ、又は光記憶装置などの、不揮発性メモリ、レジスタ、又はその他の同様のタイプのメモリ要素などであり得る。媒体２７１０は、他のタイプの非一時的メモリ、及びそれらの組合せも含んでもよい。媒体２７１０は、異なる場所、例えば、ネットワークを通じて接続された異なるコンピュータシステムに存在することができる２つ以上の記憶媒体を含んでもよい。

【０２８３】

設計情報２７１５は、ＶＨＤＬ、Ｖｅｒｉｌｏｇ、ＳｙｓｔｅｍＣ、ＳｙｓｔｅｍＶｅｒｉｌｏｇ、ＲＨＤＬ、Ｍ、ＭｙＨＤＬなど（これらに限定されない）のハードウェア記述言語を含む様々な適切なコンピュータ言語のいずれかを使用して指定され得る。設計情報２７１５は、集積回路２７３０の少なくとも一部分を作製するために半導体作製システム２７２０によって使用可能であり得る。設計情報２７１５のフォーマットは、少なくとも１つの半導体作製システム２７２０によって認識されてもよい。いくつかの実施形態では、設計情報２７１５はまた、集積回路２７３０の合成及び／又はレイアウトを指定する１つ以上のセルライブラリを含んでもよい。いくつかの実施形態では、設計情報は、セルライブラリ要素及びそれらの接続性を指定するネットリストの形態で、全体的に又は部分的に指定される。

【０２８４】

半導体作製システム２７２０は、集積回路を作製するように構成された様々な適切な要素のうちのいずれかを含んでもよい。これは、例えば、半導体材料を堆積させること（例えば、ウェハ上に、これはマスキングを含み得る）と、材料を除去することと、堆積された材料の形状を変更することと、材料を改質すること（例えば、材料をドープすること、又は紫外線処理を使用して誘電定数を変更することによって）と、のための要素を含んでもよい。半導体作製システム２７２０はまた、正しい動作のために作製された回路の様々な試験を実行するように構成されてもよい。

【０２８５】

様々な実施形態では、集積回路２７３０は、設計情報２７１５によって指定された回路設計にしたがって動作するように構成されており、これは、本明細書に記載された機能の

いずれかを実行することを含み得る。例えば、集積回路２７３０は、図１Ａ～図１Ｃ又は図２に示される様々な要素のいずれかを含み得る。更に、集積回路２７３０は、他の構成要素と併せて本明細書に記載された様々な機能を実行するように構成されてもよい。更に、本明細書に記載された機能は、複数の接続された集積回路によって実行されてもよい。

【０２８６】

本明細書で使用する「．．．ように構成された回路の設計を指定する設計情報」という形態の語句は、その要素が満たされるために対象の回路が作製されなければならないことを意味するものではない。むしろ、この語句は、設計情報には、作製されると、示されたアクションを実行するように構成されるか、又は指定された構成要素を含む回路について記載されていることを示す。

【０２８７】

図２６は、いくつかの実施形態に係る、他のデバイスからの署名付き証明書を検証した後まで、デバイスが識別情報を送信しない認証の例示的な方法を示すフローチャートである。図２６に示す方法は、とりわけ、本明細書で開示するコンピュータ回路、システム、デバイス、要素又は構成要素のいずれかと共に使用することができる。様々な実施形態では、図示の方法要素の一部は、同時に実行してもよく、図示のものとは異なる順序で実行してもよく、又は省略してもよい。必要に応じて、追加の方法要素をも実行してもよい。

【０２８８】

２８１０で、例示された実施形態では、デバイス（例えば、モバイルデバイス）は、第１の公開鍵及び第１の非公開鍵を含む第１の短期鍵ペアを生成する。ｐｈｏｎｅ．ｅＰＫ及びｐｈｏｎｅ．ｅＳＫは、第１の短期鍵ペアの一例である。

【０２８９】

２８２０で、例示された実施形態では、デバイスは、システムによって生成された第２の公開鍵であって、この第２の公開鍵は、第２の短期鍵ペアに含まれる、第２の公開鍵を判定する。ｓｙｓｔｅｍ．ｅＰＫは、第２の公開鍵の一例である。

【０２９０】

２８３０で、例示された実施形態では、デバイスは、第１の非公開鍵及び第２の公開鍵を入力として使用する鍵交換関数を使用して第１の共有シークレットを生成する。例えば、鍵交換関数は、ＤＨ（ｃａｒ．ｅＰＫ、ｐｈｏｎｅ．ｅＳＫ）であってもよく、その出力は、第１の共有シークレットであってもよい。

【０２９１】

２８４０で、例示された実施形態では、デバイスは、少なくとも、第１の共有シークレットと、第１の公開鍵と、デバイスとシステムとの間のペアリングセッションの間に以前に確立されたシステムの公開鍵と、を入力に使用する鍵導出関数を使用して導出された共有シークレットを生成する。ＫＡＥｓｅｅｄは、導出された共有シークレットの一例であり、ｓｙｓｔｅｍ．ＰＫは、システムの公開鍵の一例である。

【０２９２】

２８５０で、例示された実施形態では、デバイスは、ペアリングセッション中に確立されたデバイスの非公開鍵でトランザクション情報に署名することによって署名を生成する。Ｐｈｏｎｅ．Ｓｉｇは、このような署名の一例である。

【０２９３】

２８６０で、例示された実施形態では、デバイスは、導出された共有シークレットに基づいて、署名と、デバイスを識別する情報と、を暗号化する。ｐｈｏｎｅＩｄｅｎｔｉｆｉｅｒは、デバイスを識別する情報の一例である。

【０２９４】

２８７０で、例示された実施形態では、デバイスは、システムの公開鍵を使用してシステムから受信された署名付き証明書であって、この証明書は、ペアリングセッション中に確立されたシステムの対応する非公開鍵で署名される、証明書を検証する。様々な実施形態では、デバイスは、署名付き証明書の検証後まで、トランザクション中に識別情報を送信しない。

【０２９５】
２８８０で、例示された実施形態では、署名付き証明書の検証に応じて、デバイスは、暗号化された署名及び情報をシステムに送信する。いくつかの実施形態では、この送信は、ＡＵＴＨ１応答に対応する。
【０２９６】
図２７は、いくつかの実施形態に係る、システム側認証のための例示的な方法を示すフローチャートである。図２７に示す方法は、とりわけ、本明細書で開示するコンピュータ回路、システム、デバイス、要素又は構成要素のいずれかと共に使用することができる。様々な実施形態では、図示の方法要素の一部は、同時に実行してもよく、図示のものとは異なる順序で実行してもよく、又は省略してもよい。必要に応じて、追加の方法要素をも実行してもよい。
【０２９７】
２９１０で、例示された実施形態では、システム（例えば、車両）は、モバイルデバイスとのペアリングセッション中に確立されたシステムの非公開鍵でトランザクション情報に署名することによって署名を生成する。
【０２９８】
２９２０で、例示された実施形態では、システムは、署名をモバイルデバイスに送信する。
【０２９９】
２９３０で、例示された実施形態では、システムは、送信された署名の応答で、モバイルデバイスから暗号化された署名を受信する。
【０３００】
２９４０で、例示された実施形態では、システムは、第１の公開鍵及び第１の非公開鍵を含む第１の短期鍵ペアを生成する。
【０３０１】
２９５０で、例示された実施形態では、システムは、モバイルデバイスによって生成された第２の公開鍵であって、この第２の公開鍵は、第２の短期鍵ペアに含まれる、第２の公開鍵を判定する。
【０３０２】
２９６０で、例示された実施形態では、システムは、第１の非公開鍵及び第２の公開鍵を入力として使用する鍵交換関数を使用して第１の共有シークレットを生成する。
【０３０３】
２９７０で、例示された実施形態では、システムは、少なくとも，第１の共有シークレットと、第１の公開鍵と、ペアリングセッションの間に以前に確立されたシステムの公開鍵と、を入力に使用する鍵導出関数を使用して導出された共有シークレットを生成する。
【０３０４】
２９８０で、例示された実施形態では、システムは、導出された共有シークレットを使用して署名を復号する。
【０３０５】
２９９０で、例示された実施形態では、システムは、ペアリングセッション中に確立されたモバイルデバイスの公開鍵を使用して署名を検証する。
【０３０６】
２９９５で、例示された実施形態では、システムは、検証に基づいて、１つ以上のアクションを許可する。
例示的なデジタル鍵証明技術
【０３０７】
図２８は、いくつかの実施形態に係る、ペアリング中の例示的なデジタル鍵証明を示すブロック図である。例示された実施形態では、サーバ３０１０は、ペアリングパスワード３００２を生成し、システムパスワード及びソルト３００４をシステム１１０に送信するように構成されている。例示の目的で、例示的な実施例では、セキュアリモートパスワー

