(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7337912号
(P7337912)

(45)発行日　令和5年9月4日(2023.9.4)

(24)登録日　令和5年8月25日(2023.8.25)

(51)国際特許分類

	FI	
H04W 12/43 (2021.01)	H04W	12/43
H04L 12/22 (2006.01)	H04L	12/22
H04M 1/72505(2021.01)	H04M	1/72505
H04W 12/04 (2021.01)	H04W	12/04
H04W 12/0433(2021.01)	H04W	12/0433

請求項の数　15　（全31頁）　最終頁に続く

(21)出願番号　特願2021-510401(P2021-510401)
(86)(22)出願日　令和1年8月27日(2019.8.27)
(65)公表番号　特表2021-536687(P2021-536687A)
(43)公表日　令和3年12月27日(2021.12.27)
(86)国際出願番号　PCT/EP2019/072866
(87)国際公開番号　WO2020/043730
(87)国際公開日　令和2年3月5日(2020.3.5)
審査請求日　令和4年8月26日(2022.8.26)
(31)優先権主張番号　18191727.9
(32)優先日　平成30年8月30日(2018.8.30)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　590000248
コーニンクレッカ フィリップス エヌヴェ
Koninklijke Philips N.V.
オランダ国 5656 アーヘー アインドーフェン ハイテック キャンパス 52
High Tech Campus 52, 5656 AG Eindhoven, Netherlands
(74)代理人　110001690
弁理士法人M&Sパートナーズ
(72)発明者　バーンセン ヨハネス アーノルダス コーネリス
オランダ国 5656 アーエー アインドーフェン ハイテック キャンパス 44
最終頁に続く

(54)【発明の名称】　コアネットワークへの非３ＧＰＰデバイスアクセス

(57)【特許請求の範囲】

【請求項１】

ローカル通信プロトコルに従うローカルネットワーク内でのワイヤレス通信のために構成された非加入者識別デバイスであって、

前記ローカル通信プロトコルが、プロトコルメッセージと、限られたエリアにわたるワイヤレス送受信とを定義し、

前記非加入者識別デバイスが加入者識別データを備えておらず、前記加入者識別データへのアクセスを有する加入者識別デバイスと協働し、

前記加入者識別データが、コアネットワークにアクセスするためのプロバイダへの加入者の加入者識別データを備え、前記コアネットワークが、少なくとも局地的エリアにわたりモバイルデバイスにワイヤレス通信を提供し、

前記非加入者識別デバイスが、

非加入者識別公開鍵とペアを構成する非加入者識別プライベート鍵と、

前記ローカル通信プロトコルに従うローカル送受信のために構成された送受信機と、

前記加入者識別データとの関連付けを確立するために関連付けシーケンスを実行するプロセッサと、

を備え、前記関連付けシーケンスが、

前記非加入者識別公開鍵を、第１の通信チャネルを介して前記加入者識別デバイスに提供することと、

前記加入者識別デバイスが前記非加入者識別公開鍵を取得したことを検証するために、

第２の通信チャネルを介して前記加入者識別デバイスと検証コードを共有することと、
前記第１の通信チャネルと前記第２の通信チャネルとが異なり、前記通信チャネルの一方が帯域外チャネルであることと、
前記第１の通信チャネル又は前記第２の通信チャネルを介して、前記非加入者識別プライベート鍵の所有の証明を前記加入者識別デバイスに提供することと、
前記加入者識別デバイスから、前記加入者識別データに関係し、前記非加入者識別公開鍵の少なくとも一部分に対して証明機関によって生成された署名を備える証明書を受信することと、を含み、
前記証明書は、前記非加入者識別デバイスが、前記ローカルネットワーク及び前記ローカルネットワークと前記コアネットワークとの間のゲートウェイを介して前記コアネットワークにアクセスすることを可能にする、
非加入者識別デバイス。
【請求項２】
前記関連付けシーケンスは、
前記非加入者識別デバイスがサーバとして機能する、セキュアソケット層プロトコル若しくはトランスポート層セキュリティプロトコルであって、前記非加入者識別デバイスが、自己署名された証明書の中で前記非加入者識別公開鍵を提供し、当該証明書をサーバ証明書メッセージ内でサーバ証明書として使用する、セキュアソケット層プロトコル若しくはトランスポート層セキュリティプロトコル、
前記非加入者識別デバイスがクライアントとして機能する、セキュアソケット層プロトコル若しくはトランスポート層セキュリティプロトコルであって、前記非加入者識別デバイスが、クライアントによって認証されたハンドシェイクの際に、自己署名された証明書の中で前記非加入者識別公開鍵を提供する、セキュアソケット層プロトコル若しくはトランスポート層セキュリティプロトコル、
前記非加入者識別公開鍵若しくは非加入者識別プライベート鍵が使用される公開鍵暗号化によって設定されたインターネットプロトコルセキュリティトンネル、又は
デバイスプロビジョニングプロトコル認証プロトコルであって、前記非加入者識別デバイスが、前記非加入者識別公開鍵又はさらなる非加入者識別公開鍵を、デバイスプロビジョニングプロトコルブートストラップ鍵として又はデバイスプロビジョニングプロトコルプロトコル鍵として提供する、デバイスプロビジョニングプロトコル認証プロトコル、
を利用することにより、前記第１及び第２の通信チャネルのうちの他方の通信チャネルとしてセキュアチャネルを提供することを含む、
請求項１に記載の非加入者識別デバイス。
【請求項３】
前記証明書を受信することが、前記セキュアチャネルを介して前記証明書を受信することを含む、請求項２に記載の非加入者識別デバイス。
【請求項４】
前記帯域外チャネルが、
ＮＦＣ又はＢｌｕｅｔｏｏｔｈ（登録商標）のような短距離無線通信プロトコル、
前記非加入者識別デバイス側においてバーコード又はＱＲコード（登録商標）のような視覚的コードを使用し、前記加入者識別デバイス側においてスキャナ又はカメラを使用する、視覚的チャネル、
前記加入者識別デバイス側においてコードが表示されるユーザチャネルであって、前記コードが前記非加入者識別デバイス側において入力される、ユーザチャネル、
前記非加入者識別デバイス側においてコードが表示されるユーザチャネルであって、前記コードが前記加入者識別デバイス側において入力されるか、又は前記加入者識別デバイス側においてさらなるコードと比較される、ユーザチャネル、及び
コードが前記非加入者識別デバイスに入力され、関連するコードが前記加入者識別デバイスに入力される、ユーザチャネル、
の群のうち１つを介して提供される、請求項１から３のいずれか一項に記載の非加入者

識別デバイス。
【請求項５】
前記非加入者識別公開鍵が、第１の非加入者識別プライベート鍵及び第２の非加入者識別プライベート鍵にそれぞれ対応する第１の非加入者識別公開鍵及び第２の非加入者識別公開鍵を含み、
前記第１の非加入者識別公開鍵が、初めに、前記帯域外チャネルを介して前記加入者識別デバイスに提供され、前記第２の非加入者識別公開鍵が、その後、前記証明書内で識別として使用される、
請求項１から４のいずれか一項に記載の非加入者識別デバイス。
【請求項６】
所定の間隔の間に前記非加入者識別デバイスからハートビートメッセージを受信しない場合に、前記コアネットワークが前記コアネットワークへの前記非加入者識別デバイスのアクセスを無効にすることを可能にするために、前記プロセッサがさらに、
前記加入者識別デバイスから前記ハートビートメッセージを受信し、前記加入者識別デバイスは、前記ハートビートメッセージを前記コアネットワークから受信すると前記ハートビートメッセージを転送し、前記プロセッサが、前記ハートビートメッセージを、前記ゲートウェイを介して前記コアネットワークに転送する、又は、
前記コアネットワークから前記ゲートウェイを介して前記ハートビートメッセージを受信し、前記ハートビートメッセージを前記加入者識別デバイスに転送し、前記加入者識別デバイスが前記ハートビートメッセージを前記コアネットワークに転送する、
請求項１から５のいずれか一項に記載の非加入者識別デバイス。
【請求項７】
前記プロセッサがさらに、多数のユーザアカウントを管理し、
それぞれのユーザアカウントに対して選択的に、複数のそれぞれの証明書を確立するために前記関連付けシーケンスを実行し、
それぞれのユーザアカウントに対して選択的に、前記それぞれの証明書に基づいて前記非加入者識別デバイスが前記コアネットワークにアクセスすることを可能にする、
請求項１から６のいずれか一項に記載の非加入者識別デバイス。
【請求項８】
非加入者識別デバイスとのワイヤレス通信のために構成された加入者識別デバイスであって、前記加入者識別デバイスが加入者識別データへのアクセスを有し、
前記加入者識別データが、コアネットワークにアクセスするためのプロバイダへの加入者の加入者識別データを備え、前記コアネットワークが、少なくとも局地的エリアにわたりモバイルデバイスにワイヤレス通信を提供し、
前記加入者識別デバイスが、
前記非加入者識別デバイスとのワイヤレス通信のために構成された送受信機と、
前記加入者識別データとの関連付けを確立するために関連付けシーケンスを実行するプロセッサと、
を備え、前記関連付けシーケンスが、
前記非加入者識別デバイスから第１の通信チャネルを介して非加入者識別公開鍵を取得することと、
前記加入者識別デバイスが前記非加入者識別公開鍵を取得したことを検証するために、第２の通信チャネルを介して前記非加入者識別デバイスと検証コードを共有することと、
前記第１の通信チャネルと前記第２の通信チャネルとが異なり、前記通信チャネルの一方が帯域外チャネルであることと、
前記第１の通信チャネル又は前記第２の通信チャネルを介して、前記非加入者識別デバイスからの前記非加入者識別公開鍵とペアを構成する非加入者識別プライベート鍵の所有の証明を受信することと、
受信された前記証明の評価が成功すると、前記加入者識別データに関係し、前記非加入者識別公開鍵の少なくとも一部分に対して証明機関によって生成された署名を備える証明

書を取得することと、
前記証明書を前記非加入者識別デバイスに送信することと、を含み、
前記証明書は、前記非加入者識別デバイスが、ローカルネットワーク及び前記ローカルネットワークと前記コアネットワークとの間のゲートウェイを介して前記コアネットワークにアクセスすることを可能にする、
加入者識別デバイス。
【請求項９】
前記加入者識別データを備える加入者識別モジュール、
前記コアネットワークとのワイヤレス通信のためのさらなる送受信機、
を備える、請求項８に記載の加入者識別デバイス。
【請求項１０】
所定の間隔の間に前記非加入者識別デバイスからハートビートメッセージを受信しない場合に、前記コアネットワークが前記コアネットワークへの前記非加入者識別デバイスのアクセスを無効にすることを可能にするために、前記プロセッサが、
前記コアネットワークから前記ハートビートメッセージを受信し、前記ハートビートメッセージを前記非加入者識別デバイスに転送する、又は
前記非加入者識別デバイスから前記ハートビートメッセージを受信し、前記ハートビートメッセージを前記コアネットワークに転送する、
請求項８又は９に記載の加入者識別デバイス。
【請求項１１】
前記非加入者識別デバイスのデータ通信が前記加入者識別デバイスを介して可能にされることを決定するために、前記プロセッサが、
前記非加入者識別デバイスと前記コアネットワークとの間の前記データ通信の特定部分を受信及び中継し、そのとき、中継されるデータの一部を前記加入者識別データに関連する鍵を使用して暗号化する、
請求項８、９、又は１０に記載の加入者識別デバイス。
【請求項１２】
前記非加入者識別デバイスが許可された範囲内にないことが判明した場合に前記コアネットワークが前記コアネットワークへの前記非加入者識別デバイスのアクセスを無効にするために、前記プロセッサが、
前記非加入者識別デバイスの位置が、前記許可された範囲内であるかどうかを判定する、又は
前記加入者識別デバイスと前記非加入者識別デバイスとの間の距離が前記許可された範囲内であるかどうかを測定する、
請求項８から１１のいずれか一項に記載の加入者識別デバイス。
【請求項１３】
加入者識別デバイスとのワイヤレス通信のため非加入者識別デバイスにおいて使用するための方法であって、前記加入者識別デバイスが、加入者識別データへのアクセスを有し、
前記加入者識別データが、コアネットワークにアクセスするためのプロバイダへの加入者の加入者識別データを備え、前記コアネットワークが、少なくとも局地的エリアにわたりモバイルデバイスにワイヤレス通信を提供し、
前記非加入者識別デバイスが、非加入者識別公開鍵とペアを構成する非加入者識別プライベート鍵を備え、
前記方法は、
前記非加入者識別公開鍵を、第１の通信チャネルを介して前記加入者識別デバイスに提供するステップと、
前記加入者識別デバイスが前記非加入者識別公開鍵を取得したことを検証するために、第２の通信チャネルを介して前記加入者識別デバイスと検証コードを共有するステップと、
前記第１の通信チャネルと前記第２の通信チャネルとが異なり、前記通信チャネルの一方が帯域外チャネルであるステップと、

前記第１の通信チャネル又は前記第２の通信チャネルを介して、前記非加入者識別プライベート鍵の所有の証明を前記加入者識別デバイスに提供するステップと、
前記加入者識別デバイスから、前記加入者識別データに関係し、前記非加入者識別公開鍵の少なくとも一部分に対して証明機関によって生成された署名を備える証明書を受信するステップと、を有し、
前記証明書は、前記非加入者識別デバイスが、ローカルネットワーク及び前記ローカルネットワークと前記コアネットワークとの間のゲートウェイを介して前記コアネットワークにアクセスすることを可能にする、
方法。
【請求項１４】
非加入者識別デバイスとのワイヤレス通信のために構成された加入者識別デバイスにおいて使用するための方法であって、前記加入者識別デバイスが加入者識別データへのアクセスを有し、
前記加入者識別データが、コアネットワークにアクセスするためのプロバイダへの加入者の加入者識別データを備え、前記コアネットワークが、少なくとも局地的エリアにわたりモバイルデバイスにワイヤレス通信を提供し、
前記方法は、
前記非加入者識別デバイスから第１の通信チャネルを介して非加入者識別公開鍵を取得するステップと、
前記加入者識別デバイスが前記非加入者識別公開鍵を取得したことを検証するために、第２の通信チャネルを介して前記非加入者識別デバイスと検証コードを共有するステップと、
前記第１の通信チャネルと前記第２の通信チャネルとが異なり、前記通信チャネルの一方が帯域外チャネルであるステップと、
前記第１の通信チャネル又は前記第２の通信チャネルを介して、前記非加入者識別デバイスからの前記非加入者識別公開鍵とペアを構成する非加入者識別プライベート鍵の所有の証明を受信するステップと、
受信された前記証明の評価が成功すると、前記加入者識別データに関係し、前記非加入者識別公開鍵の少なくとも一部分に対して証明機関によって生成された署名を備える証明書を取得するステップと、
前記証明書を前記非加入者識別デバイスに送信するステップと、を有し、
前記証明書は、前記非加入者識別デバイスが、ローカルネットワーク及び前記ローカルネットワークと前記コアネットワークとの間のゲートウェイを介して前記コアネットワークにアクセスすることを可能にする、
方法。
【請求項１５】
ネットワークからダウンロード可能な、並びに／又はコンピュータ可読媒体及び／若しくはマイクロプロセッサ実行可能媒体に記憶された、コンピュータプログラムであって、前記コンピュータプログラムが、コンピューティングデバイス上で実行されたときに請求項１３又は１４に記載の方法を実施するためのプログラムコード命令を備える、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ローカル通信プロトコルに従うローカルネットワーク内でのワイヤレス通信のために構成された非加入者識別（非ＳＩ）デバイスに関する。本発明はさらに、加入者識別（ＳＩ）デバイス及びＳＩシステムにおいて使用するための方法に関する。
【０００２】
本発明は、コアネットワーク、例えば３Ｇ、ＬＴＥ、４Ｇ又は５Ｇネットワークとも呼ばれる、少なくとも局地的エリアモバイル通信システムへのローカルワイヤレス通信デバ

