(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-513526
(P2024-513526A)
(43)公表日　令和6年3月25日(2024.3.25)

(51)国際特許分類		FI		
H04L 9/08 (2006.01)		H04L	9/08	F
H04L 9/10 (2006.01)		H04L	9/10	Z
H04L 9/32 (2006.01)		H04L	9/32	200B
		H04L	9/32	200F

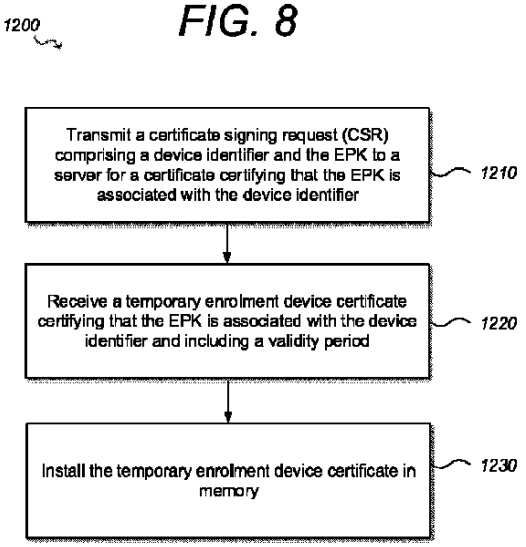
審査請求　未請求　予備審査請求　未請求　（全48頁）

(21)出願番号　特願2023-562579(P2023-562579)
(86)(22)出願日　令和4年4月12日(2022.4.12)
(85)翻訳文提出日　令和5年12月7日(2023.12.7)
(86)国際出願番号　PCT/GB2022/050911
(87)国際公開番号　WO2022/219320
(87)国際公開日　令和4年10月20日(2022.10.20)
(31)優先権主張番号　2105185.9
(32)優先日　令和3年4月12日(2021.4.12)
(33)優先権主張国・地域又は機関
英国(GB)
(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,
最終頁に続く

(71)出願人　521452588
クリプト・クオンティーク・リミテッド
Ｃｒｙｐｔｏ Ｑｕａｎｔｉｑｕｅ Ｌｉｍｉｔｅｄ
英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８０、ザ・プリント・ルームズ、ユニット３０４－５
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100135703
弁理士　岡部 英隆
(74)代理人　100227927
弁理士　中村 拓
(72)発明者　ウッデージ，ジョアン
最終頁に続く

(54)【発明の名称】　ルートオブトラスト登録及びデバイス拘束された公開鍵登録

(57)【要約】
方法、装置、デバイス、及びコンピュータ可読媒体が登録に関連して提供される。一例では、電子デバイスが提供される。電子デバイスは、物理複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える。電子デバイスは、１つ以上のメモリを更に備える。電子デバイスは、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のためのデバイス識別子及びＥＰＫを含む証明書署名要求（ＣＳＲ）をサーバに送信するように構成される１つ以上のプロセッサを更に備え、ＣＳＲがＥＳＫを使用して署名され、デバイス識別子がＥＰＫの関数に基づく。１つ以上のプロセッサは、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書を受信するように更に構成される。１つ以上のプロセッサは、一時的登録デバイス証明書をメモ



【特許請求の範囲】
【請求項１】
物理複製困難関数（ＰＵＦ）を有するセキュリティモジュールであって、前記ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、前記登録鍵対が登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える、セキュリティモジュールと、
１以上のメモリと、
プロセッサと、
を備え、
前記プロセッサは、セキュア接続を介して、前記ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のための証明書署名要求（ＣＳＲ）をサーバに送信するように構成され、前記ＣＳＲは、
前記デバイス識別子と、
前記ＥＰＫと、
を含み、
前記ＣＳＲは、前記ＥＳＫを使用して署名され、前記デバイス識別子は、前記ＥＰＫの関数に基づき、
前記プロセッサは、
前記セキュア接続を介して、前記ＥＰＫが前記デバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書を受信し、
前記一時的登録デバイス証明書をメモリにインストールする、
ように構成される、電子デバイス。
【請求項２】
前記１以上のメモリは、プライマリトラステッドルート証明書を更にインストールしており、前記プロセッサは、前記セキュア接続を介して発行証明書を受信するように更に構成され、前記発行証明書が前記プライマリトラステッドルート証明書の下位である、請求項１に記載の電子デバイス。
【請求項３】
前記プロセッサは、
前記発行証明書がプライマリトラステッドルート証明書から直接派生していることを検証し、
前記検証に応じて、前記発行証明書を前記１つ以上のメモリにインストールする、
ように更に構成される、請求項２に記載の電子デバイス。
【請求項４】
前記プロセッサは、
セキュア接続発行証明書及びセキュア接続証明書を前記サーバから受信し、前記セキュア接続発行証明書及び前記セキュア接続証明書が前記プライマリトラステッドルート証明書の下位であり、
前記プライマリトラステッドルート証明書を使用して前記セキュア接続証明書を検証し、
前記検証に応じて、前記サーバに対する前記セキュア接続を確立する、
ように更に構成される、請求項２又は３に記載の電子デバイス。
【請求項５】
前記セキュア接続証明書を検証することは、前記セキュア接続証明書が前記プライマリトラステッドルート証明書の下位であることを検証すること、任意選択的に、前記セキュア接続証明書に含まれるサーバ識別子を前記電子デバイスの前記１つ以上のメモリに記憶されるサーバアイデンティティと比較することを含む、請求項４に記載の電子デバイス。
【請求項６】
前記プロセッサは、前記電子デバイスの前記１つ以上のメモリに記憶される前記サーバ識別子によって識別される前記サーバに対する前記セキュア接続を開始するように更に構

成される、請求項５に記載の電子デバイス。
【請求項７】
前記デバイスは、前記ＰＵＦに対する第２のチャレンジ及び応答に基づいてデバイス鍵対（ＤＰＫ、ＤＳＫ）を確立するように更に構成され、前記デバイス鍵対は、デバイス公開鍵（ＤＰＫ）及びデバイス秘密鍵（ＤＳＫ）を備え、
前記プロセッサは、第２のセキュア接続を介して、前記ＤＰＫがデバイス識別子と関連付けられることを証明する証明書のための第２の証明書署名要求（ＣＳＲ）をサーバに送信するように更に構成され、前記第２のＣＳＲは、
前記ＤＰＫと、
前記デバイス識別子と、
を含み、
前記第２のＣＳＲは、前記ＤＳＫを使用して署名され、
前記プロセッサは、
前記第２のセキュア接続を介して、前記ＤＰＫを前記デバイス識別子と関連付けるデバイス証明書を受信し、
前記デバイス証明書が前記プライマリトラステッドルート証明書の下位であることを検証し、
前記検証に応じて、前記デバイス証明書をメモリにインストールする、
ように更に構成される、請求項２から６のいずれかに記載の電子デバイス。
【請求項８】
前記デバイス識別子が前記ＥＰＫのハッシュ関数に基づく、請求項１から７のいずれか一項に記載の電子デバイス。
【請求項９】
前記一時的登録デバイス証明書の有効期間が１０分未満である、請求項１から８のいずれか一項に記載の電子デバイス。
【請求項１０】
前記１以上のメモリには、一時的登録トラステッドルート証明書がインストールされており、
前記プロセッサは、前記一時的登録デバイス証明書を受信した後、前記一時的登録トラステッドルート証明書を使用して前記一時的登録デバイス証明書を検証するように更に構成され、
前記一時的登録デバイス証明書をインストールすることが前記検証に応答したものである、
請求項１から９のいずれか一項に記載の電子デバイス。
【請求項１１】
電子デバイスによる実行のための方法であって、前記電子デバイスは、
物理複製困難関数（ＰＵＦ）を有するセキュリティモジュールであって、前記ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、前記登録鍵対が登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える、セキュリティモジュールと、
１以上のメモリと、
を備え、
前記方法は、
セキュア接続を介して、前記ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のための証明書署名要求（ＣＳＲ）をサーバに送信するステップであって、前記ＣＳＲが、
前記デバイス識別子と、
前記ＥＰＫと、
を含み、
前記ＣＳＲが、前記ＥＳＫを使用して署名され、前記デバイス識別子が、前記ＥＰＫの

関数に基づく、送信するステップと、
前記セキュア接続を介して、前記ＥＰＫが前記デバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書を受信するステップと、
前記一時的登録デバイス証明書をメモリにインストールするステップと、
を含む方法。
【請求項１２】
サーバであって、
デバイス識別子と、電子デバイスによって確立される登録鍵対の登録公開鍵（ＥＰＫ）とを含む証明書署名要求（ＣＳＲ）を受信し、前記ＣＳＲが、前記ＥＰＫが前記デバイス識別子と関連付けられることを証明する証明書のためのものであり、前記デバイス識別子が前記ＥＰＫの関数に基づき、
前記デバイス識別子が、前記サーバが証明書に署名することができる前記デバイス識別子のデータベースと照合されるようにし、
前記デバイス識別子が前記ＥＰＫの関数であることを証明するために前記デバイス識別子の照合が実行されるようにし、
前記ＥＰＫが前記データベース内の前記デバイス識別子と関連付けられるようにし、
前記ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書に署名し、
前記デバイス識別子によって識別される前記電子デバイスに対するセキュア接続を介した前記署名された一時的登録デバイス証明書の送信を開始する、
ように構成されるサーバ。
【請求項１３】
前記サーバは、前記セキュア接続を介して発行証明書を送信するように更に構成され、前記発行証明書は、前記電子デバイスに知られているプライマリトラステッドルート証明書の下位である、請求項１２に記載のサーバ。
【請求項１４】
前記サーバは、前記デバイス識別子に基づいて、前記プライマリトラステッドルート証明書の下位である複数の発行証明書から前記セキュア接続を介して送信するための前記発行証明書を選択するように更に構成される、請求項１３に記載のサーバ。
【請求項１５】
前記セキュア接続を介して送信される発行証明書は、前記デバイス識別子と関連付けられるセキュリティポリシーに基づく、請求項１２から１４のいずれか一項に記載のサーバ。
【請求項１６】
電子デバイスのデバイス識別子がデータベースと照合されるようにすることは、前記ＣＳＲで受信される前記デバイス識別子が前記データベースに既に記憶されていることの照合を行なわせることを含み、前記受信されたデバイス識別子が前記データベースに既に記憶されている場合、前記サーバは、前記一時的登録デバイス証明書に署名することを許可される、請求項１２から１５のいずれか一項に記載のサーバ。
【請求項１７】
前記デバイス識別子が前記ＥＰＫの関数であることを証明するために前記デバイス識別子の照合が実行されるようにすることは、前記デバイス識別子が前記ＥＰＫのハッシュ関数に基づくことを証明するために前記デバイス識別子の照合が実行されるようにすることを含む、請求項１２から１６のいずれか一項に記載のサーバ。
【請求項１８】
前記一時的登録デバイス証明書の有効期間が１０分未満である、請求項１２から１７のいずれか一項に記載のサーバ。
【請求項１９】
セキュア接続発行証明書及びセキュア接続証明書の前記電子デバイスに対する送信を開始するように更に構成され、前記セキュア接続発行証明書及びセキュア接続証明書は、前

記電子デバイスに知られているプライマリトラステッドルート証明書の下位である、請求項１２から１８のいずれか一項に記載のサーバ。
【請求項２０】
前記サーバは、
一時的登録デバイス証明書を受信し、
前記デバイス識別子と、前記電子デバイスによって確立されるデバイス鍵対のデバイス公開鍵（ＤＰＫ）とを含む第２のＣＳＲを受信し、前記第２のＣＳＲが、前記ＤＰＫが前記デバイス識別子に関連付けられることを証明する証明書のためのものであり、
前記第２のＣＳＲの前記デバイス識別子が、前記サーバが証明書に署名することができるデバイス識別子のデータベースと照合されるようにし、
前記第２のＣＳＲの前記デバイス識別子が前記受信された一時的登録デバイス証明書において指定された前記デバイス識別子と一致することを検証するために前記第２のＣＳＲの前記デバイス識別子の照合が実行されるようにし、
前記ＣＳＲに基づいてデバイス証明書に署名し、前記デバイス証明書が、前記電子デバイスに知られているプライマリトラステッドルート証明書の下位であり、
前記デバイス識別子によって識別される前記電子デバイスに対する第２のセキュア接続を介した前記デバイス証明書の送信を開始する、
ように更に構成される、請求項１３から２２のいずれか一項に記載のサーバ。
【請求項２１】
前記デバイス証明書の送信を開始する前に、前記第２のＣＳＲの前記デバイス識別子が前記ＥＰＫの関数であることを検証するために前記第２のＣＳＲの前記デバイス識別子の照合が実行されるようにするべく更に構成される、請求項２０に記載のサーバ。
【請求項２２】
サーバにおいて、
デバイス識別子と、電子デバイスによって確立される登録鍵対の登録公開鍵（ＥＰＫ）とを含む証明書署名要求（ＣＳＲ）を受信するステップであって、前記ＣＳＲが、前記ＥＰＫが前記デバイス識別子と関連付けられることを証明する証明書のためのものであり、前記デバイス識別子が前記ＥＰＫの関数に基づく、受信するステップと、
前記デバイス識別子が、前記サーバが証明書に署名することができるデバイス識別子のデータベースと照合されるようにするステップと、
前記デバイス識別子が前記ＥＰＫの関数であることを証明するために前記デバイス識別子の照合が実行されるようにするステップと、
前記ＥＰＫが前記データベース内の前記デバイス識別子と関連付けられるようにするステップと、
前記ＥＰＫがデバイス識別子に関連付けられることを証明して有効期間を含む一時的登録デバイス証明書に署名するステップと、
前記デバイス識別子によって識別される前記電子デバイスに対するセキュア接続を介した前記署名された一時的登録デバイス証明書の送信を開始するステップと、
を含む方法。
【請求項２３】
電子デバイスであって、
物理複製困難関数（ＰＵＦ）を有するセキュリティモジュールであり、前記ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、前記登録鍵対が登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える、セキュリティモジュールと、
１以上のメモリと、
プロセッサと、
を備え、
前記プロセッサが、セキュア接続を介して、前記ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のための証明書署名要求（ＣＳＲ）を１つ以上のサーバのうち

の１つのサーバに送信するように構成され、前記ＣＳＲが、
前記デバイス識別子と、
前記ＥＰＫと、
を含み、
前記ＣＳＲが、前記ＥＳＫを使用して署名され、前記デバイス識別子が、前記ＥＰＫの関数に基づき、
前記プロセッサが、
前記セキュア接続を介して、前記ＥＰＫが前記デバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書を受信し、
検証に応じて、前記一時的登録デバイス証明書をメモリにインストールする、
ように構成される、電子デバイスと、
１つ以上のサーバであって、
前記セキュア接続を介して、前記デバイス識別子と、前記デバイス識別子と関連付けられることを証明する証明書のための前記ＥＰＫとを含む前記ＣＳＲを前記電子デバイスから受信し、
前記デバイス識別子を、前記１つ以上のサーバが証明書に署名することができるデバイス識別子のデータベースと照合し、
前記デバイス識別子が前記ＥＰＫの関数であることを証明するために前記デバイス識別子を照合し、
前記ＥＰＫを前記データベース内の前記デバイス識別子と関連付け、
前記ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む前記一時的登録デバイス証明書に署名し、
前記セキュア接続を介して前記署名された一時的登録デバイス証明書を前記電子デバイスに送信する、
ように構成される、１つ以上のサーバと、
を備えるシステム。
【請求項２４】
電子デバイスコンピューティングデバイスのプロセッサによって読み取られるときに前記プロセッサに請求項１１に記載の方法を実行させる命令が記憶されたコンピュータ可読媒体。
【請求項２５】
電子デバイスコンピューティングデバイスのプロセッサによって読み取られるときに前記プロセッサに請求項２２に記載の方法を実行させる命令が記憶された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、一般に、当事者間の信頼を確立するための方法及びシステムに関する。特に、本開示は、暗号化方法及びそのような方法を実行するように構成されるコンピューティング装置に関する。本明細書の開示は、多くのデバイス及びネットワークに適用可能であるが、特にインターネット接続デバイスに適用可能である。
【背景技術】
【０００２】
インターネットなどのネットワークは、日常的なタスクの実行方法を変化させており、これは情報セキュリティに大きな影響を及ぼしている。多くの日常タスクは、デジタルデバイスが安全に認証し、別の当事者によって認証され、及び／又は個人情報を安全に処理することを必要とする。モノのインターネット（ＩｏＴ）の発展に伴い、暖房や照明などのシステムがインターネットに接続されたデバイスによって制御されることが益々一般的になり、益々多くのデバイスが毎年インターネットに接続されるようになっている。
【０００３】

デバイス認証とは、それを信頼できるようにするためにデバイスの識別情報を安全に確立する行為を指す。デバイスが接続するサービス（例えば、クラウドベースのサービス）は、デバイスが本物であり、信頼できるソフトウェアを実行しており、信頼できるユーザに代わって動作していることを知る必要がある。

【０００４】

プロビジョニングとは、エンドユーザに渡すのに適するようにデバイスを準備し、サービスに登録するプロセスを指す。認証はそのプロセスの一部であるため、適切なクレデンシャルを提示するデバイスのみが登録される。プロビジョニングの正確な詳細は実施に基づいて大きく異なり得るが、殆どの状況において、デバイスには製造時に暗号鍵及び証明書が提供されるため、デバイスが展開される（サービスに接続するためにエンドユーザにいつでも提供できる状態にある）とき、適切なクレデンシャルを提供することができる。

【０００５】

多くの場合、ＩｏＴデバイスの組み込みシステムは事前共有鍵に依存しており、事前共有鍵は、それらがインターネットに接続されてグローバルにアドレス指定可能になる時点で問題になる。デバイスの展開前に事前共有鍵を共有しなければならず、また、集中型リソースは、一般に、通信するために各デバイスと鍵を共有する必要があるため、単一のサーバの妥協は、デバイスのネットワーク全体のセキュリティを危険にさらす場合がある。更に、そのような事前共有鍵は、任意の通信の発信元の証明及びアクセス制御などの様々なセキュリティ保証を可能にしない。

【０００６】

公開鍵インフラストラクチャ（ＰＫＩ）は、事前共有鍵に伴う問題に対処する１つの方法を提供する。ＰＫＩは、集中型クレデンシャル管理及び鍵配布のために多くのネットワークシステムで使用されるが、ＩｏＴコミュニティは、経済的理由及び技術的理由の両方のためにＰＫＩを採用するのに時間がかかっている。公開鍵暗号化、すなわち非対称暗号化は、広く普及することができる公開鍵と、デバイス／所有者にのみ知られている対応する秘密鍵（ｓｅｃｒｅｔ　ｋｅｙ）／プライベート鍵（ｐｒｉｖａｔｅ　ｋｅｙ）とを含む鍵の対を使用する暗号システムである。ＰＫＩは、デジタル証明書を作成、管理、配布、使用、記憶及び無効にする並びに公開鍵暗号化を管理するのに必要な役割、ポリシー、ハードウェア、ソフトウェア及び手順のセットである。ＰＫＩは、公開鍵をエンティティのそれぞれの識別情報（人、組織、又は個々のデバイスなど）とバインディングする。バインディングは、信頼できる認証局（ＣＡ）による証明書の登録及び発行のプロセスを介して確立される。

【０００７】

事前共有鍵又は公開鍵インフラストラクチャをうまく利用するために、幾つかの秘密情報が、一般に、デバイス製造時又はその直後に電子デバイスのセキュア領域に注入される。例えば、秘密情報は事前共有鍵であってもよく、又は秘密情報は、公開鍵暗号化に依存するシステム内の鍵対の秘密鍵を含んでもよい。この手法は、秘密情報を電子デバイスに注入する、及び／又は鍵を安全に注入する第三者の能力を信頼するセキュア設備を必要とする。セキュア設備は、コストが高く、管理が困難であり、新たな脅威に対する堅牢な応答を確保するためにセキュリティ手順の継続的な保守及び評価を必要とする。一般に、鍵を生成及び記憶するためにハードウェアセキュリティモジュール（ＨＳＭ）が必要とされる場合があり、電子デバイスに鍵を注入するために一体型鍵注入システムが必要とされる場合があり、その場合でも、ＨＳＭ及び／又はセキュア設備が損なわれる場合、注入された鍵の完全性を確保することができない。

【０００８】

電子デバイスに秘密情報を安全に提供する際の固有の困難は、デバイスの登録－相互接続されたデバイスのグリッドへのその開始などの更なる下流側プロセスに影響を及ぼす可能性がある。多くの場合、デバイス証明書は、サービスに登録するための幾つかの基本的なクレデンシャルをデバイスに提供するために、製造時にデバイスに安全に提供されなければならない。ここでも、これをどの程度確実に行なうことができるかには限界がある。