ド（secure remote password、ＳＲＰ）（拡張ＰＡＫＥプロトコル）が使用されるが、開示された証明技術は、様々なセキュリティプロトコルと共に使用されてもよいことに留意されたい。例示された実施形態では、ソルトは、一方向ハッシュ関数への追加の入力として使用されるランダムデータであり、システムパスワードを保護するために使用されてもよい。

【０３０８】

３００６で、モバイルデバイスＯＳ２１２０は、サーバ３０１０にログインし、オーナーパスワードをフェッチする。３００８で、ＳＲＰは、セキュアチャネルを作成するために使用され、システム１１０は、デジタル鍵構成データを提供する。この構成情報は、様々なフィールド、例えば、どのタイプのトランザクションが許可されているかを示す、システムメタデータ、開始日、失効日、公開鍵、システム識別子などを含み得る。いくつかの実施形態では、システム１１０は、モバイルデバイスが構成データにしたがってデジタル鍵が作成されたことを適切に証明しない限り、ペアリングを拒否するように構成されている。

【０３０９】

３０１２で、モバイルデバイスＯＳ２１２０は、コマンドをＳＥアプレット３０３０に送信して、構成情報にしたがってデジタル鍵を作成する。ＳＥアプレット３０３０は、（ペアリングセッションのための長期公開鍵ペアなどの本明細書で論じられる様々な情報を含み得る）デジタル鍵を作成し、３０１４で、証明及び公開鍵をモバイルデバイスＯＳ２１２０に送信する。ＯＳは、次いで、証明３０１６をシステム１１０に送信する。

【０３１０】

システム１１０は、次いで、３０１８で、証明データを検証し、検証に基づいて公開鍵を承認又は拒否する。これは、ＯＳからの署名付き証明書に埋め込まれた構成データと３００８で送信された構成データとを比較することと、証明書の署名を検証して、証明書がＳＥからのものであることを確認することと、を含み得る。様々な実施形態では、これにより、システム１１０は、モバイルデバイス１３０とのペアリングを可能にする前に、デジタル鍵が適切に作成されたことを確認することができる。

【０３１１】

ＯＳ２１２０及びアプレット３０３０に関して記載された機能は、単一のモジュールによって実行されてもよく、これは、他の実施形態では、単一のプロセッサで実行されてもよいことに留意されたい。図２８に開示された機能の分布は、例示的な目的で含まれるが、本開示の範囲を限定することを意図するものではない。

＊＊＊

【０３１２】

特定の実施形態が上に記載されており、かつ以下の添付の付属書類に示されているが、これらの実施形態は本開示の範囲を限定する意図はなく、特定の機能に対して単一の実施形態のみが記載されている場合でも同様である。本開示で提供されている機能の実施例は、別途記載がない限り、例示的な性質のものであって、限定的な目的を意図していない。一例として、用語「電話」への言及は、任意の好適なモバイルデバイスを包含し得る。したがって、上記及び下記の記載は、本開示の利点を有する当業者に明らかであるように、このような代替物、改変例、及び均等物を包含することが意図されている。

【０３１３】

本開示の範囲は、本願で取り組まれている問題の一部又はすべてを軽減するかどうかに関係なく、本願で（明示的又は暗黙的に）開示されているすべての機能若しくはそれら機能の組み合わせ、又はそれらの一般化を含む。したがって、新しい特許請求は、本願のこのような機能の組み合わせに対する本願（又は、本願に対する優先権を主張する出願）の手続き中に策定し得る。特に、特許請求の範囲に関しては、従属クレームの機能は独立クレームの機能と組み合わされる場合があり、それぞれの独立クレームの機能は、任意の適切な方法で、かつ、単に添付の特許請求の範囲で列挙されている特定の組み合わせではない形で組み合わされる場合がある。