イスの統合の分野に関する。コアネットワークへのアクセスは、加入者識別ＳＩと呼ばれる加入者データの組を使用して加入者のモバイルデバイスにコアネットワークへのアクセスを提供する、いわゆるプロバイダによって管理される。ＳＩは、コアネットワークにアクセスするための加入者識別データを、プロバイダへのそれぞれの加入者に対して含む。

【０００３】

一般に、そのようなローカルワイヤレス通信デバイスは、Ｗｉ－Ｆｉ（登録商標）などのローカル通信プロトコルに従ったワイヤレス通信のための機能を備えており、コアネットワークとワイヤレス通信するための送受信機ユニットは有さない。例えば、いわゆるモノのインターネットでは、様々な種類のローカルワイヤレス通信デバイス、例えば、ユーザインターフェースを持たないいわゆるヘッドレスデバイスや、タッチ画面、ディスプレイ及び／又はボタンのようなユーザインターフェースを持ついわゆるＵＩデバイスが、Ｗｉ－Ｆｉ（登録商標）を介してインターネットに接続可能である。そのため、少なくとも最初、そのようなデバイスは、コアネットワークにアクセスするために必要とされる加入者識別データ又はクレデンシャルを一切有していない。そのようなローカルワイヤレス通信デバイスは、本文献において非ＳＩデバイスと呼ばれる。

【０００４】

コアネットワークへの非ＳＩデバイスの統合は、現在、既存のコアネットワークの新世代及び拡張を定義する３ＧＰＰと呼ばれる様々な関係者間で論議されている。第３世代パートナーシッププロジェクト（３ＧＰＰ）は、Ｏｒｇａｎｉｚａｔｉｏｎａｌ Ｐａｒｔｎｅｒｓとして知られる、遠隔通信規格団体のグループ間の共同作業である。３ＧＰＰは、３ＧＰＰの用語でＵＥ又はユーザ機器と呼ばれるモバイルデバイスが、例えば他のアクセスネットワークを通じてセルラートラフィックを軽減するために、Ｗｉ－Ｆｉ（登録商標）などの非３ＧＰＰアクセスネットワークを使用してコアセルラーネットワークにアクセスできるようにするためのいくつかの機構を提案している。Ｅｖｏｌｖｅｄパケットコア又はＥＰＣと呼ばれる、４Ｇコアネットワークへの非３ＧＰＰアクセスは、特に次の３ＧＰＰ仕様、［ＴＳ ２３．４０２］（最新バージョン１５．３．０）、［ＴＳ ２４．３０２］（最新バージョン１５．３．０）及び［ＴＳ ３３．４０２］（最新バージョン１５．１．０）、で指定される。５Ｇコアネットワークへの非３ＧＰＰアクセスは、特に、特に次の３ＧＰＰ仕様、［ＴＳ ２３．５０１］（最新バージョン１５．２．０）項４．２．８、［ＴＳ２３．５０２］（最新バージョン１５．２．０）項４．１２、及び［ＴＳ２４．５０２］（最新バージョン１５．０．０）、で指定される。現在、この取り組みは、住宅ゲートウェイ（ＲＧ）の後ろ側で非３ＧＰＰデバイスをサポートすることに的を絞っているが、これは、Ｗｉ－Ｆｉ（登録商標）を各社の５Ｇネットワーク提供の一部として統合し、それらのサービス（ｍｅｔｅｒｅｄ ｖｏｉｃｅ ｏｖｅｒ Ｗｉ－Ｆｉ（登録商標）、ライブ映像サービス等）を使用したいという５Ｇセルラー事業者の需要を鑑みて、非３ＧＰＰデバイスのより汎用的なサポートに拡張される可能性がある。

【０００５】

普通、スマートフォンのようなモバイルデバイスは、コアネットワークと通信するための専用送受信機を備え、さらに加入者識別（ＳＩ）を備えている。ＳＩは、加入者の識別及びコアネットワークにアクセスするために必要とされる他のデータを表し、一方、コアネットワークの使用は、例えば音声及びデータのいわゆるバンドルを介して、プロバイダによってそれぞれの加入者に課金される。例えば、ＳＩは、ＩＭＳＩ（国際モバイル加入者識別）のような加入者識別コードを備える。そのようなデバイスは、通常、ＳＩＭと呼ばれる物理的な半導体モジュールをモバイルデバイスに挿入することによって、ＳＩを提供される。ＳＩＭカードは、国際モバイル加入者識別（ＩＭＳＩ）番号及びそれに関連する鍵をセキュアに記憶することが意図されるプラスチックカードに埋め込まれた集積回路であり、ＩＭＳＩ番号及び鍵は、モバイル電話デバイス（携帯電話やコンピュータなど）上で加入者を識別及び認証するために使用される。様々な種類モジュールやカードが知られており、例えば、ＵＳＩＭは、ユニバーサル加入者識別モジュールを指し、３Ｇコアネットワーク規格であるＵＭＴＳ（ユニバーサルモバイル遠隔通信システム）上で動作する

。関連する物理的カードは、ＵＩＣＣ（ユニバーサル集積回路カード）としても知られ、ＵＳＩＭは、ＵＩＣＣの上位で実行されるアプリケーションである。さらに他の種類のＳＩＭは、ｅ－ＳＩＭ若しくはｅＳＩＭ（埋め込みＳＩＭ）、又は埋め込みユニバーサル集積回路カード（ｅＵＩＣＣ）と呼ばれる。これは、回路基板に直接はんだ付けされた、交換不可能な埋め込みチップである。さしあたり、コアネットワークとのワイヤレス通信のための機能を備え、ＳＩＭカード又はその他を介して当初のＳＩを提供される任意種のデバイスを、本文献においてＳＩＭデバイスと呼ぶ。

【０００６】

さらに、ＳＩデータは、通常は証明書機関（ＣＡ）と呼ばれる認可サーバを使用して加入者クレデンシャルが認証及び認可される際に、コアネットワークのプロバイダの管理システムのような他の場所、例えば、加入者識別データを管理するサーバ上の加入者データベース、でも入手可能であることがある。例えば、ＳＩデータは、ユーザ名やパスワードのようなユーザクレデンシャルを使用して、又は２要素認証を使用して、インターネットを介してアプリケーションサーバ（ＡＳ）上のユーザアカウントにログインすることにより、加入者によってアクセスされることもある。ＡＳは、加入者データベース及びＣＡに結合されるか又はそれらを備える。

【０００７】

本文献において、いわゆるＳＩデバイスは、ＳＩを備えているか、又はコアネットワークの少なくとも１つのプロバイダサーバに結合されているかのいずれかである、ＳＩへのアクセスを有するローカルデバイスであり、サーバはＳＩデータを管理するように構成される。ＳＩデバイスは、非ＳＩデバイスと通信するように構成され、ＣＡへのアクセスを有する。ＳＩデバイスの第１の例は、加入者データベースを記憶する１つ又は複数のサーバとコアネットワークを介して通信するために構成され、一方で非ＳＩデバイスと通信するようにも構成されたＳＩＭデバイスである。ＳＩデバイスのさらなる例は、非ＳＩデバイスと通信するためのユーザインターフェース（ＵＩ）デバイスであり、ＵＩデバイスはさらに、コアネットワークを介してサーバ上のＳＩデータ及びＣＡにアクセスするように構成され、ここで、加入権所有者は、ＳＩデータへのアクセスを得るためにログインしなければならない。別の例は、ローカルネットワークを介して非ＳＩデバイスと通信するように構成されたＵＩデバイスであり、一方で、ＵＩデバイスはさらに、インターネットへの接続を介してサーバ上のＳＩデータ及びＣＡにアクセスするように構成される。ＳＩシステムは、ローカルネットワーク内でのワイヤレス通信のためのローカルアクセスポイントに結合された、サーバベースの管理システム、及びコアネットワークのそれぞれのデータサーバに適正に結合された、上記で定義されたＳＩＭデバイス又はＵＩデバイスを含むことがある。

【背景技術】

【０００８】

非３ＧＰＰデバイスが４Ｇ／５Ｇコアネットワークに接続することを可能にするための可能なシステム及び方法は、Ｈｏｔｓｐｏｔ２．０技術仕様［ＨＯＴＳＰＯＴ］に定義されるＨｏｔｓｐｏｔ２．０（別称Ｗｉ－Ｆｉ（登録商標） Ｃｅｒｔｉｆｉｅｄ Ｐａｓｓｐｏｉｎｔ）を使用して、事業者がデバイスに例えばＸ．５０９証明書を具備できるようにすることによるものである。しかし、多くのデバイスは、事業者によって制御されることができず、また人々の住宅にある他の基本的なＷｉ－Ｆｉ（登録商標）のみのデバイスをどのように４Ｇ／５Ｇコアネットワークにアクセスさせることができるかは明確でない。

【０００９】

文献米国特許第９６４８０１９（Ｂ２）号は、非ＳＩＭデバイスに関するＷｉ－Ｆｉ（登録商標）統合について記載する。提案されるシステムは、非３ＧＰＰデバイスが４Ｇ／５Ｇコアネットワークに接続することを可能にする。アプリケーションサーバ（ＡＳ）は、非加入者識別モジュール（非ＳＩＭ）デバイスが第２のネットワーク（例えばＷｉ－Ｆｉ（登録商標））を介して第１のネットワーク（例えばモバイル又は３ＧＰＰネットワーク）にアクセスするのを可能にするために使用されることが可能であり、ここで、非ＳＩ

ＭデバイスはＳＩＭデバイスと関連付けられ、ＡＳは、ＳＩＭデバイスから、ＳＩＭデバイスとそれに関連付けられた非ＳＩＭデバイスとに関する情報を受信する。ＳＩＭデバイスと非ＳＩＭデバイスとの間の関連付けは、ＳＩＭデバイスから受信される情報に基づいてＡＳによって作成される。非ＳＩＭデバイスとＳＩＭデバイスとの間の関連付けは、加入者データベースに記憶される。

【００１０】

その後、第２のネットワークを介して第１のネットワークにアクセスするために、非ＳＩＭデバイスからの第１のネットワークに対する認可の要求に基づいて、システムは、非ＳＩＭデバイスに関連付けられた識別を取得し、非ＳＩＭデバイスのユーザに関連付けられたユーザプロファイルを求める要求を加入者データベースに送信し、この要求は、取得された非ＳＩＭデバイスの識別を含む。次いで、システムは、加入者データベースから、非ＳＩＭデバイスに対応する要求されるユーザプロファイルを受信し、非ＳＩＭデバイスに対応する要求されるユーザプロファイルは、ＳＩＭデバイスに関連付けられている。受信されたユーザプロファイルに基づいて、システムは、非ＳＩＭデバイスが第２のネットワークを介して第１のネットワークにアクセスすることを認可する。そのため、非ＳＩＭデバイスとＳＩＭデバイスとの間の関連付けが確立されて加入者データベースに記憶された後、非ＳＩＭデバイスは、第１のネットワークにアクセスしたいときに、第１のネットワークにアクセスする認可を得ることができる。

【００１１】

米国特許第９６４８０１９（Ｂ２）号では、図１ｂの説明が、３ＧＰＰの文献［ＴＳ２３．４０２］、特に、図４．２．２－１及び図４．２．２－２による非ローミング事例並びにそれらの図に示されるノード及びリンクの説明、並びに例えば［ＴＳ２３．４０２］の節７におけるそれらのノード及びリンクをどのように使用するか、に対応している。［ＴＳ　２３．４０２］の図４．２．３－１～図４．２．３－５は、ローミング事例を示している。非ＳＩＭデバイスは、ノード「信頼できる非３ＧＰＰ　ＩＰアクセス」又はノード「信頼できない非３ＧＰＰ　ＩＰアクセス」を通じて第１のネットワークにアクセスすることができる。

【発明の概要】

【発明が解決しようとする課題】

【００１２】

米国特許第９６４８０１９（Ｂ２）号では、どのようにしてＳＩＭデバイスが非ＳＩＭデバイスの識別を確実に取得するか、又はどのようにしてＳＩＭデバイスが取得された識別に対する信頼性を得ることができるかは説明されていない。信頼性の欠如は、攻撃者がＳＩＭデバイスを使用（悪用）することによって自身のデバイスをモバイルネットワーク又は３ＧＰＰネットワークにアクセスさせる道を開く可能性がある。また、非ＳＩＭデバイスとＳＩＭデバイスとの間の関連付けが確立された後、非ＳＩＭデバイスはＳＩＭデバイスから独立して動作することができる。非ＳＩＭデバイスはハッキングに対してより脆弱であるため、非ＳＩＭデバイスがコアセルラーネットワークに接続することを可能にするクレデンシャルが盗まれる可能性があり、その後、ハッカーはその情報を使用してコアネットワークへのアクセスを得、ＳＩＭデバイスのユーザの加入に課金する可能性がある。

【００１３】

本発明の目的は、非ＳＩデバイスに対してコアネットワークへのワイヤレスアクセスを確実に設定するためのシステムを提供することである。

【課題を解決するための手段】

【００１４】

この目的のために、添付の特許請求の範囲に定められるようにデバイス及び方法が提供される。本発明の一態様によれば、請求項１に定められるように非ＳＩデバイスが提供される。本発明のさらなる態様によれば、請求項８に定められるようにＳＩデバイスが提供される。本発明のさらなる態様によれば、請求項１３及び１４に定められるように方法が提供される。本発明のさらなる態様によれば、ネットワークからダウンロード可能な、並

びに／又はコンピュータ可読媒体及び／若しくはマイクロプロセッサ実行可能媒体に記憶されたコンピュータプログラム製品が提供され、この製品は、コンピュータ上で実行されたときに、上記方法を実施するためのプログラムコード命令を備える。

【００１５】

上記の非ＳＩデバイスは、ローカル通信プロトコルに従うローカルネットワーク内でのワイヤレス通信のために構成される。ローカル通信プロトコルは、プロトコルメッセージと、限られたエリアにわたるワイヤレス送受信とを定義する。加入者識別（ＳＩ）は、コアネットワークにアクセスするための加入者の加入者識別データを備え、コアネットワークは、少なくとも局地的エリアにわたりモバイルデバイスにワイヤレス通信を提供する。非ＳＩデバイスはＳＩを備えておらず、ＳＩへのアクセスを有するＳＩデバイスと協働するために構成される。非ＳＩデバイスは、ローカル通信プロトコルに従うローカル送受信のために構成された送受信機と、ＳＩとの関連付けを確立するために関連付けシーケンスを実行するように構成されたプロセッサと、を備える。関連付けシーケンスは、非ＳＩ公開鍵とペアを構成する非ＳＩプライベート鍵を記憶することと、非ＳＩ公開鍵を、第１の通信チャネルを介してＳＩデバイスに提供することと、ＳＩデバイスが非ＳＩ公開鍵を取得したことを検証するために、第２の通信チャネルを介してＳＩデバイスと検証コードを共有することと、を含む。第１の通信チャネルと第２の通信チャネルとは異なり、一方のチャネルとして帯域外（ＯＯＢ）チャネルを備える。関連付けシーケンスは、第１の通信チャネル又は第２の通信チャネルを介して、非ＳＩプライベート鍵の所有の証明をＳＩデバイスに提供することと、その後ＳＩデバイスから証明書を受信することとをさらに含む。証明書は、通常はクレデンシャルと呼ばれる、ＳＩに関係するデータを備える。