【０００９】
典型的なシナリオにおいて、相手先ブランド製品の製造業者（ＯＥＭ）は、製造されたデバイスに登録を可能にするための識別情報を提供し、デバイスにファームウェアを安全にインストールすることを求めることができる。デバイスは、例えば、鍵を記憶するためのセキュア領域を有するマイクロコントローラを含むことができ、マイクロコントローラは、第三者の製造業者によって製造されていてもよい。ＯＥＭ又は製造業者は、例えば、秘密鍵及びデバイス証明書を、セキュア設備を必要とするセキュア領域に注入することができる。デバイスにファームウェア／証明書をインストールするために、ＯＥＭは、信頼を必要とするデバイスを構成するためのプログラミングハウスのサービスを採用することができる。プログラミングハウスは、セキュア設備を運用し、正しい情報を注入し、ＯＥＭに代わって証明書に安全に署名するために、信頼できなければならない。状況によっては、デバイスをプロビジョニングするには、複数の異なる当事者が電子デバイスと対話する必要があり得る。

【００１０】
本発明の実施形態の目的は、当技術分野で知られている１つ以上の問題を少なくとも緩和することである。

【発明の概要】

【００１１】
本発明の一態様によれば、電子デバイスが提供される。電子デバイスは、物理複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える。電子デバイスは、１つ以上のメモリを更に備える。電子デバイスは、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のためのデバイス識別子及びＥＰＫを含む証明書署名要求（ＣＳＲ）をサーバに送信するように構成される１つ以上のプロセッサを更に備え、ＣＳＲがＥＳＫを使用して署名され、デバイス識別子がＥＰＫの関数に基づく。１つ以上のプロセッサは、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書を受信するように更に構成される。１つ以上のプロセッサは、一時的登録デバイス証明書をメモリにインストールするように更に構成される。

【００１２】
従来、デバイスがサービスに関して認証できるようにするために、デバイス証明書（一時的又は他の方法）が、デバイス証明書と関連付けられる秘密鍵と共に、製造中にデバイスにインストールされる。これに対し、本開示の方法及び装置は、好適には、製造後に、製造時に電子デバイスに秘密鍵を埋め込む必要なく、一時的デバイス証明書を電子デバイスに提供できるようにする。

【００１３】
１つ以上のメモリには、プライマリトラステッドルート証明書がインストールされていてもよい。１つ以上のプロセッサは、セキュア接続を介して、発行証明書を受信するように更に構成されてもよく、発行証明書は、プライマリトラステッドルート証明書の下位（descendant）である。発行証明書は、電子デバイスのための永続的デバイス証明書に関連する後続の手順で使用され得る。

【００１４】
１つ以上のプロセッサは、発行証明書がプライマリトラステッドルート証明書から直接派生していることを検証するように更に構成されてもよい。１つ以上のプロセッサは、検証に応じて、発行証明書をメモリにインストールするように更に構成されてもよい。

【００１５】
１つ以上のプロセッサは、サーバからセキュア接続発行証明書及びセキュア接続証明書を受信するように更に構成されてもよく、セキュア接続発行証明書及びセキュア接続証明書はプライマリトラステッドルート証明書の下位である。１つ以上のプロセッサは、プラ

イマリトラステッドルート証明書を使用してセキュア接続証明書を検証するように更に構成されてもよい。１つ以上のプロセッサは、検証に応じて、サーバに対するセキュア接続を確立するように更に構成されてもよい。

【００１６】

セキュア接続証明書を検証することは、セキュア接続証明書がプライマリトラステッドルート証明書の下位であることを検証すること、任意選択的に、セキュア接続証明書に含まれるサーバ識別子を電子デバイスの１つ以上のメモリに記憶されるサーバ識別子と比較することを含んでもよい。サーバ識別子は、例えば、サーバの名前又はサーバのアドレス（例えば、ＵＲＬ又はＩＰアドレス）を含んでもよい。

【００１７】

１つ以上のプロセッサは、電子デバイスの１つ以上のメモリに記憶されるサーバ識別子によって識別されるサーバに対するセキュア接続を開始するように更に構成されてもよい。

【００１８】

デバイスは、ＰＵＦに対する第２のチャレンジ及び応答に基づいてデバイス鍵対（ＤＰＫ、ＤＳＫ）を確立するように更に構成されてもよく、デバイス鍵対は、デバイス公開鍵（ＤＰＫ）及びデバイス秘密鍵（ＤＳＫ）を含む。１つ以上のプロセッサは、第２のセキュア接続を介して、ＤＰＫがデバイス識別子と関連付けられることを証明する証明書のための第２の証明書署名要求（ＣＳＲ）をサーバに送信するように更に構成されてもよい。第２のＣＳＲはＤＰＫ及びデバイス識別子を含んでもよく、第２のＣＳＲはＤＳＫを使用して署名される。１つ以上のプロセッサは、第２のセキュア接続を介して、ＤＰＫをデバイス識別子と関連付けるデバイス証明書を受信するように更に構成されてもよい。１つ以上のプロセッサは、デバイス証明書がプライマリトラステッドルート証明書の下位であることを検証するように更に構成されてもよい。１つ以上のプロセッサは、検証に応じて、デバイス証明書をメモリにインストールするように更に構成されてもよい。

【００１９】

好適には、本明細書を読むと明らかになるように、そのような方法は、デバイス識別子がそのデバイス識別子に関連するものとして認証されたデバイス公開鍵に関連しないデバイス証明書を電子デバイスに提供できるようにする。これにより、下流側での更なるセキュリティが可能になる。例えば、デバイス鍵対が何らかの予期しない方法で危険にさらされる場合、電子デバイスは、新しいデバイス識別情報を必要とせずに再鍵付き証明書を取得することができる。

【００２０】

デバイス識別子は、ＥＰＫのハッシュ関数に基づいてもよい。例えば、デバイス識別子は、ＥＰＫに適用される暗号化ハッシュ関数に基づいてもよい。

【００２１】

一時的登録デバイス証明書の有効期間は、関連する実施目的に適した任意の期間であってもよい。幾つかの例において、有効期間は、１０分未満、５分未満、又は２分未満であってもよい。

【００２２】

幾つかの例において、一時的登録デバイス証明書は、その識別情報が電子デバイスのファームウェアから電子デバイスに知られていたコンピューティング装置／サーバからセキュア接続を介して受信されたため、電子デバイスによって信頼され得る。

【００２３】

他の例において、電子デバイスの１つ以上のメモリには、一時的登録トラステッドルート証明書がインストールされていてもよい。１つ以上のプロセッサは、一時的登録デバイス証明書を受信した後、一時的登録トラステッドルート証明書を使用して一時的登録デバイス証明書を検証するように構成されてもよく、一時的登録デバイス証明書をインストールすることは検証に応答したものである。

【００２４】

一時的登録デバイス証明書は、一時的登録発行証明書と関連付けられる秘密鍵を使用してサーバによって署名されてもよい。

【００２５】

本発明の一態様によれば、電子デバイスによる実行のための方法が提供される。電子デバイスは、物理複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備え、セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える。電子デバイスは、１つ以上のメモリを更に備える。方法は、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のための証明書署名要求（ＣＳＲ）をサーバに送信するステップを含み、ＣＳＲはデバイス識別子及びＥＰＫを含む。ＣＳＲはＥＳＫを使用して署名され、デバイス識別子はＥＰＫの関数に基づく。方法は、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書を受信するステップを更に含む。方法は、一時的登録デバイス証明書をメモリにインストールすることを更に含む。

【００２６】

本発明の一態様によれば、サーバが提供される。サーバは、本明細書では鍵管理サーバ又はコンピューティング装置とも呼ばれ得る。サーバは、デバイス識別子と、電子デバイスによって確立される登録鍵対の登録公開鍵（ＥＰＫ）とを含む証明書署名要求（ＣＳＲ）を受信するように構成される。ＣＳＲは、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のためのものである。デバイス識別子は、ＥＰＫの関数に基づく。サーバは、サーバが証明書に署名することができるデバイス識別子のデータベースとデバイス識別子が照合されるようにするべく更に構成される。サーバは、デバイス識別子がＥＰＫの関数であることを証明するためにデバイス識別子の照合が実行されるようにするべく更に構成される。サーバは、ＥＰＫがデータベース内のデバイス識別子と関連付けられるようにするべく更に構成される。サーバは、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書に署名するように更に構成される。サーバは、デバイス識別子によって識別される電子デバイスに対するセキュア接続を介した署名された一時的登録デバイス証明書の送信を開始するように更に構成される。

【００２７】

サーバは、電子デバイスからセキュア接続を介してＣＳＲを受信するように構成されてもよい。サーバは、サーバシステムの１つのサーバであってもよく、ＣＳＲは、電子デバイスとのセキュア接続を介してＣＳＲを受信したサーバシステムの他のサーバを介して受信されてもよい。

【００２８】

サーバは、セキュア接続を介して発行証明書を送信するように更に構成されてもよく、発行証明書は、電子デバイスに知られているプライマリトラステッドルート証明書の下位である。

【００２９】

サーバは、デバイス識別子に基づいて、プライマリトラステッドルート証明書の下位である複数の発行証明書からセキュア接続を介して送信するための発行証明書を選択するように更に構成されてもよい。このようにして、異なるデバイスに関して異なるセキュリティポリシーを設定することができ、例えば、第１の発行証明書を第１のクラスの電子デバイス（例えば、スマート電球）で使用し、第２の発行証明書を第２のクラスの電子デバイス（例えば、スマート洗濯機）で使用することができる。

【００３０】

セキュア接続を介して送信される発行証明書は、電子デバイスと関連付けられるセキュリティポリシーに基づくことができる。

【００３１】

電子デバイスのデバイス識別子がデータベースと照合されるようにすることは、ＣＳＲ

において受信されたデバイス識別子がデータベースに既に記憶されることを検証するために照合が実行されるようにすることを含んでもよい。サーバは、受信されたデバイス識別子がデータベースに既に記憶される場合にのみ、一時的登録デバイス証明書に署名することを許可されてもよい。好適には、そのような条件は、関連するデバイス識別子がデータベース内にある電子デバイスのための証明書にのみサーバが署名するため、セキュリティを向上させ、したがって、危険にさらされた電子デバイスはサーバと通信することができない。

【００３２】

デバイス識別子がＥＰＫの関数であることを証明するためにデバイス識別子の照合が実行されるようにすることは、デバイス識別子がＥＰＫのハッシュ関数に基づくことを証明するためにデバイス識別子の照合が実行されるようにすることを含んでもよい。

【００３３】

一時的登録デバイス証明書の有効期間は、関連する実施目的に適した任意の期間であってもよい。幾つかの例において、有効期間は、１０分未満、５分未満、又は２分未満であってもよい。

【００３４】

サーバは、電子デバイスに対するセキュア接続発行証明書及びセキュア接続証明書の送信を開始するように更に構成されてもよく、セキュア接続発行証明書及びセキュア接続証明書は、電子デバイスに知られているプライマリトラステッドルート証明書の下位である。

【００３５】

サーバは、一時的登録デバイス証明書を受信するように更に構成されてもよい。サーバは、デバイス識別子と、電子デバイスによって確立されるデバイス鍵対のデバイス公開鍵（ＤＰＫ）とを含む第２のＣＳＲを受信するように更に構成されてもよく、第２のＣＳＲは、ＤＰＫがデバイス識別子と関連付けられることを証明する証明書のためのものである。サーバは、サーバが証明書に署名することができるデバイス識別子のデータベースと第２のＣＳＲのデバイス識別子が照合されるようにするべく更に構成されてもよい。サーバは、第２のＣＳＲのデバイス識別子が受信した一時的登録デバイス証明書で指定されたデバイス識別子と一致することを検証するために、第２のＣＳＲのデバイス識別子の照合が実行されるようにするべく更に構成されてもよい。サーバは、ＣＳＲに基づいてデバイス証明書に署名するように更に構成されてもよく、デバイス証明書は、電子デバイスに知られているプライマリトラステッドルート証明書の下位である。サーバは、デバイス識別子によって識別される電子デバイスに対する第２のセキュア接続を介したデバイス証明書の送信を開始するように更に構成されてもよい。幾つかの例において、サーバは、デバイス証明書の送信を開始する前に、第２のＣＳＲのデバイス識別子がＥＰＫの関数であることを検証するために、第２のＣＳＲのデバイス識別子の照合が実行されるようにするべく更に構成されてもよい。

【００３６】

サーバは、電子デバイスから第２のセキュア接続を介してＤＰＫのためのＣＳＲを受信するように構成されてもよい。サーバは、サーバシステムの１つのサーバであってもよく、第２のＣＳＲは、電子デバイスとのセキュア接続を介して第２のＣＳＲを受信したサーバシステムの他のサーバを介して受信されてもよい。

【００３７】

一時的登録デバイス証明書は、サーバに記憶された一時的登録発行証明書によって署名されてもよい。

【００３８】

本発明の一態様によれば、サーバにおける実行のための方法が提供される。方法は、デバイス識別子と、電子デバイスによって確立される登録鍵対の登録公開鍵（ＥＰＫ）とを含む証明書署名要求（ＣＳＲ）を受信するステップを含む。ＣＳＲは、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のためのものであり、デバイス識別子はＥ

ＰＫの関数に基づく。方法は、サーバが証明書に署名することができるデバイス識別子のデータベースとデバイス識別子が照合されるようにするステップを含む。方法は、デバイス識別子がＥＰＫの関数であることを証明するために、デバイス識別子の照合が実行されるようにするステップを含む。方法は、ＥＰＫがデータベース内のデバイス識別子と関連付けられるようにするステップを含む。方法は、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書に署名するステップを含む。方法は、デバイス識別子によって識別される電子デバイスに対するセキュア接続を介した署名された一時的登録デバイス証明書の送信を開始するステップを含む。

【００３９】

本発明の一態様によれば、システムが提供される。システムは、電子デバイス及び１つ以上のサーバを備える。電子デバイスは、物理複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備え、セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える。電子デバイスは、１つ以上のメモリを更に備える。電子デバイスは、１つ以上のプロセッサを更に備える。１つ以上のプロセッサは、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のための証明書署名要求（ＣＳＲ）を１つ以上のサーバのうちの１つのサーバに送信するように構成される。ＣＳＲは、デバイス識別子及びＥＰＫを含み、ＣＳＲは、ＥＳＫを使用して署名される。デバイス識別子は、ＥＰＫの関数に基づく。１つ以上のプロセッサは、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書を受信するように更に構成される。１つ以上のプロセッサは、検証に応じて、一時的登録デバイス証明書をメモリにインストールするように更に構成される。１つ以上のサーバは、セキュア接続を介して、デバイス識別子とＥＰＫがデバイス識別子と関連付けられることを証明する証明書のためのＥＰＫとを含むＣＳＲを電子デバイスから受信するように構成される。１つ以上のサーバは、１つ以上のサーバが証明書に署名することができるデバイス識別子のデータベースとデバイス識別子を照合するように更に構成される。１つ以上のサーバは、デバイス識別子がＥＰＫの関数であることを証明するためにデバイス識別子を照合するように更に構成される。１つ以上のサーバは、ＥＰＫをデータベース内のデバイス識別子と関連付けるように更に構成される。１つ以上のサーバは、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書に署名するように更に構成される。１つ以上のサーバは、セキュア接続を介して署名された一時的登録デバイス証明書を電子デバイスに送信するように更に構成される。

【００４０】

本発明の一態様によれば、コンピュータ可読媒体が提供される。コンピュータ可読媒体は、電子デバイスのプロセッサによって実行されるときに電子デバイスに本明細書に記載の方法を実行させる命令を含む。

【００４１】

本発明の一態様によれば、コンピュータ可読媒体が提供される。コンピュータ可読媒体は、サーバのプロセッサによって実行されるときにサーバに本明細書に記載の方法を実行させる命令を含む。

【００４２】

本明細書に記載のような方法を実行するためのコンピュータプログラム及び／又はコード／命令は、コンピュータ可読媒体又はコンピュータプログラムプロダクト上のコンピュータなどの装置に提供されてもよい。コンピュータ可読媒体は、例えば、電子、磁気、光学、電磁気、赤外線、もしくは半導体システム、又はデータ伝送のための、例えばインターネットを介してコードをダウンロードするための伝搬媒体とすることができる。或いは、コンピュータ可読媒体は、半導体又はソリッドステートメモリ、磁気テープ、取り外し可能なコンピュータディスケット、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、剛体磁気ディスク、及びＣＤ－ＲＯＭ、ＣＤ－Ｒ／Ｗ、又はＤＶＤな

どの光ディスクなどの物理的なコンピュータ可読媒体の形態を成すことができる。
【００４３】
本明細書に提示された教示に照らして、これらの発明が関連する当業者には、本明細書に記載された発明の多くの修正及び他の実施形態が思い浮かび得る。したがって、本明細書の開示は、本明細書に開示された特定の実施形態に限定されるものではないことが理解され得る。更に、本明細書で提供される説明は、要素、ステップ、及び／又は機能の特定の組み合わせの文脈で例示的な実施形態を提供するが、本発明の範囲から逸脱することなく代替の実施形態によって提供されてもよい。
【００４４】
ここで、添付図面に関連して、本発明の実施形態を単なる例として説明する。
【図面の簡単な説明】
【００４５】
【図１】例示のみを目的として詳細な説明を通して参照される様々な当事者の図を示す。
【図２】通信システムを示す。
【図３Ａ】電子デバイスのブロック図を示す。
【図３Ｂ】マイクロコントローラの図を示す。
【図４Ａ】セキュリティモジュールのブロック図を示す。
【図４Ｂ】ＰＵＦモジュールのブロック図を示す。
【図５】コンピューティング装置のブロック図を示す。
【図６Ａ】公開鍵インフラストラクチャによって提供される信頼チェーンにおける証明書の一例を示す。
【図６Ｂ】一時的登録デバイス証明書を電子デバイスに提供するために使用される信頼チェーンにおける証明書の一例を示す。
【図６Ｃ】電子デバイスにデバイス証明書を提供するために使用される信頼チェーンにおける証明書の一例を示す。
【図６Ｄ】ファームウェアを認証するための信頼チェーンにおける証明書の一例を示す。
【図７】一時的登録デバイス証明書を電子デバイスに提供するための方法のスイムレーンフローチャートを示す。
【図８】フローチャートを示す。
【図９】フローチャートを示す。
【図１０】電子デバイスにデバイス証明書を提供するための方法のスイムレーンフローチャートを示す。
【図１１】フローチャートを示す。
【図１２】フローチャートを示す。
【図１３】コンピュータ可読媒体のブロック図を示す。
【発明を実施するための形態】
【００４６】
説明及び図面を通して、同様の参照番号は同様の部分を指す。
【００４７】
様々な実施形態が以下に説明されるが、本発明はこれらの実施形態に限定されず、これらの実施形態の変形は、添付の特許請求の範囲によってのみ限定されるべき本発明の範囲内に十分に含まれ得る。
【００４８】
以下では、ＩｏＴデバイスのセキュリティ及び登録について言及する。しかしながら、当業者であれば分かるように、本明細書に記載の方法、システム、及び装置がはるかに広く適用可能である。
【００４９】
以下では、一時的登録デバイス証明書を電子デバイスに安全に提供する方法、及びデバイス証明書を電子デバイスに安全に提供する方法について説明する。本明細書に記載の方法は、関与する様々な当事者が電子デバイスのセキュリティを特に互いに信頼する必要な

く、電子デバイスを展開し、電子デバイスがサービス（例えば、ＩｏＴハブによって提供されるクラウドベースのサービス）にいつでも接続できるようにする。説明を容易にするために、幾つかの関与する当事者（例えば、相手先ブランド製品の製造業者及びＩｏＴハブ）の例示的なシナリオが、図１に記載されている、詳細な説明全体を通して参照される。しかしながら、本明細書に記載の方法は、当業者により理解されるように、より一般的に適用可能である。

【００５０】

詳細な説明を読むと理解されるように、電子デバイスには物理複製困難関数が与えられてもよい。物理複製困難関数（物理的に複製が困難な関数又はＰＵＦとしても知られている）は、セキュアＥＥＰＲＯＭ及び他の高価なハードウェアを必要とせずに、認証及び秘密鍵記憶のために使用される暗号プリミティブである。秘密をデジタルメモリに記憶する代わりに、ＰＵＦは、通常は製造中に導入される１つ以上の構成要素の固有の物理的特性から秘密を導き出す。既知のＰＵＦは、小さなシリカ球が懸濁された硬化エポキシシートを通るレーザ光の散乱、又は幾つかの回路におけるゲート遅延の製造ばらつきなどの現象に基づいている。