【図１Ａ】

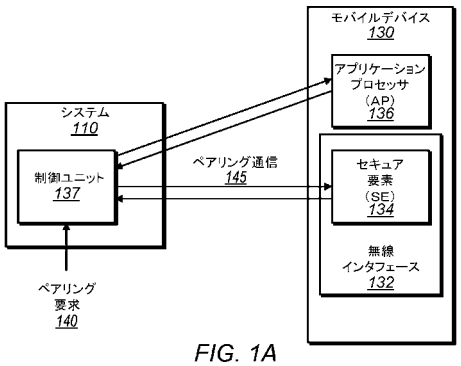


FIG. 1A

【図１Ｂ】

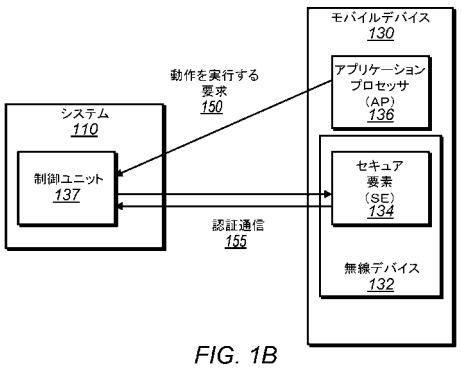


FIG. 1B

【図１Ｃ】

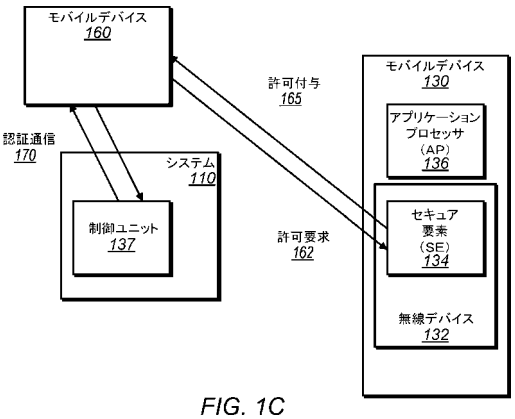


FIG. 1C

【図２】

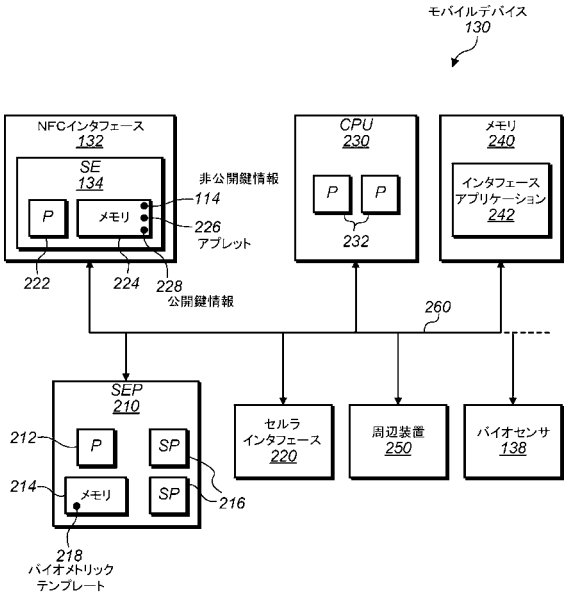


FIG. 2

【図３】

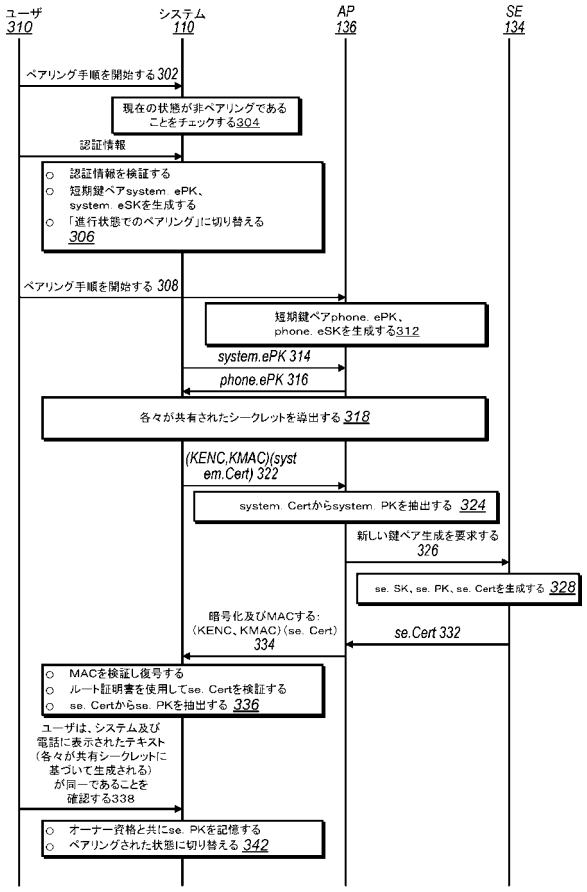


FIG. 3

【図４】

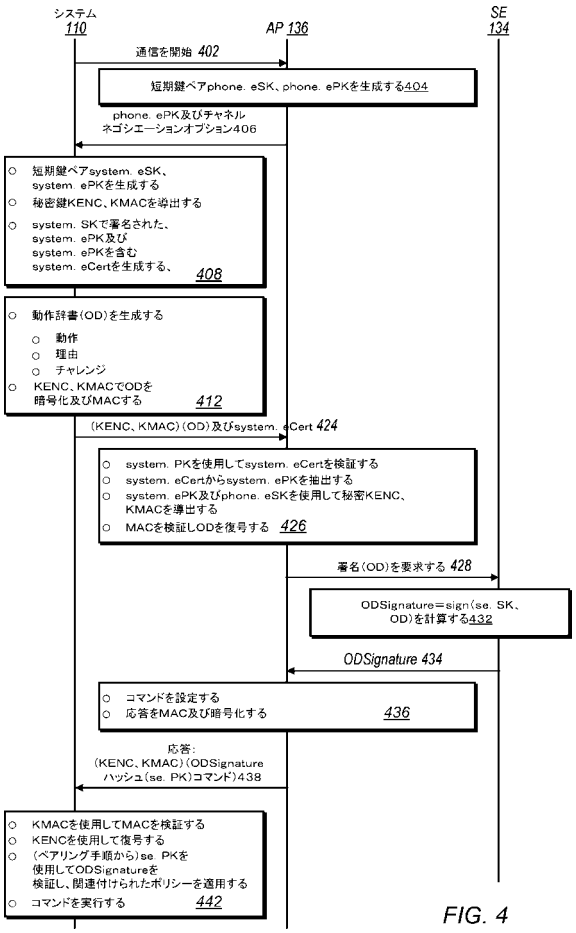