【００１６】

証明書は、非ＳＩ公開鍵の少なくとも一部分に対して証明機関（ＣＡ）によって生成された署名を含む。このコンテキストにおいて、証明書は、証明書の所有者が、その時点ではＳＩに関係付けられた非ＳＩ公開鍵及びプライベート鍵に基づいてコアネットワークを使用する権利を有することの、確証された証明を構成する。

【００１７】

署名は、例えば、ＣＡによって生成された、非ＳＩ公開鍵の少なくとも一部分に対する従来の署名である。加えて、ＳＩに関係するクレデンシャルは、非ＳＩ公開鍵の少なくとも一部分を使用して暗号化されてよい。例えば、クレデンシャルは、ユーザ名／パスワードの組み合わせ、又はパスワードのみであり、少なくともパスワードは暗号化され、ユーザ名は暗号化されないままであってよい。非ＳＩデバイスは、例えば署名の出所がＣＡであることを検証することにより、又は証明の正しさを検証することにより、署名を検証し、さらに暗号化されたクレデンシャルを、非ＳＩプライベート鍵を用いて解読してもよい。

【００１８】

クレデンシャルは、アプリケーションサーバ、ＣＡ及び／又は加入者データベースを介して先に生成されたものであり、例えば加入者データベースに記憶される。クレデンシャルは、ＣＡによって取り出され、ＳＩデバイスに送られる前に非ＳＩ公開鍵で暗号化される。クレデンシャルは、非ＳＩデバイスが、ローカルネットワーク及びローカルネットワークとコアネットワークとの間のゲートウェイを介してコアネットワークにアクセスすることを可能にする。クレデンシャルの暗号化は、非ＳＩデバイスが非ＳＩプライベート鍵を知っている唯一のデバイスであるため、追加的なセキュリティを提供する。そのため、非ＳＩデバイスは、暗号化されたクレデンシャルを解読することのできる唯一のデバイスであり、そのため、クレデンシャルを使用してコアネットワークにアクセスすることができる。さらに、非ＳＩ公開鍵の少なくとも一部分を用いて少なくとも一部のクレデンシャルを暗号化することは、クレデンシャルを暗号化するための他の鍵の使用を排除しない。

【００１９】

証明書は、署名を検証した後、非ＳＩデバイスが、ローカルネットワーク及びローカルネットワークとコアネットワークとの間のゲートウェイを介してコアネットワークにアクセスすることを可能にする。

【００２０】
上記の関連付けシーケンスは、非ＳＩデバイスにおいて使用するための方法として、例えばいわゆるアプリ内のソフトウェア内で、実施されてもよい。
【００２１】
上記のＳＩデバイスは、上記の非ＳＩデバイスとのワイヤレス通信のために構成される。ＳＩデバイスは、例えばデバイスがＳＩＭを含んでいるか若しくはＳＩＭに結合され得るため、又はＳＩを含んでいるサーバにネットワークを介してアクセスするように構成されているため、加入者識別データへのアクセスを有する。ＳＩデバイスは、非ＳＩデバイスとのワイヤレス通信のために構成された送受信機と、ＳＩとの関連付けを確立するために関連付けシーケンスを実行するように構成されたプロセッサと、を備える。ＳＩデバイスにおける関連付けシーケンスは、非ＳＩデバイスから第１の通信チャネルを介して非ＳＩ公開鍵を取得することと、第２の通信チャネルを介して非ＳＩデバイスと検証コードを共有することと、を含む。ＳＩデバイスにおける関連付けシーケンスは、第１の通信チャネル又は第２の通信チャネルを介して、非ＳＩデバイスからの非ＳＩ公開鍵とペアを構成する非ＳＩプライベート鍵の所有の証明を受信することをさらに含む。受信された証明の評価が成功すると、関連付けシーケンスは、上記の証明書を取得し、証明書を非ＳＩデバイスに送信することによって継続する。この関連付けシーケンスは、ＳＩデバイスにおいて使用するための方法内で実施されてもよい。
【００２２】
上記の特徴は、以下の効果を有する。非ＳＩデバイスにおいて、非ＳＩプライベート鍵は、ペアにされた非ＳＩ公開鍵に基づいて関連付けシーケンスを実行する際に使用するために入手可能でなければならない。そのため、プロセッサは、鍵がすでに記憶されているメモリにアクセスするか、又は最初に生成するか、又はその他の形で鍵ペアを取得し、一方、非ＳＩプライベート鍵はその後、関連付けシーケンス中に使用するために記憶される。
【００２３】
非ＳＩ公開鍵は、第１の通信チャネルを介してＳＩデバイスに転送され、一方、検証コードは、ＳＩデバイスが非ＳＩ公開鍵を取得したことを検証するために、第２の異なる通信チャネルを介してＳＩデバイスと共有される。そのため、非ＳＩデバイスは、ＳＩデバイスへの前記第１及び第２の通信チャネルを確立するように構成され、これらのチャネルは、１つのＯＯＢチャネルを含み、両方とも独立して設定される。このコンテキストにおいて、通信チャネルは、無線送信などの物理的機構を介したデータリンク、又は表示及びスキャンされる視覚的情報、又はユーザによって読み取られ、比較されるコード、又はユーザによって読み取られ、手動で入力されるコード、又は両方のデバイスに手動で入力されるコードである。各チャネルは、チャネルの終点、この場合は非ＳＩデバイスとＳＩシステム、の間でデータを転送する。一方のチャネルは、例えば、非ＳＩデバイスとＳＩデバイスとの間でプロトコルメッセージを交換することにより、ローカル通信ネットワークを介して作成されるワイヤレスチャネルである。別の例は、ローカル通信ネットワークではなく、Ｂｌｕｅｔｏｏｔｈ（登録商標）又は別個のＷｉ－Ｆｉ（登録商標）ネットワークのような何らかの他のワイヤレス通信プロトコルを使用するワイヤレスチャネルである。他方のチャネルは、無線送信のために何らかの周波数帯を使用する前記１つのワイヤレスチャネルに対して帯域外（ＯＯＢ）チャネルである。そのため、ＯＯＢチャネルは、前記１つのワイヤレスチャネルとは異なる物理的機構、例えばユーザによる視覚的又は手動のデータ入力、を使用している。チャネルの少なくとも１つは、統合されることが意図される非ＳＩデバイスが、それぞれのチャネルの物理的終点を構成するＳＩデバイスから限られた範囲内にあることをユーザが検証することを可能にするように、限られた範囲を有する物理的機構を介して作成される。様々な例が後に提供される。
【００２４】
２つの異なる通信チャネルを適用し、チャネルの一方がＯＯＢチャネルであることは、非ＳＩデバイスが限られた範囲内に、すなわち第１及び第２の通信チャネル両方の通信範囲内にあることを確実に保証するという利点を有する。ＯＯＢチャネルを有利に使用する

と、悪意のある中間パーティーがすべてのワイヤレス通信を検出し、その通信を操作して、アクセス権及び／又はユーザデータトラフィックを取得又は変更すること、いわゆる中間者攻撃が回避される。また、ＯＯＢチャネルは、非ＳＩデバイスを関与させるユーザ対話を必要とし、このことは、加入者のクレジット又は音声／データバンドルを使用するために、意図される非ＳＩデバイスが実際にユーザの加入者識別（ＳＩ）に結合されているという確認を有利にユーザに提供する。

【００２５】

検証コードは、ＳＩデバイスが意図されるように非ＳＩ公開鍵を取得したことを非ＳＩデバイスが検証することを可能にする。実質的に、検証コードは、予め定められたプロトコルに従って送信者が意図される非ＳＩデバイスと実際に結合されている、又はそれと通信状態にあるという証明を表す。そのようなプロトコルに従って動作する通信チャネルを介してそのようなコードを共有するために多数の変形例がある。このコンテキストにおいて使用される単語「共有する」は、非ＳＩデバイスとＳＩデバイスとの間で通信チャネルを通じて検証コードを転送するための任意の方式を包含する。例えば、非ＳＩ公開鍵は、ＯＯＢチャネルであるワイヤレスチャネル、例えばＢｌｕｅｔｏｏｔｈ（登録商標）又はＮＦＣ、を通じて送られ、それらはこのコンテキストにおいて、他方の通信チャネルとは異なる送信帯を使用するので、ＯＯＢである。検証コードは、第２のワイヤレスチャネルを通じて、例えばＷｉ－Ｆｉ（登録商標）を介して、通じて送り返される。代替として、非ＳＩ公開鍵は、ワイヤレスチャネルを介して転送され、非ＳＩデバイスによって生成された検証コードは、ユーザを関与させるＯＯＢチャネルを介して転送される。例えば、検証コードは、例えばディスプレイ又はオーディオ信号を介してユーザに通信され、一方、ユーザは、同じコードを、例えばキーボードを介して、ＳＩデバイスに入力しなければならない。又は、その逆に、コードがＳＩデバイスに表示され、それが非ＳＩデバイスにおいて入力される。また、検証コードは、非ＳＩデバイスとＳＩデバイスの両方によって表示されてもよく、一方、確定は、例えばボタンを押す又はアイコンをクリックすることにより、一方の側又は両方の側で入力されなければならない。また、検証コードは、ユーザが知っている又は生成しなければならないコードであってもよく、そのコードが後に両方の側で入力されなければならない。

【００２６】

検証コードは、ＳＩデバイスによって取得された非ＳＩ公開鍵のハッシュであってよい。検証コードは、非ＳＩ公開鍵自体であるか、又はそれを含んでもよい。検証コードは、デバイス又はユーザの一方によって生成される任意の数値コード、パスワード又はパスフレーズであってもよい。第１の例は、送信者がプロトコルに従って正しい非ＳＩ公開鍵を取得したことの証明を定義する。例えば、非ＳＩ公開鍵は、ＱＲコード（登録商標）をスキャンすることによりＳＩデバイスによって取得される。そのようなスキャンは、ＯＯＢチャネル（この場合は一方向の通信チャネル）を構成し、ＳＩデバイスは、検証コードとして、非ＳＩ公開鍵自体、及び／又はそのハッシュを、Ｗｉ－Ｆｉ（登録商標）（他方の通信チャネル）を介して、非ＳＩデバイスに送る。そのため、非ＳＩデバイスは、Ｗｉ－Ｆｉ（登録商標）を通じて自身と通信しているデバイスが、たった今自身の非ＳＩ公開鍵をスキャンしたことを知る。代替として、非ＳＩ公開鍵は、Ｗｉ－Ｆｉ（登録商標）を介して転送され、一方、検証コードは、ＯＯＢチャネルを使用して（例えばコードを手動で入力することにより）ＳＩデバイスから再度非ＳＩデバイスに転送され、これは、この一方向の通信チャネルを介して非ＳＩデバイスに同じ確証を与える。

【００２７】

非ＳＩプライベート鍵の所有の証明は、例えば、ローカル通信ネットワーク、第１若しくは第２の通信チャネル、又はさらなるネットワークを介して、ＳＩデバイスに転送される。パーティーに対するプライベート鍵の所有の証明は、そのパーティーからのデータをプライベート鍵で暗号化することによって行われる。他方のパーティーは、暗号化されたデータを対応する公開鍵で解読し、結果が提供されたデータと同じであるかどうかを調べることにより、結果を調べることができる。他方のパーティーはまた、プライベート鍵の

所有を証明しなければならないデバイスの公開鍵で何かを暗号化し、暗号化された結果を送り、デバイスに、それを解読して結果を戻すことによってプライベート鍵の所有を証明するように求める。プライベート鍵の所有の証明は、例えばＳＳＬ、ＴＬＳ及びＤＰＰ認証プロトコルで行われるように、デバイス同士が、１つ又は複数の公開鍵を交換することにより、セキュアチャネルを設定するときにも行われる。このようにして、非ＳＩデバイス及びＳＩデバイスは、非ＳＩ公開鍵に基づいて、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、又はローカルネットワークのようなネットワークを通じてセキュアチャネルを設定することができる。所有の証明は、非ＳＩデバイスが実際に非ＳＩ鍵ペアの所有者であることを、確実にＳＩデバイスに対して保証する。

【００２８】

証明書は、コアネットワークを使用し、コアネットワークのプロバイダに対してユーザを識別するために必要とされるデータを表す。証明書は、その認可を表す証明機関ＣＡによって発行されたセキュリティデータを含んでよく、このコンテキストにおいて、コアネットワークにとって既知の加入者のＳＩに関連付けられた状態で、コアネットワークを使用する権利を担保する。証明書は、非ＳＩ公開鍵の少なくとも一部分に対してＣＡによって生成された署名を含む。基本的な形態において、署名は、非ＳＩ公開鍵に対して、若しくは非ＳＩ公開鍵の一部分に対してＣＡによって算出された署名、又は非ＳＩ公開鍵の何らかの部分の署名されたバージョンである。

【００２９】

証明書は、ＳＩに関係するクレデンシャルをさらに含んでよく、このクレデンシャルは、非ＳＩデバイスがコアネットワークにアクセスすることを可能にする。そのようなクレデンシャルは、ＳＩに関係し、（少なくとも部分的に）非ＳＩ公開鍵に基づくか又はそれから導出される。３ＧＰＰに従って管理されるコアネットワークでは、クレデンシャルは３ＧＰＰクレデンシャルと呼ばれることがある。証明書は、コア識別コード、ＩＭＥＩ（国際モバイル機器識別）のようなデバイスコード、又はＩＭＳＩ（国際モバイル加入者識別）のような加入者識別コードのような、さらなるコアネットワークデータを含んでよい。また、証明書は、加入者名、公開鍵及び関連付けられたプライベート鍵の所有者、その者のアドレス等のような、他の情報も含んでよい。証明書は、ローカルネットワークを介してすでに確立されているセキュアチャネルを使用して非ＳＩデバイスに転送される。

【００３０】

証明書を受信すると、非ＳＩデバイスは証明書を調べる。例えば、ＣＡの公開検証鍵を使用し、同時に証明書内の非ＳＩ公開鍵の少なくとも一部分及び／又は非ＳＩ公開鍵の自身のコピーを使用して、証明書の署名を調べる。クレデンシャル、又はさらなるコアネットワークデータは、例えば非ＳＩ公開鍵を使用して、少なくとも部分的に、暗号化され、一方、非ＳＩデバイスは、非ＳＩプライベート鍵を使用しながら解読することにより証明書を検証する。

【００３１】

証明書は、非ＳＩデバイスが、ローカルネットワーク及びローカルネットワークとコアネットワークとの間のゲートウェイを介してコアネットワークにアクセスすることを可能にする。実際には、非ＳＩデバイスは、異なる場所にある様々なゲートウェイを使用して、コアネットワークを通じて通信してよい。ゲートウェイは、ローカルネットワーク側、例えばＷｉ－Ｆｉ（登録商標）、におけるプロトコル及びメッセージを、コア通信プロトコルに従って、コアネットワーク側の対応するメッセージに変換する。