【００５１】

以下では、物理的に複製が困難な関数、物理複製困難関数、及びＰＵＦという用語は互換的に使用される。ＰＵＦは、機能的操作を実行するオブジェクトを含み、すなわち、特定の入力で照会されると、ＰＵＦは測定可能な出力を生成する。一般に、ＰＵＦへの入力は「チャレンジ」と呼ばれ、結果として生じるＰＵＦの出力は「応答」と呼ばれる。適用されたチャレンジ及びその測定された応答は、「チャレンジ－応答対」（ＣＲＰ）として知られている。本明細書で使用される用語「チャレンジ」は、ＰＵＦ（例えば、アレイの特定のセルの選択、特定の電圧の印加など）に提供される選択された入力を意味すると理解され、用語「応答」は、ＰＵＦの対応する出力を指すために本明細書で使用される。

【００５２】

ＰＵＦが電子デバイスでの使用に適している限り、任意の適切なＰＵＦを本明細書に記載のシステム及び方法で使用することができる。例えば、ＰＵＦはＳＲＡＭ　ＰＵＦであってもよい。ＳＲＡＭ　ＰＵＦは、ＳＲＡＭの閾値電圧のランダム差を使用して、固有のチャレンジ－応答対を作成する。

【００５３】

適切なＰＵＦの他の例は、チップ上のワイヤ又はゲートにおける遅延のランダムな変動を利用する遅延ＰＵＦである。入力チャレンジが与えられると、回路内にレース条件が設定され、異なる経路に沿って伝播する２つの遷移が比較されて、どちらが最初に来るかが分かる（応答）。

【００５４】

ＰＵＦの他の例では、量子閉じ込めが役割を果たすことができる。例えば、ＰＵＦは、幾つかの共振トンネルダイオードから形成することができる。

【００５５】

ＰＵＦの他の例では、量子トンネル障壁を通る量子トンネルが役割を果たす場合がある。ＰＵＦの一例は、「Ｄｅｖｉｃｅ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｗｉｔｈ　Ｑｕａｎｔｕｍ　Ｔｕｎｎｅｌｌｉｎｇ　Ｃｕｒｒｅｎｔｓ」と題されて国際公開第２０２０／２１２６８９号として公開された、２０２０年４月８日に出願された国際特許出願番号ＰＣＴ／ＧＢ２０２０／０５０９１８号に記載されている。一例によれば、ＰＵＦは、複数の個別にアドレス指定可能なセルを有するアレイを含み得る。各セルは、量子トンネル障壁を有する要素回路を備えてもよい。セルは、トランジスタの形態の第１の電子部品と、第２の電子トランジスタの形態の第２の電子部品とを備えてもよい。第１のトランジスタのソース、ドレイン及び本体は、同電位（例えば、地面）に保持されてもよい。第２のトランジスタのソース、ドレイン、及び本体も全て同じ電位に保持されてもよい。第１のトランジスタは、トランジスタのチャネルとゲート端子との間に第１の量子トンネル障壁を有する。第２のトランジスタは、トランジスタのチャネルとゲート端子との間に第２の量

子トンネル障壁を有する。製造中に導入されるトランジスタの固有の違いにより、第１の量子トンネル障壁は第１のトランジスタを固有に特徴付け、第２の量子トンネル障壁は第２のトランジスタを固有に特徴付ける。セルは、第１の量子トンネル障壁及び第２の量子トンネル障壁にわたって電位差を印加するために、行デコーダ及び列デコーダを使用して選択され得る。電位差は、電流が第１の量子トンネル障壁又は第２の量子トンネル障壁のいずれかを古典的に通過することができる閾値電圧未満であり得る。したがって、セルが選択されると、量子トンネル電流は第１のトランジスタの第１の量子トンネル障壁を通って流れることができ、量子トンネル電流は第２のトランジスタの第２の量子トンネル障壁を通って流れることができ、古典的な電流は流れない場合がある。量子トンネル電流を比較及び増幅することができる。セルと印加電圧との組み合わせをチャレンジと見なすことができ、出力量子トンネル電流を応答と見なすことができる。

【００５６】

他の例では、ＰＵＦは、電子的に相互作用することができる限り、電子部品に基づく必要はない。

【００５７】

以下では、非対称鍵対として知られる幾つかの公開鍵対を参照する。非対称鍵対は、他の当事者と共有され得る公開鍵と、共有されない対応する秘密鍵とを含む。公開鍵は、秘密に保つ必要はないが、改ざんされないように保存されるべき公開値である。一例では、公開鍵は、電子デバイス内のＲＯＭに記憶されて、決して書き換え又は変更することができないようにすることができる。本明細書で説明される公開鍵対は、多くの場合名前を有する。例えば、１つの公開鍵対は、「登録公開鍵」（ＥＰＫ）と対応する「登録秘密鍵」（ＥＳＫ）とを含む「登録公開鍵対」として説明される。別の公開鍵対は、「デバイス公開鍵」（ＤＰＫ）と対応する「デバイス秘密鍵」（ＤＳＫ）とを含む「デバイス公開鍵対」として説明される。別の公開鍵対は、「公開認証局鍵」（ＰＡＫ）と対応する「秘密認証局鍵」（ＳＡＫ）とを含む「認証局鍵対」として説明される。読者は、これらの公開鍵対の名前が公開鍵対を区別することのみを意図していることを理解し得る。

【００５８】

本明細書で説明される公開鍵対は、任意の適切な公開鍵暗号システム、例えばＲＳＡ又は楕円曲線ベースの暗号システムと共に使用され得る。本明細書で説明される公開鍵対の多くは、デジタル署名と共に使用するためのものである。デジタル署名は、デジタルメッセージ又は文書の真正性を検証するための数学的スキームである。本明細書の例では、任意の適切なデジタル署名スキーム、例えばＲＳＡ、ＥｌＧａｍａｌ署名スキーム又はＥＣＤＳＡを使用することができる。

【００５９】

本明細書に記載のサーバ／サーバシステム／コンピューティング装置の幾つかには、「認証局サーバシステム」又は「鍵管理サーバ」などの名前も付けられている。読者は、そのような名称が異なるコンピューティング装置を区別することのみを意図していることを理解し得る。

【００６０】

図１は、電子デバイス１００の安全な作成、プロビジョニング、及び展開に関与することができる商用（又は他の）当事者を描く図を示す。当業者は、他の設定が想定され、この図が例示のみを目的として提供されていることを理解し得る。高レベルでは、セキュリティモジュールが製造され、次いで、電子デバイス１００にインストールするために相手先ブランド製品の製造業者（ＯＥＭ）１６０にセキュリティモジュールが（必ずしもそうとは限らないが、一般に、マイクロコントローラの一部として）提供される。次いで、ＯＥＭ１６０は、プログラミングハウス１８０の助けを借りて、電子デバイス１００にファームウェアをインストールし、最終的に展開のために電子デバイス１００を準備するステップをとることができる。展開されると、電子デバイス１００は、ＩｏＴハブ１７０を介して提供されるサービスと通信することができる。

【００６１】

図を参照すると、認証局（authority）１４０は、電子デバイス１００にインストールするためのセキュリティモジュール１１０を作成するために、製造能力１５０を有することができる（又は信頼できる製造業者と密接に協働することができる）。セキュリティモジュール及び電子デバイスの例を以下で更に説明する。

【００６２】

本説明の目的のために、セキュリティモジュール１１０は、公開鍵対を確立するように動作可能な、図１には示されていない物理複製困難関数（ＰＵＦ）を含む。公開鍵対は、他の当事者と共有され得る公開鍵と、共有されない対応する秘密鍵とを含む。公開鍵対は、非対称鍵対としても知られ得る。公開鍵及び秘密鍵は、ＰＵＦに対するチャレンジ及び応答に基づくことができる。例えば、公開鍵はＰＵＦに対するチャレンジに基づくことができ、秘密鍵はそのチャレンジに対する応答に基づくことができる。したがって、セキュリティモジュール１１０は、製造業者１５０又は下流側のいずれかの当事者によって任意の秘密鍵が注入されることを必要とせずに公開鍵対を確立することができる。

【００６３】

本説明の目的のために、セキュリティモジュール１１０は、対応する少なくとも２つのチャレンジ－応答対に基づいて少なくとも２つの鍵対を確立するように構成される。好適には、ＰＵＦベースの公開鍵対では、秘密鍵は、電子デバイスに記憶される必要はないが、セキュリティモジュールによって提供されるセキュア境界／信頼ゾーン内でＰＵＦから動的に再生成され得る。したがって、たとえ電子デバイスがハッキングされたとしても、盗まれる秘密鍵がそこに記憶されていない可能性がある。

【００６４】

登録公開鍵（ＥＰＫ）及び対応する登録秘密鍵（ＥＳＫ）は、第１のＣＲＰに基づく。ＥＰＫは、電子デバイスに識別子を提供するために使用され、以下で更に説明するように、一時的登録デバイス証明書を電子デバイスに提供するプロセスで使用される。一時的登録デバイス証明書は、ＥＰＫをデバイス識別子と関連付け、電子デバイスのためのデバイス証明書を取得するために後続の通信で使用可能である。デバイス識別子は、ＥＰＫの関数に基づく。本明細書で説明される例の多くでは、関数が暗号化ハッシュ関数であるが、これはそうである必要はなく、別の関数が使用されてもよい。

【００６５】

デバイス公開鍵（ＤＰＫ）及び対応するデバイス秘密鍵（ＤＳＫ）は、第２のＣＲＰに基づく。デバイス鍵対は、ＥＰＫに基づく特定のデバイス識別子を有する適切な電子デバイスにデバイス証明書を提供する際に使用される。デバイス証明書は、ＤＰＫがデバイス識別子と関連付けられることを証明する。後述するように、デバイス証明書を認証する信頼チェーンは、ＯＥＭ１６０によって制御される。

【００６６】

本開示の目的のために、電子デバイス１００は、マイクロコントローラ（ＭＣＵ）などの低レベル回路から成ると理解されてもよい。電子デバイス１００は、代替的に、より高いレベルの回路、例えば湿度又は温度を検知するための回路を備えると理解されてもよく、又はスマートフォン又はコンピュータなどのより大規模な電子デバイスであると理解されてもよい。製造業者１５０は、セキュリティモジュール１１０のみを製造してもよく、或いは、セキュリティモジュール１１０が搭載されたマイクロコントローラを製造してもよい。

【００６７】

以下で更に説明するように、認証局１４０は、公開鍵対と関連付けられてもよい。すなわち、認証局１４０は、公開鍵（以下、公開認証局鍵ＰＡＫと呼ぶ）及び対応する秘密鍵（以下、秘密認証局鍵ＳＡＫと呼ぶ）と関連付けられ得る。ＳＡＫは他の当事者と共有されないが、ＰＡＫはより広く共有され得る。例えば、ＰＡＫは、セキュリティモジュール１１０、例えばセキュアメモリにインプリントされてもよい。或いは、製造業者１５０がセキュリティモジュールを備えるマイクロコントローラ（又は他の電子デバイス）を製造する場合、ＰＡＫは、セキュリティモジュールの外部の電子デバイスの他のリードオンリ

ーメモリ（ＲＯＭ）にインストールされてもよい。セキュリティ目的のために、セキュリティモジュール／電子デバイスに記憶されたＰＡＫがその完全性を保つために書き換えることも変更することもできないことが重要である。ＰＡＫは、後の段階でセキュリティモジュール１１０によって使用されて、受信した情報がＳＡＫを使用して署名され、したがって認証局１４０によって承認されたことを検証することができる。他の非秘密情報、例えば、ＳＡＫを使用して認証局１４０によって署名され、ＰＡＫが認証局１４０と関連付けられることを示すルート証明書も、セキュリティモジュール／電子デバイスにインプリントすることができる。認証局１４０によってセキュリティモジュール１１０に秘密情報は提供されない。認証局１４０又は製造業者１５０によってセキュリティモジュール１１０から秘密情報が抽出されない。

【００６８】

デバイス識別子及び１つ以上の公開鍵をセキュリティモジュール１１０から抽出できるようにするために、初期登録ファームウェア（ＩＥＦ）もセキュリティモジュール／電子デバイスに提供される。

【００６９】

認証局１４０は、１つ以上のサーバを備えるサーバシステム１３０を所有及び／又は運用することができる。図１の認証局サーバシステム１３０には３つのサーバが示されるが、当業者であれば分かるように、サーバシステム１３０はより多くの又はより少ないサーバを備えてもよい。

【００７０】

認証局システムのサーバの少なくとも１つは、ＳＡＫを使用して証明書に署名するように構成される（これに関する詳細は以下で更に提供される）。ＳＡＫは、ファームウェアの署名にも使用することができる。

【００７１】

認証局サーバシステム１３０のサーバの少なくとも１つは、デバイス識別子等のセキュリティモジュール１１０に関する情報を有するデータベースを保持するように構成される。

【００７２】

認証局サーバシステム１３０のサーバのうちの少なくとも１つは、相手先ブランド製品の製造業者（ＯＥＭ）１６０によって運営されるコンピューティング装置１２０と安全に通信するように構成される。

【００７３】

サーバの少なくとも１つは、ＩｏＴハブ１７０と通信するように構成される。ＩｏＴハブは、ＩｏＴアプリケーションとそれが管理する電子デバイスとの間の双方向通信のためのメッセージハブとして機能する、クラウドでホストされるマネージドサービスである。本説明の目的のために、本明細書に記載の方法は、電子デバイスがＩｏＴハブ１７０と通信する準備ができた状態で展開され得るように、電子デバイスをプロビジョニングするのに適している。

【００７４】

単に明確にする目的のために、サーバシステム１３０のサーバは、本明細書では「認証局サーバ」と呼ばれることがある。

【００７５】

当業者であれば分かるように、サーバシステム１３０の機能の少なくとも一部がクラウドサービスとして提供されてもよい。サーバのうちの１つ以上は、認証局１４０の物理的に外部に位置され得る。サーバシステム１３０の認証局サーバは、特定のセキュリティモジュール１１０を識別するためのデバイス識別子を受信することができる。デバイス識別子は、登録秘密鍵（ＥＳＫ）及びＥＰＫを含む登録鍵対の登録公開鍵（ＥＰＫ）の関数に基づく。ＥＰＫ及びＥＳＫは、セキュリティモジュール１１０のＰＵＦに対するチャレンジ及び応答に基づいており、ＥＳＫはセキュリティモジュール１１０を離れない。一例では、ＥＰＫがＰＵＦに対するチャレンジに基づいており、ＥＳＫがＰＵＦに対するチャレ

ンジへの応答に基づいている。サーバシステム１３０は、デバイス識別子をデータベースに記憶するように構成される。幾つかの例において、サーバシステム１３０は、特定のセキュリティモジュール１１０のＥＰＫを受信してもよいが、受信する必要はない。

【００７６】

サーバシステム１３０がセキュリティモジュール１１０のデバイス識別子を受信して記憶すると、セキュリティモジュール１１０（場合によってはマイクロコントローラに既にインストールされている）がＯＥＭ１６０に提供される。ＯＥＭは、一般に、ＯＥＭ１６０によって製造されている幾つかの電子デバイス１００にインストールするために、そのようなセキュリティモジュールのバッチを購入することができる。

【００７７】

ＯＥＭ１６０は、認証局１４０のサーバシステム１３０と安全に通信することができるコンピューティング装置１２０にアクセスすることができる。参照を容易にするために、ＯＥＭによって操作されるコンピューティング装置１２０は、以下では「鍵管理サーバ」と呼ばれる。「鍵管理サーバ」という用語は単数形で使用されているが、当業者であれば分かるように、コンピューティング装置１２０の機能は複数のコンピューティングデバイス間で共有されてもよく、したがって「鍵管理サーバ」は、所望の機能を有する複数のコンピューティングデバイス（１つ以上のサーバ／コンピューティングデバイスを含む鍵管理サーバシステム）も指すと理解されるべきである。

【００７８】

以下でＫＭＳ１２０と呼ばれる鍵管理サーバ１２０は、状況によっては、ＯＥＭ１６０が直接対話することができるサーバではあるが、認証局サーバシステム１３０の別の認証局サーバと考えることができる。特に、ＫＭＳ１２０は、認証局サーバシステム１３０と安全に通信することができ、そのため、認証局１４０によってＯＥＭの使用について認証され得る。

【００７９】

鍵管理サーバ１２０は、オンプレミス動作のためにＯＥＭ１６０に提供される物理サーバを備えることができる。例えば、ＯＥＭ１６０は、認証局１４０から物理ＫＭＳ１２０を取得するように構成され得る。認証局１４０は、ＯＥＭ１６０に提供されるべき特定のＫＭＳインスタンスを識別するためのＫＭＳ識別子を生成及び記録することができる。認証局１４０は、ＫＭＳ１２０内部のハードウェアセキュリティモジュール（ＨＳＭ）でＫＭＳ公開鍵対を生成し、ＫＭＳ公開鍵対のＫＭＳ公開鍵を抽出し、ＫＭＳ識別子をＫＭＳ公開鍵と関連付けるためにＳＡＫを使用して証明書に署名し、証明書をＫＭＳソフトウェアに埋め込むことができる。また、認証局１４０は、ＫＭＳが認証局サーバシステム１３０の認証局サーバと接続できるようにするＵＲＬと共に、ＰＡＫを認証局１４０と関連付けるルート証明書をＫＭＳ１２０に埋め込むこともできる。その後、物理的ＫＭＳ１２０は、ＯＥＭ１６０に物理的に転送されてもよい。その後、ＫＭＳ１２０は、サーバシステム１３０とのセキュア通信（例えば、ＴＬＳ通信）を開始することができる。サーバシステム１３０は、ＳＡＫによって署名されたＴＬＳ証明書及びチェーンを提示してＴＬＳサーバ認証を実行することによって認証することができる。そして、ＫＭＳ１２０は、ＰＡＫと認証局１４０とを関連付けるハードコードされたルート証明書を使用して証明書を検証することができる。ＫＭＳ１２０は、その証明書（認証局１４０がＳＡＫを用いて署名したもの）を提示してＴＬＳクライアント認証を実行することによって、認証局サーバに対して認証を行なうことができる。認証局１４０は、ＫＭＳにインストールされた証明書に署名するために使用されるＳＡＫに対応するルート公開鍵（ＰＡＫ）を使用して、証明書を介して署名を検証することができる。当業者であれば分かるように、ＫＭＳ１２０を認証するために使用される公開認証局鍵は、セキュリティモジュール１１０にインストールされた公開認証局鍵と同じであっても異なっていてもよい。

【００８０】

オンプレミス動作のためにＯＥＭ１６０に提供される特注の物理サーバとは対照的に、鍵管理サーバ１２０は、ＯＥＭ１６０によって動作されるが認証局１４０のサーバシステ

ム１３０と通信するために設けられたセキュアゲートウェイのための特注のソフトウェアを有するコンピューティング装置１２０を備えることができる。特注のソフトウェアは、展開を容易にするために非依存的であり、ＯＥＭ１６０によって容易にインストール及び操作することができる。特注のソフトウェアは、それがサーバシステム１３０に対して認証することができる機構（公開鍵）を含む。

【００８１】

鍵管理サーバ１２０は、他の電子デバイス１００とも通信可能である。このようにして、１つ以上の電子デバイス１００を登録することができる。ＫＭＳ１２０は、電子デバイス１００へのファームウェアの安全なインストールを容易にするために使用されてもよい。以下で更に説明するように、ＫＭＳ１２０を使用して、デバイス識別子を特定の電子デバイス１００と関連付けることができる。ＫＭＳ１２０は、証明書に署名するために使用され得る。

【００８２】

ＯＥＭ１６０は、ＫＭＳ１２０を使用して、受信した１つ以上のセキュリティモジュールを登録することができる。具体的には、ＫＭＳ１２０は、電子デバイスのセキュリティモジュール１１０と通信してデバイス識別子を抽出することができ、デバイス識別子はＥＰＫの関数を含む。ＫＭＳ１２０は、ＫＭＳインスタンス１２０とデバイス識別子との間の関連付けを信頼できる機関１４０に登録するために、認証局サーバシステム１３０とのセキュア通信チャネルを開くことができる。認証局１４０は、ローカルデータベースを更新し、デバイス識別子を正常に登録したことをＫＭＳ１２０に通知することができ、そのデバイス識別子に関連付けられた電子デバイスと通信するための特定の許可をＫＭＳ１２０に付与することができる。

【００８３】

ＯＥＭ１６０は、ＫＭＳ１２０を使用して、電子デバイスにファームウェアを安全に提供することができる。ＯＥＭのファームウェアは、任意の適切な安全な方法を使用して電子デバイスにインストールすることができる。例えば、ＯＥＭ１６０は、電子デバイス１００にインストールされるファームウェアを設計することができる。ＫＭＳ１２０は、認証局サーバシステム１３０とのセキュア通信チャネルを開き、ファームウェア又はそのハッシュを、秘密認証局鍵ＳＡＫで署名するために認証局１４０に送信することができ、その相手方（ＰＡＫ）は電子デバイス１００にインストールされる。ＫＭＳ１２０は、ＰＵＦベースのファームウェア公開鍵（ＦＰＫ）によるファームウェア及び認証局の署名を更に暗号化することができ、その相手方は、電子デバイスで動的に生成可能である。したがって、電子デバイスは、対応するファームウェア秘密鍵を使用してファームウェアを復号し、ファームウェアが認証局１４０によってメモリに記憶されたＰＡＫを使用して署名されていることを検証することができる。このようにして、ＯＥＭは、電子デバイス１００にファームウェアを安全に提供することができる。