FIG. 4

【図５】

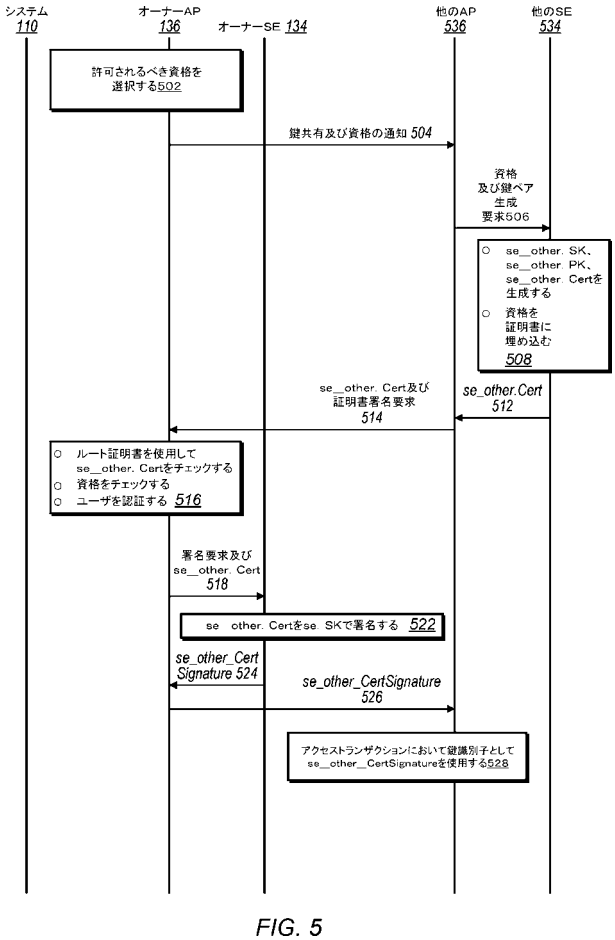


FIG. 5

【図６Ａ】

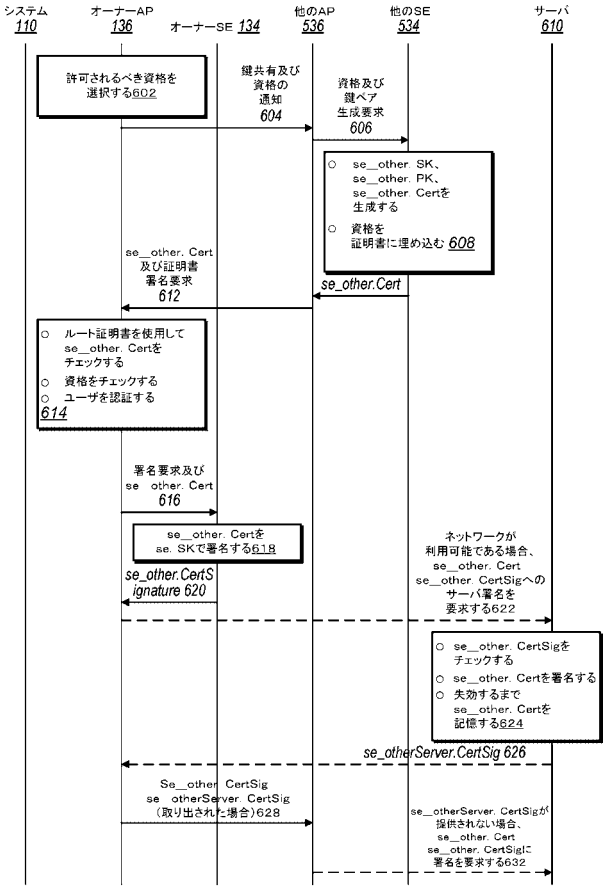


FIG. 6A

【図６Ｂ】

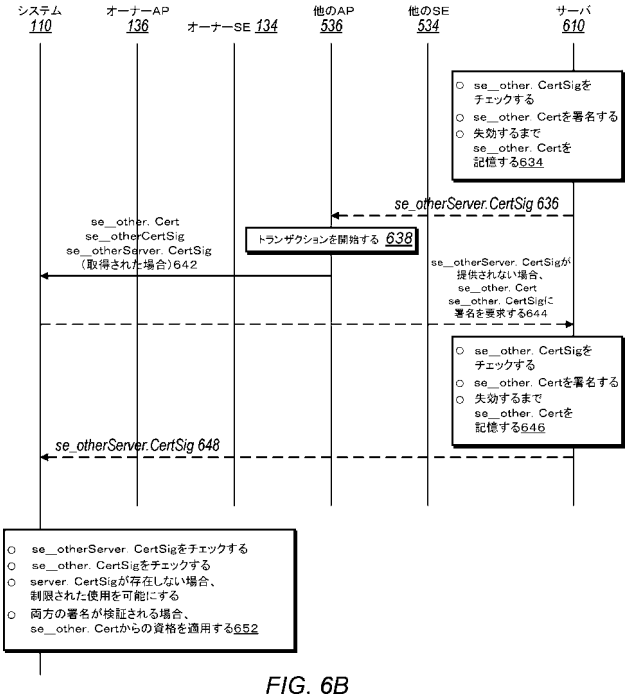


FIG. 6B

【図７Ａ】

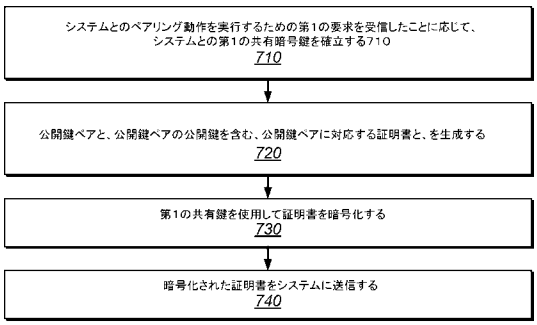


FIG. 7A

【図７Ｂ】

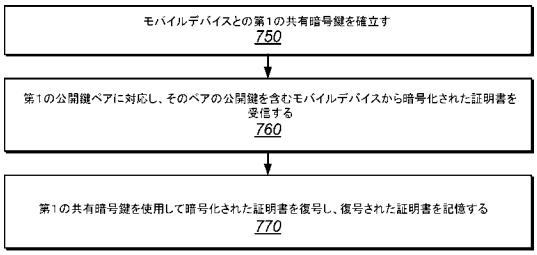


FIG. 7B

【図８Ａ】