【００３２】

デバイスが、アクセスの認可を受けるために証明書を使用するとき、コアネットワークは、様々な面でデバイスを認証することを試みる。例えば、コアネットワークは、証明書の署名を調べて、それが正しく署名されているかどうかを調べ、証明書がＣＡによって署名されているかどうかを調べる。さらに、コアネットワークは、非ＳＩ公開鍵に対応する非ＳＩプライベート鍵を所有していることを証明するようにデバイスに要求する。署名が正しい場合、又は前記証明を受信し、その検証が成功した場合、コアネットワークは、非

ＳＩ公開鍵又はさらなるコアネットワークデータの一部分などの、非ＳＩデバイスによって提供された識別データを使用して、加入者データベースを検索して、この識別がネットワークにアクセスする権利を有するかどうかを調べる。例えば、ＳＩに対して使用料が支払われると、非ＳＩデバイスとＳＩとの間の関連付けにより、非ＳＩデバイスによるコアネットワークの使用が加入者に課金される。非ＳＩデバイスと加入者との間のリンクを定義する関連付けデータは、コアネットワークのデータベースに記憶される。

【００３３】

デバイスが、アクセスの認可を受けるために、クレデンシャル、例えばユーザ名／パスワードの組み合わせ、又は識別及び秘密鍵を使用するとき、コアネットワークは、供給されたユーザ名／パスワードの組み合わせがネットワークに既知であり、正しいかどうかを調べることにより、デバイスを認証することを試みる。パスワードは、この目的のために平文でネットワークに送られてよいが、ネットワークによって供給されたノンスのような他の情報を用いてハッシュ化する前に連結されたパスワードに対するハッシュも、ネットワークに送られてよい。クレデンシャルが識別及び秘密鍵を含む場合、ネットワークは、デバイスの識別を供給し、秘密鍵で算出を行い、その結果をネットワークに送るようにデバイスに求め、この結果は、次いで、ネットワークにより正しさが調べられ得る。認証が行われて成功した場合、コアネットワークは、非ＳＩデバイスによって提供されたユーザ名又は識別データを使用して、加入者データベースを検索して、この識別がネットワークにアクセスする権利を有するかどうかを調べる。

【００３４】

一実施形態では、関連付けシーケンスは、

－　非ＳＩデバイスがサーバとして機能する、セキュアソケット層（ＳＳＬ［ＲＦＣ　６１０１］）プロトコル若しくはトランスポート層セキュリティ（ＴＬＳ［ＲＦＣ　５２４６］）プロトコルであって、非ＳＩデバイスが、自己署名された証明書の中で非ＳＩ公開鍵を提供し、この証明書をサーバ証明書メッセージ内でサーバ証明書として使用する、セキュアソケット層プロトコル若しくはトランスポート層セキュリティプロトコル、又は

－　非ＳＩデバイスがクライアントとして機能する、ＳＳＬ若しくはＴＬＳプロトコルであって、非ＳＩデバイスが、クライアントによって認証されたハンドシェイクの際に、自己署名された証明書の中で非ＳＩ公開鍵を提供する、ＳＳＬ若しくはＴＬＳプロトコル、又は

－　非ＳＩ公開鍵若しくは非ＳＩプライベート鍵が使用される公開鍵暗号化によって設定されたインターネットプロトコルセキュリティ（ＩＰｓｅｃ［ＲＦＣ　４３０１］）トンネル、又は

－　デバイスプロビジョニングプロトコル（ＤＰＰ［ＤＰＰ］）認証プロトコルであって、非ＳＩデバイスが、非ＳＩ公開鍵又はさらなる非ＳＩ公開鍵をＤＰＰブートストラップ鍵として又はＤＰＰプロトコル鍵として提供する、デバイスプロビジョニングプロトコル認証プロトコル、

を利用することにより、第１及び第２の通信チャネルのうち他方のチャネルとしてセキュアチャネルを提供することを含む。実質的に、セキュアチャネルは、非ＳＩデバイスとＳＩデバイスとの間に提供され、両デバイス間の他方のチャネルはＯＯＢチャネルである。有利には、異なる、独立したチャネルは、非ＳＩデバイスが、関連付けられることが意図されるデバイスであるという安心感をユーザに提供する。セキュアチャネルを、上述の方式で、又は他のプロトコルを使用して設定することにより、非ＳＩデバイスは、非ＳＩプライベート鍵の所有もＳＩデバイスに証明していることになる。

【００３５】

一実施形態では、証明書を前記受信することは、セキュアチャネルを介して証明書を受信することを含む。有利には、任意のクレデンシャルを含む証明書は、制御可能かつセキュアに非ＳＩデバイスに送達され、この非ＳＩデバイスは、関連付けられることが意図されるデバイスである。

【００３６】

一実施形態では、ＯＯＢチャネルは、
－　ＮＦＣ又はＢｌｕｅｔｏｏｔｈ（登録商標）のような短距離無線通信プロトコル、
－　非ＳＩデバイス側においてバーコード又はＱＲコード（登録商標）のような視覚的コードを使用し、ＳＩデバイス側においてスキャナ又はカメラを使用する、視覚的チャネル、
－　ＳＩデバイス側においてコードが表示され、そのコードが非ＳＩシステム側において入力される、ユーザチャネル、
－　非ＳＩデバイス側においてコードが表示され、そのコードがＳＩシステム側において入力されるか、又はＳＩデバイス側においてさらなるコードと比較される、ユーザチャネル、及び
－　コードが非ＳＩデバイスに入力され、関連するコードがＳＩデバイスに入力される、ユーザチャネル、
の群のうち１つを介して提供される。ＯＯＢチャネルに関する様々なオプションは、ローカルネットワークを介する上記のセキュアチャネルと大幅に異なり、それから独立している。

【００３７】

一実施形態では、非ＳＩ公開鍵は、第１の非ＳＩプライベート鍵及び第２の非ＳＩプライベート鍵にそれぞれ対応する第１の非ＳＩ公開鍵及び第２の非ＳＩ公開鍵を含み、
－　第１の非ＳＩ公開鍵は、初めに、ＯＯＢチャネルを介してＳＩデバイスに提供され、第２の非ＳＩ公開鍵が、その後、証明書内で識別として使用される。有利には、第２の非ＳＩ公開鍵は、証明書内で識別として使用するために一意であり、一方、第１の非ＳＩ公開鍵は、例えばデバイスの筐体又はマニュアルに印刷されているので、自由に配布されても固定されてもよい。

【００３８】

一実施形態では、非ＳＩデバイス内のプロセッサは、
所定の間隔の間に非ＳＩデバイスからハートビートメッセージを受信しない場合に、コアネットワークが、コアネットワークへの非ＳＩデバイスのアクセスを無効にすることを可能にするために、
－　ＳＩデバイスからハートビートメッセージを受信し、ＳＩデバイスは、ハートビートメッセージをコアネットワークから受信するとハートビートメッセージを転送し、プロセッサがハートビートメッセージを、ゲートウェイを介してコアネットワークに転送する、又は、
－　コアネットワークからゲートウェイを介してハートビートメッセージを受信し、ハートビートメッセージをＳＩデバイスに転送し、ＳＩデバイスがハートビートメッセージをコアネットワークに転送する、ためにさらに構成される。有利には、ハートビートメッセージは、ＳＩデバイスが、非ＳＩデバイスによるＳＩの使用に同意することの証明を提供する。

【００３９】

一実施形態では、非ＳＩデバイス内のプロセッサは、多数のユーザアカウントを管理し、
－　それぞれのユーザアカウントに対して選択的に、複数のそれぞれの証明書を確立するために関連付けシーケンスを実行し、
－　それぞれのユーザアカウントに対して選択的に、それぞれの証明書に基づいて非ＳＩデバイスがコアネットワークにアクセスすることを可能にする
ためにさらに構成される。有利には、複数の関連付けは、それぞれのユーザアカウントに対して提供される。

【００４０】

本発明に係る方法は、コンピュータによって実施される方法としてコンピュータ上で、又は専用ハードウェア内で、両者の組み合わせとして実施される。本発明に係る方法の実行可能コードは、コンピュータプログラム製品に記憶されてよい。コンピュータプログラム製品の例は、メモリスティックなどのメモリデバイス、光学ディスクなどの光学記憶装置、集積回路、サーバ、オンラインソフトウェア等を含む。

【００４１】
非一時的形態のコンピュータプログラム製品は、前記プログラム製品がコンピュータ上で実行されたときに本発明に係る方法を実行するためのコンピュータ可読媒体に記憶された非一時的なプログラムコード手段を備える。一実施形態では、コンピュータプログラムは、コンピュータプログラムがコンピュータ上で実行されたときに本発明に係る方法のすべてのステップ又は段階を実行するようになされたコンピュータプログラムコード手段を備える。好ましくは、コンピュータプログラムは、コンピュータ可読媒体上に具現化される。ネットワークからダウンロード可能な、並びに／又は揮発性コンピュータ可読媒体及び／若しくはマイクロプロセッサ実行可能媒体に記憶された、一時的形態のコンピュータプログラム製品も提供され、この製品は、コンピュータ上で実行されたときに、上記方法を実施するためのプログラムコード命令を備える。
【００４２】
本発明の別の態様は、一時的形態のコンピュータプログラムをダウンロードのために利用可能にする方法を提供する。この態様は、コンピュータプログラムが、例えばＡｐｐｌｅのＡｐｐ Ｓｔｏｒｅ、Ｇｏｏｇｌｅの Ｐｌａｙ Ｓｔｏｒｅ、又はＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ Ｓｔｏｒｅにアップロードされるとき、及びコンピュータプログラムがそのようなストアからダウンロードに利用可能であるときに使用される。
【００４３】
本発明に係るデバイス及び方法のさらなる好ましい実施形態が、添付の特許請求の範囲に与えられ、その開示内容は参照により本明細書に組み込まれる。
【００４４】
本発明のこれら及び他の態様は、例として以下の説明に説明され、添付図面を参照して説明される実施形態をさらに参照することから明らかになり、解説される。
【図面の簡単な説明】
【００４５】
【図１】ワイヤレス通信のための非ＳＩデバイス及びＳＩデバイス並びにＯＯＢ通信チャネルの確立を示す図である。
【図２】ワイヤレス通信のための非ＳＩデバイス及びＳＩデバイスを示す図である。
【図３】ワイヤレス通信のための非ＳＩデバイス及びＵＩデバイスを示す図である。
【図４】ワイヤレス通信のための非ＳＩデバイス及びＵＩデバイスのさらなる例を示す図である。
【図５】ＳＩデバイスとのワイヤレス通信のために構成された非ＳＩデバイスにおいて使用するための方法を示す図である。
【図６】非ＳＩデバイスとのワイヤレス通信のために構成されたＳＩデバイスにおいて使用するための方法を示す図である。
【図７ａ】コンピュータ可読媒体を示す図である。
【図７ｂ】プロセッサシステムの概略的表現である。
【発明を実施するための形態】
【００４６】
図は、純粋に図式的なものであり、実際の縮尺では描かれていない。図において、すでに説明された要素に対応する要素は、同じ参照符号を有することがある。
【００４７】
図１は、ワイヤレス通信のための非ＳＩデバイス及びＳＩデバイス並びにＯＯＢ通信チャネルの確立を示す。通信システム１００において、非加入者識別（非ＳＩ）デバイス１２０が、ローカル通信プロトコルに従ったローカルネットワーク内のワイヤレス通信のために構成される。例えばＷｉ－Ｆｉ（登録商標）などのローカル通信プロトコルは、プロトコルメッセージと、限られたエリアにわたるワイヤレス送受信とを定義し、このエリアはＷｉ－Ｆｉ（登録商標）送受信機の無線送信範囲に制限されている。
【００４８】
ＳＩシステムとも呼ばれるそのような通信システムでは、加入者識別（ＳＩ）は、コア

ネットワークにアクセスするための加入者の加入者識別データを備え、コアネットワークは、少なくとも局地的エリアにわたってモバイルデバイスにワイヤレス通信を提供する。導入部で解説されたように、コアネットワークは、非ＳＩデバイスが、Ｗｉ－Ｆｉ（登録商標）などのローカルネットワークを使用して、例えばＥｖｏｌｖｅｄパケットコア又はＥＰＣと呼ばれる４Ｇコアネットワークにアクセスすることにより、コアセルラーネットワークにアクセスするのを可能にするための、３ＧＰＰによって提案される拡張を有する３Ｇ、ＬＴＥ、４Ｇ又は５Ｇセルラーコアネットワークであってよい。

【００４９】

図１は、非ＳＩデバイス１２０とＳＩデバイス１１０との間の通信チャネルを提供するためのワイヤレス通信１３０を概略的に示す。そのようなＳＩシステムは、限られたエリアにわたる通信のための少なくとも１つのローカルワイヤレス通信ネットワークと、少なくとも局地的エリアにわたるモバイルデバイスのための少なくとも１つのコアネットワークワイヤレス通信とを有する。コアネットワークは、例えば加入者データベース及び請求書発行を管理するために、少なくとも１つのプロバイダによって管理される。ＳＩシステムは、以下の要素：

－　加入者識別データを備える少なくとも１つの加入者識別モジュール（ＳＩＭ）、

－　ＳＩＭと、コアネットワークと通信するために構成された送受信機とを備える少なくとも１つのＳＩＭデバイス、

－　プロバイダ側における関連付けシーケンスを可能にするために構成されたアプリケーションサーバ（ＡＳ）、

－　プロバイダ側で、コアネットワークの使用に関する加入者データを記憶するための加入者データベース、

－　非ＳＩ公開鍵に、又はその中にある非ＳＩ公開鍵で証明書に、署名をするために構成された証明機関（ＣＡ）、又は

－　ユーザクレデンシャルに基づいて、インターネット等を介して加入者識別データ及び加入者クレデンシャルにアクセスし、それらを提供するために構成されたユーザサーバ

の任意の組み合わせを含む。

【００５０】

非ＳＩデバイス１２０は、最初ＳＩを有しておらず、ＳＩへのアクセスを有するＳＩデバイス１１０と協働するために構成される。非ＳＩデバイスは、ローカル通信プロトコルに従うローカルな送受信のために構成された送受信機１２１と、ＳＩとの関連付けを確立するために関連付けシーケンスを実行するように構成されたプロセッサ１２２とを有する。

【００５１】

プロセッサ１２２は、例えばローカルネットワークを介して、ＳＩデバイスにワイヤレスチャネルを提供するように構成される。しかし、ワイヤレスチャネルは、異なる通信システム、例えばさらなるＷｉ－Ｆｉ（登録商標）リンク又はＢｌｕｅｔｏｏｔｈ（登録商標）システムを介して提供される場合もある。

【００５２】

プロセッサ１２２は、さらなる通信チャネルとして、破線の矢印で示されるように、帯域外（ＯＯＢ）チャネル１４０をＳＩデバイスに提供するように構成される。導入部で解説されたように、ＯＯＢチャネルは、無線送信のために何らかの周波数帯を使用する上記のワイヤレスチャネルに対して帯域外にある。そのため、ＯＯＢチャネルは、前記１つのワイヤレスチャネルとは異なる物理的機構、例えばユーザによる視覚的又は手動のデータ入力、を使用している。チャネルの少なくとも１つは、関連付けられることが意図される非ＳＩデバイスが、それぞれのチャネルの物理的終点を構成するＳＩデバイスから限られた範囲内にあることをユーザが検証することを可能にするように、限られた範囲を持つ物理的機構を介して作成される。

【００５３】

ＳＩデバイス１１０は、上記の非ＳＩデバイスとのワイヤレス通信のために構成される。ＳＩデバイスは、非ＳＩデバイスとのワイヤレス通信のために構成された送受信機１１

１と、ＳＩとの関連付けを確立するために関連付けシーケンスを実行するように構成されたプロセッサ１１２とを有する。ＳＩデバイスは、加入者識別モジュール（ＳＩＭ）１１６を備える。ＳＩデバイスは、例えばディスプレイ及び１つ又は複数のユーザ入力要素１１５を含む、ユーザインターフェース１１３も備える。例えば、ユーザ入力要素は、タッチ画面、様々なボタン、マウス、又はタッチパッド等の１つ又は複数を含む。ボタンは、従来の物理的ボタン、タッチセンサ、又は例えばタッチ画面上の仮想ボタン、又はマウスを介して起動されるアイコンである。ユーザインターフェースは、リモートユーザインターフェースであってもよい。

【００５４】

プロセッサ１１２は、例えばローカルネットワークを介して、ワイヤレスチャネルを非ＳＩデバイスに提供するように構成される。しかし、ワイヤレスチャネルは、異なる通信システム、例えばさらなるＷｉ－Ｆｉ（登録商標）リンク又はＢｌｕｅｔｏｏｔｈ（登録商標）システム、を介して提供される場合もある。プロセッサは、さらなる通信チャネルとして、破線の矢印で示されるように、帯域外（ＯＯＢ）チャネル１４０をＳＩデバイスに提供するように構成される。そのため、第１の通信と第２の通信とは、異なり、一方のチャネルとしてＯＯＢチャネルを含む。非ＳＩデバイスは、例えばメモリに記憶された、非ＳＩプライベート鍵を備える。非ＳＩプライベート鍵は、非ＳＩ公開鍵と鍵ペアを構成する。

【００５５】

非ＳＩデバイスでは、関連付けシーケンスは、第１の通信チャネルを介して非ＳＩ公開鍵をＳＩデバイスに提供することを含む。次に、第２の通信チャネルを介して検証コードがＳＩデバイスと共有される。そして、非ＳＩプライベート鍵の所有の証明が、第１又は第２の通信チャネルを介してＳＩデバイスに提供される。次に、ＳＩデバイスから、ＳＩに関係する証明書が受信されることになる。証明書は、上記で解説されたように、非ＳＩ公開鍵の少なくとも一部分に対して証明機関によって生成された署名を備えるべきである。証明書は、非ＳＩデバイスが、ローカルネットワーク及びローカルネットワークとコアネットワークとの間のゲートウェイ（図２に示される）を介してコアネットワークにアクセスすることを可能にする。

【００５６】

ＳＩデバイスにおいて、プロセッサ１１２は、第１の通信チャネルを介して非ＳＩデバイスから非ＳＩ公開鍵を受信することを含む関連付けシーケンスを実行するように構成される。次に、検証コードが第２の通信チャネルを介して非ＳＩデバイスと共有される。そして、第１又は第２の通信チャネルを介して、非ＳＩプライベート鍵の所有の証明が受信され、これは、非ＳＩデバイスからの非ＳＩ公開鍵とペアを構成する。受信された証明の評価が成功すると、上記で解説されたように、ＳＩに関係し、非ＳＩ公開鍵の少なくとも一部分に対して証明機関によって生成された署名を含む証明書が取得される。最後に、証明書が非ＳＩデバイスに送信される。

【００５７】

例えばＯＯＢチャネルを使用した公開鍵及びプライベート鍵の使用に関して、以下が留意される。２つのワイヤレスデバイスが各自の通信をセキュアにする必要があるとき、デバイスは通常、各自の通信を暗号化する。しかし、これには、両方のワイヤレスデバイスが同じ鍵を知っていることが必要となる。

【００５８】

Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ（参考文献［ＤＨ］参照）は、２つのパーティー間で秘密鍵を確立するためのよく知られた技術であり、そこでは、秘密鍵を確立するための２つのパーティー間の通信は、確立された秘密鍵について第３のパーティーに一切の情報を明らかにしない。２つのパーティーは各々、自身の公開鍵／プライベート鍵のペアを使用し、公開鍵を互いと交換する。各パーティーは、自身のプライベート鍵及び他方のパーティーの公開鍵、並びに場合によっては何らかの他の情報、例えば各パーティーからのノンス（乱数）を使用して秘密鍵を算出することができる。各パーティーは、Ｄｉｆｆｉｅ－Ｈ

ｅｌｌｍａｎを行うたびに新たに鍵ペアを生成するか、又は古い鍵ペアを再使用する。

【００５９】

Ｗｉ－Ｆｉ（登録商標） Ａｌｌｉａｎｃｅのデバイスプロビジョニングプロトコル（ＤＰＰ）（参考文献［ＤＰＰ］参照）は、構成したいＤＰＰ Ｅｎｒｏｌｌｅｅと、ＤＰＰ Ｅｎｒｏｌｌｅｅを構成することが可能なＤＰＰ Ｃｏｎｆｉｇｕｒａｔｏｒとの、２つのデバイス間で秘密鍵を確立するためにＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを使用し、それにより、それらはＤＰＰ対応ネットワークへのアクセスを得ることができる（参考文献［８０２．１１］も参照されたい）。

【００６０】

ネットワークを通じてＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを行う際、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎを行うための公開鍵を受信するデバイスは、その公開鍵がどのデバイスからのものであるかを知らない。これが、いわゆる中間者攻撃で攻撃者によって利用されることがある。攻撃者Ｅが、デバイスＡが接続しようとする実際のデバイスＢになりすます。攻撃者Ｅは、デバイスＡとの間でＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを行い、デバイスＡとの間で秘密鍵を確立する。同様に、攻撃者は、デバイスＢに対してデバイスＡになりすまし、デバイスＢとの間で秘密鍵を確立する。メッセージがデバイスＡ又はＢの一方から来ると、攻撃者は、そのメッセージを一方の秘密鍵で解読し、それを他方の秘密鍵で暗号化して他方のデバイスに送付する。このようにすると、デバイスＡ及びＢは、いくらかの追加の遅延を除いては、各自の通信に異常なことは気付かない。デバイスが、別の通信手段を使用して同じ情報を送り、その結果同士を比較することによって各自の通信を確認しても、デバイスは、各自の通信への改ざんには一切気付かない。しかし、攻撃者は、デバイスが通信する内容についての完全な知識を有する。

【００６１】

中間者攻撃を防止するために、公開鍵又は公開鍵のハッシュなどの検証コードを交換するために、追加的な短距離通信プロトコルである帯域外（ＯＯＢ）チャネルを使用することが提案されている。例えば、デバイスのユーザは、ＯＯＢで受信される公開鍵が、短距離通信プロトコルの動作範囲内にあるデバイスからのものであることを知る。公開鍵のハッシュがＯＯＢで交換される場合、デバイスは、暗号化される必要のある第１の通信チャネル、例えばＷｉ－Ｆｉ（登録商標）、を介して受信された公開鍵が、ＯＯＢで受信されるハッシュと同じハッシュになるかどうかを調べることができる。本文献における通信プロトコルという用語の使用は、送受信のための物理層を含む、ＩＳＯ－ＯＳＩモデルの複数の層を包含することに留意されたい。

【００６２】

［ＤＰＰ］には、いくつかのＯＯＢ方法が記載され、そのうちの１つは近距離通信（ＮＦＣ）である。ＮＦＣは、例えば１０～２０ｃｍなど、比較的短い距離を介したワイヤレス通信の技術である。ＮＦＣは、例えば、公開鍵を交換するためのＯＯＢ通信として使用される。ＮＦＣを使用する場合、ユーザは、ＮＦＣを通じて受信された公開鍵が、自身のデバイスから１０～２０ｃｍ以内にあるデバイス、よって自身がＮＦＣの「タッチ」を行ったデバイスから来たことを知る。ＮＦＣをピアツーピアモードで使用する場合、他方のデバイスも、ユーザのデバイスから公開鍵を受信したことを確信することができる。

【００６３】

図２は、コアネットワークを介したワイヤレス通信のための非ＳＩデバイス及びＳＩデバイスを示す。通信システム２００において、非ＳＩデバイス２２０は、ローカル通信プロトコル、例えばＷｉ－Ｆｉ（登録商標）、に従ったローカルネットワーク２３６内でのワイヤレス通信のために構成される。

【００６４】

通信システム内で、コアネットワークＣＯＲＥ＿Ｎ２３０は、少なくとも局地的エリアにわたってモバイルデバイス又は固定デバイスにワイヤレス通信２３２、２３３を提供する。導入部で解説されたように、コアネットワークは、３ＧＰＰ Ｅｖｏｌｖｅｄパケットコア又はＥＰＣであってよい。通信システムは、ローカルネットワーク２３６とコアネ

ットワークとの間のゲートウェイＧＷ２３４をさらに含む。また、コアネットワークは、アプリケーションサーバＡＳ２５２、加入者データベースＳｕｂ＿ＤＢ２５０、及び証明機関ＣＡ２５４に結合される。ＳＩデータは、コアネットワークのプロバイダの管理システムのような場所、例えば加入者識別データを管理するサーバ上の加入者データベース２５０において、入手可能である。加入者クレデンシャルは、認可サーバ又は証明書機関２５４を使用して認証及び認可される。例えば、ＳＩデータは、ユーザ名及びパスワードのようなユーザクレデンシャルを使用して、又は２要素認証を使用して、インターネットを介してアプリケーションサーバ２５２上のユーザアカウントにログインすることにより、加入者によってアクセスされることもある。ＡＳは、加入者データベース及びＣＡに結合されるか又はそれらを備える。ＡＳは、非ＳＩデバイスをＳＩに関連付けるプロセスを制御する。

【００６５】

ＳＩデバイスは、加入者データベースを記憶する１つ又は複数のサーバ及びＣＡとコアネットワークを介して通信する２３３ために構成され、一方で、ワイヤレスチャネル２４２、特にセキュアチャネルを介して非ＳＩデバイスと通信するようにも構成されたＳＩＭデバイスである。

【００６６】

一実施形態では、関連付けシーケンスは、非ＳＩデバイスがサーバとして機能する、セキュアソケット層（ＳＳＬ［ＲＦＣ　６１０１］）プロトコル又はトランスポート層セキュリティ（ＴＬＳ［ＲＦＣ　５２４６］）プロトコルを利用することにより、第１及び第２の通信チャネルの他方のチャネルとしてセキュアチャネルを提供することを含み、ここで、非ＳＩデバイスは、自己署名された証明書の中で非ＳＩ公開鍵を提供し、この証明書を、サーバ証明書メッセージ内でサーバ証明書として使用する。代替として、セキュアチャネルは、非ＳＩデバイスがクライアントとして機能する、ＳＳＬ又はＴＬＳプロトコルを利用することによって提供され、ここで、非ＳＩデバイスは、クライアントによって認証されたハンドシェイクの際に、自己署名された証明書の中で非ＳＩ公開鍵を提供する。代替として、セキュアチャネルは、非ＳＩ公開鍵又は非ＳＩプライベート鍵が使用される公開鍵暗号化によって設定されるインターネットプロトコルセキュリティ（ＩＰｓｅｃ［ＲＦＣ　４３０１］）トンネルを利用することによって提供される。代替として、セキュアチャネルは、デバイスプロビジョニングプロトコル（ＤＰＰ　［ＤＰＰ］）認証プロトコルを利用することによって提供され、ここで、非ＳＩデバイスは、非ＳＩ公開鍵又はさらなる非ＳＩ公開鍵を、ＤＰＰブートストラップ鍵として又はＤＰＰプロトコル鍵として提供する。任意選択で、関連付けシーケンスにおいて、上記のセキュアチャネルの１つを提供した後に、証明書もセキュアチャネルを介して転送される。

【００６７】

上記のＳＳＬ、ＴＬＳ、又はＩＰｓｅｃのみを使用する場合、ＳＩデバイスは、プライベート鍵の所有を証明するときに非ＳＩデバイスと通信しているという証明を持たない。非ＳＩデバイスのブートストラップ鍵を帯域外（ＯＯＢ）方式で取得することにより、ＳＩデバイスは、非ＳＩデバイスが対応するプライベート鍵の所有を証明するときに、自身がその非ＳＩデバイスと通信しているという証明を有し、これは特に、ブートストラップ鍵ペアが、ＯＯＢ通信を使用する直前に生成されており、ＯＯＢ通信に短距離通信技術が使用される場合にそうである。非ＳＩデバイスのブートストラップ鍵が上記の第１の公開鍵として使われることが可能であり、又は、別の公開鍵、すなわちプロトコル鍵が第１の公開鍵として使われることが可能である。ＤＰＰ仕様は、どのようにしてデバイスがワイヤレスネットワークを通じてプロトコル鍵を転送するか、及び、どのようにしてそのデバイスがプロトコル鍵と一致するプライベート鍵の所有を証明するかの例を提供している。

【００６８】

同様に、ＯＯＢチャネルが、非ＳＩデバイスとＳＩデバイスとの間で、それらがＳＳＬ又はＴＴＬ又はＩＰｓｅｃプロトコルセッションに参加する前に使用されることが可能であり、ここでは、第１の公開鍵、第１の公開鍵を含んでいる証明書、又は公開鍵若しくは

証明書のハッシュが、ＳＩデバイスにＯＯＢで通信される。ＳＩデバイスは、ＯＯＢで取得した第１の公開鍵に関する情報が、セキュアチャネルを通じて非ＳＩデバイスから取得した第１の公開鍵と一致するかどうかを調べなければならない。ＳＩデバイスは、オプションとして、セキュアチャネルを設定するためにそれが使用する公開鍵、自身の公開鍵を含んでいる証明書、又は自身の公開鍵若しくは証明書のハッシュを、ＯＯＢプロトコルを通じて非ＳＩデバイスが入手できるようにすることもできる。ＮＦＣ、ＱＲコード（登録商標）の表示及びスキャン、Ｂｌｕｅｔｏｏｔｈ（登録商標）等の短距離通信プロトコルは、適切なＯＯＢプロトコルである。ユーザを関与させるＯＯＢ方法の一例は、第３のネットワークを通じて受信され、ＳＩデバイスによって表示された公開鍵又は証明書の（短縮された）ハッシュとユーザが比較しなければならない、非ＳＩデバイスの公開鍵又は証明書の（短縮された）ハッシュを、非ＳＩデバイスが表示する場合である。

【００６９】

ユーザを関与させるＯＯＢ方法の別の例は、ＳＳＬ又はＴＴＬ又はＩＰｓｅｃプロトコルセッションに参加する前に、ユーザが数値コード（例えばＰＩＮコード）、パスワード、又はパスフレーズを両方のデバイスに入力し、各デバイスが、同じ検証が使用されることを調べなければならない場合である。ユーザを関与させるＯＯＢ方法の別の例は、ＤＰＰ認証プロトコルセッションに参加する前に、ユーザが数値コード（例えばＰＩＮコード）、パスワード、又はパスフレーズを、ＰＫＥＸ（公開鍵交換）「コード」として両方のデバイスに入力する場合であり、ここで、ＰＫＥＸは、ＤＰＰ認証プロトコルのセキュリティをブートストラップするために使用される（［ＤＰＰ］のＰＫＥＸ、並びにＰＫＥＸ「コード」（項５．６）及びＤＰＰ認証プロトコル（項６．２）参照）。

【００７０】

また、短距離ＯＯＢセキュアチャネルとして、ＳＩデバイス及び非ＳＩデバイスが両方とも同じＷｉ－Ｆｉ（登録商標）アクセスポイント又は住宅ゲートウェイにセキュアに接続される場合は、Ｗｉ－Ｆｉ（登録商標）インフラストラクチャ接続を、非ＳＩデバイスがプライベート鍵の所有を証明するＯＯＢチャネルとして使用することができる。

【００７１】

別の実施形態では、ＳＩデバイスは、Ｗｉ－Ｆｉ（登録商標）アクセスポイント及び住宅ゲートウェイ（例えば［ＴＲ　２３．７１６］の５Ｇ－ＲＧ。５Ｇコアネットワークに接続され、５Ｇネットワークプロトコルをサポートする）であり、ＳＩＭを備え、ＯＯＢチャネルを通じて非ＳＩデバイスと通信することが可能であり、そのＯＯＢチャネルを通じて非ＳＩデバイスが識別を提供し、この識別は後に、非ＳＩデバイスとＳＩデバイスとの間のセキュアチャネルを設定するためのＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ交換で使用される。セキュアチャネルを設定する際に使用されるこの識別又は別の公開鍵又は証明書は、次いで、非ＳＩデバイスをコアセルラーネットワークに関連付けるための非ＳＩデバイスの識別として使用される。また、識別又は証明書のいずれか一部が、次いで、ＳＩに関連付けられるさらなるクレデンシャルを暗号化するための公開鍵として使用されてもよく、このさらなるクレデンシャルは、その後、コアネットワークにアクセスするのを認可された状態になるために非ＳＩデバイスによって使用されてよい。ＳＩデバイスは、例えばスマートフォン上で、リモートＵＩを通じて操作される。セキュアチャネルは、上記で説明された４つのオプションのいずれか又は任意の他のセキュアチャネルである。

【００７２】

別の実施形態では、ＳＩデバイスは、ＤＰＰコンフィギュレータとして機能するモバイルデバイスであり（［ＤＰＰ］の５Ｇ－ＲＧ参照）、したがって、ＳＩデバイスは、非ＳＩデバイスをＳＩデバイスと関連付けたいか、又は５Ｇ－ＲＧデバイスと関連付けたいか、又はその両方と関連付けたいかをユーザに選択させるためのユーザインターフェースを有する。デバイスは、ＳＩデバイス及び５Ｇ－ＲＧデバイスに関連する加入者データベースの情報をユーザプロファイルに、又は異なるオプションに関連する価格／課金情報を示す。非ＳＩデバイスがコアネットワークにアクセスするためにＳＩデバイスに関連付けられようとする場合、非ＳＩデバイスのＤＰＰプロトコル鍵又はＤＰＰブートストラップ鍵

が、非ＳＩデバイスの識別として使用され得る。

【００７３】

上記のオプションでは、ＳＩデバイスのユーザ／所有者は、ＳＩデバイスとの非ＳＩデバイスの関連付けを承認するかどうかを尋ねられる。何故ならば、これはユーザ／所有者に対する追加費用を伴い得るためである。

【００７４】

実際には、関連付けシーケンスは、以下を伴い得る。ＳＩデバイスが、非ＳＩデバイスの識別の証明の取得に成功した後、ＳＩデバイスは、第１の公開鍵又は第１の公開鍵を含んでいる非ＳＩデバイスによって生成された証明書を非ＳＩデバイスの識別として使用し、これを、直接、又は、５Ｇ対応である場合もそうでない場合もあるＷｉ－Ｆｉ（登録商標）アクセスポイント／住宅ゲートウェイを通じてのいずれかで、例えば３ＧＰＰコアネットワークを通じて、ＡＳサーバに送る。ＡＳサーバは、非ＳＩデバイスの識別として第１の公開鍵を使用して、非ＳＩデバイスのユーザプロファイル、及びＳＩデバイスのＳＩと非ＳＩデバイス（のユーザプロファイル）との間の関連付けを作成する。ＡＳは、非ＳＩデバイスのこのユーザプロファイルを加入者データベースに送り、加入者データベースはこのユーザプロファイルを記憶する。ＡＳは、第１の公開鍵についての証明書を証明書機関又は証明機関サーバ（ＣＡ）に要求し、証明書をＳＩデバイスに送り、ＳＩデバイスはその後、好ましくは、ＳＳＬ、ＴＬＳ接続、ＩＰｓｅｃトンネルなどのセキュアチャネルを通じて、又は、例えばＤＰＰ構成オブジェクト若しくはさらにはＤＰＰコネクタにおけるＤＰＰ構成プロトコルメッセージの一部として、ＤＰＰ認証中に確立された対称鍵を使用して、この証明書を非ＳＩデバイスに送る。第１の公開鍵の他に、ＣＡへの証明書の要求は、証明書に含められる他の情報、例えば、ユーザプロファイルについての情報、非ＳＩデバイスによって使用されるべきＩＭＥＩ（存在する場合）、ＳＩデバイスによって使用されるべきＩＭＳＩ（存在する場合）等、を含んでよい。ＡＳ、ＣＡ及びＳｕｂ＿ＤＢサーバの概念のさらなる例、並びにそのようなサーバがどのようにＳＩＭと非ＳＩＭデバイスとの間の関連付けの作成を支援するかは、米国特許第９６４８０１９（Ｂ２）号に提供されているが、ここでは、識別としての非ＳＩ公開鍵及びＳＩＭデバイスと非ＳＩＭデバイス間のセキュアチャネルを使用する。ＡＳは、ＣＡ、プロバイダサーバ又は加入者データベースにクレデンシャルを要求してもよく、クレデンシャルは、非ＳＩデバイスがコアネットワークにアクセスすることを認可された状態になるのを可能にする。これらのクレデンシャルは、プロバイダにより、例えば加入者データベースに記憶される。ＡＳは、クレデンシャルの少なくとも一部分を第１の公開鍵で暗号化してよく、暗号化されたクレデンシャルを含む証明書をＳＩデバイスに送り、ＳＩデバイスは、上記のように処理するために証明書を非ＳＩデバイスに送付する。

【００７５】

図３は、コアネットワークを介したワイヤレス通信のための非ＳＩデバイス及びＵＩデバイスを示す。通信システム３００において、非ＳＩデバイス３２０が、例えばＷｉ－Ｆｉ（登録商標）を介した、ＵＩデバイス３１０とのワイヤレス通信のために構成される。通信システム３００の様々な要素は、図２を参照して説明された通信システム２００内の同様の要素に対応している。そのような要素は、同じ参照符号を有し、再度説明されることはない。ＵＩデバイス３１０は、ユーザインターフェースと、ＳＩにアクセスするためにコアネットワークを介して通信するための送受信機とを有する。そのために、ＵＩデバイスは、ＡＳ２５２に接続し、加入者データベースＳｕｂ－ＤＢ２５０からＳＩを取得し、ＣＡ２５４から署名された証明書を取得するために構成される。

【００７６】

一実施形態では、３ＧＰＰコアネットワークにアクセスするためのクレデンシャルは、人にリンクされてよく、一つのシナリオは以下である。（Ｕ－）ＳＩＭカードの所有者はまた、自身のプロバイダのウェブサイトにアカウントを有する。３ＧＰＰ接続及び３ＧＰＰ送受信機を有する任意のＵＩデバイスを使用して、自身のプロバイダのウェブサイトにログインする際、ユーザは、証明書の形態で人に基づくクレデンシャルを要求することが

できる。プロバイダのウェブサイトにログインするには、認証手順、例えばユーザ名／パスワード、証明書等、が必要とされる。ＵＩデバイスは、使用され署名されるべき公開鍵を証明書の中で供給しなければならない。また、証明書が、対応するプライベート鍵と共にウェブサイトによって送達されることもあり得る。ウェブサイトは、証明書及び可能性としては対応するプライベート鍵を、ＵＩデバイス内の適当な場所に記憶し、その後、ＵＩデバイスは、証明書を使用して、３ＧＰＰネットワークに接続されるＡＰ又は住宅ゲートウェイを通じて、３ＧＰＰネットワーク上で認証を受けることができる。（Ｕ－）ＳＩＭカードの所有者は、非ＳＩデバイスの３ＧＰＰ使用について課金される。証明書の中で、ＵＩデバイスは、先に説明されたように、公開鍵を用いて暗号化されたクレデンシャルを要求し、受信してもよい。

【００７７】

上記は、ＵＩを有するか又はそのようなアプリを実行することができるデバイス内で実施される。非ＳＩデバイス３２０としてのヘッドレスデバイス、すなわちユーザインターフェースを持たないデバイスには、３ＧＰＰ証明書又はクレデンシャルをインストールするために以下が提案される。一連のステップは図２に関して説明される通りであり、ＵＩデバイスは、上記のＳＩデバイスの役割を有するが、ここではＵＩデバイスが、ＵＩデバイスに関して上記で説明されたように証明書を取得する。ＵＩデバイスは、ＳＩＭを使用して３ＧＰＰネットワーク及びアプリケーションサーバに接続するＳＩＭデバイスであってよい。

【００７８】

図４は、コアネットワークを介したワイヤレス通信のための非ＳＩデバイス及びＵＩデバイスのさらなる例を示す。通信システム４００において、非ＳＩデバイス４２０が、例えばＷｉ－Ｆｉ（登録商標）を介した、ＵＩデバイス４１０とのワイヤレス通信のために構成される。通信システム４００の様々な要素は、図２を参照して説明された通信システム２００内の同様の要素に対応している。そのような要素は、同じ参照符号を有し、再度説明されることはない。ＵＩデバイス４１０は、ユーザインターフェースを有し、インターネットＩＮ４３３を介した通信のために構成される。例えば、ＵＩデバイス４１０は、インターネットを介してアプリケーションサーバＡＳ２５２に接続して、上記で図３と共に説明されたようにコアネットワークへの接続を介して証明書を取得するのと同様に、証明書を取得する。

【００７９】

一実施形態では、プロバイダは、ユーザがダウンロードして、３ＧＰＰ送受信機を持たないデバイス上で実行することができるアプリを提供する。ユーザは、そのアプリ内で自分のユーザ名及びパスワードを入力しなければならず、アプリは次いで、３ＧＰＰセルラーネットワークを関与させないインターネット接続を通じて証明書を要求する。アプリは、次いで、証明書を使用して、３ＧＰＰネットワークに接続されたＡＰ又は住宅ゲートウェイを通じて、非ＳＩデバイスを３ＧＰＰネットワーク上で認証させる。実際には、ＵＩデバイスは、例えば地上線を通じて、インターネット接続を有するデバイスであり得、ここで、アプリケーションサーバへの信頼できるチャネルが設定され、そこでユーザは自分のユーザ名及びパスワード、又は証明書等を提供しなければならない。

【００８０】

一実施形態では、非ＳＩデバイスは、その公開ブートストラップ鍵を、機械可読コード、例えばＱＲコード（登録商標）又はバーコード、の形態で、ステッカー又はマニュアルに示すヘッドレスデバイスである。十分に良質のディスプレイを有するヘッドレスデバイスは、新たに生成された公開ブートストラップ鍵をデバイスのディスプレイ上に示してもよい。次に、ＵＩデバイスは、ヘッドレスデバイスの公開ブートストラップ鍵をスキャンする。次に、ＵＩデバイスは、ヘッドレスデバイス情報を、Ｗｉ－Ｆｉ（登録商標）を通じて送り、それにより、ヘッドレスデバイスは、ＵＩデバイスが、例えば公開鍵のハッシュを送ることにより、自身の公開ブートストラップ鍵を読み込んだことを知ることができる。

【００８１】
その後、セキュアチャネルを設定するために、ＵＩデバイスは、Ｗｉ－Ｆｉ（登録商標）を通じてヘッドレスデバイスとＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ交換を行い、ここで、ＵＩデバイスは、ヘッドレスデバイスが、スキャンした公開鍵ブートストラップ鍵を使用することを期待し、このようにしてヘッドレスデバイスとのセキュアな接続を設定する。任意選択で、ヘッドレスデバイスは、第２の非ＳＩ公開鍵／プライベート鍵のペアを作成し、第２の非ＳＩ公開鍵をＵＩデバイスに送り、プライベート鍵の所有を証明する。このステップは、セキュアチャネルの設定と統合されてもよい。
【００８２】
次に、ＵＩデバイスは、公開ブートストラップ鍵又は第２の非ＳＩ公開鍵を公開鍵として使用して、セルラーネットワークプロバイダにおいて証明書を求める。この通信は、セルラーネットワークプロバイダにあるユーザのアカウントへのアクセスを得るために、ユーザのクレデンシャル、例えばユーザ名及びパスワード、を使用して設定される、セルラーネットワークプロバイダのサーバとのさらなるセキュアチャネルを通じて行われる。
【００８３】
ＵＩデバイスは、ここで、セルラーネットワークプロバイダからクレデンシャルを含む証明書を受信し、その証明書を、前記セキュアチャネルを使用して非ＳＩデバイスに転送する。非ＳＩデバイスは、そして、第２のネットワーク（２３６）を使用して３ＧＰＰネットワークに対して認証を受け（２３２、２３０）、３ＧＰＰネットワークを使用する。
【００８４】
上記の非ＳＩ公開鍵に基づく証明書の代替として、ＵＩデバイスは、プロバイダで生成された公開鍵に基づく代替の証明書と、それに伴うプロバイダで生成されたプライベート鍵とを受信してもよく、その両方を非ＳＩデバイスに転送する。そして、非ＳＩデバイスは、プロバイダで生成された公開鍵に基づく代替の証明書、及びプロバイダで生成されたプライベート鍵を使用して、３ＧＰＰネットワークを使用することができる。
【００８５】
一実施形態では、事業者又はユーザが、例えば追加的な安全性のために、非ＳＩデバイスがＳＩに関連付けられたままでコアネットワークへのアクセスを得るために動作できるエリアを制限することを望む。非ＳＩデバイスが意図される動作範囲内にあるかどうかを判定するために、様々なオプションが提供され、例えば２つのデバイスが互いの近くにあるままであるようにすることによる。
【００８６】
一実施形態では、コアネットワークが、第１のネットワークを通じてＳＩデバイスにハートビートメッセージ、例えばページングメッセージ、を送る。ハートビートメッセージは、無作為の構成要素を有し、そのため非ＳＩデバイスによって予測することが難しい。ＳＩデバイスは、例えば非ＳＩデバイスとＳＩデバイスとの間の関連付け手順のために設定されたセキュアチャネルを使用して、ハートビートメッセージを非ＳＩデバイスに送付するように構成される。非ＳＩデバイスは、次いで、受信されたハートビートを、第２のネットワークを介してコアネットワークに送付する。コアネットワークは、コアネットワークが正しいハートビート信号をいくらかの時間にわたって受信しない場合に、コアネットワークへの非ＳＩデバイスのアクセスを無効にする。コアネットワークは、正しいハートビート信号を再び受信した後に、アクセスを可能にしてよい。
【００８７】
任意選択で、ハートビートは、コアネットワークへの非ＳＩデバイスのアクセスを時間又は使用量において制限するために、ＳＩデバイスによって使用される。何故ならば、このアクセスは、加入者に対する追加費用を伴い得るためである。ＳＩデバイスがアクセスを制限したい場合、ＳＩデバイスはハートビート信号の送付を停止する。ＳＩデバイスが再びアクセスを可能にしたい場合、ＳＩデバイスは再びハートビート信号の送付を開始する。非ＳＩデバイスのコアネットワークへのアクセスを停止するための別の方式は、ＳＩデバイスが、ＡＳサーバにおいて関連付けられた非ＳＩデバイスの識別としての、第１の

公開鍵の関連付けを取り消すことによるものである。

【００８８】

別の実施形態では、ＳＩデバイスが、ＳＩデバイスと非ＳＩデバイスとの間の距離に関する情報を、ＳＩデバイスによって署名されたメッセージのストリームを使用して、規則的にＡＳに通信する。距離は、例えば、［８０２．１１］に記載されるように、タイミング測定（ＴＭ）又は微タイミング測定（ＦＴＭ）機構を使用することによって決定される。代替として、ＳＩデバイスが非ＳＩデバイスと同じＷｉ－Ｆｉ（登録商標）　ＡＰ／住宅ゲートウェイに接続されたとき、ＳＩデバイスは、そのような接続に関する情報を、ＳＩデバイスによって署名されたメッセージのストリームを使用してＡＳに送る。ＡＳは、この情報を検証し、この情報がＳＩデバイスによって適正に署名されていることを調べるように構成される。距離が、ある設定された閾値を超える場合、又はＡＳがそのような接続情報を最近受信していない場合、非ＳＩデバイスは、コアネットワークへのアクセスを拒絶される。

【００８９】

さらなる実施形態では、ＳＩデバイスは、非ＳＩデバイスへの及び／又は非ＳＩデバイスからのトラフィックの特定部分についてのリレーの役目を果たす。そのために、ＳＩデバイスは、ＳＩデバイス自身のクレデンシャルを使用してメッセージの一部を暗号化するように構成される。ＡＳは、暗号化された部分を使用して、ＳＩデバイスが非ＳＩデバイス通信に直接関与していること、及びコアネットワークが、コアネットワークにつながれたどこか別の場所でハッキングされた非ＳＩデバイスからアクセスされていないことを検出することができる。

【００９０】

さらなる実施形態では、非ＳＩデバイスが接続されるＳＩデバイス及び／又はＡＰ／ＲＧが、非ＳＩデバイスによって要求されるサービス／コンテンツに関する情報を継続的に追跡し、その情報をＡＳに送る。ＡＳは、そして、そのサービス及びコンテンツが、非ＳＩデバイスに割り当てられたアクセス権に準拠するかどうかを調べる。準拠しない場合、ハッキングされたデバイスが、非ＳＩデバイスによって要求されるものとは異なるサービス／コンテンツのセットへのアクセスを試みて、非ＳＩデバイスのクレデンシャルを使用している可能性がある。ＡＳは、次いで、非ＳＩデバイスに対するアクセス又はサービスを取り消す。

【００９１】

さらなる実施形態では、非ＳＩデバイスは、２つ以上のユーザアカウントを用いて設定される。通常は少なくとも１つの１次ユーザアカウントがあり、それを用いて他の２次アカウントを作成することができる。ユーザアカウントは、ＳＩＭデバイスのユーザアカウントと異なることがあり、一方、ユーザ同士は、インターネット又はセルラーネットワーク上でコンテンツ／サービスへアクセスするための異なる権利を有することがある（例えば親と子供）。各アカウントは、例えば、異なるＧｏｏｇｌｅアカウント又はＡｐｐｌｅＩＤ又はＭｉｃｒｏｓｏｆｔアカウントに接続される。各２次アカウントは、デバイスのＷｉ－Ｆｉ（登録商標）又は３ＧＰＰシステムを使用する許可を与えられている場合も与えられていない場合もある。また、各アカウントは、セルラーネットワークによって提供されるコンテンツ／サービスに対して異なる種類のアクセス制約を伴って構成されることがある（例えば、未成年の子供のアカウントのペアレンタルコントロールのために）。任意選択で、マルチユーザの非ＳＩデバイスでは、特定のユーザアカウントだけが、ＳＩデバイスに関連付けられることを許される。関連付けは、許されたユーザアカウントの各々について同じＳＩに対するものであり得、その場合、ＳＩデバイスとの関連付けは一度だけ行われればよい。代替として、複数の異なるＳＩがそれぞれのユーザアカウントに関連付けられ、その場合、関連付けは異なるＳＩの各々と別々に行われる必要がある。

【００９２】

一実施形態では、一つのユーザアカウント名、又は１つのＳＩに関連付けられた複数のユーザアカウント名が、関連付けられたＳＩデバイスがＣＡサーバに要求する証明書内に

リストされるアカウント名又はアカウントＩＤを有する。このために、非ＳＩデバイスは、非ＳＩデバイスとの間で設定されたセキュアチャネルを使用して、ユーザアカウント名をＳＩデバイスに提供する必要があり、この間に、非ＳＩデバイスは、非ＳＩデバイスの公開鍵に属するプライベート鍵の所有を証明している。任意選択で、アカウント名は、第１の公開鍵を含んでおり、第１の公開鍵に対応するプライベート鍵で署名された証明書内に（よって、非ＳＩデバイスによって生成された自己署名されたＳＳＬ又はＴＬＳ証明書内に）記述される。第１の鍵のみに代えて、ＳＩデバイスは、この証明書をＡＳサーバに送り、ＣＡサーバによって生成される証明書はアカウント名を含んでいる。ＳＩデバイスのユーザにとっての利点は、非ＳＩデバイスのどのユーザが可能にされるのかを証明書から見て取れることである。ＳＩデバイス、ＡＳ及びＣＡにとっての利点は、それが、ユーザアカウントを指定した非ＳＩデバイスであったことを調べることができることである。

【００９３】

さらなる実施形態では、コアネットワークへの非ＳＩデバイスのアクセスが付与されると、アクセスが付与される非ＳＩデバイスのユーザアカウント及び存在し得るアクセス制約に関する情報が、非ＳＩデバイスが非ＳＩデバイスの公開鍵に属するプライベート鍵の所有を証明したのと同じセキュアチャネルを通じて送られる。この情報を受信すると、非ＳＩデバイスは、非ＳＩデバイスのそれぞれの異なるユーザアカウントに対してそれらのアクセス制約を施行する。

【００９４】

図５は、ＳＩデバイスとのワイヤレス通信のために構成された非ＳＩデバイスにおいて使用するための方法を示す。各デバイスについては上記で説明されている。方法は、例えば、固定又はモバイルコンピューティングデバイス内のプロセッサ内で回路及びソフトウェアによって実行される。ローカルネットワーク、コアネットワーク又はその他の中でのワイヤレス通信及びＯＯＢチャネルに関する様々なオプションについては上記で説明されている。図５は、ＳＩデバイスと協働していることもあり得る非ＳＩデバイスについての方法を示すことが留意される。非ＳＩデバイス内に、非ＳＩ公開鍵とペアを構成する非ＳＩプライベート鍵が記憶される。鍵ペアは、恒久的若しくは一時的に記憶されるか、又は新しい関連付けを設定するために初めて生成される。

【００９５】

この方法において、関連付けシーケンスが実行され、ノードＳＴＡＲＴ５０１で開始する。第１の段階ＰＲ－ＮＰＫ５０３において、非ＳＩ公開鍵が、第１の通信チャネルを介してＳＩデバイスに提供される。そのために、第１の通信チャネルは、例えばＷｉ－Ｆｉ（登録商標）などのワイヤレスネットワークを介して設定される。第１のチャネルは、例えば上記で解説されたようなＯＯＢチャネルであってもよく、例えば、非ＳＩ公開鍵は、印刷形態でＳＩデバイスに提供されてよく、一方、対応するプライベート鍵は非ＳＩデバイスの内部に記憶されなければならない。

【００９６】

次の段階ＳＨ－ＶＥＲ５０４において、検証コードが第２の通信チャネルを介してＳＩデバイスと共有される。そのために、第２の通信チャネルは、第１の通信チャネルとは異なるワイヤレス通信、例えばＢｌｕｅｔｏｏｔｈ（登録商標）、を介して設定される。第１の通信チャネルと第２の通信チャネルとは異なり、第１及び第２の通信チャネルの一方はＯＯＢチャネルである。例えば、検証コードは、ＳＩデバイス上にそのコードを表示することにより、ＯＯＢチャネルを介して共有され、一方でユーザは非ＳＩデバイス上でコードを手動で入力しなければならない。次の段階、ＰＲ－ＰＲＯ５０５において、非ＳＩプライベート鍵の所有の証明が、このための上記のプロトコルのいずれかを使用して、第１又は第２の通信チャネルを介してＳＩデバイスに提供される。

【００９７】

証明の評価が成功しない場合、方法は、例えば所定のタイムアウト期間後に、又は入手可能な証明書がない旨のメッセージを受信したときに、受信される証明書がないために矢印５１０で示されるように終了する。証明の評価が成功した場合、ＳＩデバイスは、可能

性としてはクレデンシャルを含む証明書を取得し、証明書を非ＳＩデバイスに送る。次の段階ＲＥＣ－ＣＥＲ５０６において、証明書がＳＩデバイスから受信され、この証明書はＳＩに関係し、非ＳＩ公開鍵の少なくとも一部分に対して証明機関によって生成された署名を含む。

【００９８】

最後に、段階ＡＣ－コア５０７において、証明書は、非ＳＩデバイスが、ローカルネットワーク及びローカルネットワークとコアネットワークとの間のゲートウェイを介してコアネットワークにアクセスすることを可能にする。関連付けシーケンスは、ノードＥＮＤ５０８で終了される。

【００９９】

図６は、非ＳＩデバイスとのワイヤレス通信のために構成されたＳＩデバイスにおいて使用するための方法を示す。各デバイスについては上記で説明されている。方法は、例えば、固定又はモバイルコンピューティングデバイス内のプロセッサ内で回路及びソフトウェアによって実行される。

【０１００】

この方法において、関連付けシーケンスが実行され、ノードＳＴＡＲＴ６０１で開始する。第１の段階、ＯＢ－ＮＰＫ６０２において、非ＳＩ公開鍵が、第１の通信チャネルを介して非ＳＩデバイスから取得される。そのために、第１の通信チャネルは、例えばＷｉ－Ｆｉ（登録商標）などのワイヤレスネットワークを介して設定される。第１のチャネルは、例えば上記で解説されたようなＯＯＢチャネルであってもよく、例えば、非ＳＩ公開鍵は、印刷されたＱＲコード（登録商標）をスキャンすることによってＳＩデバイスによって取得されてよい。

【０１０１】

次の段階ＳＨ－ＶＥＲ６０３において、検証コードが第２の通信チャネルを介してＳＩデバイスと共有される。そのために、第２の通信チャネルは、例えば第１の通信チャネルとは異なるワイヤレス通信を介して設定される。第１の通信チャネルと第２の通信チャネルとは異なり、第１及び第２の通信チャネルの一方はＯＯＢチャネルである。例えば、検証コードは、ＳＩデバイス上にそのコードを表示することにより、ＯＯＢチャネルを介して共有され、一方でユーザは、非ＳＩデバイス上でコードを手動で入力しなければならない。次の段階、ＲＣ－ＰＲＯ６０４において、非ＳＩプライベート鍵の所有の証明が、このための上記のプロトコルのいずれかを使用して、第１又は第２の通信チャネルを介して受信され、この非ＳＩプライベート鍵は、非ＳＩデバイスからの非ＳＩ公開鍵とペアを構成する。

【０１０２】

次の段階ＥＶ－ＰＲＯ６０５において、受信された証明が評価され、証明の評価が成功しない場合、方法は、ノードＥＮＤ６０８への矢印６１０によって示されるように終了する。例えば所定のタイムアウト期間の後に、取得される証明書はない。また、入手可能な証明書がない旨の中止メッセージが送られてよい。証明の評価が成功した場合、ＳＩデバイスは、上記で説明されたように証明書を取得し、その証明書を次の段階ＴＲ－ＣＥＲ６０６で非ＳＩデバイスに送る。

【０１０３】

最後に、オプションの段階ＭＮ－ＮＳＩ６０７において、証明書は、非ＳＩデバイスが、ローカルネットワーク及びローカルネットワークとコアネットワークとの間のゲートウェイを介してコアネットワークにアクセスするのを可能にする一方で、非ＳＩデバイスによるコアネットワークのアクセス及び／又は使用が監視されて、例えば、非ＳＩデバイスの位置、又は非ＳＩデバイスのアクセス、サービス及び／若しくはトラフィックを監視してもよい。関連付けシーケンスは、ノードＥＮＤ６０８で終了される。

【０１０４】

当業者には明らかであるように、上記方法を実施する多くの異なる方式が可能である。例えば、段階若しくはステップの順序が変更される、又はいくつかの段階が並行して実行

されてもよい。さらに、ステップの間に他の方法のステップが挿入されてもよい。挿入されるステップは、本明細書に記載されるような方法の改良に相当するか、又は上記方法に関連しなくてもよい。

【０１０５】

ネットワークからダウンロード可能な、並びに／又はコンピュータ可読媒体及び／若しくはマイクロプロセッサ実行可能媒体に記憶されたコンピュータプログラム製品が提供され、このコンピュータプログラム製品は、コンピュータデバイス上で実行されたときに、上記方法、接続シーケンス、セキュリティプロセス、及びさらに他の動作を実施するためのプログラムコード命令を備える。そのため、本発明に係る方法は、プロセッサシステムにそれぞれの方法を実行させる命令を備えるソフトウェアを使用して実行されてよい。

【０１０６】

通例、関連付けシーケンスを実行するために対話する非ＳＩデバイス及びＳＩデバイスは各々、そのデバイスで記憶される適当なソフトウェアコードを含んでいるメモリに結合されたプロセッサを備え、例えば、そのソフトウェアは、ダウンロードされたものである、及び／又は対応するメモリ、例えばＲＡＭなどの揮発性メモリ又はフラッシュなどの不揮発性メモリ（図示せず）に記憶されている。各デバイスは、例えば、マイクロプロセッサ及びメモリ（図示せず）を備える。代替として、各デバイスは、全体又は一部が、プログラム可能論理、例えばフィールドプログラム可能ゲートアレイ（ＦＰＧＡ）、として実施される。デバイス及びサーバは、全体又は一部が、いわゆる特定用途集積回路（ＡＳＩＣ）、すなわち各自の特定の使用のためにカスタマイズされた集積回路（ＩＣ）として実施される。例えば、回路は、例えばＶｅｒｉｌｏｇ、ＶＨＤＬ等のハードウェア記述言語を使用して、ＣＭＯＳ内に実施される。

【０１０７】

ソフトウェアは、システムの特定の下位エンティティによって取られるステップのみを含んでよい。ソフトウェアは、ハードディスク、フロッピー、メモリ等の適切な記憶媒体に記憶される。ソフトウェアは、電線に沿って、又はワイヤレスに、又はデータネットワーク、例えばインターネットを使用して、信号として送られる。ソフトウェアは、ダウンロード及び／又はサーバ上でのリモート使用が利用可能にされてよい。本発明に係る方法は、方法を実行するように、プログラム可能論理、例えばフィールドプログラム可能ゲートアレイ（ＦＰＧＡ）、を構成するように構成されたビットストリームを使用して実行されてよい。ソフトウェアは、ソースコード、オブジェクトコード、部分的にコンパイルされた形態などのコードの中間ソース及びオブジェクトコード、又は本発明に係る方法の実施に使用するのに適する任意の他の形態であってよいことが理解されよう。コンピュータプログラム製品に関する実施形態は、記載される方法の少なくとも１つ方法のうちの各処理ステップに対応するコンピュータ実行可能命令を備える。これらの命令は、サブルーチンにさらに分割される、及び／又は静的若しくは動的にリンクされる１つ又は複数のファイルに記憶される。コンピュータプログラム製品に関する別の実施形態は、記載されるシステム及び／又は製品のうちの少なくとも１つの各手段に対応するコンピュータ実行可能命令を備える。

【０１０８】

図７ａは、コンピュータプログラム１０２０を備える書込み可能部分１０１０を有するコンピュータ可読媒体１０００を示し、コンピュータプログラム１０２０は、プロセッサシステムに、図１～６を参照して説明されたようにシステム内で上記方法及びプロセスの１つ又は複数を実行させる命令を備える。コンピュータプログラム１０２０は、物理的マークとしてコンピュータ可読媒体１０００上に、又はコンピュータ可読媒体１０００の磁化を用いて具現化される。しかし、任意の他の適切な実施形態も考えられる。さらに、コンピュータ可読媒体１０００はここでは光学ディスクとして示されるが、コンピュータ可読媒体１０００は、ハードディスク、固体状態メモリ、フラッシュメモリ等の任意の適切なコンピュータ可読媒体であってよく、書込み不可能又は記録可能であってもよいことが理解されよう。コンピュータプログラム１０２０は、プロセッサシステムに前記方法を実

行させるための命令を備える。
【０１０９】
図７ｂは、図１～６を参照して説明されたデバイス又は方法の一実施形態に係るプロセッサシステム１１００の模式的表現を示す。プロセッサシステムは、回路１１１０、例えば１つ又は複数の集積回路、を備える。回路１１１０のアーキテクチャは、図に概略的に示されている。回路１１１０は、一実施形態に係る方法を実行する、及び／又はそのモジュール若しくはユニットを実施するためのコンピュータプログラムコンポーネントを実行するための処理ユニット１１２０、例えばＣＰＵを備える。回路１１１０は、プログラミングコード、データ等を記憶するためのメモリ１１２２を備える。メモリ１１２２の一部は、読出し専用であってよい。回路１１１０は、通信要素１１２６、例えばアンテナ、送受信機、コネクタ又はその両方等を備える。回路１１１０は、上記方法において定義される処理の一部又はすべてを行うための専用集積回路１１２４を備える。プロセッサ１１２０、メモリ１１２２、専用ＩＣ１１２４及び通信要素１１２６は、相互接続１１３０、例えばバス、を介して互いに接続される。プロセッサシステム１１１０は、それぞれコネクタ及び／又はアンテナを使用して有線及び／又は無線通信のために構成される。
【０１１０】
明瞭のために、上記の説明は、異なる機能ユニット及びプロセッサを参照して本発明の実施形態を説明していることが理解されよう。しかし、本発明から逸脱することなく、異なる機能ユニット及びプロセッサ間での適切な機能の分散が使用されてよいことが明らかになろう。例えば、別々のユニット、プロセッサ又はコントローラによって行われると説明された機能が、同じプロセッサ又はコントローラによって行われてよい。したがって、特定の機能ユニットの言及は、厳密な論理的又は物理的構造又は編成を示すのではなく、記載される機能を提供するための適切な手段の言及としてのみ見られるべきである。本発明は、ハードウェア、ソフトウェア、ファームウェア又はそれらの任意の組み合わせを含む任意の適切な形態で実施され得る。
【０１１１】
本文献において、動詞「～を備える」は、リストされるもの以外の要素又はステップの存在を排除せず、単数形は、複数のそのような要の存在を排除しないことが留意される。要素のリストの前にある場合の「の少なくとも１つ」などの表現は、リストからの要素のすべて又は任意のサブセットの選択を表す。例えば、表現「Ａ、Ｂ、及びＣの少なくとも１つ」は、Ａのみ、Ｂのみ、Ｃのみ、ＡとＢの両方、ＡとＣの両方、ＢとＣの両方、又はＡ、Ｂ、及びＣのすべてを意味するものと理解されるべきである。参照符号はいずれも、特許請求の範囲を制限するものではない。本発明は、ハードウェア及びソフトウェア両方を用いて実施されてよい。いくつかの「手段」又は「ユニット」が、同じハードウェア又はソフトウェア品によって表現されることがあり、プロセッサが、可能性としてはハードウェア要素と協働して、１つ又は複数のユニットの機能を実現する。さらに、本発明は、実施形態に限定されず、本発明は、一つ一つの新規の特徴、又は上記に説明される、若しくは相互に異なる従属請求項に記載される特徴の組み合わせに存在する。
【０１１２】
要約すると、非ＳＩデバイスがワイヤレス通信のために構成され、加入者識別へのアクセスを有するＳＩデバイスと協働する。非ＳＩデバイスは、ローカルネットワーク内で通信するための送受信機と、ＳＩとの関連付けを確立するためのプロセッサとを有する。非ＳＩ公開鍵は、第１の通信チャネルを介してＳＩデバイスに提供される。検証コードが第２の通信チャネルを介してＳＩデバイスと共有される。それぞれのチャネルは、異なり、帯域外（ＯＯＢ）チャネルを含む。非ＳＩプライベート鍵の所有の証明は、第１又は第２の通信チャネルを介してＳＩデバイスに提供される。ＳＩデバイスから、ＳＩに関係し、非ＳＩ公開鍵の少なくとも一部分に対して算出された署名を備える証明書が受信される。証明書は、非ＳＩデバイスが、ローカルネットワーク及びローカルネットワークとコアネットワークとの間のゲートウェイを介してコアネットワークにアクセスすることを確実に可能にする。

【図面】

【図１】

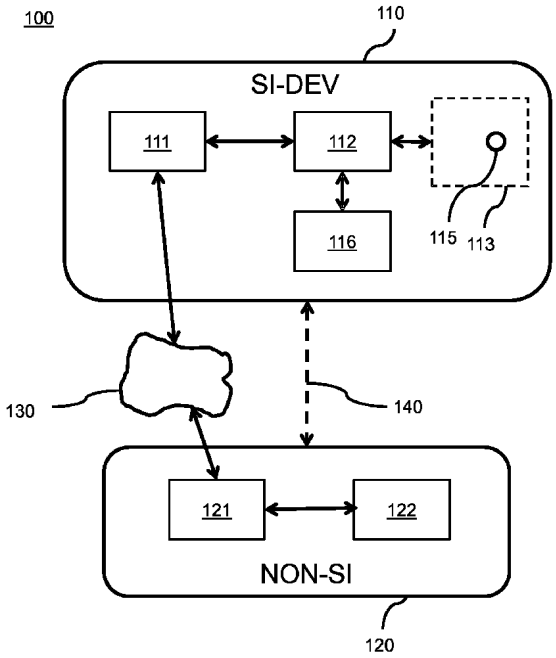

Fig. 1

【図２】

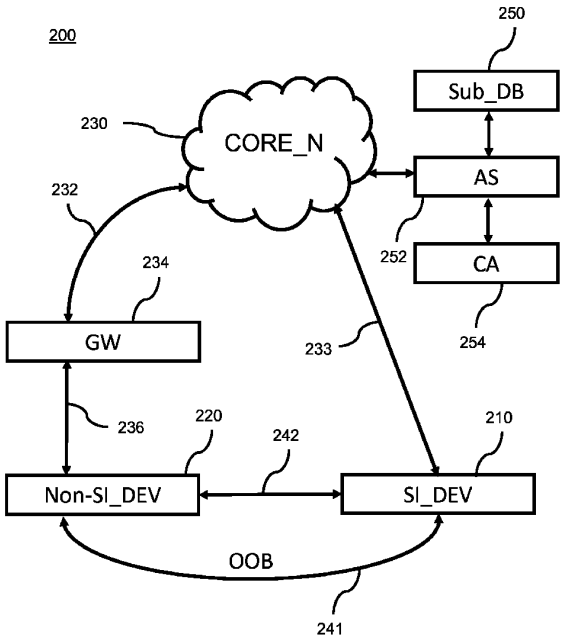

Fig. 2

【図３】

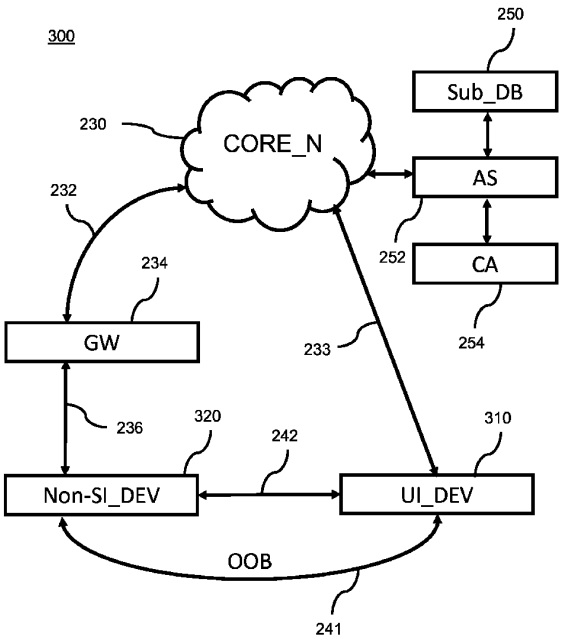

Fig. 3

【図４】

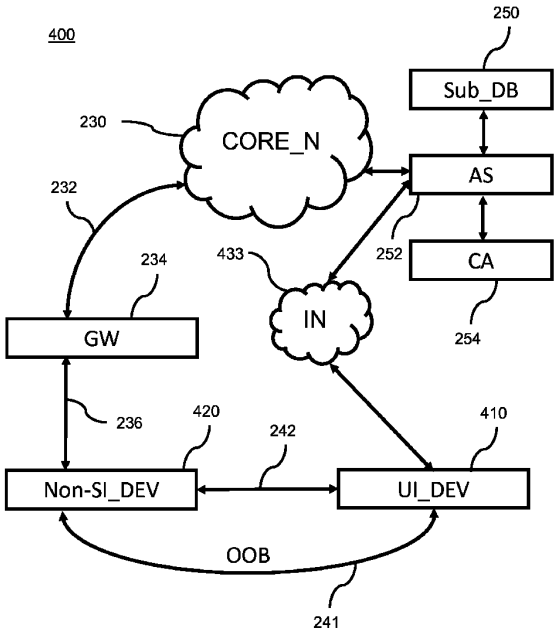

Fig. 4

【図５】

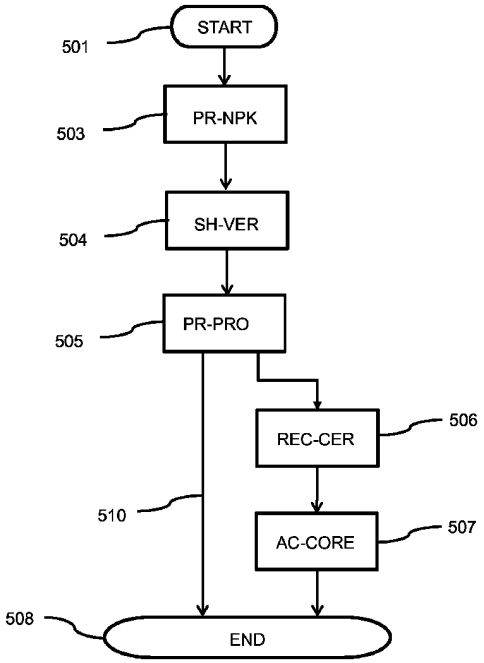

Fig. 5

【図６】

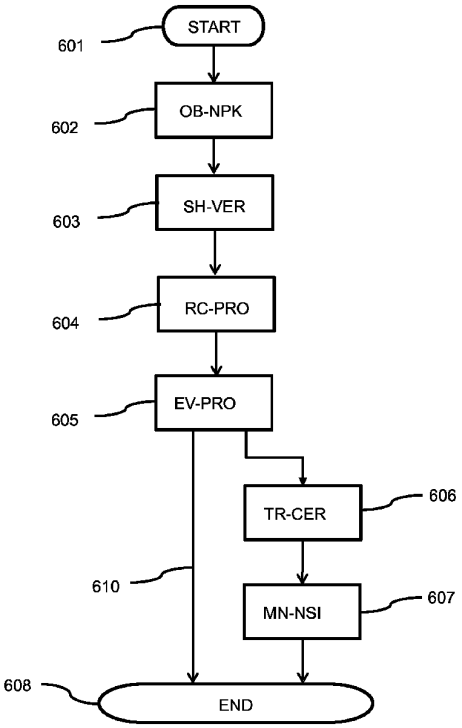

Fig. 6

【図７ａ】

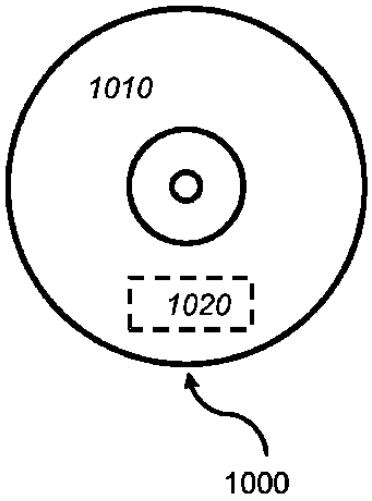

Fig. 7a

【図７ｂ】

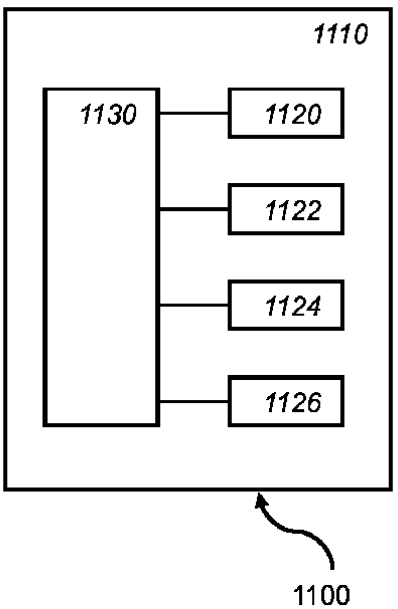

Fig. 7b

フロントページの続き

(51)国際特許分類　　ＦＩ
Ｈ０４Ｗ　12/069(2021.01)　　Ｈ０４Ｗ　12/069
Ｈ０４Ｗ　12/63　(2021.01)　　Ｈ０４Ｗ　12/63

ドーフェン ハイ テック キャンパス ５
(72)発明者　ディーズ ワルター
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５

審査官　鈴木 重幸

(56)参考文献　米国特許第９６４８０１９（ＵＳ，Ｂ２）
国際公開第２０１８／０４７６５３（WO，Ａ１）
特表２０１８－５２１５６６（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４－　７／２６
Ｈ０４Ｗ　４／００－９９／００
Ｈ０４Ｍ　１／７２５０５
Ｈ０４Ｌ１２／２２