【００８４】

ファームウェアは、電子デバイスのハードウェアを制御するための低レベル命令を含むことができる。

【００８５】

ファームウェアは、以下で更に説明する方法に従ってデバイスを登録するための１つ以上のルート証明書を含み得る。特に、ファームウェアは、プライマリトラステッドルート証明書（「ＯＥＭ＿ＲＯＯＴ」、図６Ｃ）を含み得る。

【００８６】

ファームウェアはＫＭＳ１２０の識別子を含み、該識別子を用いて電子デバイスのデバイス識別子が登録され。例えば、識別子はユニフォーム・リソース・ロケータ（ＵＲＬ）を含むことができ、このＵＲＬにより電子デバイスがＫＭＳ１２０に通信するようになっている。ファームウェアは、ＵＲＬによって識別されるコンピューティング装置／サーバとのＴＬＳ接続などのセキュア接続を開始するための命令を含むことができる。

【００８７】

ファームウェアは、電子デバイスが受信した証明書を解釈できるように、証明書命名構造の詳細を含み得る。ファームウェアは、証明書署名要求（ＣＳＲ）を確立するための詳細を更に含み得る。証明書署名要求は、通常、証明書が発行されるべき公開鍵、識別情報（デバイス識別子など）、及び完全性保護（例えば、デジタル署名）を含む。

【００８８】

また、ＫＭＳ１２０は、ＩｏＴハブ１７０に接続するために必要な情報を電子デバイスに安全に提供するために使用されてもよい。例えば、ＫＭＳ１２０は、ＩｏＴハブと直接又はサーバシステム１３０を介して通信して、登録された各電子デバイス１００のデバイス証明書をＩｏＴハブに提供するように構成されてもよい。ＫＭＳ１２０は、デバイスがＩｏＴハブ１７０と通信でいるようにするために、ＩｏＴルート証明書及びＩｏＴエンドポイントを電子デバイス１００に提供するように構成されてもよい。

【００８９】

したがって、電子デバイス１００は、ＩｏＴハブ１７０と通信するために必要な全ての情報と共に展開されてもよい。

【００９０】

図２は、図１に存在するハードウェアデバイスの多くを含む通信システムをより一般的に示す。図２は、特に、通信ネットワーク２００、セキュリティモジュール１１０を有する例示的な電子デバイス１００、例えばＯＥＭ１６０によって操作され得る鍵管理サーバ１２０、認証局サーバシステム１３０、及び例えばＩｏＴハブ１７０によって操作され得るコンピューティングデバイス２２０を示す。通信ネットワーク２００は、インターネットなどの任意の適切な通信ネットワークであってもよい。幾つかの例では、ネットワーク２００が広域ネットワーク（ＷＡＮ）を備えてもよい。

【００９１】

電子デバイス１００は、任意の適切な形態をとることができ、本明細書に記載の方法を実行するための任意の適切なコンピューティング装置を備えることができる。例えば、電子デバイスは、パーソナルコンピュータ、サーバ、ラップトップコンピュータ、又は他のそのような機械など、処理及び記憶が可能な任意のコンピューティングデバイスであってもよい。電子デバイス１００は、ＩｏＴデバイスを備えることができる。電子デバイスは、より大きなデバイスに設置するためのマイクロコントローラユニット（ＭＣＵ）を備えることができる。電子デバイス１００は、直接に又はネットワーク２００を介して他のデバイスと通信することができる。例えば、電子デバイス１００は、物理的接続又はネットワーク２００を介してＫＭＳ１２０と通信することができる。電子デバイス１００が展開されると、デバイス１００は、ネットワーク２００を介してコンピューティングデバイス２２０と通信することができる。電子デバイスは、セキュア接続、例えばＴＬＳ接続を介してＫＭＳ１２０及び／又はコンピューティングデバイス２２０と通信することができる。

【００９２】

ＫＭＳ１２０は、以下で更に説明するコンピューティング装置５００などの任意の適切なコンピューティング装置を備えることができる。ＫＭＳ１２０は、サーバのクラスタ又は単一のデバイスを備えることができる。ＫＭＳ１２０の機能は、分散データ処理環境、単一のデータ処理デバイスなどを含む多くの異なるタイプのデータ処理環境で利用することができる。

【００９３】

ＫＭＳ１２０は、ネットワーク２００を介して認証局サーバシステム１３０とセキュア接続を確立することができ、また、ネットワーク２００を介して、又は場合によっては有線接続などの直接接続を介して電子デバイス１００と通信することもできる。ＫＭＳ１２０は、電子デバイス１００のセキュリティモジュール１１０を識別するデバイス識別子及び電子デバイス１００のＥＰＫなどの１つ以上の公開鍵などの、電子デバイス１００に関する情報を記憶するように構成される。これに加えて又は代えて、ＫＭＳ１２０は、そのような情報を取得するために、認証局サーバシステム１３０のデータベース２１０と通信

するように構成されてもよい。ＫＭＳ１２０は、証明書に署名するように更に構成される。

【００９４】

認証局サーバシステム１３０は、１つ以上のサーバを備え、データベース２１０を含む。認証局サーバシステム１３０の１つ以上の認証局サーバは、例えばＫＭＳ１２０が認証局１４０によって信頼されていることを証明するために、又は電子デバイス１００にインストールするためにファームウェアに署名するために、認証局１４０に代わって証明書に署名するように構成される。データベース２１０は、電子デバイス１００を識別するデバイス識別子、幾つかの例では電子デバイス１００のファームウェア公開鍵など、電子デバイス１００に関する情報を記憶するように構成される。データベース２１０は、ＫＭＳ１２０に関する情報を記憶するように更に構成され得る。例えば、データベース２１０は、デバイス識別子のバッチを特定のＫＭＳ１２０と関連付ける情報を含むことができ、それが関連付けられるデバイス識別子のみと対話することをＫＭＳ１２０に許可するために使用され得る。

【００９５】

コンピューティングデバイス２２０は、多くの接続されたデバイス（例えば、分散型コンピューティング環境内）又は単一のコンピューティングデバイスを備えることができる。

【００９６】

図３Ａは、一例に係る電子デバイス１００のブロック図を示す。例えば、電子デバイス１００はＩｏＴデバイスであってもよい。当業者により理解されるように、図３Ａに示すものに対する他のアーキテクチャが使用されてもよい。

【００９７】

図を参照すると、電子デバイス１００は、セキュリティモジュール１１０と、１つ以上のＣＰＵ／プロセッサ３０２と、１つ以上のメモリ３０４と、センサモジュール３０６と、通信モジュール３０８と、ポート３１０と、電源３１２とを含む。構成要素３０２，３０４，３０６，３０８，３１０，３１２のそれぞれは、様々なバスを使用して相互接続される。ＣＰＵ３０２は、通信モジュール３０８を介して又はポート３１０を介して受信された、メモリ３０４に記憶された命令を含む、電子デバイス１００内で実行するための命令を処理することができる。

【００９８】

メモリ３０４は、電子デバイス１００内にデータを記憶するためのものである。１つ以上のメモリ３０４は、揮発性メモリユニットを含んでもよい。１つ以上のメモリは、１つ以上の不揮発性メモリユニットを含むことができる。また、１つ以上のメモリ３０４は、磁気又は光ディスクなどのコンピュータ可読媒体の別の形態であってもよい。１つ以上のメモリ３０４は、電子デバイス１００に大容量ストレージをもたらしてもよい。本明細書に記載の方法を実行するための命令は、１つ以上のメモリ３０４内に記憶することができる。

【００９９】

通信モジュール３０８は、プロセッサ３０２と他のシステムとの間で通信を送受信するのに適している。例えば、通信モジュール３０８は、インターネットなどの通信ネットワーク２００を介して通信を送受信するために使用され得る。通信モジュール３０８は、ＷｉＦｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＮＦＣなどの幾つかのプロトコルのいずれかによって電子デバイス１００が他のデバイス／サーバと通信できるようにしてもよい。

【０１００】

ポート３１０は、例えば、プロセッサ３０２によって処理されるべき命令を含む非一時的コンピュータ可読媒体を受信するのに適している。ポート３１０は、例えば、電子デバイス１００と鍵管理サーバ１２０との間の有線通信に使用することができる。

【０１０１】

センサモジュール３０６は、温度、湿度、又は任意の他のパラメータなどの検知パラメータのための１つ以上のセンサを備えることができる。

【０１０２】

プロセッサ３０２は、例えばセンサモジュール３０６、セキュリティモジュール１１０、又は通信モジュール３０８からデータを受信するように構成される。プロセッサ３０２は、メモリ３０４にアクセスし、前記メモリ３０４から、通信モジュール３０８から、又はポート３１０に接続されたコンピュータ可読記憶媒体から受信した命令及び／又は情報に基づいて動作するように更に構成される。

【０１０３】

図３Ｂは、より大きな電子デバイス内に設置され得る電子デバイス１００の別の例、すなわちマイクロコントローラユニット（ＭＣＵ）３１５のアーキテクチャを示す。当業者であれば分かるように、他のＭＣＵアーキテクチャが使用され得る。

【０１０４】

図３ＢのＭＣＵ３１５は、ＣＰＵ３２０と、ユーザメモリ３２２と、ブートランダムアクセスメモリ３２８とを備える。ＣＰＵ３２０、ブートＲＯＭ３２８、及びユーザメモリ３２２は、コードバス３２４を介して通信することができる。ＣＰＵ３２０、ブートＲＯＭ３２８、及びユーザメモリ３２２は、システムバス３２６に接続されてもよく、システムバスは、複数の周辺機器Ａ、Ｂ、及びＣ（３３０，３３２，３３４）並びにセキュリティモジュール１１０に接続されてもよい。ＭＣＵ３１５には、セキュリティに関する構成要素のみが示されている。当業者であれば分かるように、ＭＣＵ３１５がより多くの又はより少ない構成要素を有することができる。例えば、ＭＣＵ３１５は、より多くの周辺機器及びシステム構成要素を有することができる。

【０１０５】

図４Ａは、一例に係るセキュリティモジュール１１０のブロック図を示す。セキュリティモジュール１１０は、内部のセキュアな構成要素を電子デバイス１００の他の構成要素から分離する信頼ゾーンと考えることができる。セキュリティモジュール１１０は、ＰＵＦモジュール４０２、暗号化アクセラレータ４０４、及びセキュアメモリ４０６を備える。当業者であれば分かるように、他のアーキテクチャも想定し得る。セキュリティモジュール１１０は、電子デバイス１００のシステムバスに接続される。

【０１０６】

ＰＵＦモジュール４１０は、ＰＵＦと、ＰＵＦと相互作用するのに必要な任意の回路とを備える。特に、ＰＵＦモジュールは、暗号化アクセラレータ４０４から信号を受信し、適切な応答を提供することができる。暗号化アクセラレータ４０４は、暗号化動作を実行し、ＰＵＦモジュール４０２及びセキュアメモリ４０６と相互作用するための専用処理ユニットを備える。

【０１０７】

セキュアメモリは、ＰＵＦモジュール４０２によって生成された鍵及び／又はルート証明書などの秘密情報を記憶するように構成される。ＰＵＦモジュール４０２、セキュリティモジュール１１０内のセキュリティ周辺機器、及びセキュアメモリを制御するためにＣＰＵ３２０によって必要とされる命令は、システムの不変ブートプロセスの一部であるブートＲＯＭ３２８内に含まれる。

【０１０８】

図４Ｂは、一例に係るＰＵＦモジュール４０２の機能的な構成要素を示す。ＰＵＦモジュール４０２は、ＰＵＦ４５０と、アナログフロントエンド（ＡＦＥ）４５２と、後処理エンジン４５４と、ＲＩＳＣ－Ｖコア４５６とを備える。

【０１０９】

当業者であれば分かるようには、ＰＵＦ４５０が任意の適切なＰＵＦであり得る。

【０１１０】

アナログフロントエンド（ＡＦＥ）４５２は、ＰＵＦと相互作用するためのアナログ信号調整回路を備える。例えば、ＡＦＥは、生の「フィンガープリント」を確立するために

ＰＵＦ４５０と相互作用することができる。後処理エンジン４５４は、ＡＦＥ４５２の出力を補正し、ＡＦＥの出力を更に処理することによって更なるプライバシー強化を提供するように構成される。ＲＩＳＣ－Ｖコア４５６は、ＰＵＦ４５０からのデータの後処理、例えばデータの誤り訂正を行なうＣＰＵコアである。ＲＩＳＣ－Ｖコアは、ＰＵＦモジュール４０２を外部マイクロコントローラに容易に接続することを可能にするインターフェースを提供するが、他のＣＰＵを利用してもよい。

【０１１１】

図５は、コンピューティング装置５００のブロック図である。例えば、コンピューティング装置５００は、コンピューティングデバイス、サーバ、モバイル又はポータブルコンピュータ又は電話などを備えることができる。コンピューティング装置５００は、複数の接続された装置にわたって分散されてもよい。コンピューティング装置５００は、鍵管理サーバ１２０、認証局サーバシステム１３０の認証局サーバ、又は例えばＩｏＴハブで使用するためのサーバ２２０としての使用に適し得る。当業者により理解されるように、図５に示すものに対する他のアーキテクチャが使用されてもよい。

【０１１２】

図を参照すると、コンピューティング装置５００は、１つ以上のプロセッサ５１０と、１つ以上のメモリ５２０と、ビジュアルディスプレイ５３０及び仮想又は物理キーボード５４０などの幾つかの任意選択のユーザインターフェースと、通信モジュール５５０と、任意選択的にポート５６０と、任意選択的に電源５７０とを含む。構成要素５１０，５２０，５３０，５４０，５５０，５６０及び５７０のそれぞれは、様々なバスを使用して相互接続される。プロセッサ５１０は、通信モジュール５５０を介して、又はポート５６０を介して受信された、メモリ５２０に記憶された命令を含む、計算装置５００内で実行するための命令を処理することができる。

【０１１３】

メモリ５２０は、コンピューティング装置５００内にデータを記憶するためのものである。１つ以上のメモリ５２０は、揮発性メモリユニットを含んでもよい。１つ以上のメモリは、１つ以上の不揮発性メモリユニットを含むことができる。また、１つ以上のメモリ５２０は、磁気又は光ディスクなどのコンピュータ可読媒体の別の形態であってもよい。１つ以上のメモリ５２０は、コンピューティング装置５００に大容量ストレージをもたらすことができる。本明細書に記載の方法を実行するための命令は、１つ以上のメモリ５２０内に記憶することができる。

【０１１４】

装置５００は、ビジュアルディスプレイ５３０などの視覚化手段と、キーボード５４０などの仮想又は専用のユーザ入力デバイスとを含む幾つかのユーザインターフェースを含む。

【０１１５】

通信モジュール５５０は、プロセッサ５１０と遠隔システムとの間で通信を送受信するのに適している。例えば、通信モジュール５５０は、インターネットなどの通信ネットワーク２００を介して通信を送受信するために使用され得る。

【０１１６】

ポート５６０は、例えば、プロセッサ５１０によって処理される命令を含む非一時的コンピュータ可読媒体を受け付けるのに適している。

【０１１７】

プロセッサ５１０は、データを受信し、メモリ５２０にアクセスし、通信モジュール５５０から又はユーザ入力装置５４０から前記メモリ５２０又はポート５６０に接続されたコンピュータ可読記憶媒体のいずれかから受信した命令に基づいて動作するように構成される。

【０１１８】

コンピューティング装置５００は、暗号鍵を安全に記憶するために、図５には示されていないハードウェアセキュリティモジュール（ＨＳＭ）を更に備えることができる。例え

ば、鍵管理サーバ１２０として使用されるコンピューティング装置５００の場合、ＨＳＭは、証明書に署名するための１つ以上の秘密鍵、又はファームウェアを暗号化／復号するためのサーバ暗号化鍵及びサーバ復号鍵を記憶する必要があり得る。例えば、認証局サーバシステム１３０の認証局サーバとして使用されるコンピューティング装置５００の場合、ＨＳＭは、認証局鍵対の秘密認証局鍵（ＳＡＫ）などの１つ以上の秘密鍵を記憶する必要があり得る。当業者であれば分かるように、ＨＳＭが秘密鍵を記憶する必要はなく、他のセキュリティ構成が適用可能であり得る。例えば、コンピューティング装置はクラウドベースのＨＳＭにアクセスすることができる。

【０１１９】

ファームウェアは、電子デバイス１００に安全に提供され得る。ファームウェアは、例えば、認証局サーバシステム１３０でファームウェアに署名し、ＫＭＳ１２０で署名の前又は後のいずれかにファームウェアを暗号化し、次いで、署名された暗号化ファームウェアを電子デバイス１００にプログラムされるようにプログラミングハウス１８０に送信することによって、安全に提供され得る。

【０１２０】

ファームウェアは、電子デバイスが登録されているＫＭＳ１２０の識別子と、信頼チェーンを構築するための１つ以上のルート証明書とを含み得る。ファームウェアが電子デバイス１００に安全に提供された後、電子デバイス１００は登録を開始することができる。

【０１２１】

図７～図９に関連して、電子デバイス１００に一時的登録デバイス証明書を提供する方法を説明する。更に、図１０～図１２に関連して、電子デバイスにデバイス証明書（例えばＩｏＴハブと接続するために展開された時点で使用することができる）を提供する方法が説明される。デバイス証明書の信頼を確立するために、電子デバイスには、ＯＥＭ用の１つ以上のルート証明書が提供される必要がある。

【０１２２】

１つ以上のルート証明書は、製造時点で電子デバイス１００にインストールされてもよく、セキュリティを追加するために、登録前に安全にインストールされたファームウェアと共に又はその一部として電子デバイス１００に提供されてもよい。

【０１２３】

図６Ａは、公開鍵インフラストラクチャによって提供される信頼チェーンの一例を示す。公開鍵インフラストラクチャは、メッセージのソースを検証するために使用できる証明書の階層（１００２，１０１２，１０２４）によって表わされる。各証明書は、対応するエンティティが保持するプライベート鍵に対応する公開鍵を含む。証明書は、鍵に関する情報、その所有者（対象と呼ばれる）の身元に関する情報、及び証明書の内容を検証したエンティティ（発行者と呼ばれる）のデジタル署名を含む。信頼チェーンにおける信頼は、最終的に、ルート証明書１００２に関連付けられたルート認証局（ＣＡ）から得られる。ルート証明書１００２は、一般に、ルート認証局の識別子／識別名（１００４）、ルート認証局の公開鍵１００６、及びルート認証局の署名（１０１０）を含み、署名はルート公開鍵１００６に対応する秘密鍵１００８を使用して署名される。

【０１２４】

認証局は、ツリー構造の形態で複数の証明書を発行することができる。ルート証明書１００２は、ツリーの最上位の証明書であり、そのプライベート鍵１００８は下位の証明書に署名するために使用される。図６Ａに示されるように、ルート秘密鍵１００８は、中間／下位証明書１０１２に署名するために使用することができる。中間証明書１０１２は、仲介者／発行者の識別子／識別名１０１４、仲介者の公開鍵１０２０、ルート認証局１０１８の識別情報、及びルート認証局の署名１０１６を含む。中間証明書１０１２の正確性は、ルート認証局１０１８の識別子から、ルート公開鍵１００６を見つけることができる適切なルート証明書１００２を決定することによって照合され得る。ルート公開鍵１００６は、中間証明書１０１２に署名するために使用されるルート秘密鍵１００８に対応するので、ルート公開鍵１００６は、中間証明書１０１２のルート署名１０１６を復号するた

めに使用することができ、更に照合を行うことができる。中間証明書は、中間証明書１０１２に関連付けられた発行者／仲介者が更なる証明書に署名することを許可されているかどうかなどの更なる情報を含むことができる。中間体が、発行者公開鍵１０２０に関連する発行者秘密鍵１０２２を使用して下位証明書に署名することを許可されている場合、発行者秘密鍵１０２２を使用して署名された証明書の信頼は、最終的に、ルート証明書１００２に関連するルート認証局に由来する信頼チェーンから導出することができる。

【０１２５】

図６Ａの発行者秘密鍵１０２２は、電子デバイスに関連付けられた最終証明書１０２４に署名するために使用される。一般に、最終証明書は、最終証明書が関連付けられている当事者が信頼チェーンにおける更なる証明書に署名する権利がないことを示す。最終デバイス証明書１０２４は、証明書１０２４が発行される電子デバイスの識別子１０２６、エンド証明書１０１２を証明した発行者の識別子、電子デバイスに対応する公開鍵１０３２、発行者の署名１０２８、及び発行者によって証明された任意の更なる情報／メタデータ１０３６を含む。したがって、最終証明書１０２４は、公開鍵１０３２が、ルート認証局に由来する信頼チェーンで、最終デバイス証明書１０２４によって識別されるエンティティ（１０２６）と関連付けられることを証明する。電子デバイス公開鍵１０３２は電子デバイス秘密鍵１０３４と関連付けられる。

【０１２６】

図６Ａには３つの証明書が示されるが、当然ながら、チェーンが幾つかの中間証明書により更に長くてもよい。

【０１２７】

証明書チェーンの証明書は、更なる情報を含み得る。例えば、証明書は、バージョン番号、シリアル番号、署名アルゴリズムＩＤ、使用された公開鍵アルゴリズムに関する情報などを含み得る。証明書は有効期間を含むことができる。公開鍵証明書には幾つかの既知の標準フォーマットがあり、最も一般的に使用されているのはＸ．５０９である。Ｘ．５０９証明書は、ＴＬＳ／ＳＳＬを含む多くのプロトコルで使用され、本明細書に記載の方法で使用され得る。

【０１２８】

従来、ＯＥＭがデバイスを製造する場合、それらは、暗号化されていない形式でその電子デバイスに秘密情報が注入されることに依存している。例えば、秘密鍵がデバイスに注入される必要があり得る。更に、更なる証明書情報、例えば最終証明書１０２４も一般にデバイスに提供される。製造業者がデバイスに秘密鍵及び最終証明書１０２４を提供する場合、幾つかの欠点がある。第１に、ＯＥＭ又はＩｏＴハブなどの下流側の当事者は、秘密鍵がデバイスに安全に提供されており、それが他の当事者に知られていないことを信頼する必要がある。第２に、ＯＥＭなどの下流側の当事者は、製造業者の信頼に基づいて信頼チェーンを信頼しなければならない場合があり、これは、例えばファームウェア更新を扱うときにセキュリティ上の結果をもたらす可能性がある。或いは、製造中に一時的登録証明書がデバイスに提供されてもよい。一時的登録証明書は、デバイスに注入された秘密鍵に関連付けられた公開鍵を含み、それによってデバイスをその公開鍵に関連付け、サービスに登録するための有限の有効期間を含むことができる。しかしながら、一時的登録デバイス証明書及び関連する秘密鍵の提供は、一般に、セキュア設備を必要とする。

【０１２９】

対照的に、ここで異なるアプローチを説明する。特に、図７～図９及び添付の本文は、電子デバイスに一時的登録デバイス証明書を提供するための例示的な方法を説明しており、図１０～図１２及び添付の本文は、展開の準備ができた電子デバイスに最終デバイス証明書を提供するための例示的な方法を説明している。記載された例では、ＯＥＭ１６０は、展開された電子デバイスの信頼の基礎となる最終的な認証局がＯＥＭであることを確実にすることができる。

【０１３０】

図６Ｂ、図６Ｃ及び図６Ｄは、本明細書に記載の例で使用可能な３つの証明書チェーン

を示す。例示のみを目的として図１を参照すると、ルート証明書１０３８、１０４４、及び１０５８は全て、ＯＥＭ１６０と関連付けられ得る。すなわち、ＯＥＭ１６０は、ルート証明書１０３８、１０４４、１０５８と関連付けられたルート認証局であり得る。本明細書では３つの証明書チェーンが説明されているが、他のシナリオも想定され、例えば、単一のルート証明書が他の全ての証明書の元になるルート証明書であってもよい。ＯＥＭによって製造された電子デバイス１００には、適切なルート証明書をプロビジョニングすることができ、そこから信頼チェーンを構築して、電子デバイス１００がデバイスに提供される任意のソフトウェア又は通信を確実にすることができるようにすることができる。

【０１３１】

説明を簡単にするために、図６Ｂ～図６Ｄの証明書チェーンは、図１の当事者を参照して説明されており、ＯＥＭ１６０は、３つ全てのチェーンのルート証明書に関連付けられた認証局である。しかしながら、当業者であれば分かるように、他のシナリオも適用可能である。

【０１３２】

図６Ｂは、一例に係る証明書チェーンを示す。図６Ｂの証明書チェーンは、使用時に以下で更に説明される。図６Ｂでは、一時的登録トラステッドルート証明書１０３８（「ＴＥ＿ＯＥＭ＿Ｒｏｏｔ」とラベル付けされている）は、ＯＥＭ１６０にのみ知られている適切な秘密鍵を使用して自己署名される。一時的登録発行証明書１０４０（「ＴＥ＿ＯＥＭ＿ＩＣ」とラベル付けされている）は、ルート証明書１０３８によって認証される。すなわち、一時的登録トラステッドルート証明書１０３８で識別された公開鍵と関連付けられた秘密鍵を使用して、一時的登録発行証明書１０４０に署名する。一時的登録デバイス証明書１０４２（「ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ」とラベル付けされている）は、一時的登録発行証明書１０４０によって認証される。すなわち、一時的登録発行証明書１０４０で特定された公開鍵に対応付けられた秘密鍵を用いて、一時的登録デバイス証明書１０４２に署名する。

【０１３３】

図７に関連して説明するように、ＯＥＭ１６０は、一時的登録トラステッドルート証明書１０３８が関連付けられる認証局であってもよく、ＯＥＭ又は（ＯＥＭが所有する）ＫＭＳ１２０は、関連する秘密鍵を所有する。一時的登録発行証明書１０４０と関連付けられた秘密鍵は、ＫＭＳ１２０が所持していてもよい。ＯＥＭの一時的登録（ＴＥ）ＰＫＩは、一時的登録デバイス証明書を発行するために使用され、これにより、電子デバイスが登録プロトコル中にＫＭＳに対して認証できるようにする。これらの証明書は他の目的に使用されるべきではないため、一時的登録トラステッドルート証明書１０３８及び一時的登録発行証明書１０４０はＫＭＳを離れる必要はない。

【０１３４】

図６Ｃは、一例に係る証明書チェーンを示す。図６Ｃの証明書チェーンは、使用時に以下で更に説明される。図６Ｃでは、プライマリトラステッドルート証明書１０４４（「ＯＥＭ＿ＲＯＯＴ」とラベル付けされている）は、適切な秘密鍵を使用して自己署名される。図６Ｃには、３つの中間証明書１０４６、１０５０、１０５４が示される。

【０１３５】

ＯＥＭのプライマリＰＫＩのトラストアンカーは、自己署名されたプライマリトラステッドルート証明書１０３８であり、登録中にＫＭＳ１２０から外部で使用される全ての証明書を発行するために使用される。プライマリトラステッドルート証明書１０３８の下には、ある数の発行証明書がある。

【０１３６】

セキュア接続発行証明書１０５４は、プライマリトラステッドルート証明書１０４４に関連付けられたルート秘密鍵によって署名される。以下に説明する例では、セキュア接続自体がＴＬＳ接続であるため、図６Ｃではセキュア接続発行証明書１０５４が「ＩＣ＿ＴＬＳ」とラベル付けされる。セキュア接続発行証明書１０５４と関連付けられた発行者秘密鍵は、セキュア接続証明書１０５６（「ＫＭＳ＿ＴＬＳ＿Ｃｅｒｔ」とラベル付けされ

る）に署名するために使用される。以下に説明する例では、セキュア接続証明書１０５６は、ＴＬＳサーバ認証中に電子デバイス１００を認証するためにＫＭＳ１２０によって使用される。

【０１３７】

図６Ｃは、プライマリトラステッドルート証明書１０４４から派生した２つの更なる中間証明書１０４６、１０５０を示す。中間証明書１０４６、１０５０（それぞれ「ＩＣ＿Ａ」及び「ＩＣ＿Ｂ」とラベル付けされている）は、デバイス固有のポリシーと関連付けられた派生デバイス証明書を認証するために使用される。例えば、ＩＣ＿Ａ１０４６は、第１のクラスのＩｏＴデバイスのセキュリティポリシーに基づいて、第１のクラスのＩｏＴデバイス（例えば、焙煎器）のデバイス証明書を認証するために使用されてもよく、ＩＣ＿Ｂ１０５０は、第２のクラスのＩｏＴデバイスのセキュリティポリシーに基づいて、第２のクラスのＩｏＴデバイス（例えば、電球）のデバイス証明書を認証するために使用されてもよい。これは、どの発行証明書が署名に使用されたかを確認することによって、証明書から所与のタイプのデバイスを識別できるため、セキュリティポリシーを実施するのに有用であり得る。

【０１３８】

中間証明書ＩＣ＿Ａ及びＩＣ＿Ｂによって署名されたデバイスの最終証明書も図６Ｃに示されている（それぞれ「Ｄｅｖ＿Ｃｅｒｔ＿Ａ」１０４８及び「Ｄｅｖ＿Ｃｅｒｔ＿Ｂ」１０５２とラベル付けされている）。以下の例に見られるように、デバイス証明書１０４８は、そのＩｏＴハブ１７０に対して認証するために電子デバイス１００によって使用され得る。

【０１３９】

当業者であれば分かるように、デバイス証明書を発行するための２つの中間証明書１０４６、１０５０が図６Ｃに示されているが、より多くの又はより少ない中間発行証明書がプライマリトラステッドルート証明書１０４４から派生し得る。

【０１４０】

図６Ｄは、一例に係る証明書チェーンを示す。図６Ｄでは、ファームウェアルート証明書１０５８（「ＯＥＭ＿Ｆｉｒｍｗａｒｅ」とラベル付けされる）が認証局によって自己署名される。そのルート証明書からファームウェア署名証明書１０６０（「Ｆｉｒｍ＿ＳＣ」とラベル付けされている）が派生する。

【０１４１】

ファームウェア署名証明書１０６０は、電子デバイス１００に導入されるファームウェアに署名するために使用され得る。ファームウェア署名ＰＫＩは、プライマリ登録及び一時的登録ＰＫＩとは別個のルートを有する。これは、ＯＥＭ１６０がファームウェア署名証明書を使用して任意のメッセージ、証明書などに署名することができ、このＰＫＩを別々に保つことにより、ファームウェアＰＫＩを使用して（偶然又は悪意を持って）登録のセキュリティを損なうものに署名することができないことが保証されるためである。

【０１４２】

当業者であれば分かるように、図６Ｂ、図６Ｃ及び図６ＤのＰＫＩの上記の説明で使用された証明書の名前は、３つのＰＫＩのみを区別するために使用されている。

【０１４３】

電子デバイス１００又はＫＭＳ１２０が証明書を検証するときはいつでも、できるだけ多くの有用な属性（例えば、対象名、使用制限、発行当事者の名前など）を照合する必要がある。電子デバイスがこれを行うことができるようにするために、それらのファームウェアは、ＫＭＳ１２０の識別子及び異なる証明書に期待する命名構造など、これらの照合を行うために必要な情報を含まなければならない。電子デバイスは、可能な場合、チェーン内の全ての署名を検証し、チェーン内の中間証明書が証明書を発行することを許可されていることを確認し（例えば、侵入されたデバイスがそのデバイス証明書を使用して証明書を発行しようとするのを防ぐために、）、全ての証明書が期限切れでないことを確認する（時間にアクセスできる場合）。

【０１４４】
図７は、一時的登録デバイス証明書１０４２を電子デバイス１００に提供するための例示的な方法を示す。
【０１４５】
電子デバイス１００は、ＰＵＦ４５０を有するセキュリティモジュール１１０を備え、セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む。一例では、セキュリティモジュールは、ＰＵＦ４５０に対する第１のチャレンジに基づいて登録公開鍵（ＥＰＫ）を確立し、ＰＵＦ４５０に対する第１のチャレンジへの応答に基づいて登録秘密鍵を確立するように構成されてもよい。
【０１４６】
この交換の目的は、電子デバイス１００が、そのＥＰＫについての一時的登録デバイス証明書１０４２を要求し、発行されることである。デバイスは、これを使用して、図１０に関連して以下で更に詳述される第２のハンドシェイクでＫＭＳ１２０を認証する。この例のＫＭＳ１２０は、所有するデバイス識別子（すなわち、登録されているデバイス識別子）に対応するＥＰＫ用の証明書のみを発行する。ＫＭＳ１２０はまた、最終的にその最終デバイス証明書（この例ではＤｅｖ＿Ｃｅｒｔ＿Ａ１０４８）を発行するために使用される発行証明書ＩＣ＿Ａ１０４６を電子デバイスに送信し、電子デバイス１００は、ＫＭＳ１２０によって発行された後続の証明書を検証するために記憶する。
【０１４７】
電子デバイス１００は、電子デバイス１００上のファームウェアにインストールされたＵＲＬによって識別されるＫＭＳ１２０へのＴＬＳ接続を開始する（１１０２）。ハンドシェイク中に、ＫＭＳ１２０は、ＫＭＳ＿ＴＬＳ＿Ｃｅｒｔ１０５６及びＴＬＳ発行証明書ＩＣ＿ＴＬＳ１０５４を提示することによってクライアントを認証し（１１０４で）、電子デバイス１００が（電子デバイス１００に以前にインストールされた）プライマリルート証明書１０４４からＴＬＳ証明書１０５６へのチェーンを構築でいるようにする。電子デバイス１００は、ＴＬＳ接続のための信頼チェーンを検証する（１１０６）。電子デバイス１００は、プライマリトラステッドルート証明書１０４４で始まる証明書チェーンのみを受け入れる。電子デバイス１００は、証明書１０５６の対象名がファームウェアに含まれるＫＭＳ識別子と同一であることを確認する。可能であれば、電子デバイス１００は、ＴＬＳ証明書１０５６がＴＬＳ発行証明書１０５４によって署名されていることを確認すべきである。認証が失敗した場合、デバイスは接続を終了する。クライアント認証が要求されると、デバイス１００は、適切な証明書を持っていないことを示し、ＫＭＳ１２０に対して認証しない。
【０１４８】
ＯＥＭの鍵のいずれも危険にさらされていないと仮定すると、このステップは、デバイスのファームウェア内のＫＭＳ識別子と関連付けられた実際のＫＭＳ１２０と通信していることを電子デバイス１００に証明する。電子デバイス１００は、ＴＬＳの対象名が予想されるものと一致することを確認する必要があり、そうでない場合、電子デバイス１００は、プライマリトラステッドルート証明書１０４４によって署名された任意の証明書からの接続を受け入れる脆弱性がある可能性があり、そのため、例えば、侵入されたデバイスと通信する可能性がある。同じ対象名で他の証明書が発行されないことを保証する必要があり、そうでなければ、この証明書を所有する当事者は、証明書を使用してＫＭＳ１２０を電子デバイス１００になりすますことができる。
【０１４９】
１１０６でＴＬＳ接続が検証された場合、電子デバイス１００とＫＭＳ１２０との間でセキュアなＴＬＳ通信チャネルが開かれる（１１０８）。
【０１５０】
電子デバイス１００は、１１１０において、証明書署名要求（ＣＳＲ）を作成する。公

開鍵インフラストラクチャ（ＰＫＩ）システムでは、ＣＳＲは、デジタル識別証明書を申請するために、申請者から公開鍵インフラストラクチャの登録局に送信されるメッセージである。これは、通常、証明書が発行されるべき公開鍵、識別情報（ＥＰＫに基づくドメイン名又はデバイス識別子など）、及び完全性保護（例えば、デジタル署名）を含む。ＣＳＲのための最も一般的なフォーマットは、ＰＫＣＳ＃１０仕様であり、もう１つは、署名付き公開鍵及びチャレンジＳＰＫＡＣフォーマットである。

【０１５１】

１１１０において、登録公開鍵ＥＰＫをデバイス識別子に関連付けるためのＣＳＲが作成される。更に前述したように、デバイス識別子はＥＰＫの関数ｆ（ＥＰＫ）であり、この説明の目的のために、デバイス識別子はＥＰＫのハッシュＨ（ＥＰＫ）を含む。したがって、ＣＳＲでは、公開鍵がＥＰＫとして識別され、対象名／識別名／識別子がＨ（ＥＰＫ）として識別される。今後、要求された証明書は、後続のＴＬＳハンドシェイク中にＫＭＳ１２０に対して認証するために電子デバイス１００によって使用される。ＣＳＲは、１１１２においてＫＭＳ１２０に送信される。

【０１５２】

ＣＳＲは、ＣＳＲに対する署名の形態の登録秘密鍵ＥＳＫの所有証明を含む。しかしながら、これは、必ずしも、ＴＬＳ接続の他端において電子デバイス１００によってＣＳＲが計算されたことをＫＭＳ１２０に証明しない。攻撃者が何らかの方法でデバイスによって計算された以前のＣＳＲを知ることができた場合（これらがＴＬＳ接続下で暗号化されて送信されるため、可能性は低い）、攻撃者はこれを別の接続でＫＭＳ１２０に再生することができる。しかしながら、攻撃者は、そのような攻撃を実行することができたとしても、対応するＥＰＫを知らないため、返された証明書を使用することができない。

【０１５３】

ＫＭＳ１２０は、ＣＳＲを受信すると、幾つかの照合を行う。

【０１５４】

ＫＭＳ１２０は、１１１４で、ＣＳＲの対象フィールドに提供されたデバイス識別子をデータベースと照合して、ＫＭＳ１２０がそのデバイス識別子に関連付けられた電子デバイス１００の証明書に署名することを許可されていること、言い換えれば、ＫＭＳ１２０がそのデバイス識別子を「所有」していることを検証する。適切なデータベースは、ＫＭＳ１２０上にローカルに保持されてもよく、又は認証局サーバシステム１３０への要求を介してアクセスされてもよい。

【０１５５】

ＫＭＳ１２０は、１１１６において、ＣＳＲの公開鍵フィールド内の登録公開鍵ＥＰＫが対象名フィールド内のデバイス識別子にハッシュすることを更に照合する。すなわち、ＫＭＳは、デバイス識別子ＤｅｖｉｃｅＩＤ＝Ｈ（ＥＰＫ）であることを検証する。

【０１５６】

１１１４及び１１１６における照合は、任意の順序で、又は同時に実行されてもよい。いずれかの照合に失敗した場合、ＫＭＳ１２０は、接続を終了する。成功した場合、ＫＭＳ１２０はＥＰＫをデバイス識別子に関連付ける－ＫＭＳ１２０はＥＰＫをデータベース内のデバイス識別子のエントリに追加する。

【０１５７】

ＣＳＲ内の公開鍵がデータベース内のデバイス識別子の１つに対応することを確認することは重要であり、そうでなければ、攻撃者は任意の鍵対の証明書を要求する可能性がある。この照合を課すことは、ＫＭＳ１２０が所有するデバイス識別子のいずれかにハッシュする公開鍵に対してのみ証明書を要求できることを意味する。攻撃者がＫＭＳ１２０に、デバイス識別子の根底にある実際のＥＰＫ以外の公開鍵に対する証明書を発行させることができる唯一の方法は、同じデバイス識別子にハッシュする異なるＥＰＫを見つけることができる場合である。これは、攻撃者がハッシュ関数において衝突を見つけることを必要とし、これは、定義により非常に困難なタスクである。

【０１５８】

全ての照合が完了すると、ＫＭＳ１２０は、（「ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ」とラベル付けされた）一時的登録デバイス証明書１０４２に署名する。一時的登録デバイス証明書１０４２は、対象名としてのデバイス識別子、公開鍵としてのＥＰＫ、及び有効期間を含む。ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２は、一時的登録発行証明書１０４０（ＴＥ＿ＯＥＭ＿ＩＣ）に対応付けられた秘密鍵によって署名される。

【０１５９】

前述したように、ＯＥＭは、製造中にＫＭＳが所有する電子デバイス１００によって生成されたＥＰＫの証明書のみを要求するように効果的に制限され、実際のデバイス以外の第三者は対応するＥＳＫを知らない。したがって、一時的登録デバイス証明書１０４２は、実際の電子デバイス１００を除く全ての当事者にとって役に立たないはずである。一時的登録デバイス証明書１０４２は、登録のみで使用される一時的なクレデンシャルとしての使用を強制するのに役立つ短い有効期間を有する。例えば、有効期間は５分以下であってもよい。

【０１６０】

１１２２において、そのデバイスのバッチに関連付けられたセキュリティポリシーによって指定された発行証明書ＩＣ＿Ａ１０４６と、署名されたＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２との両方が、電子デバイス１００に通信される。

【０１６１】

ＴＬＳ接続は、１１２４において閉じられる。

【０１６２】

次いで、電子デバイス１００は、１１２２で受信したクレデンシャルを照合し（１１２６）、成功した場合、ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２及びＩＣ＿Ａ１０４６をインストールする（１１２８）。

【０１６３】

電子デバイス１００は、ハンドシェイクで付与された発行証明書ＩＣ＿Ａ１０４６を検証する。電子デバイス１００は、対象名フィールドが期待値と一致すること、すなわち発行証明書ＩＣ＿Ａ１０４６を使用して証明書を発行できることを確認し、プライマリトラステッドルート証明書１０４４を使用して発行証明書ＩＣ＿Ａ１０４６上で署名を検証する。セキュリティを追加するために、電子デバイス１００は、中間ＣＡではなくプライマリトラステッドルート証明書１０４４によって直接署名されている場合にのみ、発行証明書ＩＣ＿Ａを受け入れるべきである。可能であれば、実行された照合は、電子デバイス１００が証明書を発行する実デバイスのみを受け入れることに十分であることが保証されるべきである。特に、ＴＬＳ発行証明書１０５４及びそれによって発行された証明書を拒否すべきであり、デバイス証明書及びデバイス証明書によって発行された証明書を拒否すべきである。照合に合格すると、電子デバイス１００は、発行証明書ＩＣ＿Ａ１０４６をインストールし、その結果、ＯＥＭ１６０によって発行された後続の証明書を認証するために使用できる。

【０１６４】

電子デバイス１００は、ＫＭＳの実際の発行証明書（これが事前に分かっている場合、理想的には、デバイスの特定の発行証明書）のいずれでもない証明書を拒否する必要がある。

【０１６５】

また、電子デバイス１００は、ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２内の機器ＩＤ及びＥＰＫが電子デバイス１００に属するものと一致することを確認する。これにより、ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２が次のハンドシェイクにおける認証に使用するのに適していることが保証される。

【０１６６】

これらの照合のいずれかが失敗した場合、電子デバイス１００は登録を中止する。

【０１６７】

この例では、ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２は、ＫＭＳ１２０が認証したＴＬＳチャ

ネルを介して電子デバイス１００に受信されたので、ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２は、ＫＭＳ１２０によって承認されたものとして暗黙的に信頼することができる。したがって、電子デバイスは、ＴＥ＿Ｄｅｖ＿Ｃｅｒｔ１０４２が特定の一時的登録ルート証明書ＴＥ＿ＯＥＭ＿ＲＯＯＴ１０３８の下位であることを照合する必要はない。好適には、これは、ＴＥ＿ＯＥＭ＿ＲＯＯＴ１０３８又は発行証明書ＴＥ＿ＯＥＭ＿ＩＣ１０４０のいずれもＫＭＳ１２０から出る必要がないことを意味する。しかしながら、他の例では、一時的登録ルート証明書１０３８は、ＯＥＭファームウェアの一部としてデバイスに予めインストールされてもよく、ＫＭＳ１２０はまた、セキュア接続を介して一時的登録発行証明書１０４０を送信して、電子デバイスが一時的登録デバイス証明書１０４２への信頼チェーンを構築できるようにしてもよい。

【０１６８】

図７の交換が実行された後、電子デバイス１００は、ＥＰＫが電子デバイス１００に関連付けられていることを証明する一時的登録デバイス証明書１０４２を所有している。一時的登録デバイス証明書１０４２はまた、電子デバイスがＫＭＳと更に交換を行うことができる有効期間を提供する。ＥＰＫは、この段階では、例えば認証局サーバ１３０などによって広く知られている。電子デバイス１００はまた、後続の交換で発行されたデバイス証明書１０４８を検証するために使用できる発行証明書１０４６を所有している。

【０１６９】

好適には、デバイスに安全な情報を注入する必要なく、一時的登録デバイス証明書がデバイスに提供される。安全な情報を注入するには、秘密情報を電子デバイスに注入するセキュア設備、及び／又は情報を安全に注入する第三者の能力を信頼する必要がある。セキュア設備は、コストが高く、管理が困難であり、新たな脅威に対する堅牢な応答を確保するためにセキュリティ手順の継続的な保守及び評価を必要とする。一般に、ハードウェアセキュリティモジュール（ＨＳＭ）は、鍵を生成及び記憶するために必要とされてもよく、統合された鍵注入システムは、電子デバイスに鍵を注入するために必要とされてもよく、その場合でも、ＨＳＭ及び／又はセキュア設備が損なわれた場合、注入された情報の完全性を保証することができない。したがって、安全な情報を注入する必要性を回避することにより、電子デバイスの管理が容易になり、情報の完全性が保証され、より安全になる。

【０１７０】

図８は、電子デバイス１００による実行のための一般的な方法１２００のフローチャートを示す。電子デバイス１００は、物理複製困難関数（ＰＵＦ）４５０を有するセキュリティモジュール１１０を備え、セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成され、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を備える。一例では、セキュリティモジュール１１０は、ＰＵＦ４５０に対する第１のチャレンジに基づいて登録公開鍵（ＥＰＫ）を確立し、ＰＵＦ４５０に対する第１のチャレンジへの応答に基づいて登録秘密鍵（ＥＳＫ）を確立するように構成されてもよい。電子デバイス１００は、一時的登録トラステッドルート証明書１０３８がインストールされた１つ以上のメモリを更に備える。

【０１７１】

方法１２００は、１２１０において、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のためのデバイス識別子及びＥＰＫを含む証明書署名要求（ＣＳＲ）をサーバに送信するステップを含み、ＣＳＲは、ＥＳＫを使用して署名され、デバイス識別子は、ＥＰＫの関数に基づく。セキュア接続は、ＴＬＳ接続を含み得る。例えば、セキュア接続は、鍵管理サーバ１２０とのＴＬＳ接続を含み得る。

【０１７２】

方法１２００は、１２２０において、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書１０４２を受信することを更に含む。

【０１７３】
有効期間は、セキュア接続の他端における当事者との更なるセキュア接続を確立することができる期間を規定することができる。
【０１７４】
電子デバイス１００の１つ以上のメモリはまた、プライマリトラステッドルート証明書１０４４をインストールしていてもよく、方法１２００は、プライマリトラステッドルート証明書１０４４の下位である発行証明書１０４６を受信するステップを含んでもよい。方法は、発行証明書１０４６がプライマリトラステッドルート証明書１０４４から直接派生したものであることを検証するステップを更に含むことができる。
【０１７５】
方法１２００は、１２３０において、一時的登録デバイス証明書１０４２をメモリにインストールすることを更に含む。ＫＭＳ１２０が電子デバイス１００に対して認証した後に、セキュアチャネルを介して一時的登録デバイス証明書が受信された場合、一時的登録デバイス証明書１０４２は、ＫＭＳから来たものとして電子デバイスによって信頼され得る。しかしながら、他の例では、一時的登録ルート証明書１０３８は、ＯＥＭファームウェアの一部としてデバイスに予めインストールされてもよいし、通信チャネルを介して電子デバイスによって受信されてもよい。
【０１７６】
図９は、方法１３００のフローチャートを示す。この方法は、例えば、鍵管理サーバ１２０によって実行され得る。
【０１７７】
１３１０において、方法１３００は、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のための、デバイス識別子と電子デバイスによって確立された登録鍵対の登録公開鍵（ＥＰＫ）とを含む証明書署名要求（ＣＳＲ）を受信するステップを含み、デバイス識別子はＥＰＫの関数に基づく。
【０１７８】
１３２０において、方法１３００は、サーバが証明書に署名することができるデバイス識別子のデータベースとデバイス識別子が照合されるようにするステップを含む。例えば、データベースはローカルに記憶されてもよく、その場合、図７に関して説明したシナリオで想定されるように、データベースを直接参照することができる。しかしながら、他の例では、データベースは、例えば認証局サーバ１３０を有するリモートサーバに配置されてもよく、その場合、データベースに対してデバイス識別子を照合する要求が行われてもよい。
【０１７９】
１３３０において、方法１３００は、デバイス識別子がＥＰＫの関数であることを検証するためにデバイス識別子の照合が実行されるようにすることを更に含む。サーバは、デバイス識別子がＥＰＫの関数であるかどうかを直接評価してもよく、又はデバイス識別子がＥＰＫの関数であることを検証するために別のコンピューティングデバイスと通信してもよい。幾つかの例では、関数は暗号化ハッシュ関数であってもよい。
【０１８０】
１３４０において、方法１３００は、ＥＰＫがデータベース内のデバイス識別子と関連付けられるようにするステップを含む。例えば、データベースはローカルに記憶されてもよく、その場合、図７に関して説明したシナリオで想定されるように、データベースは直接修正されてもよい。しかしながら、他の例では、データベースは、例えば認証局サーバ１３０を有するリモートサーバに配置されてもよく、その場合、デバイス識別子をデータベース内のＥＰＫに関連付ける要求が行われてもよい。
【０１８１】
１３５０において、方法１３００は、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書に署名するステップを含む。
【０１８２】

１３６０において、方法１３００は、デバイス識別子によって識別される電子デバイスに対するセキュア接続を介した署名された一時的登録デバイス証明書の送信を開始するステップを含む。署名された一時的登録証明書は、デバイス識別子によって識別される電子デバイスに直接送信されてもよいし、セキュア接続を介して電子デバイス１００に前方送信するために別のコンピューティングデバイスに渡されてもよい。

【０１８３】

方法は、電子デバイスへの発行証明書１０４６の通信を開始するステップを更に含むことができる。

【０１８４】

図１０は、電子デバイス１００を登録するための方法を示す。電子デバイス１００は、物理複製困難関数（ＰＵＦ）４５０を有するセキュリティモジュール１１０を含む。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成されており、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む。一例では、セキュリティモジュール１１０は、ＰＵＦ４５０に対する第１のチャレンジに基づいて登録公開鍵（ＥＰＫ）を確立し、ＰＵＦ４５０に対する第１のチャレンジへの応答に基づいて登録秘密鍵（ＥＳＫ）を確立するように構成されてもよい。電子デバイス１００は、ＰＵＦに対する第２のチャレンジ及び応答に基づいてデバイス鍵対（ＤＰＫ、ＤＳＫ）を確立するように更に構成され、デバイス鍵対は、デバイス公開鍵（ＤＰＫ）及びデバイス秘密鍵（ＤＳＫ）を含む。電子デバイス１００は、プライマリトラステッドルート証明書１０４４（例えば、図６Ｃの「ＯＥＭ＿ＲＯＯＴ」）がインストールされた１つ以上のメモリを更に備える。

【０１８５】

この方法では、電子デバイス１００及びＫＭＳ１２０は互いに認証し、電子デバイス１００は、ＩｏＴハブ１７０と通信するために使用するデバイス公開鍵（ＤＰＫ）の証明書を要求する。

【０１８６】

電子デバイス１００は、１４０２において、ＫＭＳ１２０へのＴＬＳ接続を開始する。ハンドシェイク中に、ＫＭＳ１２０は、セキュア接続証明書（「ＫＭＳ＿ＴＬＳ＿Ｃｅｒｔ」）１０５６とセキュア接続発行証明書（「ＩＣ＿ＴＬＳ」）１０５４を提示する（１４０４）ことで、電子デバイス１００に対して再度認証を行う。

【０１８７】

電子デバイス１００は、図７に関連して前述したように、この証明書に対する全ての照合を実行しなければならない（特に、対象名を慎重に照合する）。これは、電子デバイス１００に、ファームウェア内のＫＭＳ識別子に関連付けられたＫＭＳ１２０と通信していることを証明する。

【０１８８】

ＫＭＳ認証が成功した場合、電子デバイス１００は、１４０６において、以前の交換で受信した一時的登録デバイス証明書１０４６を提示し、ＴＬＳクライアント認証を実行することによってサーバに認証する。ＫＭＳ１２０は、一時的登録発行証明書１０４０（「ＴＥ＿ＯＥＭ＿ＩＣ」）によって署名された一時的登録デバイス証明書のみを受け付ける。１４０８において、ＫＭＳ１２０は、一時的登録デバイス証明書の照合を実行する。

【０１８９】

クライアント認証が成功すると、電子デバイス１００は、一時的登録デバイス証明書１０４２内の登録公開鍵（ＥＰＫ）に対応する登録秘密鍵（ＥＳＫ）を知っていることが証明される。証明書を発行するときのＫＭＳ１２０による照合は、デバイス識別子がそれらが所有するデバイスに対応することを保証し、一時的登録デバイス証明書１０４２内の登録公開鍵がその証明書で指定されたデバイス識別子にハッシュするので、デバイスの対が衝突ＩＤを有さず、攻撃者がハッシュ関数内の衝突を見つけることができなかった場合（両方のイベントが非常に小さな確率で発生する）、これは、電子デバイス１００が、一時的登録デバイス証明書１０４２内のＥＰＫに対応するＥＳＫを知っているＨ（ＥＰＫ）に

よって与えられる識別子を有する一意のデバイスであることをＫＭＳ１２０に証明する。
【０１９０】
一時的登録署名鍵が危険にさらされた場合、攻撃者は、ＫＭＳ１２０へのＴＬＳクライアント認証を正常に完了することを可能にする既知の鍵対の任意の証明書を発行することができる。しかしながら、この場合は、更に後述するＫＭＳ１２０によって実行される照合によって捕捉される。
【０１９１】
双方が認証されると、セキュアなＴＬＳ通信チャネルが開かれる（１４１０）。
【０１９２】
電子デバイス１００は、１４１２において、デバイス公開鍵ＤＰＫのための証明書署名要求（ＣＳＲ）を作成する。ＣＳＲにおける対象名は、ＥＰＫの暗号ハッシュＨ（ＥＰＫ）であるデバイス識別子（図では「ＤｅｖｉｃｅＩＤ」とラベル付けされている）と等しい。電子デバイス１００は、１４１４において、ＣＳＲをＫＭＳ１２０に送信する。
【０１９３】
ＣＳＲにおける所有の証明は、電子デバイス１００がＣＳＲにおけるデバイス公開鍵（ＤＰＫ）に対応するデバイス秘密鍵（ＤＳＫ）を知っているという何らかの保証をＫＭＳ１２０に与える。将来的にチャネルバインディング情報をＣＳＲに含めることができる場合、これは、ＴＬＳ接続のクライアント側の電子デバイス１００がＤＰＫに対応するＤＳＫを知っていることを証明する。
【０１９４】
ＣＳＲを受信した後、ＫＭＳ１２０は、幾つかの照合を実行する。
【０１９５】
ＫＭＳ１２０は、１４１６において、一時的登録デバイス証明書１０４２が有効期間内であり、一時的登録デバイス証明書１０４２に署名するために使用された署名が正しく検証されていることを照合する。
【０１９６】
ＫＭＳ１２０は、１４１８において、一時的登録デバイス証明書１０４２内のデバイス識別子がＫＭＳのデータベース内のエントリに対応することを更に照合する。これにより、（ＴＥ＿ＯＥＭ＿ＩＣ証明書１０４０に関連付けられた）ＴＥ発行秘密鍵の侵害が軽減される。そのようなイベントが発生すると、攻撃者は任意の有効な一時的登録デバイス証明書１０４２を発行することができる。しかしながら、ＫＭＳが所有するセットの外部にあるデバイス識別子の一時的登録デバイス証明書は、この照合後に拒否される。これは、攻撃者が発行できるのは、ＫＭＳが所有するデバイス識別子に対する悪意のある一時的登録デバイス証明書のみであることを意味する。これは、以下の照合で軽減される。
【０１９７】
ＫＭＳ１２０は、１４２０において、一時的登録デバイス証明書１０４２内のデバイス識別子がＨ（ＥＰＫ）に等しいことを照合し、ＥＰＫは一時的登録デバイス証明書１０４２の公開鍵フィールド内にある。
【０１９８】
悪意のある証明書は、一時的登録デバイス証明書（これは、前の照合によって、ＫＭＳに属するデバイス識別子に対応する）内のデバイス識別子にハッシュするＥＰＫを有していなければならない。ＴＬＳクライアント認証がそのような証明書で成功するためには、攻撃者は、デバイスのＥＳＫを侵害している（この場合、デバイスはいずれにしても完全に侵害されている）か、又はハッシュ関数の衝突を発見している必要があり、これは、ＥＰＫ以外の公開鍵を一時的登録デバイス証明書１０４２で使用できることを意味する（良好な衝突耐性ハッシュ関数には実行不可能）。
【０１９９】
１４１６、１４１８、１４２０における照合は、必要に応じて、セキュアなチャネルが開かれる前に１４０８において実行され得ることに留意されたい。
【０２００】

ＫＭＳは、１４２２において、一時的登録デバイス証明書１０４２内のデバイス識別子がＣＳＲ内のデバイス識別子と等しいことを照合する。ＣＳＲの対象名が、一時的登録デバイス証明書１０４２の対象名と一致することを照合することは、認証電子デバイス１００の識別情報を発行された証明書の識別情報にリンクするために必要である。これは、電子デバイス１００が異なるデバイス識別子の証明書を要求し、その証明書を使用してその異なるデバイスになりすますことを防止するためである。

【０２０１】

１４２４において、ＫＭＳ１２０は、そのデータベースから所与のデバイス識別子に関連付けられたセキュリティポリシーを検索し、証明書の有効期限、鍵の使用などに基づいて全ての必要な照合を実行して、ＣＳＲの詳細がＫＭＳのセキュリティポリシーに準拠するようにする。

【０２０２】

全ての照合に成功した場合、ＫＭＳ１２０は、ポリシーに関連付けられた発行証明書１０４６（「ＩＣ＿Ａ」）の秘密鍵を使用して、ＣＳＲの詳細に従って電子デバイス１００にデバイス証明書１０４８を発行する。

【０２０３】

新しく作成されたデバイス証明書１０４８は、１４２６で、ＩｏＴハブエンドポイント及びＩｏＴルート証明書と共に電子デバイス１００に送信される。デバイス証明書１０４８もＩｏＴハブ１７０に送信される。電子デバイス１００は、これで、そのＩｏＴハブ１７０に接続するために必要な全ての情報を有する。

【０２０４】

電子デバイス１００がそのＩｏＴハブ１７０に対して認証できるようにするためには、デバイス証明書１０４８に署名した発行証明書１０４６が事前にＩｏＴハブ１７０に登録されている必要がある。証明書ＩＣ＿Ａ、ＩＣ＿Ｂなどを発行する全てのデバイスは、電子デバイスが接続する前にＩｏＴハブ１７０に登録される。

【０２０５】

１４３０において、ＴＬＳ接続が終了する。

【０２０６】

１４３２において、電子デバイス１００は、以前にインストールされた発行証明書ＩＣ＿Ａ１０４６を使用して、送信されたデバイス証明書１０４８を検証する。電子デバイス１００は、デバイス証明書１０４８が、以前にインストールされた発行証明書１０４６によって発行されたものであることを照合し、他の証明書によって発行されたデバイス証明書を受け入れてはならない。

【０２０７】

電子デバイス１００は、デバイス証明書１０４８の対象名及び公開鍵が想定通りであること（すなわち、対象がデバイス識別子Ｈ（ＥＰＫ）であり、公開鍵がＤＰＫであること）を照合する。更なるセキュリティのために、電子デバイス１００は、可能な場合、有効期限及び有効期限が不規則性（有効期限が過去である、又はデバイス証明書１０４８が期限切れであるなど）を表示しないことを照合するべきである。証明書１０４８が更新されている（したがって、公開鍵が変更されていない）場合、電子デバイス１００は、例えば、有効期限が以前の証明書と異なることを照合して、ＫＭＳ１２０になりすました攻撃者が電子デバイスの古い証明書を返していないことをある程度保証することができる。

【０２０８】

電子デバイス１００は、検証が失敗した場合、接続を終了し、オプションで詳細を示すエラーメッセージを表示しなければならない。

【０２０９】

このステップは、電子デバイス１００が、現在信頼されている発行証明書ＩＣ＿Ａ１０４６によって有効なデバイス証明書１０４８を発行され、その詳細が電子デバイス１００の期待通りであることを確認するために使用される。攻撃者が（ＫＭＳ＿ＴＬＳ＿Ｃｅｒｔ証明書１０５６のための）ＴＬＳ鍵を侵害したが、（ＩＣ＿Ａ証明書１０４６のための

）発行秘密鍵を侵害していない場合、攻撃者は、ＫＭＳ１２０を電子デバイス１００になりすますことができるが、電子デバイス１００のための有効な新しいデバイス証明書１０４８を発行することができない。電子デバイス１００は、適切な証明書を受信したことを確認するためと、ＫＭＳ１２０になりすましているが発行秘密を知らない攻撃者が、電子デバイス１００に錯覚を与えて既に発行されたデバイス証明書を受け取らせようとしているかどうかを検出するための両方で、受信した証明書の詳細を慎重に照合する必要がある。

【０２１０】

好適には、図１０の方法の後、電子デバイスは、デバイス公開鍵（ＤＰＫ）がデバイス識別子（Ｈ（ＥＰＫ））に関連付けられていることを証明するための有効なデバイス証明書１０４８を所有している。デバイス証明書１０４８の信頼は、ＯＥＭ１６０に関連付けられたプライマリルート証明書１０４４から導出される。

【０２１１】

図１１は、電子デバイス１００による実行のための一般的な方法１５００のフローチャートを示す。電子デバイス１００は、物理複製困難関数（ＰＵＦ）４５０を有するセキュリティモジュール１１０を備える。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及び応答に基づいて登録鍵対（ＥＰＫ、ＥＳＫ）を確立するように構成されており、登録鍵対は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む。一例では、セキュリティモジュール１１０は、ＰＵＦ４５０に対する第１のチャレンジに基づいて登録公開鍵（ＥＰＫ）を確立し、ＰＵＦに対する第１のチャレンジへの応答に基づいて登録秘密鍵（ＥＳＫ）を確立するように構成されてもよい。電子デバイス１００は、ＰＵＦに対する第１のチャレンジ及び応答に基づいてデバイス鍵対（ＤＰＫ、ＤＳＫ）を確立するように構成されており、デバイス鍵対は、デバイス公開鍵（ＤＰＫ）及びデバイス秘密鍵（ＤＳＫ）を含む。電子デバイス１００は、プライマリトラステッドルート証明書１０４４がインストールされた１つ以上のメモリを更に備える。

【０２１２】

１５１０において、方法１５００は、セキュア接続を介して、ＤＰＫがデバイス識別子と関連付けられることを証明する証明書１０４８のための証明書署名要求（ＣＳＲ）をサーバに送信するステップを含み、ＣＳＲはＤＳＫを使用して署名される。ＣＳＲは、ＤＰＫ及びデバイス識別子を含む。デバイス識別子は、ＥＰＫの関数に基づく。

【０２１３】

１５２０において、方法１５００は、セキュア接続を介して、ＤＰＫをデバイス識別子と関連付けるデバイス証明書１０４８を受信するステップを含む。

【０２１４】

１５３０において、方法１５００は、デバイス証明書１０４８がプライマリトラステッドルート証明書１０４４の下位であることを検証するステップを含む。電子デバイス１００は、デバイス証明書１０４８の対象名及び公開鍵が予想通りであること（すなわち、対象がデバイス識別子Ｈ（ＥＰＫ）であり、公開鍵がＤＰＫであること）を更に照合することができる。更なるセキュリティのために、電子デバイス１００は、有効期限及び有効期限が不規則性（有効期限が過去である、又はデバイス証明書１０４８が期限切れであるなど）を表示しないことを照合することができる。証明書１０４８が更新されている（したがって、公開鍵が変更されていない）場合、電子デバイス１００は、有効期限が以前の証明書の有効期限と異なることを照合して、攻撃者が電子デバイスの古い証明書を返していないことをある程度保証することができる。

【０２１５】

１５４０において、方法１５００は、検証に応じて、デバイス証明書１０４８をメモリにインストールするステップを含む。

【０２１６】

図１２は、方法１６００のフローチャートを示す。方法は、（すなわち、鍵管理サーバシステム）１つ以上のコンピューティング装置を含むことができる鍵管理サーバ１２０な

どのコンピューティング装置による実行に適している。

【０２１７】

１６１０において、方法１６００は、デバイス鍵対のデバイス公開鍵（ＤＰＫ）がデバイス識別子と関連付けられることを証明する証明書のための証明書署名要求（ＣＳＲ）を受信するステップを含む。ＣＳＲは、デバイス識別子及びＤＰＫを含み、デバイス鍵対のデバイス秘密鍵（ＤＳＫ）を使用して署名される。デバイス識別子は、電子デバイスに属することが知られている登録鍵対の登録公開鍵の関数に基づく。

【０２１８】

ＫＭＳ１２０は、電子デバイス１００からのセキュア接続を介してＣＳＲを受信してもよいし、電子デバイス１００からのセキュア接続を介してＣＳＲを受信した鍵管理サーバシステムの別のサーバからＣＳＲを受信してもよい。

【０２１９】

１６２０において、方法１６００は、サーバが証明書に署名することができるデバイス識別子のデータベースとデバイス識別子が照合されるようにするステップを含む。例えば、データベースはローカルに記憶されてもよく、その場合、図１０に関して説明したシナリオで想定されるように、データベースを直接参照することができる。しかしながら、他の例では、データベースは、例えば認証局サーバ１３０を有するリモートサーバに配置されてもよく、その場合、データベースに対してデバイス識別子を照合する要求が行われてもよい。

【０２２０】

１６３０において、方法１６００は、デバイス識別子が電子デバイスを識別することが知られていることを検証するためにデバイス識別子の照合が実行されるようにするステップを含む。例えば、ＫＭＳ１２０は、ＫＭＳ１２０がデバイス識別子を所有していること、デバイス識別子がＥＰＫの関数であること、及びＣＳＲのデバイス識別子が以前に発行された一時的登録デバイス証明書１０４２内のデバイス識別子と等しいことを検証するために照合が実行されるようにし得る。

【０２２１】

１６４０において、方法１６００は、ＣＳＲに基づいてデバイス証明書１０４８に署名するステップを含み、デバイス証明書１０４８は、電子デバイスに知られているプライマリトラステッドルート証明書の下位である。

【０２２２】

１６５０において、本方法は、デバイス識別子によって識別される電子デバイスへのセキュア接続を介したデバイス証明書１０４８の送信を開始するステップを含む。方法は、電子デバイスが関連するＩｏＴハブと通信することを可能にするために、ＩｏＴハブのＩｏＴルート証明書、及びＵＲＬなどのエンドポイントの送信を開始するステップを更に含むことができる。方法は、デバイス証明書１０４８をＩｏＴハブ１７０に通信するステップを更に含み得る。

【０２２３】

図１３は、幾つかの例に係るコンピュータ可読媒体１７００を示す。

【０２２４】

コンピュータ可読媒体１７００はユニットを記憶し、各ユニットは、実行されるときにプロセッサ１７２０又は他の処理／コンピューティング装置もしくは装置に特定の動作を実行させる命令１７１０を含む。

【０２２５】

例えば、命令１７１０は、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のためのデバイス識別子と登録公開鍵ＥＰＫとを含む証明書署名要求（ＣＳＲ）をプロセッサ１７２０がサーバに送信するようにしてもよく、ＣＳＲは登録秘密鍵ＥＳＫを使用して署名され、デバイス識別子はＥＰＫの関数に基づく。命令１７１０は、更に、セキュア接続を介して、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書をプロセッサ１７２０に受信させ

ることができる。命令１７１０は、更に、プロセッサ１７２０が一時的登録デバイス証明書をメモリにインストールするようにし得る。

【０２２６】

例えば、命令１７１０は、ＥＰＫがデバイス識別子と関連付けられることを証明する証明書のための、デバイス識別子と電子デバイスによって確立された登録鍵対の登録公開鍵（ＥＰＫ）とを含む証明書署名要求（ＣＳＲ）を、プロセッサ１７２０に受信させることができ、デバイス識別子はＥＰＫの関数に基づく。命令１７１０は、更に、プロセッサ１７２０に、サーバが証明書に署名することができるデバイス識別子のデータベースとデバイス識別子とを照合させることができる。命令１７１０は、更に、プロセッサ１７２０に、デバイス識別子がＥＰＫの関数であることを検証するためにデバイス識別子の照合を実行させることができる。命令１７１０は、更に、プロセッサ１７２０に、ＥＰＫをデータベース内のデバイス識別子と関連付けさせることができる。命令１７１０は、更に、プロセッサ１７２０に、ＥＰＫがデバイス識別子と関連付けられることを証明して有効期間を含む一時的登録デバイス証明書に署名させることができる。命令１７１０は、更に、プロセッサ１７２０に、デバイス識別子によって識別される電子デバイスに対するセキュア接続を介した署名された一時的登録デバイス証明書の送信を開始させることができる。

【０２２７】

例えば、命令１７１０は、プロセッサ１７２０に、セキュア接続を介して、ＤＰＫがデバイス識別子と関連付けられることを証明する証明書のための、登録公開鍵（ＥＰＫ）の関数に基づくデバイス識別子を含むデバイス公開鍵（ＤＰＫ）のための証明書署名要求（ＣＳＲ）をサーバへ送信させることができ、ＣＳＲはデバイス秘密鍵（ＤＳＫ）を使用して署名される。命令１７１０は、更に、プロセッサ１７２０に、セキュア接続を介して、ＤＰＫをデバイス識別子と関連付けるデバイス証明書を受信させることができる。命令１７１０は、更に、プロセッサ１７２０に、デバイス証明書がプライマリトラステッドルート証明書の下位であることを検証させることができる。命令１７１０は、更に、プロセッサ１７２０に、検証に応じて、デバイス証明書をメモリにインストールさせることができる。

【０２２８】

例えば、命令１７１０は、プロセッサ１７２０に、電子デバイスによって確立されたデバイス鍵対のデバイス公開鍵（ＤＰＫ）に対する証明書署名要求（ＣＳＲ）を受信させることができ、ＣＳＲは、電子デバイスによって確立された登録鍵対の登録公開鍵（ＥＰＫ）の関数に基づくデバイス識別子を含み、ＣＳＲは、ＤＰＫがデバイス識別子と関連付けられることを証明する証明書のためのものである。命令１７１０は、更に、プロセッサ１７２０に、デバイス識別子を、プロセッサ１７２０が証明書に署名することができるデバイス識別子のデータベースと照合させることができる。命令１７１０は、更に、プロセッサ１７２０に、デバイス識別子が電子デバイスを識別することが知られていることを検証するためにデバイス識別子の照合を実行させることができる。命令１７１０は、更に、プロセッサ１７２０に、ＣＳＲに基づいてデバイス証明書に署名させることができ、デバイス証明書は、プライマリトラステッドルート証明書の下位である。命令１７１０は、更に、プロセッサ１７２０に、デバイス識別子によって識別される電子デバイスに対するセキュア接続を介したデバイス証明書の送信を開始させることができる。

【０２２９】

１つ以上のコンピュータ可読媒体の任意の組み合わせを利用することができる。コンピュータ可読媒体は、コンピュータ可読信号媒体又はコンピュータ可読記憶媒体であってもよい。コンピュータ可読記憶媒体は、例えば、電子、磁気、光学、電磁気、赤外線、又は半導体システム、装置、デバイス、又はこれらの任意の適切な組み合わせであってもよいが、これらに限定されない。コンピュータ可読媒体のより具体的な例（非網羅的なリスト）には、１つ以上の配線を有する電気的接続、ポータブルコンピュータディスケット、ハードディスク、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、消去可能プログラマブルリードオンリーメモリ（ＥＰＲＯＭ又はフラッシュメモリ）、光

ファイバ、ポータブルコンパクトディスクリードオンリーメモリ（ＣＤＲＯＭ）、光記憶装置、磁気記憶装置、又はこれらの任意の適切な組み合わせが含まれる。本明細書の文脈では、コンピュータ可読記憶媒体は、命令実行システム、装置、又はデバイスによって、又はそれに関連して使用するためのプログラムを含むか又は記憶することができる任意の有形媒体であってもよい。

【０２３０】

コンピュータ可読信号媒体は、例えばベースバンドにおいて、又は搬送波の一部として、コンピュータ可読プログラムコードが内部に具現化された伝搬データ信号を含むことができる。そのような伝搬信号は、電磁的、光学的、又はそれらの任意の適切な組み合わせを含むがこれらに限定されない様々な形態のいずれかをとることができる。コンピュータ可読信号媒体は、コンピュータ可読記憶媒体ではなく、命令実行システム、装置、又はデバイスによって、又はそれらと関連して使用するためのプログラムを通信、伝播、又は輸送することができる任意のコンピュータ可読媒体であってもよい。

【０２３１】

コンピュータ可読媒体上に具現化されたコンピュータコードは、無線、有線、光ファイバケーブル、無線周波数（ＲＦ）など、又はそれらの任意の適切な組み合わせを含むがこれらに限定されない任意の適切な媒体を使用して送信され得る。

【０２３２】

本発明の態様のための動作を実行するためのコンピュータプログラムコードは、Ｊａｖａ（商標）、Ｓｍａｌｌｔａｌｋ（商標）、Ｃ＋＋などのオブジェクト指向プログラミング言語、及び「Ｃ」プログラミング言語又は同様のプログラミング言語などの従来の手続き型プログラミング言語を含む、１つ以上のプログラミング言語の任意の組み合わせで記述することができる。プログラムコードは、完全にユーザのコンピュータ上で、部分的にユーザのコンピュータ上で、スタンドアロンソフトウェアパッケージとして、部分的にユーザのコンピュータ上及び部分的にリモートコンピュータ上で、又は完全にリモートコンピュータもしくはサーバ上で実行することができる。後者のシナリオでは、リモートコンピュータは、ローカルエリアネットワーク（ＬＡＮ）又はワイドエリアネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを介してユーザのコンピュータに接続されてもよく、又は外部コンピュータ（例えば、インターネットサービスプロバイダを使用してインターネットを介して、）に接続されてもよい。

【０２３３】

本明細書に記載の方法の多くの変形形態が当業者には明らかである。

【０２３４】

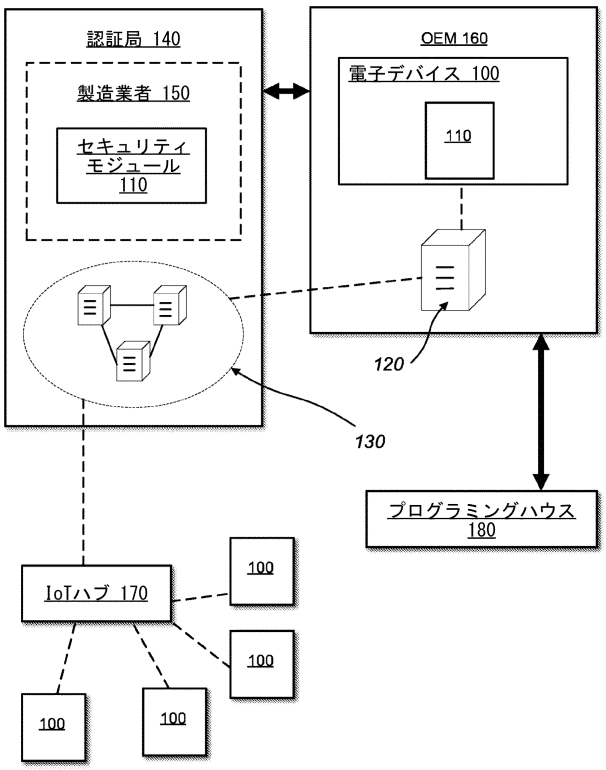
本明細書に開示されている各特徴（添付の特許請求の範囲、要約、及び図面を含む）は、特に明記しない限り、同じ、同等、又は同様の目的を果たす代替的な特徴に置き換えることができる。したがって、特に明記しない限り、開示された各特徴は、一般的な一連の同等又は類似の特徴の一例にすぎない。

【０２３５】

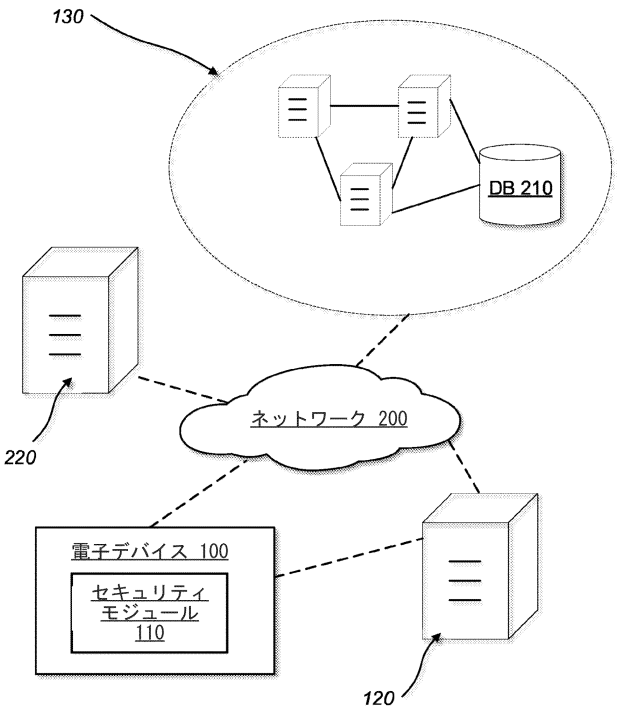
本発明は、任意の前述の実施形態の詳細に限定されない。本発明は、本明細書（添付の特許請求の範囲、要約、及び図面を含む）に開示された特徴の任意の新規なもの、もしくは任意の新規な組み合わせ、又はそのように開示された任意の方法もしくはプロセスのステップの任意の新規なもの、もしくは任意の新規な組み合わせに及ぶ。特許請求の範囲は、前述の実施形態だけでなく、特許請求の範囲内に入る任意の実施形態も包含すると解釈されるべきである。

【図面】

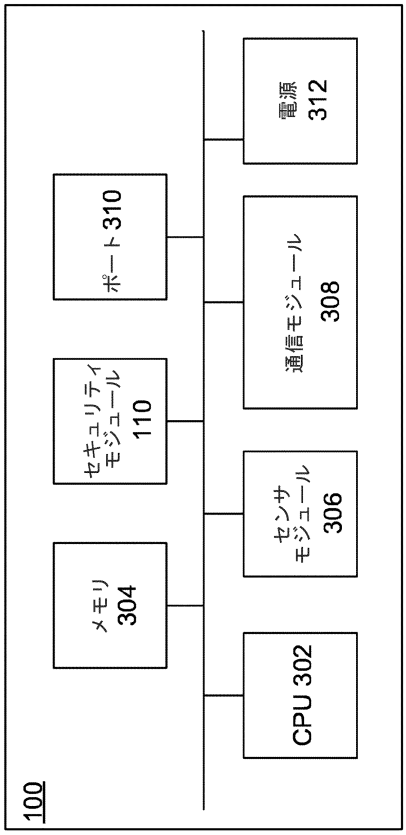
【図１】



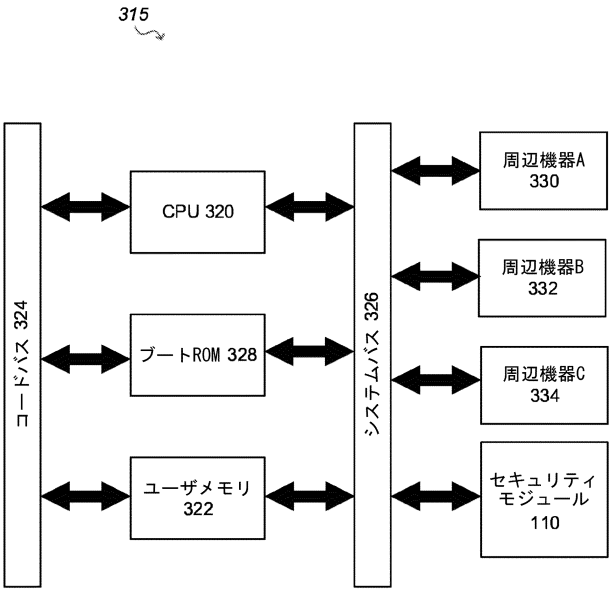
【図２】



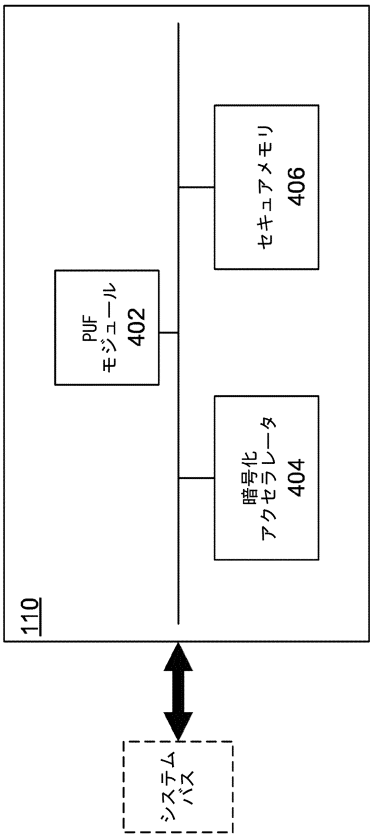
【図３Ａ】



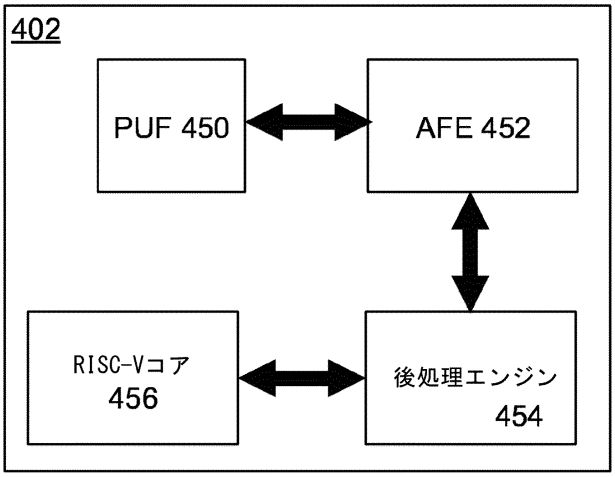
【図３Ｂ】



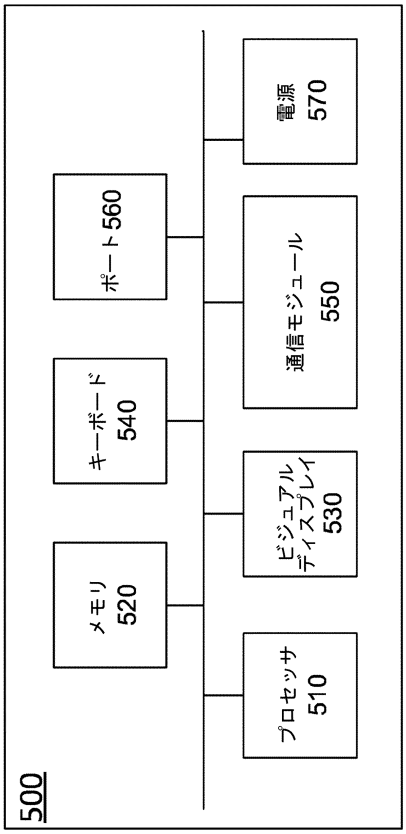
【図４Ａ】



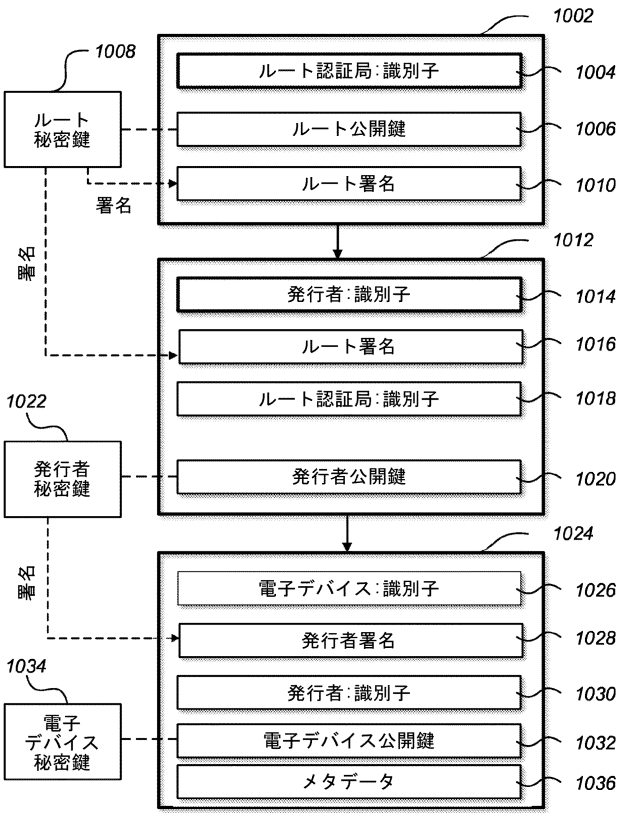
【図４Ｂ】



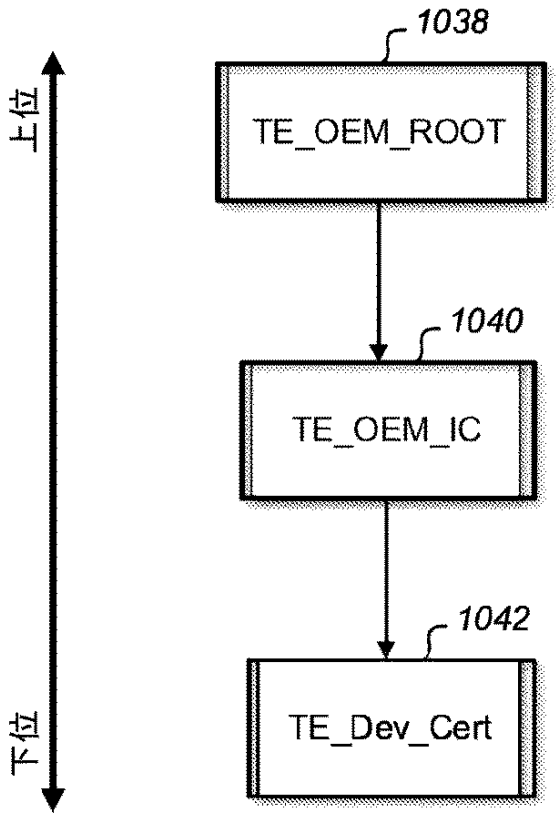
【図５】



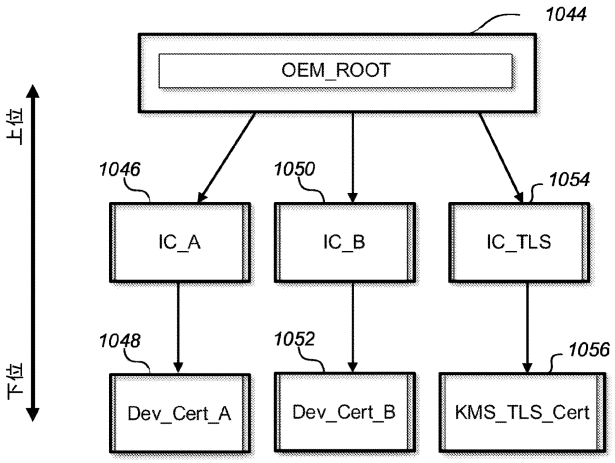
【図６Ａ】



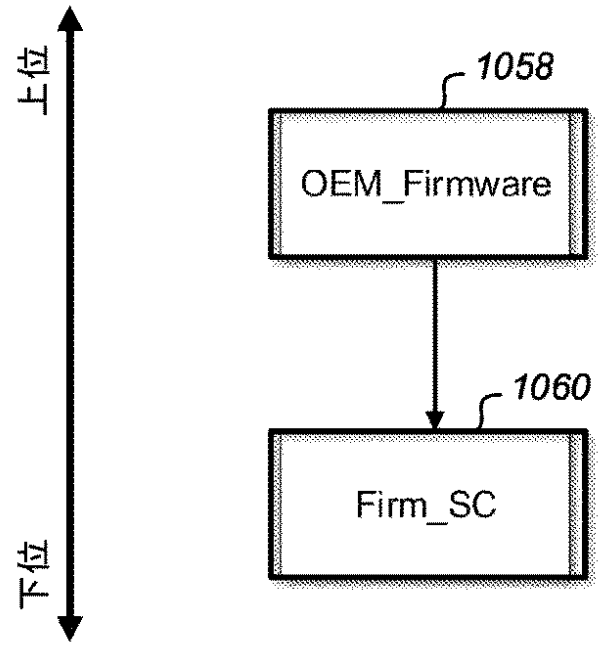
【図６Ｂ】



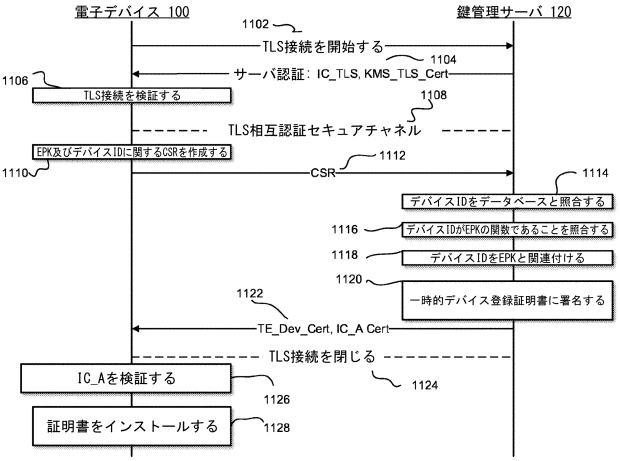
【図６Ｃ】



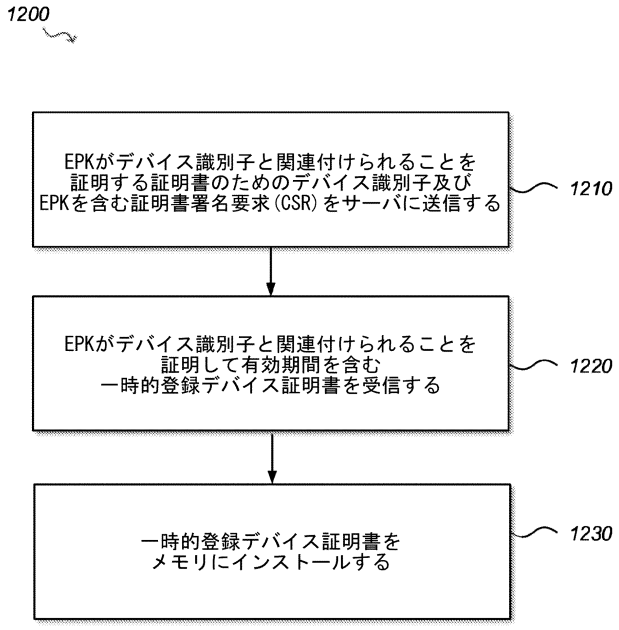
【図６Ｄ】



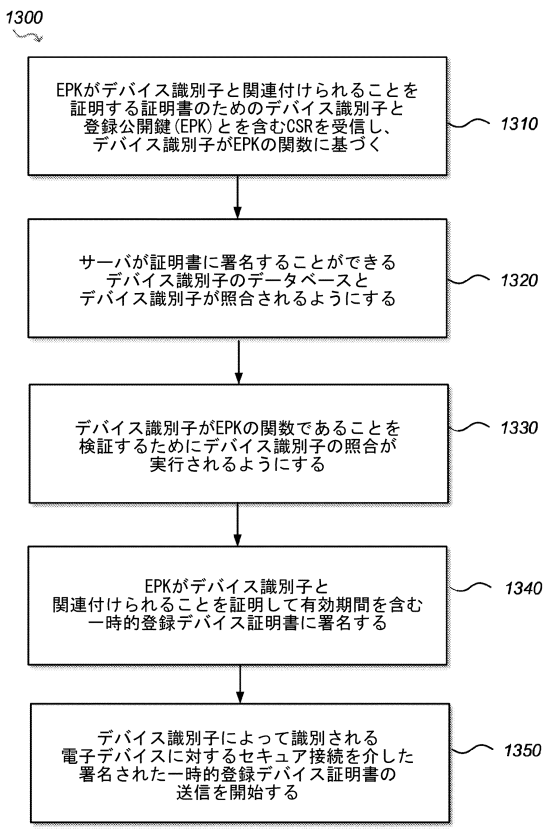
【図７】



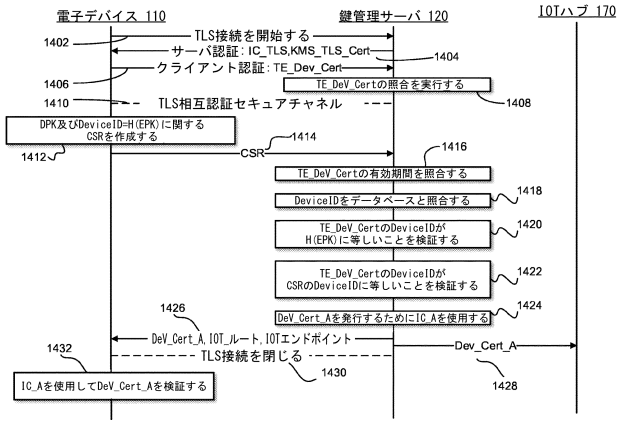
【図８】


1200
EPKがデバイス識別子と関連付けられることを
証明する証明書のためのデバイス識別子及び
EPKを含む証明書署名要求(CSR)をサーバに送信する
1210
EPKがデバイス識別子と関連付けられることを
証明して有効期間を含む
一時的登録デバイス証明書を受信する
1220
一時的登録デバイス証明書を
メモリにインストールする
1230

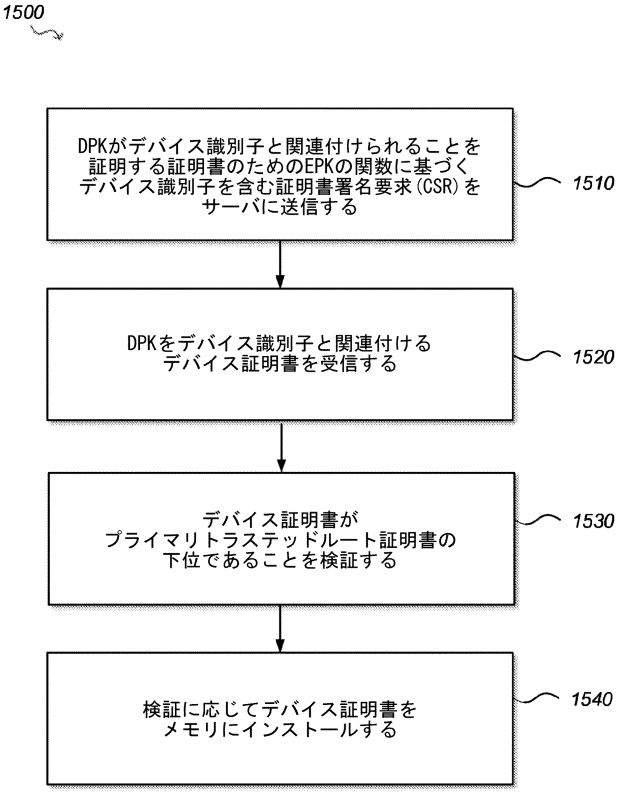
【図９】


1300
EPKがデバイス識別子と関連付けられることを
証明する証明書のためのデバイス識別子と
登録公開鍵(EPK)とを含むCSRを受信し、
デバイス識別子がEPKの関数に基づく
1310
サーバが証明書に署名することができる
デバイス識別子のデータベースと
デバイス識別子が照合されるようにする
1320
デバイス識別子がEPKの関数であることを
検証するためにデバイス識別子の照合が
実行されるようにする
1330
EPKがデバイス識別子と
関連付けられることを証明して有効期間を含む
一時的登録デバイス証明書に署名する
1340
デバイス識別子によって識別される
電子デバイスに対するセキュア接続を介した
署名された一時的登録デバイス証明書の
送信を開始する
1350

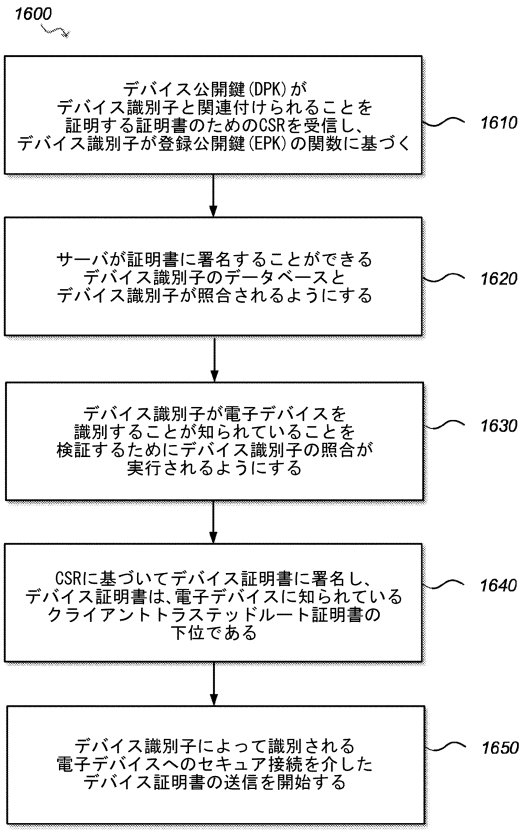
【図１０】


電子デバイス 110
鍵管理サーバ 120
IOTハブ 170
1402
TLS接続を開始する
サーバ認証：IC_TLS,KMS_TLS_Cert
1404
1406
クライアント認証：TE_Dev_Cert
TE_DeV_Certの照合を実行する
1408
1410
TLS相互認証セキュアチャネル
DPK及びDeviceID=H(EPK)に関する
CSRを作成する
1412
CSR
1414
1416
TE_DeV_Certの有効期間を照合する
1418
DeviceIDをデータベースと照合する
TE_DeV_CertのDeviceIDが
H(EPK)に等しいことを検証する
1420
TE_DeV_CertのDeviceIDが
CSRのDeviceIDに等しいことを検証する
1422
1424
DeV_Cert_Aを発行するためにIC_Aを使用する
1426
DeV_Cert_A, IOT_ルート, IOTエンドポイント
Dev_Cert_A
1428
1432
TLS接続を閉じる
1430
IC_Aを使用してDeV_Cert_Aを検証する

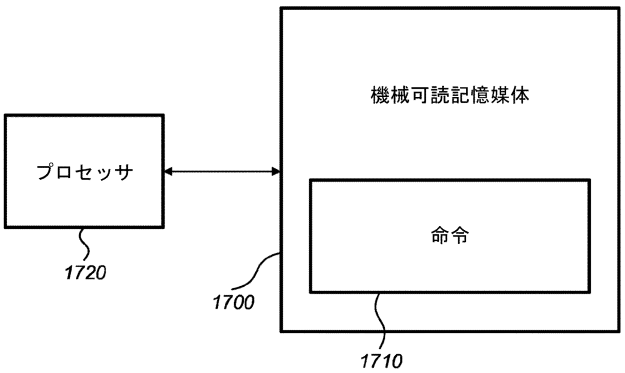
【図１１】


1500
DPKがデバイス識別子と関連付けられることを
証明する証明書のためのEPKの関数に基づく
デバイス識別子を含む証明書署名要求(CSR)を
サーバに送信する
1510
DPKをデバイス識別子と関連付ける
デバイス証明書を受信する
1520
デバイス証明書が
プライマリトラステッドルート証明書の
下位であることを検証する
1530
検証に応じてデバイス証明書を
メモリにインストールする
1540

【図１２】


1600
デバイス公開鍵(DPK)が
デバイス識別子と関連付けられることを
証明する証明書のためのCSRを受信し、
デバイス識別子が登録公開鍵(EPK)の関数に基づく
1610
サーバが証明書に署名することができる
デバイス識別子のデータベースと
デバイス識別子が照合されるようにする
1620
デバイス識別子が電子デバイスを
識別することが知られていることを
検証するためにデバイス識別子の照合が
実行されるようにする
1630
CSRに基づいてデバイス証明書に署名し、
デバイス証明書は、電子デバイスに知られている
クライアントトラステッドルート証明書の
下位である
1640
デバイス識別子によって識別される
電子デバイスへのセキュア接続を介した
デバイス証明書の送信を開始する
1650

【図１３】


機械可読記憶媒体
プロセッサ
命令
1720
1700
1710

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2022/050911

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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.
X	Schrijen Geert-Jan ET AL: "Secure Device Management for the Internet of Things", , 1 April 2019 (2019-04-01), XP055865750, Retrieved from the Internet: URL:https://www.intrinsic-id.com/wp-content/uploads/2019/05/Secure-Device-Management-for-the-Internet-of-Things.pdf [retrieved on 2021-11-25]	1-6, 8-19, 23-25
A	sections II, III, figures 1-5	7,20,21

-/--

[x] Further documents are listed in the continuation of Box C.

[x] 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
15 June 2022	24/06/2022

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	Spranger, Stephanie

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2022/050911

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BATINA L ET AL: "Public-Key Cryptography for RFID-Tags", PROCEEDINGS, FIFTH ANNUAL IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, PERCOM WORKSHOPS 2007 : 19 - 23 MARCH 2007, WHITE PLAINS, NEW YORK, USA, IEEE, LOS ALAMITOS, CA, USA, 1 March 2007 (2007-03-01), pages 217-222, XP031070454, DOI: 10.1109/PERCOMW.2007.98 ISBN: 978-0-7695-2788-8 section 3 -----	1-25
A	US 2020/259668 A1 (LORESKAR CHRIS [GB] ET AL) 13 August 2020 (2020-08-13) paragraph [0036] - paragraph [0050]; figure 2 -----	1-25

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2022/050911

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020259668 A1	13-08-2020	CA 3073647 A1	07-03-2019
		CN 111066016 A	24-04-2020
		EP 3676743 A1	08-07-2020
		GB 2566264 A	13-03-2019
		KR 20200046080 A	06-05-2020
		US 2020259668 A1	13-08-2020
		WO 2019043360 A1	07-03-2019

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

フロントページの続き

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,IT,JM,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,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８０、ザ・プリント・ルームズ、ユニット３０４－５

(72)発明者　パターソン，ケネス

英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８０、ザ・プリント・ルームズ、ユニット３０４－５

(72)発明者　モサイェビ，シャフラム

英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８０、ザ・プリント・ルームズ、ユニット３０４－５

【要約の続き】

リにインストールするように更に構成される。