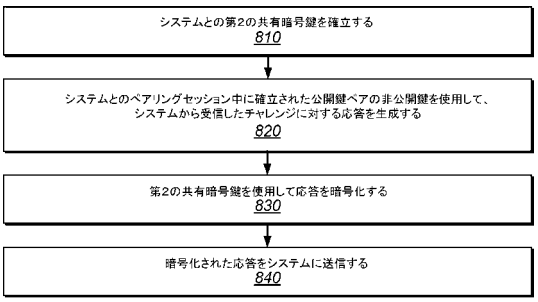


FIG. 8A

【図８Ｂ】

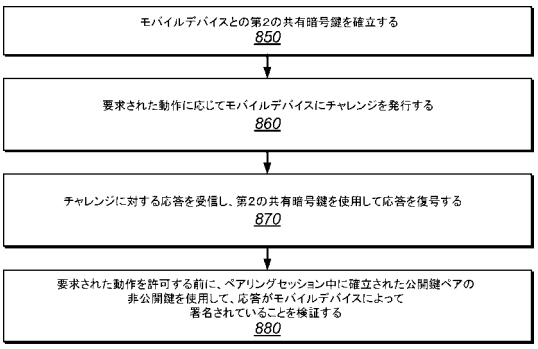


FIG. 8B

【図９Ａ】

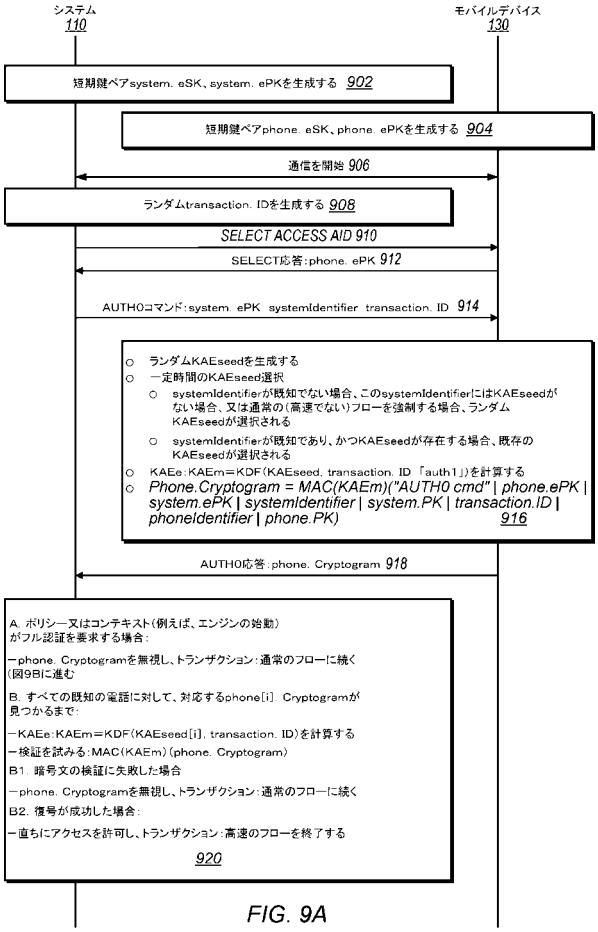


FIG. 9A

【図９Ｂ】

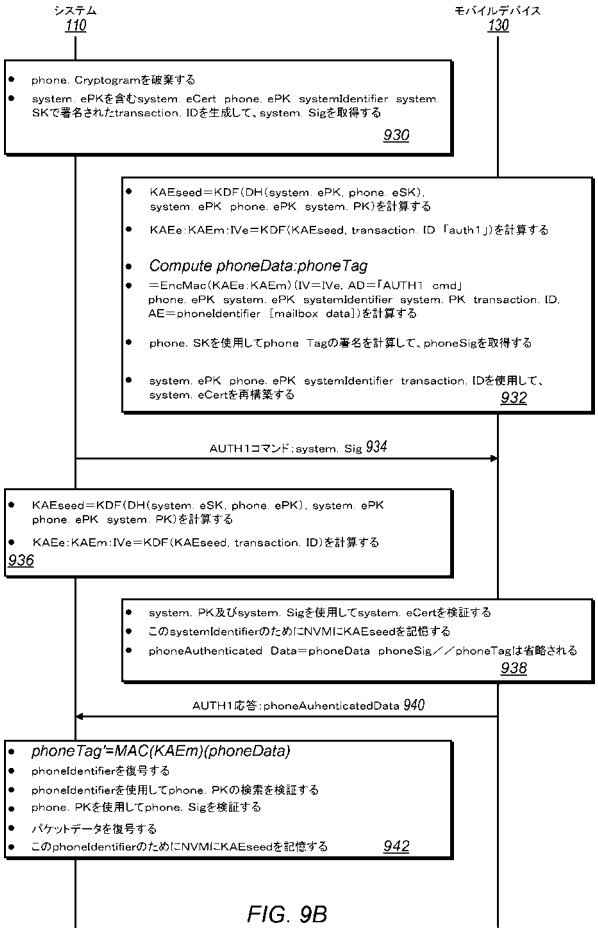


FIG. 9B

【図９Ｃ】

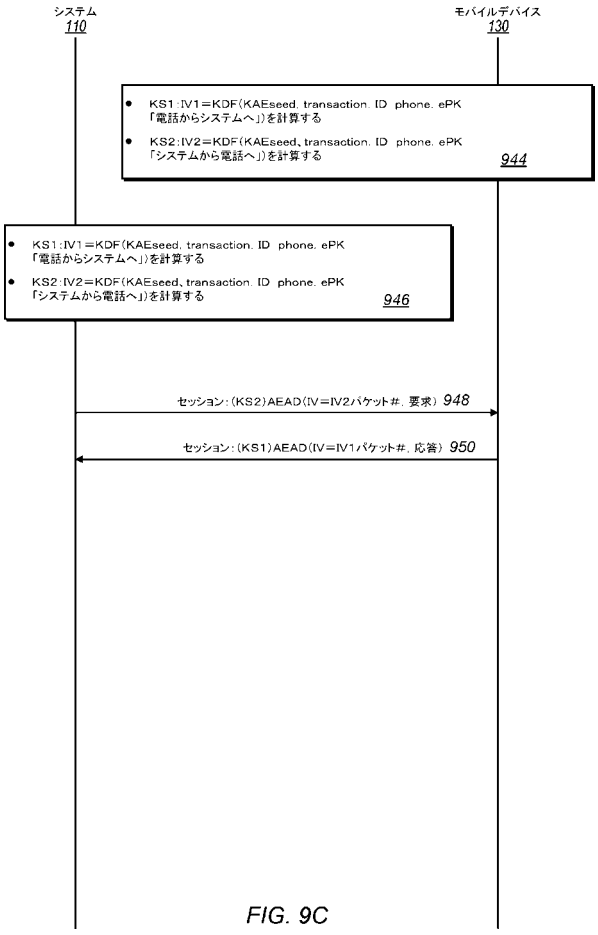


FIG. 9C

【図１０】

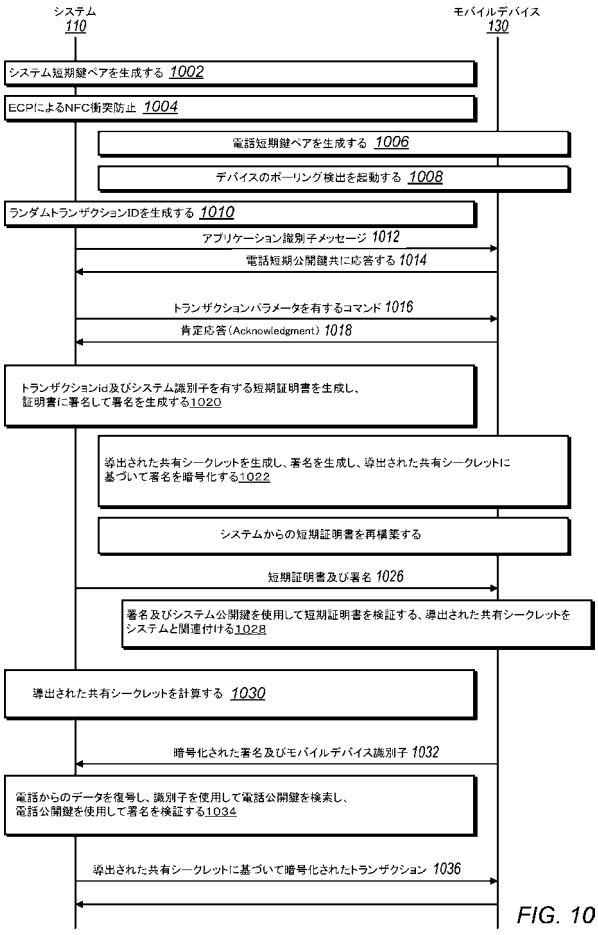


FIG. 10

【図１１】

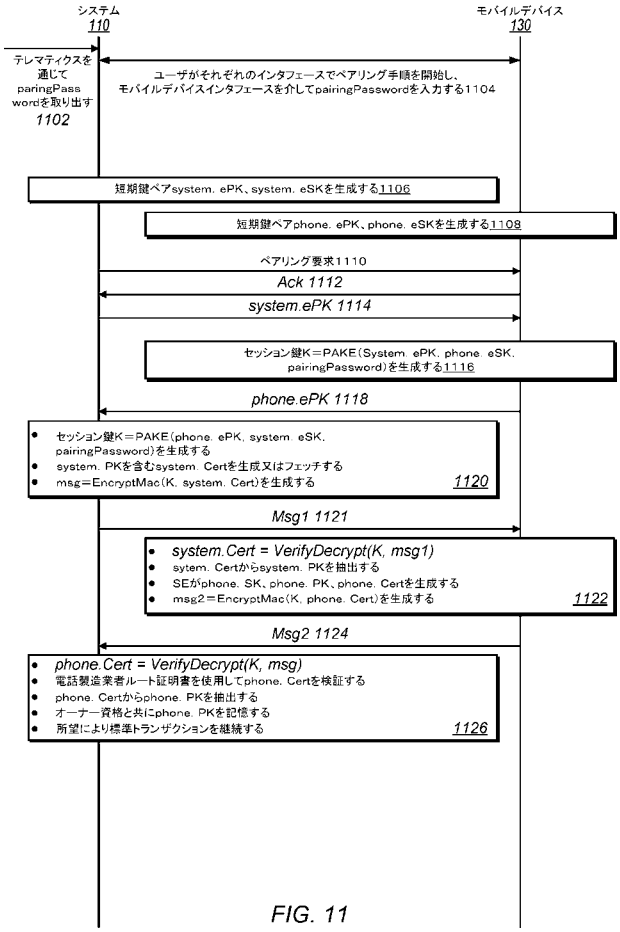


FIG. 11

【図１２】

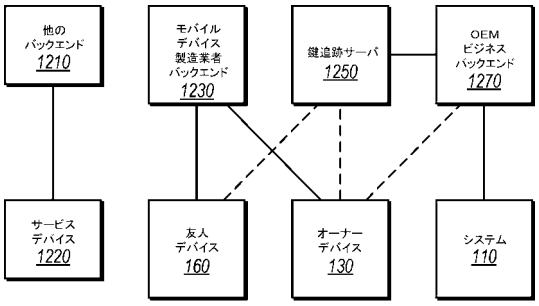


FIG. 12

【図１３】

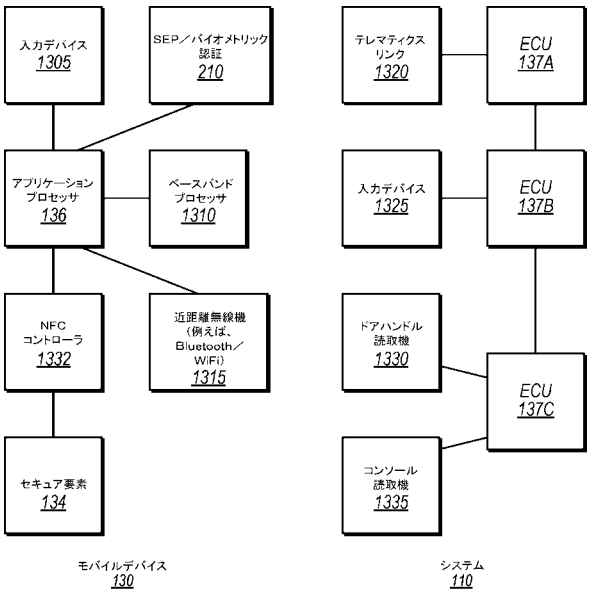


FIG. 13

【図１４】

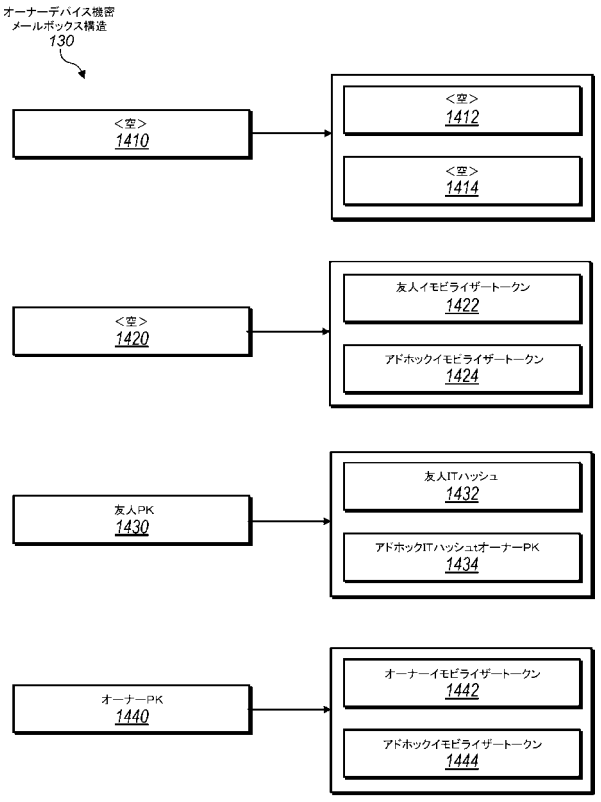


FIG. 14

【図１５】

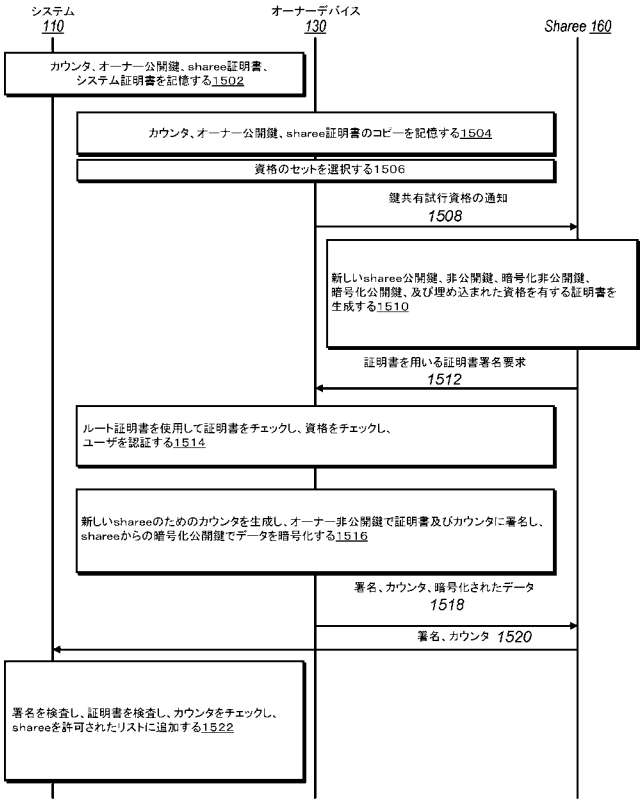
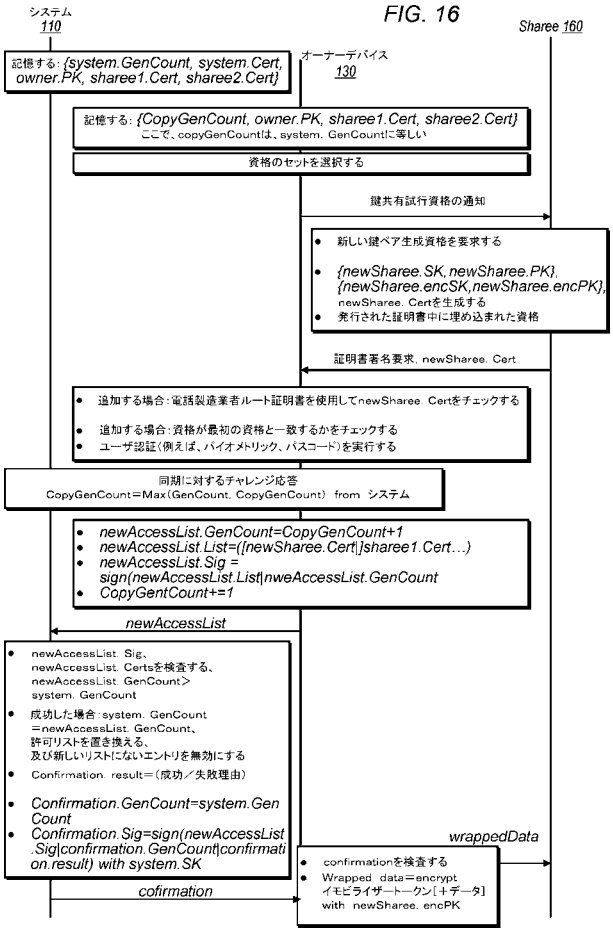


FIG. 15

【図１６】

FIG. 16



【図１７】

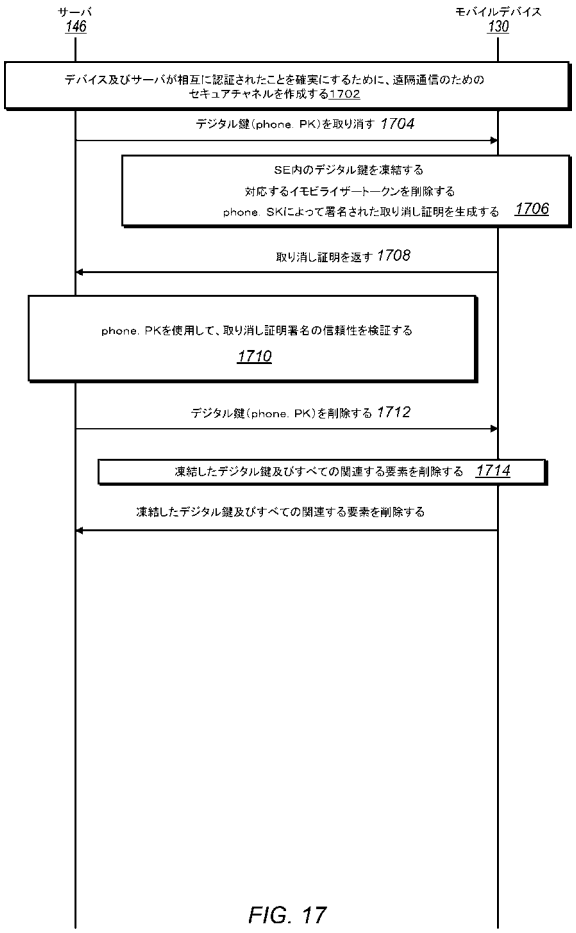


FIG. 17

【図１８】

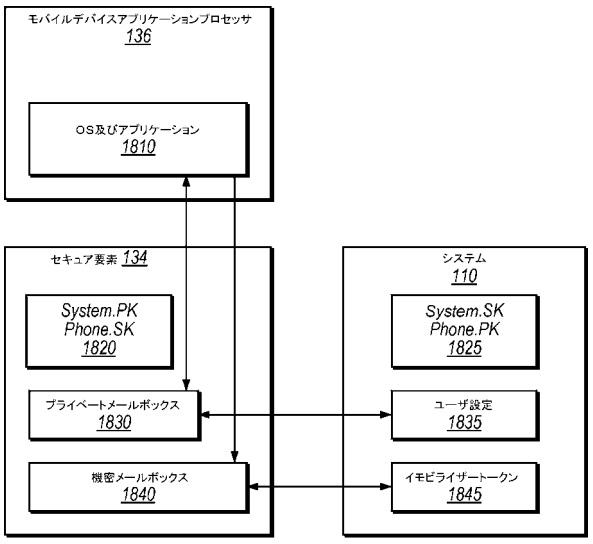


FIG. 18

【図１９】

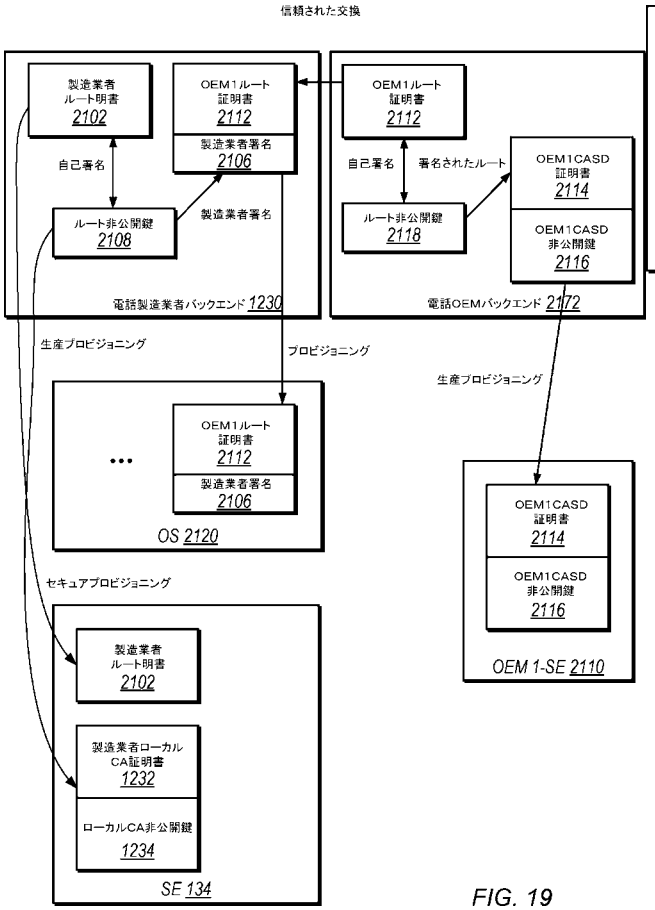


FIG. 19

【図２０】

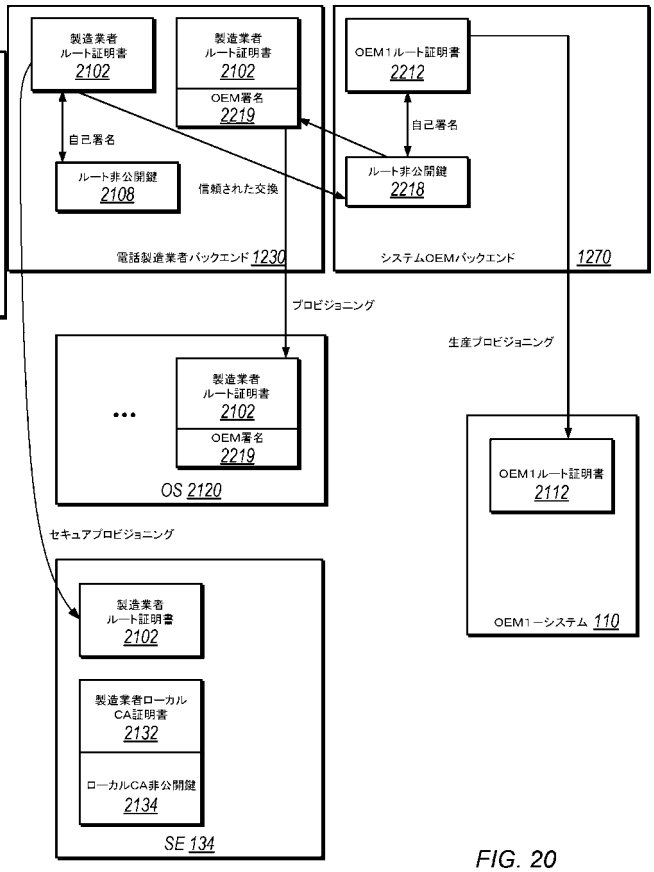


FIG. 20

【図２１】

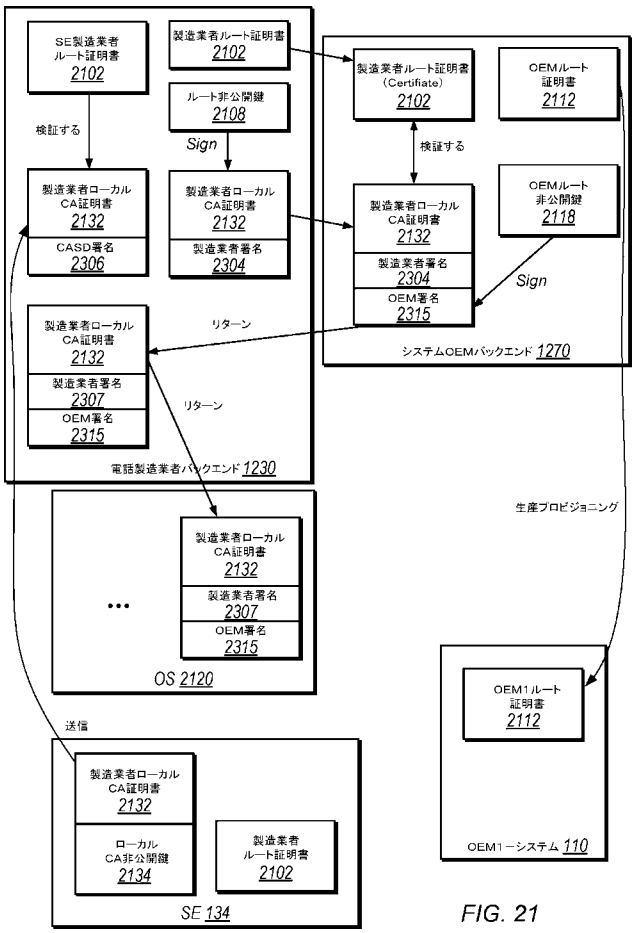
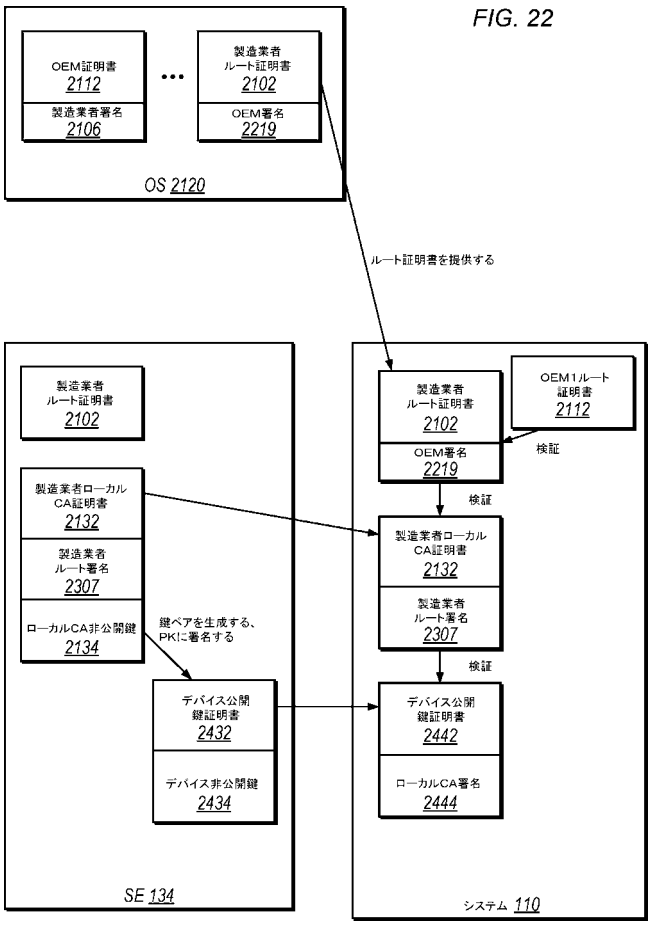


FIG. 21

【図２２】

FIG. 22



【図２３】

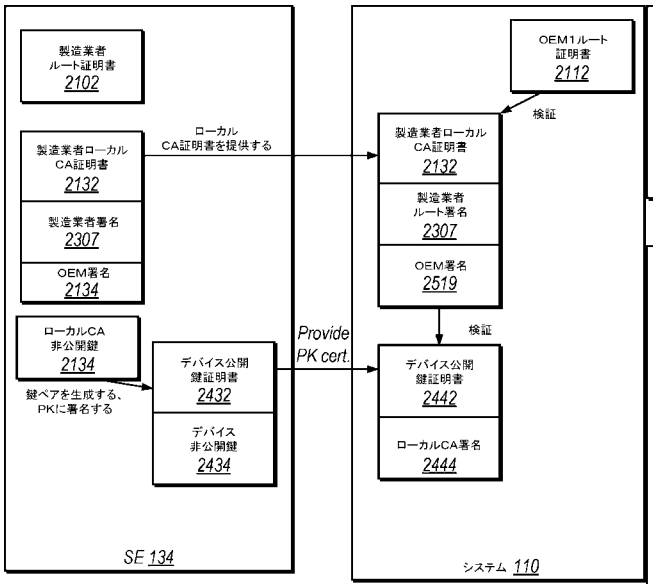


FIG. 23

【図２４】

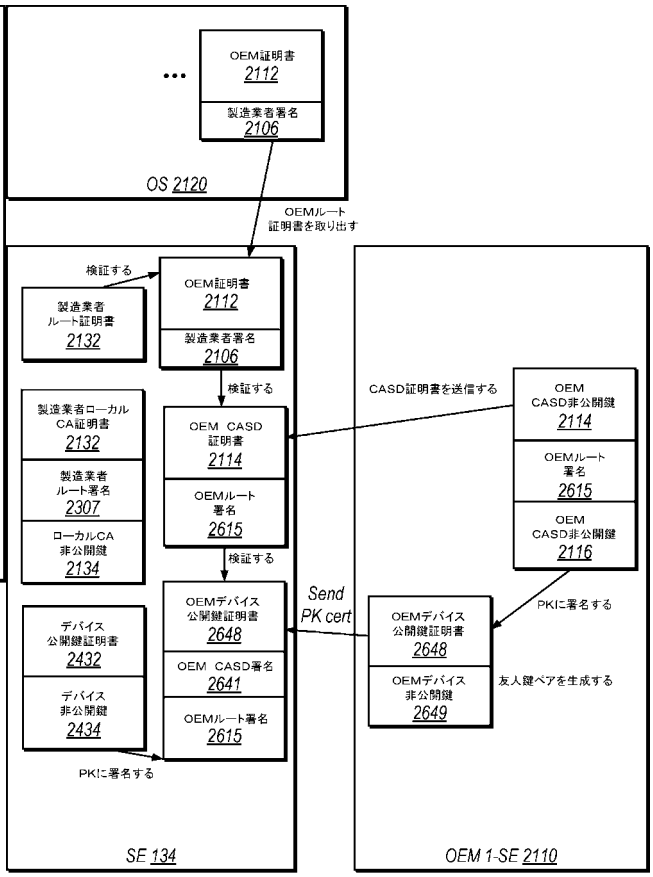


FIG. 24

【図２５】

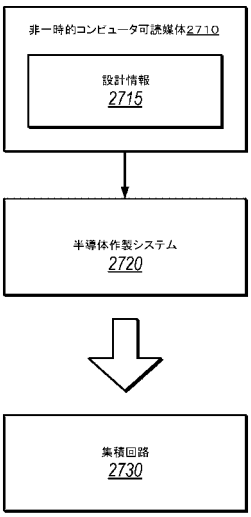


FIG. 25

【図２６】

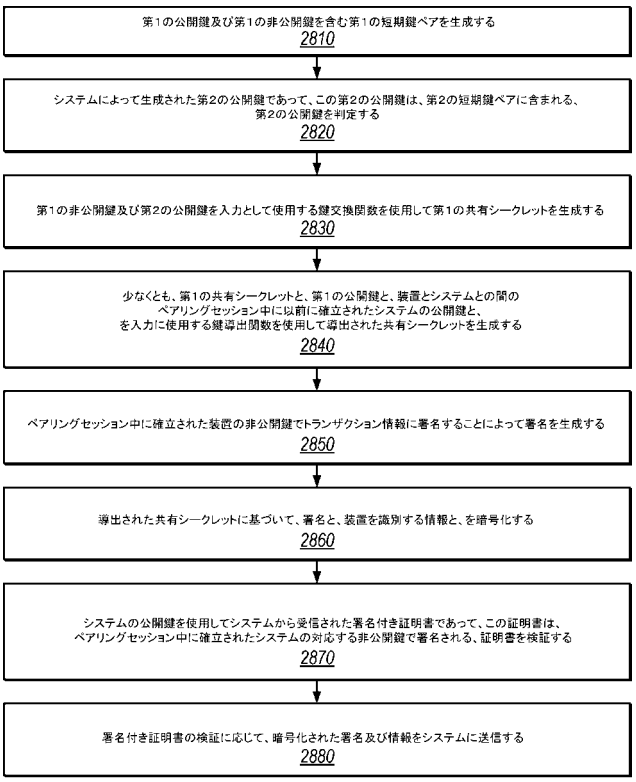


FIG. 26

【図２７】

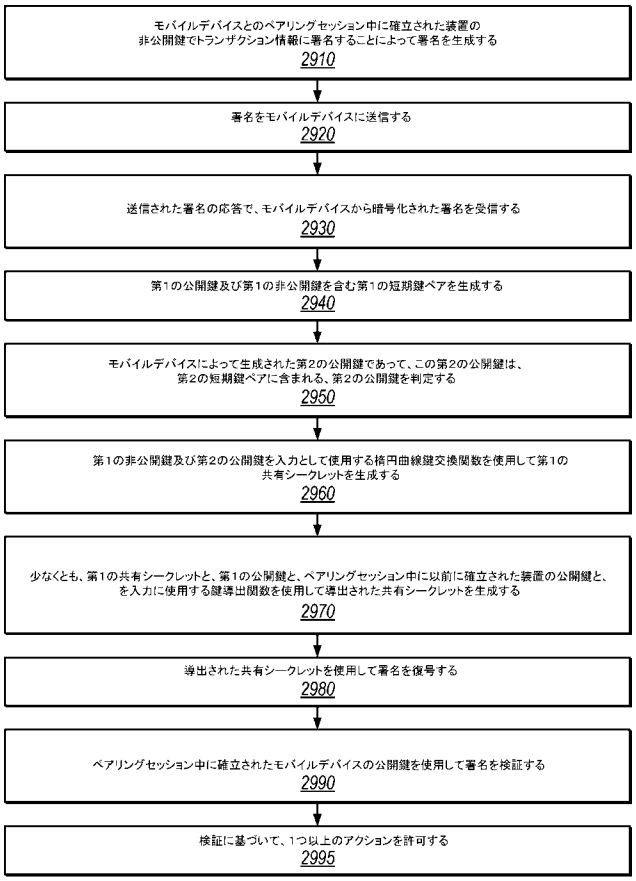


FIG. 27

【図２８】

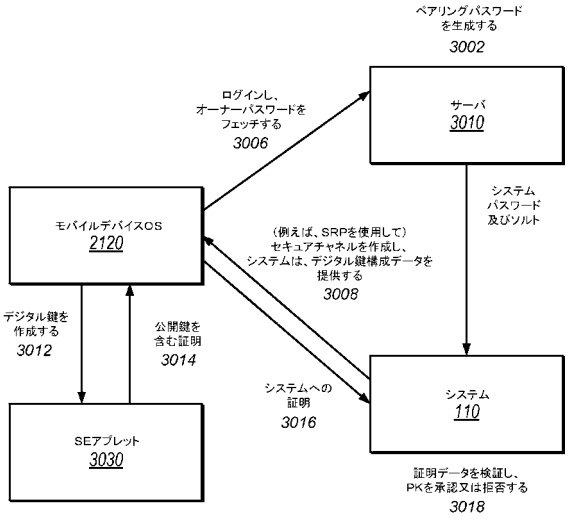


FIG. 28

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/020494

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/00 H04L9/32
ADD.

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)
H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015/372811 A1 (LE SAINT ERIC [US] ET AL) 24 December 2015 (2015-12-24) abstract paragraph [0120] - paragraph [0128] -----	1-18
A	US 2016/099814 A1 (NEGI ANSUYA [US] ET AL) 7 April 2016 (2016-04-07) abstract -----	1-18

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

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 May 2018	14/05/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Apostolescu, Radu

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/020494

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015372811 A1	24-12-2015	AU 2015277000 A1	17-11-2016
		CN 106664206 A	10-05-2017
		EP 3158680 A1	26-04-2017
		US 2015372811 A1	24-12-2015
		WO 2015195978 A1	23-12-2015
US 2016099814 A1	07-04-2016	US 2016099814 A1	07-04-2016
		WO 2014200496 A1	18-12-2014

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(31)優先権主張番号　62/565,039
(32)優先日　平成29年9月28日(2017.9.28)
(33)優先権主張国・地域又は機関
米国(US)

(81)指定国・地域　AP(BW,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,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,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,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,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

（特許庁注：以下のものは登録商標）
１．ＢＬＵＥＴＯＯＴＨ

(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光
(72)発明者　マティアス,　アルン　ジー.
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
(72)発明者　ガルド,　フロリアン
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
(72)発明者　レルヒ,　マティアス
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
(72)発明者　アブドゥルラヒマン,　ナジーブ　エム.
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
(72)発明者　タッキン,　オヌール　イー.
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
(72)発明者　シエラ,　ヤンニック
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン