(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6893913号
(P6893913)

(45)発行日　令和3年6月23日(2021.6.23)　(24)登録日　令和3年6月4日(2021.6.4)

(51)Int.Cl.		F I		
G06F 21/10	(2013.01)	G06F	21/10	350
H04L 9/32	(2006.01)	H04L	9/00	675D
G06F 21/64	(2013.01)	G06F	21/64	
H04W 12/06	(2021.01)	H04W	12/06	

請求項の数 14　(全 63 頁)

(21)出願番号　特願2018-505703 (P2018-505703)
(86)(22)出願日　平成28年7月7日(2016.7.7)
(65)公表番号　特表2018-529153 (P2018-529153A)
(43)公表日　平成30年10月4日(2018.10.4)
(86)国際出願番号　PCT/US2016/041402
(87)国際公開番号　WO2017/027134
(87)国際公開日　平成29年2月16日(2017.2.16)
審査請求日　令和1年6月21日(2019.6.21)
(31)優先権主張番号　62/202,664
(32)優先日　平成27年8月7日(2015.8.7)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　15/082,919
(32)優先日　平成28年3月28日(2016.3.28)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ス・ボム・イ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】デバイスの特徴のセットを使用する許可の確認

(57)【特許請求の範囲】
【請求項１】
デバイスにおいて実行可能な方法であって、
第1の許可サーバによって署名された、前記デバイスにおける選択的にアクティブ化される特徴の第1のセットを使用する前記デバイスの権限の証拠を取得するステップであって、前記アクティブ化される特徴が、前記デバイスのアクティブ化される回路、アクティブ化されるサービス、および/またはアクティブ化される機能を参照する、ステップと、
ネットワークサービスを使用する要求をネットワークノードに送るステップであって、選択的にアクティブ化される特徴の前記第1のセットは、前記ネットワークサービスを使用するために前記デバイスによって必要とされる第1の選択的にアクティブ化される特徴を含む、ステップと、
前記ネットワークノードから、前記ネットワークサービスを使用する前記要求を送ったことに応答して、前記デバイスの権限の前記証拠を求める要求を取得するステップと、
前記ネットワークノードに、前記デバイスの権限の前記証拠を送るステップと、
前記ネットワークノードに、前記ネットワークサービスを提供する前記ネットワークノードの権限の証拠を求める要求を送るステップと、
前記ネットワークノードから、第2の許可サーバによって署名された、前記ネットワークノードにおいて選択的にアクティブ化される特徴の第2のセットを使用する前記ネットワークノードの権限の前記証拠を取得するステップであって、選択的にアクティブ化される特徴の前記第2のセットが、前記ネットワークサービスを提供するために前記ネットワ

ークノードによって必要とされる第2の選択的にアクティブ化される特徴を含む、ステップと、
前記ネットワークサービスを使用する前に前記ネットワークノードの権限の前記証拠を確認するステップと、
前記ネットワークサービスを使用するために前記ネットワークノードによって必要とされる選択的にアクティブ化される特徴の第3のセットを識別するステップと、
選択的にアクティブ化される特徴の前記第3のセットが選択的にアクティブ化される特徴の前記第2のセットに含まれるかどうかの判断に基づいて、前記ネットワークサービスを使用するステップとを含む、
方法。

【請求項２】
前記デバイスの権限の前記証拠は、前記第1の許可サーバにおいて発生し、前記第1の許可サーバの秘密鍵により署名され、前記第1の選択的にアクティブ化される特徴のリスティングを含み、
前記方法は、
前記第1の許可サーバの公開鍵を使用して、前記第1の選択的にアクティブ化される特徴の前記リスティングを確認することによって、前記デバイスの権限の前記証拠を確認するステップと、
前記デバイスの公開鍵により暗号化された、前記第1の選択的にアクティブ化される特徴に関連する特徴アクティブ化鍵を取得するステップと、
前記デバイスにのみ知られている、前記デバイスの秘密鍵を使用して、前記特徴アクティブ化鍵を解読するステップと、
前記特徴アクティブ化鍵により前記第1の選択的にアクティブ化される特徴をアクティブ化し、かつ/または前記第1の選択的にアクティブ化される特徴のアクティブ化を維持するステップとをさらに含む、
請求項１に記載の方法。

【請求項３】
前記ネットワークノードの権限の前記証拠は、前記第2の許可サーバにおいて発生し、前記第2の許可サーバの秘密鍵により署名され、前記第2の選択的にアクティブ化される特徴のリスティングを含み、
前記方法は、
前記第2の許可サーバの公開鍵を使用して、前記第2の選択的にアクティブ化される特徴の前記リスティングを確認することによって、前記ネットワークノードの権限の前記証拠を確認するステップをさらに含む、
請求項１に記載の方法。

【請求項４】
前記デバイスの権限の前記証拠は、前記第1の選択的にアクティブ化される特徴をアクティブ化する許可を前記デバイスが取得する特徴アクティブ化プロセス中に、前記第1の許可サーバから取得される、
請求項１に記載の方法。

【請求項５】
ネットワーク通信回路と、
前記ネットワーク通信回路に結合された処理回路とを備えたデバイスであって、前記処理回路は、
第1の許可サーバによって署名された、前記デバイスにおける選択的にアクティブ化される特徴の第1のセットを使用する前記デバイスの権限の証拠を取得することであって、前記アクティブ化される特徴が、前記デバイスのアクティブ化される回路、アクティブ化されるサービス、および/またはアクティブ化される機能を参照する、ことと、
ネットワークサービスを使用する要求をネットワークノードに送ることであって、選択的にアクティブ化される特徴の前記第1のセットが、前記ネットワークサービスを使用す

るために前記デバイスによって必要とされる第1の選択的にアクティブ化される特徴を含む、ことと、
前記ネットワークノードから、前記ネットワークサービスを使用する前記要求を送ったことに応答して、前記デバイスの権限の前記証拠を求める要求を取得することと、
前記ネットワークノードに、前記デバイスの権限の前記証拠を送ることと、
前記ネットワークノードに、前記ネットワークサービスを提供する前記ネットワークノードの権限の証拠を求める要求を送ることと、
前記ネットワークノードから、第2の許可サーバにおいて署名された、前記ネットワークノードにおいて選択的にアクティブ化される特徴の第2のセットを使用する前記ネットワークノードの権限の前記証拠を取得することであって、選択的にアクティブ化される特徴の前記第2のセットが、前記ネットワークサービスを提供するために前記ネットワークノードによって必要とされる第2の選択的にアクティブ化される特徴を含む、ことと、
前記ネットワークサービスを使用する前に前記ネットワークノードの権限の前記証拠を確認することと、
前記ネットワークサービスを使用するために前記ネットワークノードによって必要とされる選択的にアクティブ化される特徴の第3のセットを識別することと、
選択的にアクティブ化される特徴の前記第3のセットが選択的にアクティブ化される特徴の前記第2のセットに含まれるかどうかの判断に基づいて、前記ネットワークサービスを使用することとを行うように構成される、
デバイス。

【請求項６】
ネットワークノードにおいて実行可能な方法であって、
デバイスから、ネットワークサービスを使用する要求を取得するステップと、
許可サーバによって署名された、前記デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用する前記デバイスの権限の証拠を取得するステップであって、前記アクティブ化される特徴が、前記デバイスのアクティブ化される回路、アクティブ化されるサービス、および/またはアクティブ化される機能を参照する、ステップと、
前記デバイスの権限の前記証拠を確認するステップと、
前記ネットワークサービスを使用する前記デバイスによって必要とされる選択的にアクティブ化される特徴の第2のセットを識別するステップと、
前記デバイスの権限の前記証拠を確認した結果に基づいて前記要求への応答を送るとともに、選択的にアクティブ化される特徴の前記第2のセットが、選択的にアクティブ化される特徴の前記第1のセットに含まれているかどうかを決定するステップとを含む、
方法。

【請求項７】
選択的にアクティブ化される特徴の前記第1のセットは、第1の選択的にアクティブ化される特徴を含み、
前記デバイスの権限の前記証拠は、前記許可サーバにおいて発生し、前記第1の選択的にアクティブ化される特徴のリスティングを含み、前記許可サーバの秘密鍵によって署名され、
前記方法は、
前記許可サーバの公開鍵を使用して、前記第1の選択的にアクティブ化される特徴の前記リスティングを確認することによって、前記デバイスの権限の前記証拠を確認するステップをさらに含む、
請求項６に記載の方法。

【請求項８】
選択的にアクティブ化される特徴の前記第2のセットを識別するステップは、
前記許可サーバによって維持される許可された選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、前記ネットワークサービスを使用するために前記デバイスによって必要とされる選択的にアクティブ化される特徴を導出するス

テップ、または、
前記許可サーバによって維持されるライセンス可能な選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、前記ネットワークサービスを使用するために前記デバイスによって必要とされる選択的にアクティブ化される特徴を導出するステップを含む、
請求項６に記載の方法。
【請求項９】
前記方法は、
前記デバイスの権限の前記証拠とともに含まれる前記デバイスの公開鍵に対応する秘密鍵を前記デバイスが保有していることを検証するステップをさらに含み、前記要求への前記応答を送るステップは、前記検証の結果にさらに基づく、
請求項６に記載の方法。
【請求項１０】
ネットワーク通信回路と
前記ネットワーク通信回路に結合された処理回路とを備えたネットワークノードであって、前記処理回路は、
デバイスから、ネットワークサービスを使用する要求を取得することと、
許可サーバによって署名された、前記デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用する前記デバイスの権限の証拠を取得することであって、前記アクティブ化される特徴が、前記デバイスのアクティブ化される回路、アクティブ化されるサービス、および/またはアクティブ化される機能を参照する、ことと、
前記デバイスの権限の前記証拠を確認することと、
前記ネットワークサービスを使用する前記デバイスによって必要とされる選択的にアクティブ化される特徴の第2のセットを識別することと、
選択的にアクティブ化される特徴の前記第2のセットが、選択的にアクティブ化される特徴の前記第1のセットに含まれているかどうかの決定に基づいて、前記要求への応答を送ることとを行うように構成される、
ネットワークノード。
【請求項１１】
サーバにおいて実行可能な方法であって、
デバイスの選択的にアクティブ化される特徴の第1のリストを取得するステップであって、前記アクティブ化される特徴が、前記デバイスのアクティブ化される回路、アクティブ化されるサービス、および/またはアクティブ化される機能を参照する、ステップと、
前記第1のリストに基づいて、前記サーバに記憶された、前記デバイスの選択的にアクティブ化される特徴の第2のリストを、前記第2のリストにおける少なくとも1つの選択的にアクティブ化される特徴の許可ステータスの変更を反映するように更新するステップであって、前記第2のリストが、前記デバイスのサブスクリプションプロファイルに関連付けられる、ステップとを含む、
方法。
【請求項１２】
前記サーバはホーム加入者サーバ(HSS)であり、
前記方法は、
前記デバイスの能力に関するクエリに応答して、前記デバイスの選択的にアクティブ化される特徴の前記第2のリストを含む能力プロファイルを送るステップをさらに含む、
請求項１１に記載の方法。
【請求項１３】
選択的にアクティブ化される特徴の前記第1のリストは、許可サーバにおいて発生し、前記許可サーバの秘密鍵により署名され、
前記方法は、
前記許可サーバの公開鍵を使用して、選択的にアクティブ化される特徴の前記第1のリ

ストを確認するステップをさらに含む、
請求項１１に記載の方法。
【請求項１４】
ネットワークを介して通信するネットワーク通信回路と、
前記ネットワーク通信回路に結合された処理回路とを備えたサーバであって、前記処理回路は、
デバイスの選択的にアクティブ化される特徴の第1のリストを取得することであって、前記アクティブ化される特徴が、前記デバイスのアクティブ化される回路、アクティブ化されるサービス、および/またはアクティブ化される機能を参照する、ことと、
前記第1のリストに基づいて、前記サーバに記憶された、前記デバイスの選択的にアクティブ化される特徴の第2のリストを、前記第2のリストにおける少なくとも1つの選択的にアクティブ化される特徴の許可ステータスの変更を反映するように更新することであって、前記第2のリストが、前記デバイスのサブスクリプションプロファイルに関連付けられる、こととを行うように構成される、
サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、2015年8月7日に米国特許商標庁に提出された仮出願第62/202,664号、および2016年3月28日に米国特許商標庁に提出された非仮出願第15/082,919号の優先権および利益を主張し、それらの内容全体が参照により本明細書に組み込まれる。
【０００２】
本出願は、選択的にアクティブ化され得る特徴のセットをアクティブ化し、それによって、デバイスと許可を確認するエンティティとの間のサービスを開始または維持するための、デバイスによって受信された許可の確認に関する。
【背景技術】
【０００３】
たいていの通信デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)は、複数の特徴を提供する。特徴は、ハードウェアおよび/またはソフトウェアにおいて実装され得る。
【０００４】
通信デバイスのいくつかの特徴は、エンティティが通信デバイスを取得したときにアクティブ化され得る。他の特徴は、アクティブ化されないことがある。たとえば、製造業者、サブ構成要素の製造業者、または相手先商標製造会社(OEM)が、1つまたは複数の特徴を内包する異なるモデル(たとえば、バージョン)の通信デバイスを生成し、1つまたは複数の特徴がデバイスモデルに基づいてアクティブ化または非アクティブ化され得る。結果として、通信デバイスの特徴のサブセット(たとえば、セット全体に満たない)が、最終製品において実行可能であり得る。たとえば、第1のモデルと第2のモデルの両方が、ある特徴を実装するために使用されるすべてのハードウェアおよびソフトウェアを含むにもかかわらず、製造業者は、第1のモデルにおいて当該特徴をアクティブ化するが、第2のモデルにおいて当該特徴をアクティブ化しないことがある。追加または代替として、通信デバイス上に記憶された処理回路可読命令の部分が、特徴のアクティブ化を妨げるように実行されないことがある。ハードウェアおよび/またはソフトウェアを有効化および/または無効化することは、最終製品においてアクティブ化される特徴の数を増加および/または減少させ、たとえば、最終製品の価格に影響を与え得る。
【０００５】
したがって、通信デバイスが配備されるとき、通信デバイスは、それの動作の一部としていくつかの特徴を実行することが(たとえば、ハードウェアおよび/またはソフトウェアまたはファームウェアに関して)可能であり得るが、いくつかの特徴を使用することを許

可されていないことがある。特徴を使用する権限に対する制限は、たとえば、通信デバイスにとって利用可能な特徴および/またはサービスの使用を制限する購入契約に基づき得る。

【発明の概要】

【課題を解決するための手段】

【０００６】

本明細書で開示する態様は、電子デバイスの1つまたは複数の特徴から成るセットを使用する許可を動的に確認するための方法および装置を提供する。

【０００７】

いくつかの態様では、方法は、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を取得するステップを含み得る。デバイスの権限の証拠は、第1の許可サーバによって署名され得る。本方法は、ネットワークサービスを使用する要求をネットワークノードに送るステップを含むことができ、選択的にアクティブ化される特徴の第1のセットは、ネットワークサービスを使用するためにデバイスによって必要とされる第1の選択的にアクティブ化される特徴を含む。デバイスはネットワークノードから、ネットワークサービスを使用する要求を送ったことに応答して、デバイスの権限の証拠を求める要求を取得し得る。デバイスはネットワークノードに、デバイスの権限の証拠と、ネットワークサービスを提供するネットワークノードの権限の証拠を求める要求とを送り得る。デバイスはネットワークノードから、第2の許可サーバによって署名された、ネットワークノードにおいて選択的にアクティブ化される特徴の第2のセットを使用するネットワークノードの権限の証拠を取得することができ、選択的にアクティブ化される特徴の第2のセットは、ネットワークサービスを提供するためにネットワークノードによって必要とされる第2の選択的にアクティブ化される特徴を含む。本方法はまた、ネットワークサービスを使用する前にネットワークノードの権限の証拠を確認するステップを含み得る。

【０００８】

いくつかの例では、デバイスは、チップ構成要素、クライアントデバイス、ネットワークアクセスノード、モビリティ管理エンティティ、またはゲートウェイデバイスであり得る。一例では、デバイスはクライアントデバイスまたはチップ構成要素であり得、ネットワークノードはネットワークアクセスノードであり得る。

【０００９】

一態様では、デバイスの権限の証拠は、第1の許可サーバにおいて発生し得、第1の許可サーバの秘密鍵により署名され得、第1の選択的にアクティブ化される特徴のリスティングを含み得る。本方法は、第1の許可サーバの公開鍵を使用して、第1の選択的にアクティブ化される特徴のリスティングを確認することによって、デバイスの権限の証拠を確認するステップをさらに含み得る。本方法は、またさらに、デバイスの公開鍵により暗号化された、第1の選択的にアクティブ化される特徴に関連する特徴アクティブ化鍵を取得するステップと、デバイスにのみ知られている、デバイスの秘密鍵を使用して、特徴アクティブ化鍵を解読するステップと、特徴アクティブ化鍵により第1の選択的にアクティブ化される特徴をアクティブ化し、かつ/または第1の選択的にアクティブ化される特徴のアクティブ化を維持するステップとを含み得る。

【００１０】

ネットワークノードの権限の証拠が第2の許可サーバにおいて発生し、第2の許可サーバの秘密鍵により署名され、第2の選択的にアクティブ化される特徴のリスティングを含む例では、本方法は、第2の許可サーバの公開鍵を使用して、第2の選択的にアクティブ化される特徴のリスティングを確認することによって、ネットワークノードの権限の証拠を確認するステップをさらに含み得る。

【００１１】

一態様では、第1の許可サーバはローカル許可サーバであり得る。

【００１２】

別の態様では、本方法は、ネットワークサービスを使用するためにネットワークノードによって必要とされる選択的にアクティブ化される特徴の第3のセットを識別するステップと、選択的にアクティブ化される特徴の第3のセットが選択的にアクティブ化される特徴の第2のセットに含まれるかどうかの判断に基づいてネットワークサービスを使用するステップとをさらに含み得る。

【００１３】

一実装形態では、デバイスの権限の証拠は、第1の許可サーバにおいて発生し、デバイスにおいて、第1の許可サーバから取得され、ネットワークノードの権限の証拠は、第2の許可サーバにおいて発生し、デバイスにおいて、ネットワークノードから取得される。一態様では、第1の許可サーバおよび第2の許可サーバは、1つの許可サーバであり得る。

【００１４】

いくつかの態様では、デバイスの権限の証拠は、第1の選択的にアクティブ化される特徴をアクティブ化する許可をデバイスが取得する特徴アクティブ化プロセス中に、第1の許可サーバから取得される。いくつかの態様では、デバイスの権限の証拠は、許可証明を表すデータであり得る。他の態様では、デバイスの権限の証拠は、デバイスが第1の選択的にアクティブ化される特徴をアクティブ化することを許可されていることを示す許可合意を表すデータであり得る。

【００１５】

一例では、デバイスは、ネットワーク通信回路と、ネットワーク通信回路に結合された処理回路とを含む。処理回路は、上述の方法を実行するように構成され得る。

【００１６】

別の態様では、ネットワークノードにおいて実行可能な方法は、デバイスから、ネットワークサービスを使用する要求を取得するステップを含み得る。本方法は、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を取得するステップを含み得る。デバイスの権限の証拠は、許可サーバによって署名され得る。本方法はまた、デバイスの権限の証拠を確認するステップを含み得る。本方法は、ネットワークサービスを使用するためにデバイスによって必要とされる選択的にアクティブ化される特徴の第2のセットを識別するステップと、デバイスの権限の証拠を確認し、選択的にアクティブ化される特徴の第2のセットが選択的にアクティブ化される特徴の第1のセットに含まれるかどうかを判断した結果に基づいて、要求への応答を送るステップとをさらに含み得る。いくつかの態様では、ネットワークノードは、ネットワークアクセスノード、モビリティ管理エンティティ、またはゲートウェイデバイスであり得る。

【００１７】

一例では、選択的にアクティブ化される特徴の第1のセットは、第1の選択的にアクティブ化される特徴を含み、デバイスの権限の証拠は、許可サーバにおいて発生する。デバイスの権限の証拠は、許可サーバの秘密鍵により署名された、第1の選択的にアクティブ化される特徴のリスティングを含むことができる。本方法は、許可サーバの公開鍵を使用して、第1の選択的にアクティブ化される特徴のリスティングを確認することによって、デバイスの権限の証拠を確認するステップをさらに含むことができる。

【００１８】

一態様では、デバイスの権限の証拠は、許可サーバにおいて発生し得、ネットワークノードにおいて、デバイスから取得され得る。別の態様では、デバイスの権限の証拠は、許可サーバにおいて発生し得、ネットワークノードにおいて、ホーム加入者サーバ(HSS)から、デバイスの能力プロファイルの形式で取得され得る。

【００１９】

一実装形態では、デバイスの権限の証拠は、許可証明を表すデータであり得る。別の実装形態では、デバイスの権限の証拠は、デバイスが選択的にアクティブ化される特徴の第1のセットをアクティブ化することを許可されていることを示す許可合意を表すデータであり得る。

【００２０】

一態様では、選択的にアクティブ化される特徴の第2のセットを識別するステップは、許可サーバによって維持される許可された選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、ネットワークサービスを使用するためにデバイスによって必要とされる選択的にアクティブ化される特徴を導出するステップを含むことができる。別の態様では、選択的にアクティブ化される特徴の第2のセットを識別するステップは、許可サーバによって維持されるライセンス可能な選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、ネットワークサービスを使用するためにデバイスによって必要とされる選択的にアクティブ化される特徴を導出するステップを含むことができる。

【００２１】

一実装形態では、本方法は、デバイスの権限の証拠とともに含まれるデバイスの公開鍵に対応する秘密鍵をデバイスが保有していることを検証するステップを含むことができ、要求への応答を送るステップは、検証の結果にさらに基づく。

【００２２】

一態様では、ネットワークノードは、ネットワーク通信回路と、ネットワーク通信回路に結合された処理回路とを含むことができる。処理回路は、上述の方法を実行するように構成され得る。

【００２３】

一態様では、サーバにおいて実行可能な方法は、デバイスの選択的にアクティブ化される特徴の第1のリストを取得するステップと、第1のリストに基づいて、サーバに記憶された、デバイスの選択的にアクティブ化される特徴の第2のリストを、第2のリストにおける少なくとも1つの選択的にアクティブ化される特徴の許可ステータスの変更を反映するように更新するステップであって、第2のリストは、デバイスのサブスクリプションプロファイルに関連付けられる、ステップとを含み得る。

【００２４】

一例では、サーバはホーム加入者サーバ(HSS)であり得る。

【００２５】

一実装形態では、本方法は、デバイスの能力に関するクエリに応答して、デバイスの選択的にアクティブ化される特徴の第2のリストを含む能力プロファイルを送るステップをさらに含むことができる。

【００２６】

一態様では、選択的にアクティブ化される特徴の第1のリストが許可サーバにおいて発生し、許可サーバの秘密鍵により署名されるとき、本方法は、許可サーバの公開鍵を使用して、選択的にアクティブ化される特徴の第1のリストを確認するステップをさらに含み得る。

【００２７】

一態様では、許可サーバはローカル許可サーバであり得る。

【００２８】

一態様では、選択的にアクティブ化される特徴の第1のリストは、許可サーバによって署名された許可証明を表すデータであり得る。別の態様では、選択的にアクティブ化される特徴の第1のリストは、デバイスが選択的にアクティブ化される特徴をアクティブ化することを許可されていることを示す許可合意を表すデータであり得る。

【００２９】

一態様では、サーバ(たとえば、HSS)は、ネットワークを介して通信するためのネットワーク通信回路と、ネットワーク通信回路に結合された処理回路とを含むことができる。処理回路は、上述の方法を実行するように構成され得る。

【図面の簡単な説明】

【００３０】

【図１】本明細書で説明する態様による、1つまたは複数のデバイスから成るセット上で1つまたは複数の選択的にアクティブ化される特徴を動的に許可およびアクティブ化し得る

例示的なシステムのブロック図である。
【図２】本明細書で説明する態様による例示的な動作環境を示す図である。
【図３】本明細書で説明する態様によるシステムのアーキテクチャ参照モデルである。
【図４】本明細書で説明する態様による、第1のエンティティと1つまたは複数のデバイスの製造業者またはOEMとの間の例示的な許可合意に含まれ得るパラメータおよびデータの例示的なリストを示す図である。
【図５】本明細書で説明する態様による、製造業者またはOEMと別のエンティティとの間の例示的な許可合意に含まれ得るパラメータおよびデータの例示的なリストを示す図である。
【図６】本明細書で説明する態様による、ネットワーク事業者と別のエンティティとの間の例示的な許可合意に含まれ得るパラメータおよびデータの例示的なリストを示す図である。
【図７】本明細書で説明する態様による、デバイスへの許可証明、許可ファイル、特徴アクティブ化鍵、およびソフトウェアの送信に関係するアクションを示すフロー図である。
【図８】本明細書で説明する態様による、特徴アクティブ化要求を伴う方法を示すフロー図である。
【図９】本明細書で説明する態様による、選択的にアクティブ化される特徴のアクティブ化の一例を示すフロー図である。
【図１０】本明細書で説明する態様による、許可合意の動的な検証および実施をサポートするように構成された許可サーバを示すブロック図である。
【図１１】本明細書で説明する態様による、許可合意の動的な検証および実施をサポートするように構成されたローカル許可サーバを示すブロック図である。
【図１２】本明細書で説明する態様による、許可合意の動的な検証および実施に関係する呼フロー図である。
【図１３】本明細書で説明する態様による、デバイスのサブスクリプションプロファイルに基づいて、選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を確認することに関連して発生し得るシステムレベル呼フローを示す例示的な呼フロー図である。
【図１４】本明細書で説明する態様による、デバイスに記憶された許可証明において識別される選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を確認することに関連付けられ得る別のシステムレベル呼フローを示す例示的な呼フロー図である。
【図１５】本明細書で説明する態様による、許可合意の動的な検証および実施をサポートするように構成された例示的なデバイスを示すブロック図であって、実施が、選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠の動的な確認と、許可合意の条件に従った選択的にアクティブ化される特徴のアクティブ化/非アクティブ化とを含む、ブロック図である。
【図１６】本明細書で説明する態様による、デバイスにおいて実行可能な例示的な方法のフローチャートである。
【図１７】本明細書で説明する態様による、デバイスにおいて実行可能な例示的な方法のフローチャートである。
【図１８】本明細書で説明する態様による、ネットワークノードにおいて実行可能な例示的な方法のフローチャートである。
【図１９】本明細書で説明する態様による、ネットワークノードにおいて実行可能な別の例示的な方法のフローチャートである。
【図２０】本明細書で説明する態様による、許可合意の検証および実施をサポートするように構成された例示的なホーム加入者サーバ(HSS)を示すブロック図である。
【図２１】本明細書で説明する態様による、デバイスの1つまたは複数の特徴のセットを使用する許可を確認することに関係する、HSSにおいて実行可能な例示的な方法を示す図である。

【発明を実施するための形態】
【００３１】
以下の説明では、添付の図面に対する参照が行われ、添付の図面には、例として、本開示で説明する特定の態様および特徴が示される。本開示で説明する態様および特徴は、当業者が本開示の態様を実践することを可能にするだけ十分詳しく提供されることが意図される。本開示の範囲から逸脱することなく、他の態様および特徴が利用されてよく、また開示されたものに対して変更が行われてよい。以下の詳細な説明は限定的な意味で解釈されるべきではなく、本明細書で説明および図示する態様および特徴の範囲は、添付の特許請求の範囲によってのみ定義される。
【００３２】
「例示的」という用語は、「例、事例、または例示の働きをすること」を意味するために本明細書で使用される。「例示的」として本明細書で説明するいかなる態様または実装形態も、他の態様または実装形態よりも好ましいか、または有利であると必ずしも解釈されるべきでない。
【００３３】
本明細書で使用する「態様」という用語は、すべての態様が、説明する態様、または任意の説明する態様、利点、および/もしくは動作モードを含むことを必要としない。
【００３４】
「取得する」という用語は、導出する、生成する、計算する、要求する、受信する、獲得する、受諾する、調達する、取る、収集する、得る、配信または受信を行う、与えられる、アクセスできるようになる、入手するなどを意味するために本明細書で使用される。本明細書で使用する「取得する」という用語は、ローカルに取得すること、および/または非ローカルエンティティもしくはリモートエンティティから取得することを包含する。
【００３５】
「プロビジョニングする」という用語は、宛先まで運搬させるために送る、転送する、提供する、供給するを意味するために本明細書で使用される。「送る」という用語は、宛先まで運搬させるためにプロビジョニングする、転送する、提供する、供給するを意味するために本明細書で使用される。
【００３６】
本明細書で使用する「製造業者」という用語は、製品を作り、消費者またはOEMにエンティティ自体の名前で製品を販売するエンティティを指し得る。OEMは、別のエンティティから製品を購入し、OEMの名前で販売するために製品をリブランドするエンティティであり得る。OEMは、追加または代替として、同じまたは異なる製造業者から、異なるタイプの製品(たとえば、サーバおよびデータ記憶製品)を購入し、製品を一緒にバンドルし、得られたバンドルされた製品をOEMの名前で販売するエンティティであり得る。
【００３７】
「デバイス」という用語は、チップ構成要素、クライアントデバイス、および/またはネットワークノードなどの任意の通信デバイスを指すために本明細書で使用され得る。「チップ構成要素」は、たとえば、処理回路、モデム、チップセットを含み得る。「クライアントデバイス」は、たとえば、ワイヤレスデバイス、モバイルデバイス、加入者デバイス、携帯電話、モバイル通信デバイス、モバイルコンピューティングデバイス、デジタルタブレット、スマートフォン、ユーザ機器(UE)、ユーザデバイス、ユーザ端末、端末、局(STA)を含み得る。「ネットワークノード」は、サービングネットワークまたはホームネットワークの機能ノードである任意のデバイスまたは機械を含み得る。ネットワークノードの例としては、限定はしないが、基地局、ネットワークアクセスノード(たとえば、発展型ノードB(eNodeB、eNB))、モビリティ管理エンティティ(MME)、ゲートウェイデバイス(たとえば、サービングゲートウェイ(S-GW)、パケットデータネットワークゲートウェイ(P-GW))、ホーム加入者サーバ(HSS)、許可、認証、およびアカウンティング(AAA)サーバ(まとめてHSS/AAAサーバと呼ばれる)、ワイヤレスルータ、アクセスポイント(AP)、および/またはネットワーク機能を実行する任意のノードがある。クライアントデバイスおよび/

またはネットワークノードは、チップ構成要素を含み得る。

【００３８】

「ネットワークアクセスノード」という用語は、デバイス(たとえば、チップ構成要素、クライアントデバイス)とコアネットワークとの間のワイヤレスデバイス接続を含む任意のデバイスを指すために本明細書で使用され得る。ネットワークアクセスノードの例としては、eNB、基地局、APがあり得る。ネットワークアクセスノードは、ネットワークノードの一例であると理解され得る。

【００３９】

パケットデータネットワーク(PDN)(たとえば、インターネット)およびIPマルチメディアサービス(IMS)ネットワークなどの、セルラー通信システムのコアネットワークの外部のネットワークは、PDNへの参照によって本明細書で例示されることがあるが、コアネットワークの外部のネットワークをPDNまたはIMSネットワークに限定することは何ら意図されない。さらに、本明細書で提示する態様および特徴は例示的である。本明細書で提示する任意の態様または特徴を、セルラー通信システムにおいて使用することに限定することは、何ら意図されていない。

【００４０】

本明細書で使用する、「選択的にアクティブ化される特徴」への言及を含む「特徴」への言及は、ハードウェア、ソフトウェア、ファームウェア、またはハードウェア、ソフトウェア、およびファームウェアのうちの2つ以上から成る任意の組合せにおいて実装され得るデバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)の態様、回路、サービス、または機能への言及であり得る。

【００４１】

「選択的にアクティブ化される」という用語は、それのアクティブ化状態が変更される(たとえば、それがアクティブ化および非アクティブ化され得る)、特性、または能力を表し得る。いくつかの態様では、「選択的にアクティブ化される」という用語は、(たとえば、コマンド/要請に応じて)特に有効化/無効化され、オン/オフにされ、かつ/または開始/停止される特性、または能力を表し得る。したがって、選択的にアクティブ化される特徴は、たとえば、(たとえば、コマンド/要請に応じて)特にアクティブ化および/または非アクティブ化されることが可能である特徴である。

【００４２】

本明細書で使用する「ネットワークサービス」への言及は、ネットワークによって提供されるか、またはネットワークを通じて利用可能である機能、能力、アプリケーション、またはそれらの一部分への言及であり得る。デバイス(たとえば、クライアントデバイス、チップ構成要素、ネットワークノード)は、ネットワークサービスを実施するために、選択的にアクティブ化される特徴のセットを含み得る。

【００４３】

本明細書で使用する「許可情報」という用語は、「デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠」または「ネットワークノードにおいて選択的にアクティブ化される特徴のセットを使用するネットワークノードの権限の証拠」を意味するように理解される。許可情報は、許可合意、許可証明、もしくは許可合意および許可証明によって表されること、これらを含むこと、またはこれらを識別することがある。代替または追加として、許可情報は、許可サーバ(またはローカル許可サーバ)に記憶された許可合意から、許可サーバ(またはローカル許可サーバ)によって導出された選択的にアクティブ化される特徴のセットのリストを含むこと、または識別することがある。

【００４４】

本明細書で使用する「特徴アクティブ化鍵」への言及は、所与の特徴を有効化するために使用されるデータ(たとえば、ビットのシーケンスまたは列)への言及であり得る。特徴アクティブ化鍵は、暗号関数に関係すること、および/または暗号関数により導出されることがある。

【００４５】
「最新の」という用語は、有効性が現時点まで及んでいる物(たとえば、ライセンス)を示すか、または表すために使用され得る。したがって、たとえば、最新のライセンスは、現時点まで有効であるライセンスであり得る。
【００４６】
本明細書で使用する「合致する」という用語は、いくつかの基礎的または基本的な点で「に等しい」を意味し得るか、または「に対応すること」を意味し得る。
【００４７】
デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)がネットワークサービスを使用することを求めているとき、デバイスは、ネットワークサービスを提供するネットワークノードに対してデバイス自体を認証することに加えて、デバイスが選択的にアクティブ化される特徴のセットをアクティブ化することを許可されていることの証拠をネットワークノードに送る必要もあり得る。選択的にアクティブ化される特徴のセット、またはそのサブセットは、ネットワークサービスを使用するためにデバイスによって必要とされ得る。結果として、選択的にアクティブ化される特徴のセットをアクティブ化するデバイスの権限を証明するために、デバイスは、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠を送り得る。この権限の証拠は、デバイスによって許可サーバから取得され得る。デバイスは、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠を、ネットワークサービスを提供するネットワークノードに送り得る。一態様では、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠は、デバイスにおいてアクティブ化されることを許可されている選択的にアクティブ化される特徴のセットにおける特徴を識別するリストを含み得る。一態様では、選択的にアクティブ化される特徴のセットは、許可合意から導出され得る。許可合意は、許可サーバに記憶され得る。デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠は、ネットワークノードによって確認され得る。一態様では、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠を確認することで、ネットワークノードは、デバイスがネットワークサービスを使用する前に、ネットワークサービスを使用するためにデバイスによって必要とされる選択的にアクティブ化される特徴が、たとえば、デバイス上で使用することを許可されていることを確実にすることができる。たとえば、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠を確認することで、ネットワークノードは、デバイスがネットワークサービスを使用する前に、選択的にアクティブ化される特徴のセットに記載された選択的にアクティブ化される特徴に対して、許可合意に反映され得る、ライセンスの条件に基づいて支払いが行われていることを確実にすることができる。
【００４８】
たとえば、ネットワークアクセスノード(たとえば、eNB)が、サービスを提供することを許可されているとき、ネットワークアクセスノードの能力(たとえば、保証された配信、保証された帯域幅、および/またはサービス品質に関係する他の態様)を告知するメッセージが、メッセージを受信するデバイス(たとえば、チップ構成要素、クライアントデバイス)がサービスを使用することを望むかどうかを判断できるように、オーバージエアでブロードキャストされ得る。メッセージを受信するデバイスは、アクティブ化することをすでに許可されていることがあり、サービスを使用するために必要とされる選択的にアクティブ化される特徴のセットをすでにアクティブ化していることがある。それでも、デバイスは、ネットワークアクセスノードがサービスを提供する許可を確認することを望むことがある。デバイスは、たとえば、利用不可能なネットワークサービスに対する追加料金を回避するために、ネットワークアクセスノードがネットワークサービスを提供することを許可されていることを確認する機会を有するべきである。一態様では、ネットワークアクセスノードがサービスを提供する許可を確認することで、デバイスは、デバイスがサービスを使用する前に、ネットワークアクセスノードがサービスを提供することを許可され

ていることを確実にすることができる。

【００４９】

例として、システム情報ブロードキャスト(SIB)および(1つまたは複数のSIBを運搬するために使用される)システム情報(SI)メッセージは、ネットワークノードによって署名されたメッセージ認証コードまたは署名を一切搬送しない。デバイスが、セルにキャンプオンされ、ネットワークアクセスノードからSIBを取得する場合、デバイスは、SIBにおいて広告された特徴がネットワークノードによって有効に提供されるかどうかを検証することができない。ネットワークにアクセスできるようになるために、デバイスは基本的に、検証する能力なしで、ネットワークがSIBにおいて広告されている特徴を提供することを許可されていると信じる。

【００５０】

本明細書で開示する態様は、第1のデバイスまたはノードが、第1の許可情報を第2のデバイスまたはノードに送り、第2のデバイスまたはノードによって提供されるサービスを使用し始める前に第2のデバイスまたはノードから第2の許可情報を取得することができるように、動的に許可情報を確認するための方法および装置を提供することができる。本明細書で開示する態様は、ネットワークノードが有効なネットワークノードであるかどうか、およびネットワークノードがいくつかの特徴をアクティブ化することを許可されているかどうかをデバイスが検証することを可能にし得る。一態様では、確認、検証、または確認および検証は、暗号化動作を含み得る。

【００５１】

概要

デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)は、デバイスの1つまたは複数の選択的にアクティブ化される特徴をアクティブ化し、非アクティブ化し、かつ/または当該特徴について報告する許可回路/機能/モジュールを含み得る。許可回路/機能/モジュールはさらに、デバイスが所与の特徴をアクティブ化および/または使用/提供する権限を有することを検証し得る。いくつかの態様では、検証は、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠(たとえば、デバイスの許可情報)の確認により得る。

【００５２】

一態様では、クライアントデバイスを一例として使用すると、クライアントデバイスは、ネットワークサービスがネットワークノード(たとえば、ネットワークアクセスノード、eNB、MME)から利用可能であると判断し得る。クライアントデバイスは、クライアントデバイスがサービスを使用するために(たとえば、クライアントデバイスにとって利用可能な複数の特徴の中から)どの特徴を必要とするかを判断し得る。クライアントデバイスは、クライアントデバイスにおいて選択的にアクティブ化される特徴のセットを使用するクライアントデバイスの権限の証拠(たとえば、許可証明の形式をとる許可情報)と、ネットワークサービスを使用するために必要とされる特徴をアクティブ化するために必要とされる特徴アクティブ化鍵とを取得するために、許可サーバとの特徴アクティブ化プロセスに関与し得る。クライアントデバイスは、ネットワークサービスを使用することを求める要求をネットワークノードに送り得る。クライアントデバイスは、クライアントデバイスにおいて選択的にアクティブ化される特徴のセットを使用するクライアントデバイスの権限の証拠(たとえば、デバイスの許可情報)をネットワークノードに送り得る。応答して、クライアントデバイスは、ネットワークサービスを使用する要求を承認するネットワークノードからの応答を取得し得る。応答は、クライアントデバイスによってネットワークノードに送られた許可情報をネットワークノードが確認することに基づいていることがある。さらに、ネットワークノードがMMEである場合、ネットワークノードは、クライアントデバイスのクライアントデバイスコンテキスト(たとえば、UEコンテキスト)を構成するために、許可情報に含まれ得る、クライアントデバイスにおいてアクティブ化されることを許可された特徴のリストを使用し得る。

【００５３】

クライアントデバイスは、ネットワークサービスを使用する前に、サービスを提供するネットワークノードの権限を確認することを望むことがある。したがって、クライアントデバイスはネットワークノードから、ネットワークノードにおいて選択的にアクティブ化される特徴のセットを使用するネットワークノードの権限の証拠(たとえば、許可証明の形式をとる許可情報)を取得し得る。クライアントデバイスは、ネットワークサービスを使用する前に、ネットワークノードにおいて選択的にアクティブ化される特徴のセットを使用するネットワークノードの権限の証拠を検証し得る。

【００５４】

例示的なシステムおよびシステムの説明

図1は、本明細書で説明する態様による、1つまたは複数のデバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)から成るセット上で1つまたは複数の選択的にアクティブ化される特徴を動的に許可およびアクティブ化し得る例示的なシステム100のブロック図である。1つまたは複数のデバイスから成るセットは、図1において、デバイスA102、デバイスB104、およびデバイスC106により例示されている。デバイスA102、デバイスB104、およびデバイスC106はそれぞれ、許可回路/機能/モジュール108、112、116を含み得る。許可回路/機能/モジュール108、112、116は、たとえば、ライセンスの条件に従って、リアルタイムで、たとえば、個別にアクティブ化/非アクティブ化(たとえば、有効化/無効化)され得るデバイス特徴(たとえば、選択的にアクティブ化される特徴)を使用して全体的にまたは部分的にサービス(たとえば、ネットワークサービス)が実施され得るシステムにおいて有用であり得る。許可回路/機能/モジュール108、112、116は、選択的にアクティブ化される特徴を含むデバイスA102、デバイスB104、またはデバイスC106などの任意のデバイスとともに含まれ得、選択的にアクティブ化される特徴をアクティブ化する許可が、たとえば、許可合意120に基づき得る。したがって、許可合意120は、選択的にアクティブ化される特徴をアクティブ化する権利の証拠の源であり得る。

【００５５】

デバイスA102は、許可回路/機能/モジュールA108と、選択的にアクティブ化される特徴の第1のセット110とを含む。デバイスB104は、許可回路/機能/モジュールB112と、選択的にアクティブ化される特徴の第2のセット114とを含む。デバイスC106は、許可回路/機能/モジュールC116と、選択的にアクティブ化される特徴の第3のセット118とを含む。参照しやすいように、またいかなる限定する意図もなしに、許可回路/機能/モジュールA108、許可回路/機能/モジュールB112、および許可回路/機能/モジュールC116は、個別にかつ/またはまとめて、本明細書では「許可機能108、112、116」と呼ばれ得る。さらに、参照しやすいように、またいかなる限定する意図もなしに、デバイスA102、デバイスB104、およびデバイスC106は、個別にかつ/またはまとめて、本明細書では「デバイス102、104、106」と呼ばれ得る。

【００５６】

(デバイスA102、デバイスB104、および/またはデバイスC106などの)所与のデバイスにおいて(選択的にアクティブ化される特徴の第1のセット110、選択的にアクティブ化される特徴の第2のセット114、および/または選択的にアクティブ化される特徴の第3のセット118などの)選択的にアクティブ化される特徴のセットにおける1つまたは複数の選択的にアクティブ化される特徴をアクティブ化する許可は、所与のデバイスにおける1つまたは複数の特徴のアクティブ化の必須条件であり得る。

【００５７】

本明細書で説明するいくつかの態様では、デバイス102、104、106の許可機能108、112、116は、デバイス102、104、106が許可サーバ126によって選択的にアクティブ化される特徴をアクティブ化することを許可されていることの証拠を取得および検証することができ、デバイス102、104、106が選択的にアクティブ化される特徴をアクティブ化する前に証拠(たとえば、許可情報)を取得および検証することができる。いくつかの実装形態では、第1のデバイスにおける許可機能108、112、116はまた、第2のデバイスに証拠を送ることができ、第2のデバイスは、第1のデバイスにサービス(たとえば、ネットワークサービ

ス)を提供し得る。

【００５８】

ネットワークサービスの例としては、たとえば、デュアル接続サービス、複数サブスクリプションサービス、デバイス間(D2D)モードサービス、マルチメディアブロードキャスト/マルチキャストサービス(MBMS)、および/または非ライセンス動作サービスがあり得る。デュアル接続サービスは、たとえば、無線アクセス技術(RAT)内(たとえば、4G)とRAT間(たとえば、4Gおよび5Gならびに/またはワイヤレスローカルエリアネットワーク(WLAN)にわたる)の両方で接続を実現し得る。

【００５９】

複数サブスクリプションサービスは、たとえば、複数のサブスクリプションに同時に(たとえば、事業者サービスサブスクリプションおよびストリーミングビデオサブスクリプションおよび/またはオンライン小売販売プロバイダサブスクリプションに同時に)対応するために、単一の無線リンクを使用してデバイスにサービスを提供し得る。

【００６０】

D2Dモードサービスは、たとえば、サービス、友人、およびオファーの近接発見を実現するサービスを提供し得る。D2Dサービスは、たとえば、従来のアクセスサービスに加えて提供され得る。

【００６１】

MBMSサービスは、デバイスがユニキャストサービスへのアクセスに加えてマルチキャストサービスを受信するのを容易にするサービスであり得る。

【００６２】

非ライセンス動作サービスは、たとえば、デバイスがライセンス補助アクセスを使用するか、あるいはLTEまたは5Gまたは1つもしくは複数の他のRATを使用して非ライセンス帯域において動作することを可能にするサービスであり得る。上記の例示的なサービスならびに他のサービスを使用するためにアクティブ化される必要があり得る特徴(たとえば、選択的にアクティブ化される特徴)の完全リストは、本明細書の範囲を超える。それでも、選択的にアクティブ化され得る特徴のいくつかの例としては、キャリアアグリゲーション、いくつかの物理チャネル(たとえば、デュアル接続、D2D、および/もしくは非ライセンス動作サービスの場合)、選択的にアクティブ化されるハードウェア、ならびに/または所与の選択的にアクティブ化される特徴のアクティブ化を妨げるために本来であれば実行されないままであったデバイス上に記憶された処理回路可読命令の選択的に実行される部分があり得る。

【００６３】

第2のデバイスに証拠(たとえば、許可情報)を提供することは、第2のデバイスがサービスを提供する前の必須条件であり得る。したがって、たとえば、選択的にアクティブ化される特徴の第1のセット110が許可され、デバイスA102においてアクティブ化された後でも、別のデバイス(たとえば、デバイスC106)(たとえば、ネットワークアクセスノード)はデバイスA102に、デバイスA102において選択的にアクティブ化される特徴の第1のセット110を使用するデバイスA102の権限の証拠を送るよう要求することができ、権限の証拠は、許可サーバ126によって署名され得る。またさらに、いくつかの実装形態では、デバイスC106によって提供されるサービス(たとえば、ネットワークサービス)をデバイスA102が使用する(たとえば、アクティブ化する、利用する)前に(選択的にアクティブ化される特徴の第3のセットが、デバイスA102にサービスを提供するためにデバイスC106によって必要とされる第3の選択的にアクティブ化される特徴を含む場合)、かつ選択的にアクティブ化される特徴の第3のセット118が許可され、デバイスC106(たとえば、ネットワークアクセスノード)においてアクティブ化された後でも、デバイスA102(たとえば、クライアントデバイス)はデバイスC106に、デバイスC106において選択的にアクティブ化される特徴の第3のセット118を使用するデバイスC106の権限の証拠を送るよう要求することができ、権限の証拠は、許可サーバ126(または別の許可サーバ)によって署名され得る。

【００６４】

デバイスA102は、デバイスC106において提供されるサービスを使用する前に、証拠を求める要求をデバイスC106に送り得る。デバイスA102は、デバイスC106において提供されるサービスを使用する前に、デバイスC106から取得された証拠を取得および検証し得る。

【００６５】

許可情報(たとえば、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠)は、許可合意120に基づき得る。許可情報は、たとえば、許可合意120および/または許可証明122の形式で提供され得る。許可合意120は、許可サーバ126に記憶され得る。許可サーバ126は、許可合意120に基づいて許可証明122および(特徴アクティブ化鍵を含み得る)許可ファイル124を導出し得る。許可証明122は、たとえば、デバイス102、104、106の公開鍵、デバイス102、104、106に対して許可された選択的にアクティブ化される特徴(たとえば、選択的にアクティブ化される特徴のセット)、および選択的にアクティブ化される特徴が許可されるデバイス102、104、106の識別子(たとえば、デバイスの公開鍵のハッシュまたは何らかの他のデバイス固有の識別子)を含み得る。許可証明122はまた、たとえば、許可証明122の満了時間を含むことができ、追加または代替として、デバイス102、104、106に対して許可された選択的にアクティブ化される特徴に関係するパラメータを含み得る。許可証明は許可サーバ126によって、許可サーバ126の秘密鍵を使用して署名され得る。

【００６６】

したがって、許可証明122は、許可サーバ126の署名を伴い、署名は、許可サーバ126の公開鍵を使用して検証され得る。署名を導出するために、たとえば、許可サーバ126は、デバイス102、104、106の公開鍵、デバイス102、104、106に対して許可された選択的にアクティブ化される特徴、およびデバイス102、104、106の識別子をハッシュ関数に適用することができ、許可サーバ126は、導出されたハッシュ値および許可サーバ126の秘密鍵を署名関数に入力することができる。検証関数は、署名関数の逆であり得、エンティティ(たとえば、ネットワークノード)は、署名および許可サーバ126の公開鍵を検証関数に入力することによって、署名を検証し得る。このようにして、許可証明122が許可サーバ126によって署名されたときに、許可証明122は検証され得、デバイス102、104、106において選択的にアクティブ化される特徴のセットを使用するデバイス102、104、106の権限の証拠として使用され得る。したがって、許可証明122は、許可情報として使用され得る。

【００６７】

本質的に、デバイス102、104、106は、特徴アクティブ化中に許可サーバの証明をプロビジョニングされる。許可証明122はまた、許可サーバ126が許可ファイル124を、許可ファイル124において識別されるデバイス102、104、106に発信したことを証明する働きをし得る。

【００６８】

デバイス102、104、106がエンティティ(たとえば、ネットワークノード)に許可証明122を送るとき、デバイス102、104、106は、デバイス102、104、106の秘密鍵により許可証明122に署名し得ることに留意されたい。これは、デバイス102、104、106が許可証明122に含まれる公開鍵の所有者であること証明するデバイス102、104、106の能力を促進する。許可証明122に含まれる公開鍵を使用して、エンティティ(たとえば、ネットワークノード)は、許可証明122を送ったデバイスが、許可証明122において許可サーバ126によって識別される同じデバイスであることを検証することができる。

【００６９】

許可情報は、デバイス102、104、106によっていつでも(たとえば、初期接続中、サービス要求中、ハンドオーバ中、要請に応じて)要求され得る。

【００７０】

許可機能108、112、116が、許可合意120または許可合意120から導出された許可証明122を取得および検証した場合、許可機能108、112、116は、所与の選択的にアクティブ化される特徴をアクティブ化し得る(または所与の選択的にアクティブ化される特徴をアクティブ化することを、許可機能108、112、116をホスティングするデバイス102、104、106に

対して許可/指令/命令し得る)。許可合意120ならびに許可証明122は、所与の選択的にアクティブ化される特徴をアクティブ化するデバイス102、104、106の権利を記録することができる。

【００７１】

許可機能108、112、116は、特徴アクティブ化要求(たとえば、1つまたは複数の選択的にアクティブ化される特徴をアクティブ化する要求、1つまたは複数の選択的にアクティブ化される特徴をアクティブ化する許可を求める要求)をローカル許可サーバ128に送り得る。特徴アクティブ化要求への応答は、許可情報(たとえば、デバイス102、104、106において、特徴アクティブ化要求において識別される1つまたは複数の選択的にアクティブ化される特徴を含む、選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠)を含み得る。応答はまた、許可ファイル124を含み得る。許可ファイル124は、1つまたは複数の特徴アクティブ化鍵を含み得る。許可サーバ126は、許可情報、許可ファイル、および/または1つもしくは複数の特徴アクティブ化鍵を暗号化し得る。

【００７２】

許可サーバ126は、許可サーバ126に属する公開/秘密鍵ペアの秘密鍵により許可情報に署名し得る。許可情報が許可証明を含む場合、許可サーバ126は、たとえば、許可サーバ126に属する公開/秘密鍵ペアの秘密鍵により許可証明に署名し得る。デバイス102、104、106は、許可証明122が真正であることを検証するために、許可サーバ126の公開鍵を使用し得る。当業者は、許可証明122などのアイテムに署名する代替方法が、本明細書で提示する態様の範囲内にあることを諒解されよう。

【００７３】

許可サーバ126は、デバイス102、104、106に属する公開/秘密鍵ペアの公開鍵を使用して、1つまたは複数の特徴アクティブ化鍵を含み得る許可ファイル124を暗号化し得る。いくつかの態様では、許可機能108、112、116のみが、デバイス102、104、106に属する公開/秘密鍵ペアの秘密鍵にアクセスできるので、許可機能108、112、116のみが、1つまたは複数の特徴アクティブ化鍵を含み得る許可ファイル124を解読することができる。当業者は、特徴アクティブ化鍵を含み得る許可ファイル124などのアイテムのための他のタイプの暗号化が、本明細書で提示する態様の範囲内にあることを諒解されよう。

【００７４】

ローカル許可サーバ128は、許可サーバ126に特徴アクティブ化要求を送り得る。いくつかの態様では、特徴アクティブ化要求は、最初にローカル許可サーバ128に送られることなく、許可機能108、112、116から許可サーバ126に直接送られ得る。

【００７５】

許可サーバ126は、デバイスA102、デバイスB104、またはデバイスC106などのデバイスに関連する許可合意120を考慮/評価/処理した後、特徴アクティブ化要求への応答を送ることができる。特徴アクティブ化要求への応答は、特徴アクティブ化要求において識別される1つまたは複数の選択的にアクティブ化される特徴をアクティブ化するデバイス102、104、106の権利を検証するために使用され得る許可情報を含み得る。

【００７６】

応答はまた、許可ファイル124を含み得る。許可ファイル124は、1つもしくは複数の特徴アクティブ化鍵、許可パラメータ、または1つもしくは複数の特徴アクティブ化鍵および許可パラメータを含み得る。許可パラメータは、たとえば、許可の満了日または失効日を含み得る。ローカル許可サーバ128、またはいくつかの態様では許可サーバ126は、許可証明122と特徴アクティブ化鍵および許可パラメータを含む許可ファイル124とを許可機能108、112、116に転送し得る。

【００７７】

上記のように、デバイス102、104、106の選択的にアクティブ化される特徴をアクティブ化するために、選択的にアクティブ化される特徴は、許可される必要があり得る。1つの非限定的な例によれば、エンティティ(たとえば、ユーザ、サービスプロバイダ、OEM、製造業者)は、許可合意120に規定された条件に基づいて、ライセンス供与サービスに対し

て、選択的にアクティブ化される特徴をアクティブ化するための許可料(たとえば、ライセンス料)を支払い得る。支払いの検証の前または後に、許可合意120は、許可サーバ126および/またはローカル許可サーバ128にアップロードされ得る。許可サーバ126は、ライセンス供与サービスによってホスティングされ得る。許可サーバ126(たとえば、ライセンス供与サーバ)は、許可合意および/またはそれに関連する選択的にアクティブ化される特徴の確認、アクティブ化、および/または実施に使用され得る。

【００７８】

一態様では、デバイス102、104は、ネットワークサービスが利用可能であると判断し得る。デバイス102、104は、デバイスにとって利用可能である(ただし、必ずしもデバイスにおいてアクティブ化されるとは限らない)、ネットワークサービスを使用するために必要とされる、選択的にアクティブ化される特徴を識別し得る。ネットワークサービスを使用するために必要とされる選択的にアクティブ化される特徴の識別情報は、たとえば、デバイス102、104に記憶されたリスティング/テーブル、ローカル許可サーバ128から取得されたリスティング/テーブル、許可サーバ126から取得されたリスティング/テーブルなど、任意の適切なソースから取得され得、またはリモートネットワークノードもしくは他のソース(たとえば、パケットデータネットワーク上のノード)から取得され得る。デバイス102、104は、それ(すなわち、デバイス102、104)がネットワークサービスを使用するために必要とされる選択的にアクティブ化される特徴をアクティブ化することを許可されているかどうかを判断し得る。

【００７９】

デバイス102、104が、ネットワークサービスを使用するために必要とされる選択的にアクティブ化される特徴のすべてをアクティブ化することを許可されていない場合、デバイス102、104、またはデバイス102、104の許可機能108、112は、1つの選択的にアクティブ化される特徴(または複数の選択的にアクティブ化される特徴)をアクティブ化する許可を要求し得る。デバイス102、104、またはデバイス102、104の許可機能108、112は、デバイス102、104が要求された選択的にアクティブ化される特徴をアクティブ化することを許可されていることの証拠を要求し得る。要求された選択的にアクティブ化される特徴のアクティブ化は、デバイス102、104が、たとえば、アプリケーションサーバ上で提供されるサービスを取得すること、またはネットワークアクセスノード(たとえば、eNB)によって提供されるサービスを使用することを可能にし得る。

【００８０】

例示的な動作環境

図2は、本明細書で説明する態様による例示的な動作環境200を示す。参照しやすいように、またいかなる限定する意図もなしに、各許可回路/機能/モジュールは、本明細書では「許可機能」と呼ばれる。例示的な動作環境200では、第1のデバイス202(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)が第1の許可機能203を含む。第2のデバイス204(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)が第2の許可機能205を含む。第1のデバイス202および第2のデバイス204は、ネットワークアクセスノード(たとえば、eNodeB)として示される第3のデバイス206とワイヤレス通信し得る。第3のデバイス206(たとえば、ネットワークアクセスノード)は、第3の許可機能207を含み得る。

【００８１】

第1のデバイス202は、第1のネットワークサービスを使用するために必要とされる1つまたは複数の選択的にアクティブ化される特徴を含み得る。第2のデバイス204は、第2のネットワークサービスを使用するために必要とされる1つまたは複数の選択的にアクティブ化される特徴を含み得る。第3のデバイス206は、第1のデバイス202に対する第1のネットワークサービスおよび/または第2のデバイス204に対する第2のネットワークサービスを使用/提供するために必要とされる1つまたは複数の選択的にアクティブ化される特徴を含み得る。

【００８２】

第3のデバイス206(たとえば、ネットワークアクセスノード)は、無線アクセスネットワーク(RAN)210(たとえば、拡張ユニバーサル地上波無線アクセスネットワーク(E-UTRAN:enhanced universal terrestrial radio access network))の一部であり得る。セルラー通信システム(たとえば、4G、LTE、LTE-A、5G)の非限定的な例では、RAN210は、制御シグナリングおよびデータトラフィックをコアネットワーク212(たとえば、発展型パケットコア(EPC))に通信することができる。ネットワーク事業者(たとえば、モバイルネットワーク事業者(MNO))は、コアネットワーク212を運営し得る。制御シグナリングは、S1-MME参照ポイントを介して通信され得る。データトラフィックは、S1-U参照ポイントを介して通信され得る。

【００８３】

コアネットワーク212は、モビリティ管理エンティティ(MME)214と、ホーム加入者サーバ/許可、認証、およびアカウンティングサーバ(HSS/AAA)216と、サービングゲートウェイデバイス(S-GW)218と、パケットデータネットワークゲートウェイデバイス(P-GW)220とを含み得る。上記で識別された構成要素に加えて、コアネットワーク212は、ローカル許可サーバ222も含み得る。ローカル許可サーバ222は、RAN210における第3のデバイス206(たとえば、ネットワークアクセスノード)ならびに他のネットワークアクセスノード(図示せず)と通信し得る。ローカル許可サーバ222は、第3のデバイス206(たとえば、ネットワークアクセスノード)を介して第1のデバイス202および第2のデバイス204と通信し得る。コアネットワーク212の内部で、ローカル許可サーバ222は、MME214および/またはHSS/AAA216と通信し得る。ローカル許可サーバ222は、ローカル許可サーバ222に関連するコアネットワーク212に結合された第1のデバイス202、第2のデバイス204、および第3のデバイス206(たとえば、ネットワークアクセスノード)に対する許可サーバ234のプロキシの働きをし得る。

【００８４】

P-GW220は、パケットデータネットワーク(PDN)232(たとえば、インターネット)上のアプリケーションサーバ228、230と通信し得る。アプリケーションサーバ228、230は、たとえば、小売販売プロバイダ、インターネット検索エンジンプロバイダ、エンターテインメントプロバイダ、およびソーシャルメディアサービスプロバイダなど、サービスプロバイダに関連付けられ得る。アプリケーションサーバ228、230は、サービスプロバイダに関連するアプリケーションおよび/またはアプリケーションサービスをホスティングし得る。

【００８５】

コアネットワーク212におけるローカル許可サーバ222は、パケットデータネットワーク232における許可サーバ234と通信し得る。許可サーバ234がどこでも位置し得ることが理解されよう。言い換えれば、許可サーバ234をアプリケーションサーバ228、230とともにパケットデータネットワーク232上に配置することは随意である。たとえば、コアネットワーク212が、ローカル許可サーバ222に加えて許可サーバ234を含んでよい。

【００８６】

許可サーバ234は、第1のデバイス202、第2のデバイス204、第3のデバイス206によって、ならびに無線アクセスネットワークプロバイダ、モバイルネットワーク事業者、またはアクセスポイントプロバイダなどの任意の数のエンティティによってアクセスされ得る。各エンティティも、それ自体のローカル許可サーバを維持し得る。許可サーバおよびローカル許可サーバの態様は、以下で提供する。

【００８７】

アーキテクチャ参照モデル

図3は、本明細書で説明する態様によるシステム300のアーキテクチャ参照モデルである。図3は、デバイス302(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)、ローカル許可サーバ306、および許可サーバ308を示す。デバイス302は、少なくとも1つの選択的にアクティブ化される特徴320を含み得る。選択的にアクティブ化される特徴320をアクティブ化するデバイス302の権利は、許可合意330(たとえば、契約、合意、ライセンス)に基づき得る。一態様では、選択的にアクティブ化される特徴320をアクテ

ィブ化するデバイス302の権利は、許可合意330(または許可合意330から導出された許可情報)の確認に基づき得る。一態様では、選択的にアクティブ化される特徴320をアクティブ化するデバイス302の権利は、その選択的にアクティブ化される特徴320に関係する支払いに基づき得る。一態様では、選択的にアクティブ化される特徴320に関係する支払いのステータスが、許可合意330(または許可合意330から導出された許可情報)に反映され得る。一実装形態では、許可サーバ308は、たとえば、(たとえば、選択的にアクティブ化される特徴320を使用する権利の)確認中、(たとえば、選択的にアクティブ化される特徴320の)アクティブ化中、および(たとえば、選択的にアクティブ化される特徴320に関係する許可合意330の条件の)実施中を含め、選択的にアクティブ化される特徴320に関連する様々な事例における効用(utility)を発見し得る。

【００８８】

デバイス302は、ローカル許可サーバ306に結合され得る。ローカル許可サーバ306は、許可サーバ308に結合され得る。デバイス302、ローカル許可サーバ306、および許可サーバ308について、ここで説明する。

【００８９】

デバイス302は、許可回路/機能/モジュールを含むことができ、許可回路/機能/モジュールは、参照しやすいように、またいかなる限定する意図もなしに、本明細書では「許可機能304」と呼ばれる。

【００９０】

許可機能304は、デバイス302の処理回路314および/またはデバイス302のセキュア動作環境305において、セキュアなプロセスを実施する(たとえば、セキュアな処理を実行する)ことができる。本明細書で使用する「セキュア」という用語は、外部および内部のプロセスを含む他のプロセスによるアクセスから、かつ/またはユーザから保護されていること、または安全であることを意味し得る。一態様では、セキュア動作環境305、および/またはセキュア動作環境305において実施されるセキュアなプロセスは、ユーザにとってアクセス不可能および/または許可機能304によって実施されるセキュアなプロセス以外のプロセスにとってアクセス不可能であり得る。一態様では、許可機能304がデバイス302の処理回路314においてセキュアなプロセスを実施する場合、セキュアなプロセスは、ユーザにとってアクセス不可能および/または許可機能304によって実施されるセキュアなプロセス以外のプロセスにとってアクセス不可能であり得る。

【００９１】

許可機能304は、デバイス302がデバイス302の選択的にアクティブ化される特徴320をアクティブ化することを許可されていることを検証するためのプロセスを実施し得る。プロセスは、セキュアなプロセスであり得る。一態様では、デバイス302が選択的にアクティブ化される特徴320をアクティブ化することを許可されていることを検証するために、許可機能304は、選択的にアクティブ化される特徴320がアクティブ化されることを許可されていることの証拠(たとえば、許可情報)を取得し得る。選択的にアクティブ化される特徴320は、初期使用、反復使用、および/または継続的使用のためにアクティブ化されることを許可され得る。検証は、取得された証拠を確認することにより得る。

【００９２】

許可機能304はまた、デバイス302が接続されているか、または接続する予定であるネットワークに関連付けられるネットワークノード(たとえば、eNB、MME、S-GWなど)が、選択的にアクティブ化される特徴320に対応する特徴をアクティブ化することを許可されていることを検証するためのプロセスを実施し得る。プロセスは、セキュアなプロセスであり得る。ネットワークノードにおける選択的にアクティブ化される特徴320に対応する特徴は、ネットワークによってネットワークノードを介して提供されるサービスを促進するために使用され得る。例として、デバイス302は、ネットワークノードにおいて提供されるネットワークサービスを使用するために、ネットワークノードにおいてアクティブ化される選択的にアクティブ化される特徴320に対応する特徴を必要とし得る。さらなる例として、デバイス302は、デバイス302において選択的にアクティブ化される特徴320をアクテ

ィブ化することによって達成され得る改善されたサービスを実現するために、ネットワークノードにおいてアクティブ化される選択的にアクティブ化される特徴320に対応する特徴を必要とし得る。たとえば、この例ではクライアントデバイスであり得るデバイス302は、選択的にアクティブ化される特徴320をアクティブ化するとキャリアアグリゲーションを実施するように製造され得る。キャリアアグリゲーションは、送信帯域幅を増大させるための複数のキャリアの使用を可能にする。キャリアアグリゲーションは、デバイス302のパフォーマンスを改善し得る。デバイス302は、選択的にアクティブ化される特徴320をアクティブ化することを許可され得、キャリアアグリゲーションを使用するようにそれ自体を構成することを許可され得る。ただし、有効になるために、デバイス302に結合されたネットワークアクセスノード(たとえば、eNB)も、ネットワークアクセスノードがキャリアアグリゲーションを使用するように構成されるように、対応する特徴をアクティブ化するべきである。したがって、いくつかの態様では、選択的にアクティブ化される特徴320は、2つのデバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード、またはそれらのうちの2つ以上から成る任意の組合せ)によって一緒にアクティブ化され、使用され得る。

【００９３】

一例では、許可機能304は、許可合意330において規定された(また、許可合意330から導出され、許可機能304において取得された許可情報に反映された)条件に従って、選択的にアクティブ化される特徴320をアクティブ化および/または非アクティブ化し得る。本例では、アクティブ化および使用が容認できる条件は、許可合意330によって規定されるか、または許可合意330に記載され得る。本例では、条件は、選択的にアクティブ化される特徴320を使用する権利と引き換えの支払いを含み得る。一実装形態では、デバイス302の許可機能304は、たとえば、(たとえば、選択的にアクティブ化される特徴320を使用する権利の)確認中、(たとえば、選択的にアクティブ化される特徴320の)アクティブ化中、および(たとえば、選択的にアクティブ化される特徴320に関係する許可合意330の条件の)実施中を含め、デバイス302に関連する選択的にアクティブ化される特徴320に関連する様々な事例における効用を発見し得る。いくつかの態様では、選択的にアクティブ化される特徴320のアクティブ化により、デバイス302が、たとえば、(eNBなどの)別のデバイスを介してネットワーク(たとえば、インターネット)上のアプリケーションサーバから、サービスを取得することが可能になり得る。

【００９４】

デバイス302はまた、セキュア記憶回路310(たとえば、回路/機能/モジュール)を含み得る。一態様では、セキュア記憶回路310は、セキュア記憶回路310との間でデータの読み書きを行う(デバイス302の内部および/または外部の)構成要素/エンティティの能力に基づいてセキュアと見なされ得る。一態様では、セキュア記憶回路310は、永続的にデバイス302に組み込まれること、または統合されることがある。たとえば、セキュア記憶回路310は、デバイス302とともに含まれる処理回路314と同じ基板上に作られた不揮発性メモリアレイを含み得る。

【００９５】

セキュア記憶回路310内には、デバイス302のために導出された秘密/公開鍵ペアの秘密鍵316のための記憶空間があり得る。一態様では、製造業者またはOEMは、秘密/公開鍵ペアを生成し得る。別の態様では、別のエンティティは、秘密/公開鍵ペアを生成し得る。秘密/公開鍵ペアの秘密鍵316は、製造業者、OEMによって、または別のエンティティによってセキュア記憶回路310に記憶され得る。一態様では、秘密鍵316は、デバイス302の所有権を製造業者またはOEMから第3のエンティティに移転する前に、セキュア記憶回路310に記憶され得る。他の態様では、秘密鍵316は、任意の時点に任意のエンティティによってセキュア記憶回路310に記憶され得る。いくつかの態様では、秘密鍵316は、デバイス302にのみ知られている。いくつかの態様では、秘密鍵316は、デバイス302の許可機能304にのみ知られている。

【００９６】

秘密鍵316はデバイス302(または許可機能304)によって、特徴アクティブ化鍵318および/または特徴アクティブ化鍵318を含み得る許可ファイルを解読するために使用され得る。特徴アクティブ化鍵318および/または特徴アクティブ化鍵318を含み得る許可ファイルは、第3のエンティティ(たとえば、許可サーバ308)によって、デバイス302に特徴アクティブ化鍵318を送る前にデバイス302の公開鍵を使用して署名/暗号化され得る。

【００９７】

一態様では、特徴アクティブ化鍵318は、デバイス302の選択的にアクティブ化される特徴320をアクティブ化するために使用され得る。本明細書で説明する態様では、特徴アクティブ化鍵318は、暗号化された形式で記憶され得る。いくつかの例では、特徴アクティブ化鍵318は、許可機能304によってのみ(たとえば、デバイス302の秘密鍵316を使用して)解読され得る。いくつかの例では、特徴アクティブ化鍵318は、セキュア記憶回路310などのセキュアな環境に記憶され得る。

【００９８】

デバイス302は、セキュア記憶回路310とは別個であり得るデータ記憶デバイス312(たとえば、回路/機能/モジュール)をさらに含み得る。一態様では、セキュア記憶回路310がデータ記憶デバイス312のパーティションであること、またはその逆であることがある。セキュア記憶回路310および/またはデータ記憶デバイス312は、たとえば、ハードディスク、ハードディスクのパーティション、光ディスク、光ディスクのパーティション、固体メモリ、または固体メモリのパーティションを含み得る。

【００９９】

データ記憶デバイス312内には、特徴および許可パラメータのリスト322が記憶され得る。たとえば、特徴および許可パラメータのリスト322は、デバイス302がアクティブ化/非アクティブ化する権限を有する選択的にアクティブ化される特徴320、およびそれらの関連する許可パラメータを識別し得る。特徴および許可パラメータのリスト322は、たとえば、(許可ファイルを確認するために署名が使用され得る場合に)許可サーバによって署名された1つまたは複数の許可ファイルからまとめられ得る。許可ファイルは、ローカル許可サーバ306または許可サーバ308から、たとえば、デバイスアクティブ化、デバイスハンドオーバ、デバイス更新に伴って、またはデバイス302からの要求に応答して取得され得る。特徴および許可パラメータのリスト322における、許可パラメータは、たとえば、選択的にアクティブ化される特徴320がアクティブ化されているか、それとも非アクティブ化されているか、および選択的にアクティブ化される特徴320を使用するデバイス302の権限が満了または失効する日を示し得る。本明細書で使用する、選択的にアクティブ化される特徴320を使用するデバイス302の権限は、選択的にアクティブ化される特徴320を提供するデバイス302の権限を包含する。

【０１００】

データ記憶デバイス312内には、許可証明323も記憶され得る。一態様では、許可証明323は、任意のエンティティによって検証されてよく、したがって、セキュアなストレージに記憶される必要はない。他方では、許可ファイル324は、特徴アクティブ化鍵などの秘密情報を含む。したがって、一態様では、許可ファイル324はセキュア記憶回路310に記憶され得る。

【０１０１】

デバイス302はまた、デバイス302とともに含まれる許可機能304、セキュア動作環境305、セキュア記憶回路310、データ記憶デバイス312、処理回路314、および/またはネットワーク通信回路326の間の通信を実現するための通信バス325を含み得る。ネットワーク通信回路326も、ローカル許可サーバ306および/または許可サーバ308との通信を実現し得る。

【０１０２】

いくつかの態様では、ローカル許可サーバ306は、許可サーバ308に対するローカルプロキシとして機能し得る。いくつかの態様では、ローカル許可サーバ306は、ローカル許可サーバ306によって署名された、デバイス302において選択的にアクティブ化される特徴320のセットを使用するデバイス302の権限の証拠を送ることができ、デバイス302は、ロー

カル許可サーバ306に関連するコアネットワークに結合され得る。いくつかの態様では、ローカル許可サーバ306は、許可サーバ308とは無関係に一時的に動作し得る。ローカル許可サーバ306が許可サーバ308に対するローカルプロキシとして機能するか、それともローカルサーバ自体として機能するかは、たとえば、許可サーバ308に記憶された許可合意330の条件いかんにより得る。

【０１０３】

許可サーバ308は、データ記憶デバイス328(たとえば、回路/機能/モジュール)を含み得る。データ記憶デバイス328は、許可合意330(たとえば、合意、契約、ライセンス)のリスティング、リポジトリ、または記録を記憶し得る。許可合意330は、複数のデバイスの様々な選択的にアクティブ化される特徴に関係し得る。データ記憶デバイス328は、許可合意330によってカバーされるデバイスのための鍵記憶332を維持し得る。鍵記憶332は、許可合意330によってカバーされる(デバイス302などの)デバイスに送られるメッセージを暗号化するために使用され得る秘密鍵および/または公開鍵を含み得る。

【０１０４】

許可サーバ308のデータ記憶デバイス328はまた、デバイス302の選択的にアクティブ化される特徴320をアクティブ化するために使用され得る特徴アクティブ化鍵334を含み得る。いくつかの態様では、デバイス302の許可機能304が、選択的にアクティブ化される特徴320のうちの1つまたは複数をアクティブ化する権限をデバイス302が有することの証拠を要求したとき、特徴アクティブ化鍵334が許可サーバ308(またはローカル許可サーバ306)からデバイス302に送られ得る。そのような態様では、選択的にアクティブ化される特徴320をアクティブ化する権限をデバイス302が有することの証拠(たとえば、許可情報)を許可サーバ308(またはローカル許可サーバ306)が許可機能304に送った後、選択的にアクティブ化される特徴320は、許可機能304によって(または許可機能304の権限で)アクティブ化され得る。

【０１０５】

一例では、許可サーバ308のデータ記憶デバイス328は、デバイスモデル番号の関数として、デバイス302における選択的にアクティブ化される特徴320ごとに、許可パラメータ336のリスティング、リポジトリ、または記録を記憶し得る。一態様では、同じモデル番号を有する個々のデバイスの区別を可能にするために、たとえば、データ記憶デバイス328は、デバイスシリアル番号、または国際移動局機器識別情報(IMEI:International Mobile Station Equipment Identity)などの他のデバイス識別子の関数として、選択的にアクティブ化される特徴320ごとに許可パラメータ336を記憶し得る。当業者に知られているように、IMEIは、第3世代パートナーシッププロジェクト(3GPP)システム(たとえば、GSM(登録商標）、UMTS、LTE、LTE-A)に従ってハードウェアを識別するために使用される一意の番号である。

【０１０６】

許可サーバ308はまた、許可サーバ308とともに含まれるデータ記憶デバイス328、処理回路340、および/またはネットワーク通信回路342の間の通信を実現するための通信バス338を含み得る。ネットワーク通信回路342も、ローカル許可サーバ306および/またはデバイス302との通信を実現し得る。

【０１０７】

上記のように、ローカル許可サーバ306は、許可サーバ308のプロキシの働きをし得る。したがって、ローカル許可サーバ306は、許可サーバ308の場合と同じまたは同様の回路/機能/モジュールを含む。したがって、同じまたは同様の回路/機能/モジュールの説明および例示は省略する。

【０１０８】

許可合意

図1に戻ると、選択的にアクティブ化される特徴のセット110、114、118を使用するデバイス102、104、106の権限が、許可合意120(たとえば、合意、契約、ライセンス)において与えられ得る。いくつかの態様では、許可合意120はライセンスと見なされ得る。本明細

書で使用する場合、一態様では、選択的にアクティブ化される特徴のセットへの言及または選択的にアクティブ化される特徴への言及は、(たとえば、セットが1つの選択的にアクティブ化される特徴を含むか、またはセットが1つもしくは複数の別個の選択的にアクティブ化される特徴を含む場合)1つの選択的にアクティブ化される特徴への言及であると理解され得る。許可合意120は、デバイス102、104、106において選択的にアクティブ化される特徴のセット110、114、118を使用する(たとえば、当該セットをアクティブ化する、当該セットのアクティブ化を維持する)デバイス102、104、106の権限の証拠として使用されてよく、または許可合意120は、当該権限の証拠を導出するために使用されてよい。

【０１０９】

許可合意120は、2者以上のエンティティの間で確立され得る。許可合意120に対するエンティティは、たとえば、デバイス、デバイスの特徴、および/またはデバイスによって使用されるサービスに対する権利を主張し得る。例として、許可合意120は、製造業者、ベンダー/OEM、デバイス購入者、再販売業者、ライセンス供与サービス、および/または製造業者、ベンダー/OEM、デバイス購入者、再販売業者もしくはライセンス供与サービスのうちのいずれか2者以上の間で確立され得る。デバイス購入者は、エンドユーザ、再販売業者、またはデバイスをリースするエンティティであり得る。ライセンス供与サービスは、ライセンスを供与し、ライセンス供与条件の遵守を監視する組織であり得る。

【０１１０】

一例では、許可合意120は、許可機能108、112、116が許可合意120の証拠を取得することを求めるときより前に確立され得る。別の例では、許可合意は、許可機能108、112、116が許可合意120の証拠を取得することを求めたときと同時に、求めたときと実質的に同時に、または求めたときに確立され得る。

【０１１１】

許可合意120は、書面と呼ばれることがある。本明細書で使用する書面は、人間が読み取れる物理的形式で許可合意がこれまでに存在したかどうかにかかわらず、そのような許可合意のすべての非一時的機械可読表現を含む。「書面」という用語は、機械によって読み取られ得る任意の形式となった、人間が読み取れるあらゆる文書を含む。機械によって読み取られ得る形式は、電気形式、光形式、磁気形式、または当業者に知られている他の記憶形式を含み得る。

【０１１２】

一例では、許可合意は、以下を含む許可証明を導出するために使用され得る。

1.使用を許可された選択的にアクティブ化される特徴のセット、
2.有効期間/満了時間、
3.(たとえば、PLMN、SSID、またはセルIDSなど、地理的またはネットワーク識別子を含む)選択的にアクティブ化される特徴が有効化されるロケーション、
4.選択的にアクティブ化される特徴を使用することができるネットワークアクセスノードの最大数、および
5.周期的使用報告要件。

【０１１３】

図4は、本明細書で説明する態様による、第1のエンティティ(たとえば、デバイスの所有者、デバイスの販売業者/再販売業者、割引ありまたはなしで顧客にデバイスを提供するサービスプロバイダ)と1つまたは複数のデバイスの製造業者またはOEMとの間の例示的な許可合意に含まれ得るパラメータおよびデータの例示的なリスト400を示す。リスティングが図4において表形式で提示されているが、本態様によれば、任意の機械可読(たとえば、処理回路可読)形式が容認できる。リスティングは、合意の日402、デバイスの所有者の識別子404、デバイスの製造業者またはOEMの識別子406、デバイスの識別子408(たとえば、IMEI番号)、許可された特徴のリスト410、許可合意の存続期間412、特徴の使用に対する制限414、および特徴の使用に対する料金416などのパラメータを含む。

【０１１４】

図5は、本明細書で説明する態様による、製造業者またはOEMと別のエンティティ(たと

えば、許可サーバを運営しているエンティティ)との間の例示的な許可合意に含まれ得るパラメータおよびデータの例示的なリスト500を示す。リスティングが図5において表形式で提示されているが、本態様によれば、任意の機械可読(たとえば、処理回路可読)形式が容認できる。リスティングは、合意の開始日502、合意の終了日504、デバイスの識別子506(たとえば、IMEI番号)、許可された特徴のリスト508、特徴の使用に対する制限510、デバイスの公開鍵の識別子512、デバイスの製造業者またはOEMの識別子514、および特徴の使用に対する料金516などのパラメータを含む。

【０１１５】

図6は、本明細書で説明する態様による、ネットワーク事業者(たとえば、モバイルネットワーク事業者(MNO))と別のエンティティ(たとえば、許可サーバの所有者/事業者)との間の例示的な許可合意に含まれ得るパラメータおよびデータの例示的なリスティング600を示す。例示的なリスティング600が図6において表形式で提示されているが、本態様によれば、任意の機械可読(たとえば、処理回路可読)形式が容認できる。例示的なリスティング600は、許可合意の開始日602、許可合意の終了日604、デバイスの識別子606(たとえば、IMEI番号)、許可されたサービスのリスト608、許可された特徴のリスト610、デバイスの製造業者またはOEMの識別子612、および特徴の使用に対する料金614などのパラメータを含む。

【０１１６】

プロビジョニング

図7は、本明細書で説明する態様による、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)への許可証明、許可ファイル、特徴アクティブ化鍵、およびソフトウェアの送信に関係するアクションを示すフロー図である。一態様では、参照番号702～712により識別されるアクションが許可サーバによって行われ得る一方、参照番号714により識別されるアクションがローカル許可サーバによって行われ得る。一態様では、参照番号702～714により識別されるアクションが許可サーバによって行われ得る。すなわち、そのような態様では、許可サーバはローカル許可サーバの介入なしで、許可証明、許可ファイル、特徴アクティブ化鍵、および/またはソフトウェアを導出し、デバイスに送り得る。一態様では、参照番号702～714により識別されるアクションがローカル許可サーバによって行われ得る。すなわち、そのような態様では、ローカル許可サーバは許可サーバの介入なしで、許可証明、許可ファイル、特徴アクティブ化鍵、および/またはソフトウェアを導出し、デバイスに送り得る。

【０１１７】

上記で説明したように、許可合意が様々なエンティティ(たとえば、デバイスの所有者、デバイスの販売業者/再販売業者、割引ありまたはなしで顧客にデバイスを提供するサービスプロバイダ、デバイスの製造業者またはOEM)の間で締結され得る。たとえば、あるエンティティは、(たとえば、3ヵ月ごとに)既定の期間にサービスまたは選択的にアクティブ化される特徴を使用する権利に対する料金を第2のエンティティに支払い得る。エンティティが許可合意を締結すると、許可サーバ上に許可合意が記憶され得る702。許可サーバは、許可合意における情報に基づいて特徴アクティブ化鍵を導出する704(たとえば、許可合意に基づいて特徴アクティブ化鍵を導出する704)ことができる。許可サーバは、許可合意における情報に基づいて許可証明を導出し得る706。許可サーバはまた、許可合意における情報に基づいて許可ファイルを導出し得る708。いくつかの態様では、許可ファイルは、1つまたは複数の特徴アクティブ化鍵を含み得る。これらのアクションの順序は例であり、限定するものではない。任意の順序が容認できる。

【０１１８】

デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)の選択的にアクティブ化される特徴をアクティブ化するために、特徴アクティブ化鍵が使用され得る。特徴アクティブ化鍵は暗号化され得、かつ/または特徴アクティブ化鍵を伴う許可ファイルは暗号化され得る。いくつかの例では、特徴アクティブ化鍵および/または許可ファイルは、デバイスの許可機能によってのみ解読され得る。

【０１１９】
いくつかの態様では、選択的にアクティブ化される特徴ごとに1つの特徴アクティブ化鍵が、選択的にアクティブ化される特徴のアクティブ化に使用され得る。他の態様では、1つの特徴アクティブ化鍵が、複数の選択的にアクティブ化される特徴をアクティブ化するために使用され得る。選択的にアクティブ化される特徴をアクティブ化することは、選択的にアクティブ化される特徴の初期アクティブ化ならびにすでにアクティブ化された選択的にアクティブ化される特徴のアクティブ化の維持を含み得る。一態様では、特徴アクティブ化鍵が、選択的にアクティブ化される特徴をロック解除し得る。例として、選択的にアクティブ化される特徴は、アクティブ化され得るが、許可合意の条件に基づいて使用されないようロックされ得る(たとえば、選択的にアクティブ化される特徴は、許可合意によって課せられた地理的または時間関連パラメータ制限に基づいて使用されないようロックされ得る)。アクティブ化された選択的にアクティブ化される特徴は、適切な特徴アクティブ化鍵の取得および使用に基づいてロック解除され得る(たとえば、すでにアクティブ化された選択的にアクティブ化される特徴を使用するデバイスの能力が有効化され得る)。

【０１２０】
許可ファイルは、選択的にアクティブ化される特徴に関係するデータを含み得る。選択的にアクティブ化される特徴に関係するデータは、たとえば、選択的にアクティブ化される特徴を使用するデバイスの権限が満了または失効する日を含み得る。選択的にアクティブ化される特徴に関係する他のデータも、許可ファイルに含まれ得る。

【０１２１】
一態様では、許可サーバは、許可証明と特徴アクティブ化鍵を含む許可ファイルとをローカル許可サーバに送るか、またはアップロードする710(たとえば、プロビジョニングする)ことができる。許可サーバは随意に、デバイスの選択的にアクティブ化される特徴に関係するソフトウェア、またはデバイスに関係する任意の特徴(たとえば、ハードウェアもしくはソフトウェア)をローカル許可サーバに送るか、またはアップロードし得る712。たとえば、更新されたドライバの形式をとるソフトウェアが、許可証明および許可ファイルに加えて送られるか、またはアップロードされ得る。

【０１２２】
許可サーバおよび/またはローカル許可サーバは、たとえば、デバイスから特徴アクティブ化要求を取得したことに応答して、許可証明、特徴アクティブ化鍵を含む許可ファイル、およびソフトウェア(随意)をデバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)に送り得る714。

【０１２３】
一例では、複数のデバイスが許可合意に含まれているとき、ローカル許可サーバは、最大数(たとえば、割当て量)を上回るデバイスが許可された選択的にアクティブ化される特徴を使用していないことを確実にし得る。たとえば、ローカル許可サーバは、第1のデバイスにおいて選択的にアクティブ化される特徴がいつ非アクティブ化されるかの指示を、第2のデバイスにおいて選択的にアクティブ化される特徴をアクティブ化する許可をローカル許可サーバが発信する前に受信し得る。代替的に、ローカル許可サーバは、第1のデバイスにおいて選択的にアクティブ化される特徴をアクティブ化する許可を、第2のデバイスにおいて選択的にアクティブ化される特徴をアクティブ化する許可をローカル許可サーバが発信する前に失効させ得る。失効は、たとえば、どのデバイスで選択的にアクティブ化される特徴がアクティブに使用されているかを判断するために、すべての許可されたデバイスからの周期的報告に基づき得る。

【０１２４】
特徴アクティブ化要求
図8は、本明細書で説明する態様による、特徴アクティブ化要求(たとえば、1つまたは複数の特徴をアクティブ化する要求、1つまたは複数の特徴をアクティブ化する許可を求める要求)を伴う方法を示すフロー図800である。デバイス(たとえば、チップ構成要素、

クライアントデバイス、ネットワークノード)は、選択的にアクティブ化される特徴をアクティブ化することを、デバイスがそうする許可を有する場合に行うことができる。様々なイベントの結果、デバイスは特徴アクティブ化要求を送ることがある。たとえば、選択的にアクティブ化される特徴は、ネットワークサービスを使用するために必要とされることがあり、管理者は、選択的にアクティブ化される特徴を呼び出す方式でデバイスを構成することを決定することができ、サブスクリプション更新が発生することがあり、かつ/または保守運用管理(OAM:operation, administration, and management)プロトコルが、保守目的で選択的にアクティブ化される特徴をアクティブ化する必要があることがある。

【０１２５】

選択的にアクティブ化される特徴をアクティブ化するために、デバイスは、デバイスにおいて選択的にアクティブ化される特徴を使用するデバイスの権限の証拠を取得し、特徴アクティブ化鍵を含む許可ファイルを取得し得る。権限の証拠は、たとえば、許可情報の形式で提供され得る。許可情報は、許可合意および/または許可証明を含み得る。一例では、選択的にアクティブ化される特徴を使用するデバイスの権限の証拠と特徴アクティブ化鍵を含む許可ファイルとを取得するために、デバイスは、特徴アクティブ化要求(たとえば、1つまたは複数の選択的にアクティブ化される特徴をアクティブ化する要求)をローカル許可サーバに送り得る。

【０１２６】

ローカル許可サーバは、デバイスから特徴アクティブ化要求を取得し得る802。ローカル許可サーバは、要求への応答に必要とされるアイテム(たとえば、許可情報、および特徴アクティブ化鍵を含む許可ファイルなど、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠)をローカル許可サーバが保有しているかどうかを判断し得る804。必要とされるアイテムをローカル許可サーバが保有していない場合、またはローカル許可サーバがアイテムを保有しているが、アイテムが(たとえば、許可の満了に起因して)有効ではない場合、ローカル許可サーバは、権限の証拠(たとえば、許可証明の形式をとる許可情報)と特徴アクティブ化鍵を含む許可ファイルとを許可サーバから取得しようと試み得る806。

【０１２７】

一態様では、ローカル許可サーバは、許可サーバに特徴アクティブ化要求を転送することによって、権限の証拠(たとえば、許可証明の形式をとる許可情報)と特徴アクティブ化鍵を含む許可ファイルとを許可サーバから取得し得る806。許可サーバは、権限の証拠(たとえば、許可証明の形式をとる許可情報)と特徴アクティブ化鍵を含む許可ファイルとを、たとえば、要求された選択的にアクティブ化される特徴が許可されていることを許可合意が裏付けている場合に、送ることができる。特徴アクティブ化要求が許可サーバに送られる場合、ローカル許可サーバは、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)と許可サーバとの間のセキュアなトンネルを提供するプロキシサーバとして機能し得る。(たとえば、デバイスとライセンス供与サービスとの間および/またはモバイルネットワーク事業者とライセンス供与サービスとの間の)許可合意を検証した後、許可サーバは、権限の証拠(たとえば、許可証明の形式をとる許可情報)と特徴アクティブ化鍵を含む許可ファイルとをローカル許可サーバに送り得る。

【０１２８】

ローカル許可サーバが権限の証拠(たとえば、許可証明の形式をとる許可情報)と許可ファイルとを保有している場合、ローカル許可サーバは、要求された選択的にアクティブ化される特徴に関して割当て量に達しているかどうかを判断し得る808。要求された選択的にアクティブ化される特徴に関する割当て量に達している場合、ローカル許可サーバは、選択的にアクティブ化される特徴をアクティブ化する要求を拒否する応答をデバイスに送り得る810。応答とともに拒否の理由が含まれ得る。要求された選択的にアクティブ化される特徴に関する割当て量に達していない場合、ローカル許可サーバは、たとえば、権限の証拠(たとえば、許可証明の形式をとる許可情報)と特徴アクティブ化鍵を含む許可ファイルとを含む応答をデバイスに送り得る812。

【０１２９】
ローカル許可サーバは、許可合意、許可証明、許可ファイル、特徴アクティブ化鍵、および随意のソフトウェアを、将来の使用のためにキャッシュし得る。一態様では、ローカル許可サーバが許可サーバに代わって許可証明を発信し、許可サーバに許可ステータスを報告するときに、キャッシングは適用され得る。
【０１３０】
選択的にアクティブ化される特徴のアクティブ化
図9は、本明細書で説明する態様による、選択的にアクティブ化される特徴のアクティブ化の一例を示すフロー図900である。デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)またはデバイスの許可機能は、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠(たとえば、許可証明の形式をとる許可情報)を取得することができ、権限の証拠が許可サーバによって署名され、デバイスまたはデバイスの許可機能はまた、特徴アクティブ化鍵を含む許可ファイルを取得し得る902。一態様では、権限の証拠および許可ファイルは、特徴アクティブ化要求(たとえば、1つまたは複数の選択的にアクティブ化される特徴をアクティブ化する要求)に応答して取得され得る。許可ファイルは、デバイスの公開鍵により暗号化された特徴アクティブ化鍵を含み得る。許可機能は、権限の証拠(たとえば、許可証明の形式をとる許可情報)を確認し得る904。一態様では、確認は、確認機能および許可サーバの公開鍵を使用することを含み得る。権限の証拠(たとえば、許可証明の形式をとる許可情報)が確認された場合、デバイスは、デバイスの秘密鍵を使用して、特徴アクティブ化鍵を含む許可ファイルを解読し得る906。許可機能は、解読された許可ファイルから特徴アクティブ化鍵を取り出し得る。許可機能は、許可ファイルとともに含まれる許可パラメータを評価する(たとえば、選択的にアクティブ化される特徴を使用するデバイスの権限の満了日などの許可パラメータが満了していないことを確かめる)ことができる908。許可機能は、次いで、解読された特徴アクティブ化鍵を使用して、選択的にアクティブ化される特徴のセットをアクティブ化し得る910。
【０１３１】
アクティブ化された選択的にアクティブ化される特徴はいずれも、非アクティブ化イベントが発生するまでアクティブ化されたままであり得る。非アクティブ化イベントの一例は、アクティブ化された選択的にアクティブ化される特徴に関連する許可パラメータにおいて指定された満了時間になることであり得る。他の非アクティブ化イベントも容認できる。許可機能は、デバイスのセキュアな記憶デバイスに、取り出された特徴アクティブ化鍵を記憶することができる912。許可機能はまた、デバイスのデータ記憶デバイスに、取り出された許可パラメータを記憶することができる912。
【０１３２】
一例では、デバイスの許可機能は、少なくとも、許可サーバがデバイスの(公開/秘密鍵ペアの)公開鍵を使用して許可ファイルを暗号化していてよく、デバイスがデバイスのセキュアな記憶回路に秘密鍵を記憶していてよく、秘密鍵が許可機能にのみ知られていてよいので、許可ファイルを確実に、かつ十分なセキュリティ保証により解読することが可能であり得る。デバイスは、選択的にアクティブ化される特徴のアクティブ化が適切であることを確実にするために、許可機能に依拠し得る。さらに、デバイスがネットワーク(たとえば、許可サーバ)から許可証明を受信したとき、デバイスは、許可証明が許可サーバによって送られた(たとえば、詐欺師によって送られていない)正しい許可証明であることを検証することが可能であるべきである。一例では、許可証明が許可サーバによって送られた正しい許可証明であることを検証するデバイスの能力を促進するために、許可サーバは、(許可サーバの秘密鍵により導出された)許可サーバの署名を許可証明に追加することができる。許可サーバの署名はデバイスにおいて、許可サーバの公開鍵を使用して検証され得る。同様に、デバイスがネットワーク(たとえば、許可サーバ)から許可ファイルを受信したとき、デバイスは、許可ファイルが許可サーバによって送られた(たとえば、詐欺師によって送られていない)正しい許可ファイルであることを検証することが可能である

べきである。一例では、許可ファイルが許可サーバによって送られた正しい許可ファイルであることを検証するデバイスの能力を促進するために、許可サーバは、許可サーバの署名(たとえば、許可サーバの秘密鍵により導出された署名)を許可ファイルに追加することができる。許可サーバの署名はデバイスにおいて、許可サーバの公開鍵を使用して検証され得る。

【０１３３】

デバイスは、アクティブ化された選択的にアクティブ化される特徴の使用を監視することができ、許可サーバおよび/またはローカル許可サーバに、選択的にアクティブ化される特徴の使用に関係する周期的報告を送る(たとえば、アクティブ化ステータスを報告する)ことができる914。許可サーバおよび/またはローカル許可サーバは、そのような報告を送るすべてのデバイスからの選択的にアクティブ化される特徴の使用に関係する周期的報告をアグリゲートし得る。選択的にアクティブ化される特徴の使用ステータスに関する報告は、本明細書ではステータス報告と呼ばれ得る。周期的ステータス報告は、たとえば、選択的にアクティブ化される特徴を使用するデバイスの権利に対する制限を実施するために使用され得る。たとえば、許可サーバ(またはローカル許可サーバ)は、最大数を上回るデバイスが、選択的にアクティブ化される特徴を同時に使用している、または使用していないことを検証するために、ステータス報告から取得されたデータを使用し得る。最大数を上回るデバイスが、選択的にアクティブ化される特徴を同時に使用している(たとえば、割当て量に達している)場合、選択的にアクティブ化される特徴をアクティブ化する新しい要求は拒否され得る。使用、ライセンス料などに関係する記録が導出され、維持され得る。

【０１３４】

編成手順

一態様では、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)において特徴アクティブ化が成功すると、許可サーバは、デバイスに関連するHSS/AAAサーバに、デバイスの更新された特徴/更新された能力をHSS/AAAサーバに知らせるためのデータを送信し得る。

【０１３５】

HSS/AAAサーバは、更新されたデバイス特徴がネットワーク事業者(たとえば、MNO)によって検証された後、デバイスのサブスクリプションプロファイルを更新することができ、その情報をネットワークノード(たとえば、eNodeB、MME、P-GWなど)に送ることができる。いくつかの態様では、デバイスの能力および許可ステータスに基づいてサブスクリプションプロファイルを更新することは、ネットワーク事業者の役割であり得る。

【０１３６】

デバイスのサブスクリプションプロファイルを更新することで、1つまたは複数の特徴をアクティブ化する要求が承認され、かつ/または特徴がアクティブ化されると、ネットワークノード(たとえば、eNB、MME、S-GW、P-GW)が、ネットワークノードが別の形式の証拠を取得する必要なくデバイスが特徴を使用する許可を確認することが可能になり得る。たとえば、サブスクリプションプロファイルに基づいてデバイスが特徴を使用する許可をネットワークノードが確認できるようにサブスクリプションプロファイルを更新することで、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠をネットワークノードがデバイスから取得する必要がなくなり得る。

【０１３７】

一態様では、デバイスがネットワークアクセスノード(たとえば、eNodeB)であるとき、ネットワークアクセスノードにおいてアクティブ化される特徴/サービスのあるセットの利用可能性に関する情報が、デバイスに送られ得る。いくつかの実装形態では、ネットワークアクセスノードにおいてアクティブ化される特徴/サービスのあるセットは、オーバージエアブロードキャスト(たとえば、システム情報ブロック(SIB)タイプ1ブロードキャスト)を介してデバイス(たとえば、チップ構成要素、クライアントデバイス)に告知され得る。いくつかの実装形態では、デバイスは、ネットワークアクセスノードに照会するた

めのプロトコルを使用することができ、それによって、ネットワークアクセスノードにおいてアクティブ化され得る特徴/サービスのあるセットの利用可能性を判断し得る。そのようなクエリプロトコルの一例は、アクセスネットワーククエリプロトコル(ANQP)であり得る。他のクエリプロトコルも容認できる。これらの例示的な方法で、デバイスは、ネットワークアクセスノードから利用可能な特徴/サービスを、相互認証の後に特徴/サービスを利用することをデバイスが望むかどうかをデバイスが判断できるように、認識し得る。

【０１３８】

例示的な許可サーバ

図10は、本明細書で説明する態様による、許可合意の動的な検証および実施をサポートするように構成された許可サーバ1000を示すブロック図である。一例では、許可サーバ1000は、ネットワーク通信回路1002、処理回路1004、およびメモリ回路/記憶デバイス(本明細書ではメモリ回路1006と呼ばれる)を含み得る。ネットワーク通信回路1002、処理回路1004、およびメモリ回路1006は、データおよび命令の交換のための通信バス1008に結合され得る。

【０１３９】

ネットワーク通信回路1002は、P-GWデバイス、ローカル許可サーバ、および/またはネットワークアクセスノードなどのネットワークノードと通信するための入力/出力モジュール/回路/機能1010を含むように構成され得る。当業者なら諒解するように、許可サーバ1000のネットワーク通信回路1002に他の回路/機能/モジュールが含まれることがある。

【０１４０】

処理回路1004は、許可合意の動的な検証および実施をサポートするように構成された、1つまたは複数のプロセッサ、特定用途向けプロセッサ、ハードウェアおよび/またはソフトウェアモジュールなどを含むか、または実装するように構成され得る。処理回路1004は、許可サーバ1000に記憶された許可合意の収集、保守、および編成を管理し得る許可合意管理回路/機能/モジュール1012を含み得る。処理回路1004は、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)の選択的にアクティブ化される特徴をアクティブ化するために使用され得る特徴アクティブ化鍵を導出するために使用され得る特徴アクティブ化鍵導出回路/機能/モジュール1014を含み得る。処理回路1004は、特徴アクティブ化鍵とともにデバイスに渡され得る許可パラメータ(たとえば、許可された選択的にアクティブ化される特徴の満了日)を導出するために使用され得る許可パラメータ導出回路/機能/モジュール1016を含み得る。処理回路1004は、許可合意に基づいて許可証明を導出することができ、許可サーバ1000の秘密鍵により許可証明に署名することができる許可証明導出回路/機能/モジュール1018を含み得る。当業者なら諒解するように、許可サーバ1000の処理回路1004に他の回路/機能/モジュールが含まれることがある。

【０１４１】

メモリ回路1006は、許可合意管理命令1020、特徴アクティブ化鍵導出命令1022、許可パラメータ導出命令1024、許可証明導出命令1026、ならびに特徴アクティブ化鍵記憶1030、許可パラメータ記憶1032、公開鍵記憶1034、および許可証明記憶1036のための空間を含むように構成され得る。当業者なら諒解するように、メモリ回路1006に他の命令およびデータの記憶のためのロケーションが含まれることがある。

【０１４２】

例示的なローカル許可サーバ

図11は、本明細書で説明する態様による、許可合意の動的な検証および実施をサポートするように構成されたローカル許可サーバ1100を示すブロック図である。ローカル許可サーバ1100は、許可サーバ(たとえば、1000、図10)のプロキシであり得る。一例では、ローカル許可サーバ1100は、ネットワーク通信回路1102、処理回路1104、およびメモリ回路/記憶デバイス(本明細書ではメモリ回路1106と呼ばれる)を含み得る。ネットワーク通信回路1102、処理回路1104、およびメモリ回路1106は、データおよび命令の交換のための通信バス1108に結合され得る。

【０１４３】

ネットワーク通信回路1102は、許可サーバおよび/またはネットワークアクセスノードなどのネットワークノードと通信するための入力/出力モジュール/回路/機能1110を含むように構成され得る。当業者なら諒解するように、ローカル許可サーバ1100のネットワーク通信回路1102に他の回路/機能/モジュールが含まれることがある。

【０１４４】

処理回路1104は、許可合意の動的な検証および実施をサポートするように構成された、1つまたは複数のプロセッサ、特定用途向けプロセッサ、ハードウェアおよび/またはソフトウェアモジュールなどを含むか、または実装するように構成され得る。処理回路1104は、ローカル許可サーバ1100に記憶された許可合意の収集、保守、および編成を管理し得る許可合意管理回路/機能/モジュール1112を含み得る。処理回路1104は、デバイスの選択的にアクティブ化される特徴をアクティブ化するために使用され得る特徴アクティブ化鍵を導出するために使用され得る特徴アクティブ化鍵導出回路/機能/モジュール1114を含み得る。処理回路1104は、特徴アクティブ化鍵とともにデバイスに渡され得る許可パラメータ(たとえば、許可された選択的にアクティブ化される特徴の満了日)を導出するために使用され得る許可パラメータ導出回路/機能/モジュール1116を含み得る。処理回路1104は、たとえば、許可合意におけるデータに基づいて許可証明を導出し、デバイスの公開鍵により許可証明を暗号化することができる許可証明導出回路/機能/モジュール1118を含み得る。処理回路1104は、ローカル許可サーバ1100に結合されたデバイスから特徴使用データを収集し得る特徴使用報告回路/機能/モジュール1138を含み得る。当業者なら諒解するように、ローカル許可サーバ1100の処理回路1104に他の回路/機能/モジュールが含まれることがある。

【０１４５】

メモリ回路1106は、許可合意管理命令1120、特徴アクティブ化鍵導出命令1122、許可パラメータ導出命令1124、許可証明導出命令1126、ならびに特徴アクティブ化鍵記憶1130、許可パラメータ記憶1132、許可証明記憶1134、および公開鍵記憶1136のための空間を含むように構成され得る。メモリ回路1106はまた、特徴使用報告命令1140を含むように構成され得る。当業者なら諒解するように、メモリ回路1106に他の命令およびデータの記憶のためのロケーションが含まれることがある。

【０１４６】

特徴アクティブ化の例示的な呼フロー図

図12は、本明細書で説明する態様による、許可合意の動的な検証および実施に関係する呼フロー図1200である。図12は、デバイス1202(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)、ローカル許可サーバ1204、および許可サーバ1206の間の例示的な対話を示す。一態様では、デバイス1202との間の呼フローは、デバイス1202の許可機能との間のものであり得る。

【０１４７】

許可サーバ1206は、ベンダー/OEMまたは別のエンティティからデバイス確認情報を取得し得る1208。デバイス確認情報は、たとえば、デバイス識別子、デバイス証明、デバイス公開鍵、ソフトウェアバージョン(たとえば、デバイス1202上に存在する許可機能に関連するソフトウェアのソフトウェアバージョン)、および/またはデバイス能力を含み得る。デバイス能力は、デバイス1202における選択的にアクティブ化される特徴のリスティングを含み得る。許可サーバ1206においてデバイス確認情報を取得することは進行中のプロセスであり得ることが理解されよう。デバイス確認情報がいつ追加、修正、または許可サーバ1206から除去され得るかについての制限はない。

【０１４８】

2者のエンティティの間で許可合意が締結され得る。許可合意(またはそれのコピー)が、ローカル許可サーバ1204において記憶のために取得され得1210、許可サーバ1206において記憶のために取得され得1211、またはローカル許可サーバ1204と許可サーバ1206の両方において記憶のために取得され得る。一例では、許可合意は、ローカル許可サーバにおいて実行されているソフトウェアの確認のためのプロビジョニング呼出しを含み得る。

【０１４９】
デバイス1202(またはデバイス1202の許可機能)は、ローカル許可サーバ1204に特徴アクティブ化要求(たとえば、1つまたは複数の選択的にアクティブ化される特徴をアクティブ化する要求)を送り得る1212。特徴アクティブ化要求は、証明ベースの検証を求める証明署名要求を含み得る。
【０１５０】
デバイス1202およびローカル許可サーバ1204は、リモート認証1214に関与し得る。リモート認証1214は第1のエンティティによって、(たとえば、既知の正しい状態に基づいて)第2のエンティティが正しく機能していることを検証するために使用され得る。たとえば、ローカル許可サーバ1204は、デバイス1202において実行されているソフトウェアを確認することによって、デバイス1202が正しく機能していることを検証し得る。一例では、ソフトウェアを確認することは、ローカル許可サーバ1204に送られたデバイス確認情報において識別されるソフトウェアを比較することが、デバイス1202において実行されているソフトウェアと合致することを伴い得る。リモート認証1214の結果が許可サーバ1206に送られ得る。リモート認証1214の結果は、攻撃者がデバイス1202を損なっていないこと、およびベンダー/OEMによって説明/識別されたソフトウェアをデバイス1202が実行していることを許可サーバ1206に対して保証するために使用され得る。リモート認証が成功しなかった場合、特徴アクティブ化要求は無視され得る。
【０１５１】
リモート認証1214が成功した場合、許可合意(たとえば、ローカル許可サーバにおいて記憶のために取得された許可合意)に基づいて、ローカル許可サーバ1204は、許可サーバ1206にデバイスの特徴アクティブ化を要求する(たとえば、特徴アクティブ化要求を送る1216)か、それともそれ自体の権限でデバイスの特徴アクティブ化を許可する(たとえば、許可合意/許可証明/許可ファイルを送る1222)かを決定し得る。後者のシナリオは、たとえば、ローカル許可サーバ1204が許可合意に基づいて事前に許可サーバ1206から1つまたは複数の許可鍵(たとえば、特徴アクティブ化鍵)を取得しているときに発生し得る。
【０１５２】
許可サーバ1206にデバイスの特徴アクティブ化を要求することをローカル許可サーバ1204が決定した場合、ローカル許可サーバ1204は、許可サーバ1206に特徴アクティブ化要求を送る(転送する)ことができ1216、その場合、ローカル許可サーバ1204は、デバイス1202と許可サーバ1206との間のセキュアなトンネルを提供するプロキシサーバであり得る。特徴アクティブ化要求は、デバイス確認情報(たとえば、デバイス識別子、デバイス証明、デバイス公開鍵、ソフトウェアバージョン、および/またはデバイス能力)とリモート認証1214の結果とを含み得る。許可サーバ1206に送られる特徴アクティブ化要求1216はまた、デバイスからローカル許可サーバに送られた特徴アクティブ化要求とともに証明署名要求が含まれていた場合に、証明署名要求を含み得る。
【０１５３】
一態様では、ローカル許可サーバ1204および許可サーバ1206がリモート認証1218に関与し得る。たとえば、ローカル許可サーバ1204は、ローカル許可サーバ1204が正しいソフトウェアを実行していることの証拠を許可サーバ1206に送り得る。このようにして、許可サーバ1206は、ローカル許可サーバ1204によって許可サーバ1206に送られたデバイス1202についての情報を信頼することが可能であり得る。そのような態様によれば、許可サーバ1206は、デバイス1202とローカル許可サーバ1204との間で実行されたリモート認証の結果を受諾し得る。随意にまたは代替的に、許可サーバ1206およびデバイス1202がリモート認証1219に関与し得る。
【０１５４】
許可サーバ1206が(ローカル許可サーバ1204およびデバイス1202のいずれかまたは両方による)リモート認証の結果を受諾し(たとえば、検証が成功している)、特徴アクティブ化要求が許可合意の条件に従っていることを許可サーバ1206が検証できると、許可サーバ1206は、デバイス1202において選択的にアクティブ化される特徴のセットを使用するデバ

イス1202の許可合意、許可証明、または許可合意および許可証明(たとえば、権限の証拠)と特徴アクティブ化鍵を含む許可ファイルとをローカル許可サーバ1204に送ることができる1220。一態様では、許可サーバ1206は、ネットワーク事業者(たとえば、MNO)(または第3のエンティティ)とのデバイス1202の許可合意を検証し得る。許可サーバ1206によって送られる権限の証拠は、許可合意、許可証明、または許可合意と許可証明の両方を含み得る。随意に、許可サーバ1206は、許可合意/許可証明/特徴アクティブ化鍵を含む許可ファイルを、デバイス1202に直接送り得る1223。

【０１５５】

ローカル許可サーバ1204が、許可サーバ1206に特徴アクティブ化要求を送る(たとえば、許可サーバ1206にデバイスの特徴アクティブ化を要求する)ことを決定し、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠と特徴アクティブ化鍵を含む許可ファイルとを許可サーバ1206から取得したか、または(たとえば、ローカル許可サーバ1204が、許可合意に基づいて事前に許可サーバ1206から1つもしくは複数の許可鍵を取得した場合に)デバイスの権限の証拠と許可ファイルとをそれ自体の権限で送ることを決定した場合、ローカル許可サーバは、許可合意/許可証明/許可ファイルをデバイス1202に送り得る1222。すなわち、ローカル許可サーバ1204は、選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠ならびに特徴アクティブ化鍵を含む許可ファイル(および利用可能な場合にソフトウェア)をデバイス1202に送り得る。

【０１５６】

デバイス1202が、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠(たとえば、許可合意、許可証明、または許可合意と許可証明の両方)と特徴アクティブ化鍵を含む許可ファイルとを(たとえば、特徴アクティブ化要求に応答して)取得すると、デバイス1202(および/またはデバイスの許可機能)は、(たとえば、デバイスが要求された選択的にアクティブ化される特徴をアクティブ化し使用することを許可されているかどうかを判断するために)権限の証拠を確認し得る。デバイス(および/またはデバイスの許可機能)が、デバイスが要求された選択的にアクティブ化される特徴を使用することを許可されていると判断した場合、デバイス(および/またはデバイスの許可機能)は、要求された選択的にアクティブ化される特徴のための特徴アクティブ化鍵を取り出し、要求された選択的にアクティブ化される特徴をアクティブ化することができる1224。いくつかの実装形態では、要求された選択的にアクティブ化される特徴は、権限の証拠において(たとえば、許可証明において)指定された満了時間または許可ファイルにおいて指定された満了時間まで、アクティブ化されたままであり得る。

【０１５７】

デバイス1202は、選択的にアクティブ化される特徴の使用に関する周期的報告1226をローカル許可サーバ1204に送り得る。ローカル許可サーバ1204は、複数のデバイスから受信された報告をアグリゲートし、選択的にアクティブ化される特徴の使用に関する周期的報告1228を許可サーバ1206に送り得る。当業者は、様々なシステムが様々なタイプの使用報告フォーマットを使用し得ることを諒解されよう。本明細書で説明する態様は、いずれか1つの使用報告フォーマットに限定されない。

【０１５８】

周期的報告は、アクティブ化された選択的にアクティブ化される特徴の総数が関連許可合意の条件を満たす限り、複数のデバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)において選択的にアクティブ化される特徴を事業者がアクティブ化できるようにすることによって、ローカル許可管理に柔軟性を与えることができる。たとえば、周期的報告は、事業者が同時に最大許容数の選択的にアクティブ化される特徴をアクティブ化することを可能にし得る。

【０１５９】

使用する許可の確認の例示的なシステムレベル呼フロー図

ネットワークサービスを使用する前に、各側(たとえば、クライアント側およびサービ

ング側、クライアントデバイスおよびネットワークノード)は、相手側が、ネットワークサービスを使用するために必要とされ、かつ/またはネットワークサービスを提供するために必要とされる1つまたは複数の選択的にアクティブ化される特徴をアクティブ化し使用することを許可されていることを確認し得る。言い換えれば、相互特徴検証の行為が発生し得る。このようにして、各側は、1つまたは複数の選択的にアクティブ化される特徴を使用/提供するデバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)の権利を規定し得る許可合意の条件を実施し得る。したがって、ネットワークサービスを使用/提供する前に、各側は、ネットワークサービスを提供/使用するために必要とされる選択的にアクティブ化される特徴を使用する相手側の権利の権限の証拠を取得することができ、権限の証拠を確認することができる。

【０１６０】

以下では、選択的にアクティブ化される特徴のセットを使用するデバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)の権限の証拠を確認するための2つの例示的なシステムレベルの方法を提供する。第1の方法は、デバイスのサブスクリプションプロファイルに基づく確認を実現する。第2の方法は、デバイスによって送られた許可情報に基づく確認を実現する。例示的なシステムレベルの方法は、排他的ではない。

【０１６１】

いずれかの例示的なシステムレベルの方法の実施の前に、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)ごとの許可情報がデバイスによって記憶され得る。さらに、許可情報、またはデバイスの新しいかつ/もしくは更新された選択的にアクティブ化される特徴を反映している情報は、ホーム加入者サーバ(HSS)にも記憶され得る。たとえば、デバイスが選択的にアクティブ化される特徴をアクティブ化するとき、許可サーバまたはローカル許可サーバは、選択的にアクティブ化される特徴のアクティブ化をHSSに報告し得る。デバイスの許可された新しいかつ/または更新された選択的にアクティブ化される特徴がネットワーク事業者(たとえば、MNO)によって検証されたとき、HSSはデバイスの能力プロファイルを更新することができる。デバイスの能力プロファイルは、デバイスのサブスクリプションプロファイルに関連付けられ得る。能力プロファイルは、デバイスが使用することを許可されている選択的にアクティブ化される特徴を識別し得る。一例では、HSSに記憶されたデバイスの能力プロファイルは、デバイスにとって、ネットワークノードにとって、またはデバイスおよびネットワークノードにとって利用可能であり得る。

【０１６２】

さらに、一態様によれば、ネットワークノード(たとえば、eNB)はデバイス(たとえば、チップ構成要素、クライアントデバイス)に、ネットワークノードにおいてアクティブ化された(たとえば、有効化された、使用された)選択的にアクティブ化される特徴のセットを告知し得る。特徴のセットは、たとえば、システム情報ブロック(SIB)メッセージを使用して、またはサービスクエリプロトコル(SQP)などの照会プロトコルを介して告知され得る。

【０１６３】

図13は、本明細書で説明する態様による、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)のサブスクリプションプロファイルに基づいて、選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を確認することに関連して発生し得るシステムレベル呼フローを示す例示的な呼フロー図1300である。デバイス1302(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)と、(たとえば、1つまたは複数のeNBおよび/またはアクセスポイントを含む)無線アクセスネットワーク(RAN)1304と、ネットワークノード1306(たとえば、MME)と、HSS1308と、ローカル許可サーバ1310と、許可サーバ1312とが示されている。

【０１６４】

いくつかの実装形態では、許可サーバ1312は、ベンダー/OEMまたは別のエンティティか

らデバイス確認情報を取得し得る1314。デバイス確認情報は、たとえば、デバイス識別子、デバイス証明、デバイス公開鍵、ソフトウェアバージョン(たとえば、デバイス1302上に存在する許可機能に関連するソフトウェアのソフトウェアバージョン)、および/またはデバイス能力を含み得る。デバイス能力は、デバイス1302における選択的にアクティブ化される特徴のリスティングを含み得る。許可サーバ1312においてデバイス確認情報を取得することは進行中のプロセスであり得ることが理解されよう。デバイス確認情報がいつ追加、修正、または許可サーバ1312から除去され得るかについての制限はない。

【０１６５】

2者のエンティティの間で許可合意が締結され得る。許可合意が、許可サーバ1312において記憶のために取得され得1315、許可合意が、ローカル許可サーバ1310において記憶のために取得され得1316、または許可合意が、ローカル許可サーバ1310と許可サーバ1312の両方において記憶のために取得され得る。一例では、許可合意は、ローカル許可サーバにおいて実行されているソフトウェアの確認のためのプロビジョニング呼出しを含み得る。

【０１６６】

特徴アクティブ化中、許可サーバ1312は、すべて上記のように、許可証明、許可ファイル、および特徴アクティブ化鍵を導出し得る。また、特徴アクティブ化中、許可サーバ1312は、すべて上記のように、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠(たとえば、許可合意、許可証明、または許可合意および許可証明の形式をとる許可情報)と特徴アクティブ化鍵を含み得る許可ファイルとをローカル許可サーバ1310に送り得る1318。代替的に、図面での過密状態を回避するために図示されていないが、許可サーバ1312は、すべて上記のように、デバイス1302に権限の証拠を送り得る。追加または代替として、特徴アクティブ化中、ローカル許可サーバ1310は、すべて上記のように、デバイスにおいて選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠(たとえば、許可合意、許可証明、または許可合意および許可証明の形式をとる許可情報)と特徴アクティブ化鍵を含み得る許可ファイルとをデバイス1302に送り得る1320。一態様では、ローカル許可サーバ1310は、デバイス1302の能力プロファイルをHSS1308に送り得る1322。デバイス1302の能力プロファイルは、デバイス1302においてアクティブ化されることを許可された選択的にアクティブ化される特徴を記載し得る。能力プロファイルは、選択的にアクティブ化される特徴に関連するパラメータを記載し得る。デバイスの能力プロファイルは、HSS1308に記憶され得るデバイス1302の対応する能力プロファイルを更新するために使用され得る。一態様では、許可サーバ1312は、デバイス1302の能力プロファイルをHSS1308に送り得る1324。

【０１６７】

HSS1308を参照すると、デバイス1302の能力プロファイルは、デバイス1302においてアクティブ化されることを許可された選択的にアクティブ化される特徴のリストを含むことができ、デバイス1302のサブスクリプションプロファイルに関連付けられ得る。HSS1308によって取得されたデバイス1302の能力プロファイルにより、HSS1308が、デバイス1302の新しいかつ/または更新された選択的にアクティブ化される特徴の許可ステータスを把握することが可能になる。一態様では、HSS1308は、HSS1308に記憶されたデバイス1302の対応する能力プロファイルをHSS1308が更新するべきかどうかを判断するために、ネットワーク事業者(たとえば、MNO)と相談し得る。一態様では、ネットワーク事業者の同意ありまたはなしで、HSS1308は、HSS1308に記憶されたデバイス1302の能力プロファイルを更新し得る1325。したがって、HSS1308は、デバイス1302の選択的にアクティブ化される特徴のリストを、ローカル許可サーバ1310または許可サーバ1312から取得された、デバイスにおいてアクティブ化されることを許可された選択的にアクティブ化される特徴のリストに基づいて更新し得る1325。リストを更新することは、デバイス1302においてアクティブ化されることを許可された選択的にアクティブ化される特徴のセットにおける少なくとも1つの選択的にアクティブ化される特徴の許可ステータスの変更を反映し得る。

【０１６８】

デバイス1302の初期接続手順1326中、ネットワークノード1306(たとえば、MME)は、HSS

1308からデバイス1302の能力プロファイルを取得し得る1328。一態様では、ネットワークノード1306(たとえば、MME)は、HSS1308に要求を送ることによって、HSS1308からデバイス1302の能力プロファイルを取得し得る1328。

【０１６９】

一例では、能力プロファイルは、デバイス1302のセキュアな/認証されたブートプロセス中に取得された完全性情報(たとえば、デバイス1302の許可機能のソフトウェア完全性情報)を含み得る。例として、セキュアな/認証されたブートプロセス中に(たとえば、認証および鍵一致(AKA)手順中に)完全性プロファイルが取得された場合、ネットワークノード1306(たとえば、MME)はデバイス1302に、デバイス1302において実行されているソフトウェアの完全性を証明する完全性情報を送るよう要求し得る。デバイス1302の完全性情報は、デバイス1302が正当なソフトウェアを実行している(すなわち、デバイスが許可されたソフトウェアを実行している)ことの証拠として、デバイス1302によって送られ得る。一態様では、ネットワークノード1306(たとえば、MME)は、デバイス1302との相互認証1330(たとえば、リモート認証)中に完全性情報を求める要求を行い得る。完全性情報は、相互認証1330中に使用され得る。上記は例であり、AKA手順または別個の手順中に完全性情報の送信要求が発生し得ることに留意されたい。

【０１７０】

ネットワークノード1306(たとえば、MME)は、HSS1308から取得されたデバイス1302の能力プロファイルに基づいて、デバイスコンテキスト(たとえば、特定の信号無線ベアラもしくはデフォルト無線ベアラまたはデータフローを識別し得るUEコンテキスト)を構成し得る1332。ネットワークノード1306(たとえば、MME)は、RAN1304(たとえば、RANのeNB)によりデバイスコンテキストを構成することができ1332、デバイスコンテキストおよび/または能力プロファイルをRAN1304に送り得る。これによりRAN1304は、選択的にアクティブ化される特徴をアクティブ化/非アクティブ化することが可能になり、それによって、デバイス1302に提供されるネットワークサービスを有効化(または無効化)することができる。デバイス1302のためのネットワークサービスの有効化/無効化は、デバイス1302の能力プロファイルに従ってデバイスコンテキストを更新/設定することによって達成され得る。非アクセス層(NAS)および無線リソース制御(RRC)手順が、この目的のために使用され得る。

【０１７１】

S1ハンドオーバ中に、MME再配置が実行された場合に、デバイスコンテキスト(たとえば、UEコンテキスト)がターゲットMMEに転送され得ることに留意されたい。X2ハンドオーバ中に、ソースネットワークアクセスノード(たとえば、ソースeNB)は、デバイス能力を明示するデバイスコンテキスト(たとえば、UEコンテキスト)をターゲットネットワークアクセスノード(たとえば、ターゲットeNB)に送り得る。

【０１７２】

デバイス1302の能力プロファイルが、いくつかの選択的にアクティブ化される特徴が(たとえば、満了に起因して)非アクティブ化される必要があることを示す場合、ネットワークノード1306(たとえば、MME)は、選択的にアクティブ化される特徴を非アクティブ化することができ、対応する構成を(RAN1304内の)ネットワークアクセスノード(たとえば、eNB)に適用し得る。対応する構成は、たとえば、デバイスコンテキスト修正手順(たとえば、UEコンテキスト修正手順)を使用して、ネットワークアクセスノードに適用され得る。デバイス1302は、上述したように、(許可サーバに記憶された)許可合意を更新し、次いで、特徴アクティブ化を実行する(たとえば、特徴アクティブ化要求を送る)ことによって、任意の非アクティブ化された選択的にアクティブ化される特徴を再アクティブ化し得る。

【０１７３】

第1の例示的なシステムレベルの方法は、HSS1308において、デバイス1302のサブスクリプションプロファイルに関連する、デバイス1302の能力プロファイルに記憶された許可情報を利用し得る。HSS1308は、デバイス1302においてアクティブ化されているか、または

アクティブ化されることを許可されている1つまたは複数の選択的にアクティブ化される特徴を識別するために、クエリ-応答タイプのプロトコルにおいて使用され得る(アクセスネットワーククエリプロトコル(ANQP)における情報要素と同様の)情報の要素を実装し得る。情報の要素は、どの特徴(たとえば、どの選択的にアクティブ化される特徴)がデバイス1302(たとえば、クライアントデバイス、ネットワークアクセスノードなど)上で利用可能であるかに関するクエリに対する応答を円滑にするために使用され得る。情報の要素は、本明細書ではサービスクエリプロトコル(SQP)と呼ばれ得る、強化されたANQPプロトコルに関連するパラメータと考えられ得る。

【０１７４】

例として、デバイス1302(たとえば、クライアントデバイス)は、デバイス1302がボイスオーバーIPではなくインターネットを使用することを許容するサブスクリプションを有し得る。サブスクリプション情報は、HSS1308において、デバイス1302のサブスクリプションプロファイルに記憶され得る。デバイスの能力プロファイルも、HSS1308に記憶され得る。能力プロファイルは、サブスクリプションプロファイルに関連付けられ得る。サブスクリプション情報および能力プロファイルに関係する情報の要素は、初期接続手順1326中にネットワークノード1306(たとえば、MME)に送られ得る。初期接続手順1326はまれに発生し得ることに留意されたい。

【０１７５】

本例では、説明した情報要素を受信するネットワークノード1306(たとえば、MME)は、デバイス1302が(たとえば、第2のデータサービスとして)ボイスオーバーIPではなく(たとえば、第1のデータサービスとして)インターネットを使用することができるように、ネットワークを構成し得る。したがって、デバイス1302のサブスクリプションプロファイルに関連するデバイス1302の能力プロファイルに記憶された許可情報を利用することができる第1の例示的な方法は、能力プロファイル要素を利用し得る。能力プロファイル要素は、ネットワークサービスを有効化するために必要とされる1つまたは複数の選択的にアクティブ化される特徴をデバイス1302が使用する許可を確認し実施するために使用され得る。許可は最終的には、許可サーバ1312において取得された許可合意(またはいくつかの態様では、ローカル許可サーバ1310において取得された許可合意)に基づき得る。

【０１７６】

HSS1308に記憶されたデバイス1302の能力プロファイルからの情報は、ネットワークノード1306(たとえば、MME)によって、様々なネットワーク機能を構成するために使用され得る。様々なネットワーク機能は、デバイス1302が、デバイス1302においてアクティブ化され得る(またはアクティブ化されることを許可され得る)1つまたは複数の選択的にアクティブ化される特徴を利用することを可能にし得る。

【０１７７】

図14は、本明細書で説明する態様による、デバイス1402(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)に記憶された許可証明において識別される選択的にアクティブ化される特徴の第1のセットを使用するデバイス1402の権限の証拠を確認することに関連付けられ得る別のシステムレベル呼フローを示す例示的な呼フロー図1400である。デバイス1402(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)と、無線アクセスネットワーク(RAN)1404(たとえば、1つまたは複数のeNBおよび/またはアクセスポイント)と、(たとえば、図14ではMMEとして例示されている)ネットワークノード1406とが示されている。MMEとして例示されているネットワークノード1406とデバイス1402との間で発生する、以下で説明する交換は、任意のデバイス1402とネットワークノード(たとえば、ネットワークアクセスノード、eNB、MME、S-GW、P-GW)との間で実行され得る。デバイスコンテキストを構成する動作1426は、MMEなどのネットワークノード1406に当てはまり得るが、デバイスコンテキストを構成する動作1426は、eNBなどのネットワークノードの他の例に当てはまらないことがあることに留意されたい。したがって、デバイスコンテキストを構成する動作1426および(デバイスコンテキストを構成する動作1426の受け手であり得る)RAN1404は、ネットワークノード1406がMMEとして例示

されている図14の例に当てはまるが、(たとえば、ネットワークノード1406がMME以外のノードである)他の例に当てはまらないことがあるので、破線形式で示されている。

【０１７８】

上記で説明したように、たとえば、特徴アクティブ化中、デバイス1402(たとえば、クライアントデバイス)は、デバイス1402において選択的にアクティブ化される特徴の第1のセットを使用するデバイス1402の権限の証拠(たとえば、第1の許可サーバによって署名された、許可証明の形式をとり得る第1の許可情報)と特徴アクティブ化鍵を含む許可ファイルとを取得し得る1408。ネットワークノード1406(たとえば、MME)は、ネットワークサービスを使用するデバイス1402の権限を確認するために、第1の許可情報(たとえば、許可証明)を使用し得る。同様に、ネットワークノード1406(たとえば、MME)は、ネットワークノード1406において選択的にアクティブ化される特徴の第2のセットを使用するネットワークノード1406の権限の証拠(たとえば、第2の許可サーバによって署名された、許可証明の形式をとり得る第2の許可情報)を取得し得る1410。デバイス1402(たとえば、クライアントデバイス)は、ネットワークサービスを提供するネットワークノード1406の権限を確認するために、第2の許可情報(たとえば、許可証明)を使用し得る。

【０１７９】

第1の許可情報(たとえば、許可証明)は、デバイス1402に対して許可された選択的にアクティブ化される特徴を識別することができ、第1の許可サーバによって第1の許可サーバの秘密鍵を使用して署名され得る。第1の許可情報(たとえば、許可証明)は、デバイス1402の識別情報を含むこともあり、許可証明の満了時間を含むこともある。許可ファイルは、特徴アクティブ化鍵および関連パラメータを含むことができ、デバイス1402の公開鍵により暗号化され得る。いくつかの実装形態では、デバイス1402は、第1の許可情報(たとえば、許可証明)および許可ファイルを特徴アクティブ化中に取得する。

【０１８０】

第1の許可情報(たとえば、許可証明)は、たとえば、第1の許可サーバによって署名された、デバイス1402のデバイス識別子および公開鍵を含む、対応する識別情報証明とともに使用され得る。識別情報証明は、デバイス1402からの1つまたは複数の選択的にアクティブ化される特徴を非アクティブ化しても、有効なままであり得る。一態様では、デバイス識別子は、たとえば、デバイスシリアル番号または国際移動局機器識別情報(IMEI)であり得る。本明細書における実装形態では、デバイス識別子は常に、デバイス1402がデバイス識別子の所有権を証明することができるように、デバイス公開鍵に関連付けられ得る。

【０１８１】

一態様では、デバイス1402の公開鍵(または公開鍵のハッシュ)はデバイス識別子として使用され得る。この場合、識別情報証明は、不要であることがあるが、デバイス1402の識別情報は、第1の許可サーバおよび/またはローカル許可サーバおよび/または第3のエンティティを通じて検証可能であるべきである。

【０１８２】

第1の許可情報(たとえば、許可証明)は、デバイス1402によってローカル許可サーバから取得され得る。この場合、デバイス1402は、たとえば、特徴アクティブ化中に、ローカル許可サーバの証明を取得し得る。

【０１８３】

デバイス1402は、ネットワークノード1406に接続要求1412を送り得る。一態様では、接続要求は、ネットワークサービスを使用する要求であるか、またはかかる要求を含むと理解され得る。応答して、ネットワークノード1406(たとえば、MME)は、デバイス1402において選択的にアクティブ化される特徴の第1のセットを使用するデバイス1402の権限の証拠を求める要求1414をデバイス1402に送ることができ、選択的にアクティブ化される特徴の第1のセットは、ネットワークサービスを使用するためにデバイス1402によって必要とされる第1の選択的にアクティブ化される特徴を含む。言い換えれば、ネットワークノード1406(たとえば、MME)は、デバイスの権限の証拠(たとえば、許可証明の形式をとり得る第1の許可情報)を求める要求1414をデバイス1402に送り得る。一態様では、そのような要

求1414は、認証および鍵一致(AKA)手順中に送られ得る。デバイス1402は、要求1414に応答して、デバイス1402の権限の証拠をネットワークノード1406に送り得る1416。

【０１８４】

相互認証1418は、デバイス1402とネットワークノード1406との間で発生し得る。相互認証1418は随意であってよい。相互認証1418は、セキュアなチャネルを確立することによってデバイス1402およびネットワークノード1406が正しいエンティティと通信していることの保証を提供するように実施され得る。デバイス1402との相互認証1418(たとえば、リモート認証)は、デバイス1402がネットワークに登録するために使用されるAKA手順とは異なることに留意されたい。

【０１８５】

いくつかの例では、デバイス1402の権限の証拠を求める要求1414をネットワークノード1406がデバイス1402に送る前に相互認証1418が実施され得ることにさらに留意されたい。たとえば、ネットワークノード1406が(図14において例示されるように)MMEである場合、AKA手順が完了すると、デバイス1402およびMMEは、セキュアな移送(すなわち、NASメッセージ)を介して互いに通信することができる。結果として、デバイス1402およびMMEは、互いに認証し得る。

【０１８６】

一態様では、ネットワークノード1406(たとえば、MME)はデバイス1402に、デバイス1402のセキュアな/認証されたブートプロセス中に作成された完全性情報(たとえば、デバイス1402の許可機能のソフトウェア完全性情報)を送るよう要求し得る。例として、セキュアな/認証されたブートプロセス中に完全性情報が取得された場合、完全性情報は、デバイス1402において実行されているソフトウェアの完全性を証明するために使用され得る。一態様では、ネットワークノード1406(たとえば、MME)は、デバイス1402との相互認証1418(たとえば、リモート認証)中に完全性情報を求める要求を行い得る。完全性情報は、相互認証中に使用され得る。

【０１８７】

ネットワークノード1406(たとえば、MME)は、デバイス1402において選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠(たとえば、第1の許可情報)を確認し得る1420。確認は、許可サーバの公開鍵を使用して(またはローカル許可サーバがデバイス1402の権限の証拠を作成した場合はローカル許可サーバの公開鍵を使用して)デバイス1402の権限の証拠(たとえば、第1の許可情報)を確認することによって実行され得る。さらに、一態様では、ネットワークノード1406は、デバイス1402の権限の証拠(たとえば、第1の許可情報)を送ったデバイス1402が、デバイス1402の権限の証拠(たとえば、第1の許可情報)とともに含まれるデバイス1402の公開鍵に対応する秘密鍵を保有していることを検証し得る1422。検証は、たとえば、デバイス1402の権限の証拠(たとえば、第1の許可情報)とともに含まれるデバイス1402の公開鍵を使用して、デバイス1402の権限の証拠(たとえば、第1の許可情報)とともに送られ得るデバイス1402の署名を確認することによって実行され得る。

【０１８８】

図14の例示的な説明の場合のように、ネットワークノードがMMEである場合で、確認1420と検証1422の両方が成功した場合、ネットワークノード1406(たとえば、MME)は、RAN1404においてネットワークサービスの使用を実施するためにデバイスコンテキストを構成する動作1426を実施し得る。一例では、ネットワークノード1406は、ネットワークノードが、たとえば、MMEである場合、デバイス1402が許可された選択的にアクティブ化される特徴を使用することができるように、RAN1404を構成し得る。別の例では、ネットワークノード1406は、ネットワークノードが、たとえば、MMEである場合、デバイス1402が許可された選択的にアクティブ化される特徴のみを使用することができるように、RAN1404を構成し得る。

【０１８９】

一方、上述のように、ネットワークノードがeNBであった場合、デバイスコンテキスト

を構成する動作1426は当てはまらないことがある。したがって、デバイスコンテキストを構成する動作1426およびRAN1404は、破線形式で示されている。

【０１９０】

いくつかの態様によれば、確認1420と検証1422の両方が成功した場合、ネットワークノード1406は、第1の許可情報に従って、デバイス1402においてアクティブ化された選択的にアクティブ化される特徴と、ネットワークサービスを取得するためにデバイス1402によって使用される必要がある選択的にアクティブ化される特徴が合致することを検証し得る。言い換えれば、必要とされる選択的にアクティブ化される特徴のアクティブ化を確かめる随意の動作1423が生じ得る。一態様では、必要とされる選択的にアクティブ化される特徴のアクティブ化を確かめること1423は、ネットワークサービスを使用するためにデバイス1402によって必要とされる選択的にアクティブ化される特徴の必要なセットを識別することと、選択的にアクティブ化される特徴の必要なセットが選択的にアクティブ化される特徴の第1のセットに含まれるかどうかの判断に基づいて、要求への応答1424を送ることとを伴うことができ、選択的にアクティブ化される特徴の第1のセットは、デバイスの権限の証拠(たとえば、第1の許可情報)において識別される選択的にアクティブ化される特徴のセットである。

【０１９１】

一態様では、選択的にアクティブ化される特徴の必要なセットを識別することは、第1の許可サーバによって維持される許可された選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、ネットワークサービスを使用するためにデバイス1402によって必要とされる選択的にアクティブ化される特徴を導出することを含み得る。別の態様では、選択的にアクティブ化される特徴の必要なセットを識別することは、第1の許可サーバによって維持されるライセンス可能な選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、ネットワークサービスを使用するためにデバイス1402によって必要とされる選択的にアクティブ化される特徴を導出することを含み得る。

【０１９２】

一態様では、ネットワークノード1406は、接続要求の承認を示す応答1424を送り得る。

【０１９３】

本明細書で説明する態様は、ネットワークノード1406が、ネットワークサービスを使用するデバイス1402の権利を確認することを可能にするが、そのような態様はまた、デバイス1402が、ネットワークサービスを提供するネットワークノード1406の権利を確認することを可能にする。一部のネットワークノードは、デバイス1402に特徴(たとえば、選択的にアクティブ化される特徴)の利用可能性を誤って広告することがある。実際には、ある種の特徴は、ネットワークノードによる広告にもかかわらず、アクティブ化されないことがある。ネットワークがデバイス1402に、広告された特徴またはサービスを提供しない場合、ネットワークは、たとえば、下位のサービスを使用することによって、デバイス1402にさらに料金を負担させることがある。したがって、デバイス1402は、特徴を広告しているネットワークノードがその特徴を提供することを許可されていることを検証することに関心がある。デバイス1402が、ネットワークが特徴を提供することを許可されていることを検証し、それによって、ネットワークにおいて特徴が利用可能であることを確かめると、デバイス1402は、ネットワークに結合し、ネットワークサービスを使用することができる。

【０１９４】

したがって、デバイス1402は、ネットワークサービスを提供するネットワークノードの権限の証拠を求める要求を送り得る1428。応答して、ネットワークノード1406は、第2の許可サーバによって署名された、ネットワークノードにおいて選択的にアクティブ化される特徴の第2のセットを使用するネットワークノードの権限の証拠(たとえば、第2の許可情報)を送ることができ1430、選択的にアクティブ化される特徴の第2のセットは、ネットワークサービスを提供するためにネットワークノードによって必要とされる第2の選択的

にアクティブ化される特徴を含む。デバイス1402は、ネットワークノード1406によってデバイス1402に送られた第2の許可情報(たとえば、第2の許可証明)を確認し得る1432。確認は、第2の許可サーバの公開鍵を使用して(または第2のローカル許可サーバがネットワークノード1406の権限の証拠を作成した場合は第2のローカル許可サーバの公開鍵を使用して)実行され得る。

【０１９５】

さらに、一態様では、デバイス1402は、ネットワークノード1406の権限の証拠(たとえば、第2の許可情報)を送ったネットワークノード1406が、ネットワークノード1406の権限の証拠(たとえば、第2の許可情報)とともに含まれるネットワークノード1406の公開鍵に対応する秘密鍵を保有していることを検証し得る1434。検証は、たとえば、ネットワークノード1406の権限の証拠(たとえば、第2の許可情報)とともに含まれるネットワークノード1406の公開鍵を使用して、ネットワークノード1406の権限の証拠(たとえば、第2の許可情報)とともに送られ得るネットワークノード1406の署名を確認することによって実行され得る。

【０１９６】

いくつかの態様によれば、確認1432と検証1434の両方が成功した場合、デバイス1402は、第2の許可情報に従って、ネットワークノード1406においてアクティブ化された選択的にアクティブ化される特徴と、ネットワークサービスを提供するためにネットワークノード1406によって使用される必要がある選択的にアクティブ化される特徴が合致することを検証し得る。言い換えれば、ネットワークノードがネットワークサービスを提供することを許可されていることを確かめる随意の動作1436が発生し得る。一態様では、ネットワークノードがネットワークサービスを提供することを許可されていることを確かめること1436は、ネットワークサービスを使用するためにネットワークノード1406によって必要とされる選択的にアクティブ化される特徴の第3のセットを識別することと、選択的にアクティブ化される特徴の第3のセットが選択的にアクティブ化される特徴の第2のセットに含まれるかどうかの判断に基づいて、ネットワークサービスを使用することとを伴うことができ、選択的にアクティブ化される特徴の第2のセットは、ネットワークノード1406の権限の証拠(たとえば、第2の許可情報)において識別される。一態様では、確認1432、検証1434、およびネットワークノードがネットワークサービスを提供することを許可されていることを確かめること1436が成功した場合、デバイス1402は、ネットワークノード1406によって提供されたネットワークサービスを使用し得る。

【０１９７】

例示的なデバイス

図15は、本明細書で説明する態様による、許可合意の動的な検証および実施をサポートするように構成された例示的なデバイス1500(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)を示すブロック図であり、実施は、選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠の動的な確認と、許可合意の条件に従った選択的にアクティブ化される特徴のアクティブ化/非アクティブ化とを含む。一例では、例示的なデバイス1500は、ネットワーク通信回路1502、処理回路1504、およびメモリ回路/記憶デバイス(本明細書ではメモリ回路1506と呼ばれる)を含み得る。ネットワーク通信回路1502、処理回路1504、およびメモリ回路1506は、データおよび命令の交換のための通信バス1508に結合され得る。

【０１９８】

ネットワーク通信回路1502は、ユーザとの入力/出力動作のための第1の入力/出力回路/機能/モジュール1510を含み得る。ネットワーク通信回路1502は、ワイヤレス通信のための第2の入力/出力回路/機能/モジュール1511(たとえば、受信機/送信機モジュール/回路/機能)を含み得る。当業者なら諒解するように、ネットワーク通信回路1502とともに他の回路/機能/モジュールが含まれることがある。

【０１９９】

処理回路1504は、許可合意の動的な検証および実施をサポートするように構成された、

1つまたは複数のプロセッサ、特定用途向けプロセッサ、ハードウェアおよび/またはソフトウェアモジュールなどを含むか、または実装するように構成されてよく、実施は、選択的にアクティブ化される特徴のセットを使用するデバイスの権限の証拠の動的な確認と、許可合意の条件に従った選択的にアクティブ化される特徴のアクティブ化/非アクティブ化とを含む。処理回路1504は、許可機能回路/機能モジュール1512、許可証明検証回路/機能モジュール1514、許可パラメータ評価回路/機能モジュール1516、および特徴アクティブ化鍵抽出回路/機能モジュール1518を含むように構成され得る。当業者なら諒解するように、処理回路1504とともに他の回路/機能/モジュールが含まれることがある。

【０２００】

メモリ回路1506は、許可命令1520、許可証明検証命令1522、許可パラメータ評価命令1524、および特徴アクティブ化鍵抽出命令1526を含むように構成され得る。メモリ回路1506の別個の部分は、セキュアな記憶をサポートするように構成され得る。したがって、メモリ回路1506は、セキュア記憶回路1528をさらに含み得る。セキュア記憶回路1528は、秘密鍵記憶1530を含み得る。秘密鍵記憶1530は、公開/秘密鍵ペアの秘密鍵を記憶することができ、許可サーバまたはローカル許可サーバは、公開/秘密鍵ペアの公開鍵を使用して、許可証明を暗号化することができる。セキュア記憶回路1528は、特徴アクティブ化鍵記憶1532をさらに含み得る。メモリ回路1506は、選択的にアクティブ化される特徴のリスティング1534ならびにデバイスの選択的にアクティブ化される特徴の各々に関する許可パラメータのリスティング1536をさらに記憶し得る。当業者なら諒解するように、メモリ回路1506に他の命令およびデータの記憶のためのロケーションが含まれることがある。

【０２０１】

許可合意の検証/実施の例示的な方法

図16は、本明細書で説明する態様による、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)において実行可能な例示的な方法1600のフローチャートである。一態様では、デバイスは、図15の例示的なデバイス1500および/または図3のデバイス302と同様であり得る。例示的な方法1600を実施する前に、デバイスは、ネットワークサービスの使用に関連する1つまたは複数の選択的にアクティブ化される特徴のセットを決定していることがある。例示的な方法1600を実施する前に、デバイスは、特徴アクティブ化要求(たとえば、1つまたは複数の選択的にアクティブ化される特徴をアクティブ化する許可を求める要求)を(許可サーバまたはローカル許可サーバに)送っていることがある。特徴アクティブ化要求、または何らかの他のイベントは、第1の許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠をデバイスに送ることを許可サーバ(またはローカル許可サーバ)に行わせることができるトリガイベントとして機能し得る。

【０２０２】

デバイスは、第1の許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を取得し得る1602。デバイスの権限の証拠は、本明細書では許可情報と呼ばれ得る。デバイスの権限の証拠は、許可証明を含み得る。デバイスの権限の証拠は、許可ファイルとともに取得され得る。許可ファイルは、許可パラメータおよび1つまたは複数の特徴アクティブ化鍵を含み得る。本明細書で説明するように、デバイスは、許可証明を確認し、デバイスの権限の証拠を送っている許可サーバが正しい(たとえば、詐欺師ではない)許可サーバであったことを検証し、特徴アクティブ化鍵を解読し、解読された特徴アクティブ化鍵を使用して、デバイスにおいて選択的にアクティブ化される特徴の第1のセットをアクティブ化していることがある。

【０２０３】

デバイスは、ネットワークサービスを使用する要求をネットワークノードに送り得る1604。選択的にアクティブ化される特徴の第1のセットは、ネットワークサービスを使用するためにデバイスによって必要とされる第1の選択的にアクティブ化される特徴を含み得る。第1の選択的にアクティブ化される特徴は、許可サーバから取得された権限の証拠に

よって、デバイスにおいてアクティブ化されることを許可され得る。いくつかの態様によれば、第1の選択的にアクティブ化される特徴の一部または全部は、デバイスがネットワークサービスを使用する要求を送った時点に、またはその前にデバイスにおいてアクティブ化され得る。

【０２０４】

デバイスはネットワークノードから、ネットワークサービスを使用する要求を送ったことに応答して、デバイスの権限の証拠を求める要求を取得し得る1606。応答して、デバイスはネットワークノードに、デバイスの権限の証拠(たとえば、第1の許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠)を送り得る1608。

【０２０５】

デバイスはネットワークノードに、ネットワークサービスを提供するネットワークノードの権限の証拠を求める要求を送り得る1610。

【０２０６】

随意に、デバイスは、デバイス完全性情報を送り得る1612。デバイス完全性情報は、セキュアなブートプロセス中に取得されていることがある。またさらに随意に、デバイスは、デバイスとネットワークサービスを使用する要求を確認しているネットワークノードとの間の相互認証(たとえば、リモート認証)を実行し得る1614。

【０２０７】

随意に、デバイスは、ネットワークサービスを使用する要求を承認する応答を取得し得る1616。応答は、第1の許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を送ったことに応答したものであり得る。

【０２０８】

デバイスはネットワークノードから、第2の許可サーバによって署名された、ネットワークノードにおいて選択的にアクティブ化される特徴の第2のセットを使用するネットワークノードの権限の証拠を取得し得る1618。選択的にアクティブ化される特徴の第2のセットは、ネットワークサービスを提供するためにネットワークノードによって必要とされる第2の選択的にアクティブ化される特徴を含み得る。

【０２０９】

デバイスは、ネットワークサービスを使用する前にネットワークノードの権限の証拠を確認し得る1620。

【０２１０】

いくつかの態様では、デバイスの権限の証拠はデバイスによって、許可サーバから取得され得る(たとえば、デバイスの権限の証拠は、許可サーバにおいて発生している)。いくつかの態様では、デバイスの権限の証拠はデバイスによって、ローカル許可サーバから取得され得る(たとえば、デバイスの権限の証拠は、ローカル許可サーバにおいて発生している)。いくつかの態様では、デバイスの権限の証拠は、許可証明を含み得る。いくつかの態様では、デバイスの権限の証拠は、特徴アクティブ化プロセス中に(たとえば、デバイスにおいてネットワークサービスを使用するために必要とされる選択的にアクティブ化される特徴のアクティブ化中に)許可サーバまたはローカル許可サーバから取得され得る。

【０２１１】

いくつかの態様によれば、デバイスは、チップ構成要素、クライアントデバイス、ネットワークアクセスノード、モビリティ管理エンティティ、またはゲートウェイデバイスであり得る。一態様によれば、デバイスはクライアントデバイスまたはチップ構成要素であり得、ネットワークノードはネットワークアクセスノードであり得る。一態様では、デバイスの権限の証拠は、第1の許可サーバにおいて発生し、第1の許可サーバの秘密鍵により署名され、第1の選択的にアクティブ化される特徴のリスティングを含む。そのような態様では、本方法は、第1の許可サーバの公開鍵を使用して、第1の選択的にアクティブ化さ

れる特徴のリスティングを確認することによって、デバイスの権限の証拠を確認するステップをさらに含み得る。本方法は、またさらに、デバイスの公開鍵により暗号化された、第1の選択的にアクティブ化される特徴に関連する特徴アクティブ化鍵を取得するステップを含み得る。本方法は、またさらに、デバイスにのみ知られている、デバイスの秘密鍵を使用して、特徴アクティブ化鍵を解読するステップを含み得る。本方法は、またさらに、特徴アクティブ化鍵により第1の選択的にアクティブ化される特徴をアクティブ化し、かつ/または第1の選択的にアクティブ化される特徴のアクティブ化を維持するステップを含み得る。

【０２１２】

一態様によれば、ネットワークノードの権限の証拠は、第2の許可サーバにおいて発生することがあり、第2の許可サーバの秘密鍵により署名され、第2の選択的にアクティブ化される特徴のリスティングを含む。そのような態様では、本方法はまた、第2の許可サーバの公開鍵を使用して、第2の選択的にアクティブ化される特徴のリスティングを確認することによって、ネットワークノードの権限の証拠を確認するステップを含み得る。

【０２１３】

いくつかの態様によれば、第1の許可サーバはローカル許可サーバであり得る。

【０２１４】

一態様では、本方法はまた、ネットワークサービスを使用するためにネットワークノードによって必要とされる選択的にアクティブ化される特徴の第3のセットを識別するステップと、選択的にアクティブ化される特徴の第3のセットが選択的にアクティブ化される特徴の第2のセットに含まれるかどうかの判断に基づいてネットワークサービスを使用するステップとを含み得る。

【０２１５】

さらに別の態様では、デバイスの権限の証拠は、第1の許可サーバにおいて発生することがあり、デバイスにおいて、第1の許可サーバから取得される一方、ネットワークノードの権限の証拠は、第2の許可サーバにおいて発生し、デバイスにおいて、ネットワークノードから取得される。

【０２１６】

いくつかの態様では、第1の許可サーバおよび第2の許可サーバは、1つの許可サーバである。

【０２１７】

一態様では、デバイスの権限の証拠は、第1の選択的にアクティブ化される特徴をアクティブ化する許可をデバイスが取得する特徴アクティブ化プロセス中に、第1の許可サーバから取得され得る。

【０２１８】

一例では、ネットワークノードの権限の証拠は、認証および鍵一致(AKA)プロセス中にネットワークノードから取得される。

【０２１９】

一態様では、デバイスの権限の証拠は、許可証明を表すデータであり得る。一態様では、デバイスの権限の証拠は、デバイスが第1の選択的にアクティブ化される特徴をアクティブ化することを許可されていることを示す許可合意を表すデータであり得る。

【０２２０】

一態様によれば、第1の許可情報は、デバイスにおいてアクティブ化されることを許可された選択的にアクティブ化される特徴の各々に関して、選択的にアクティブ化される特徴をアクティブ化する許可が満了する日を含み得る。

【０２２１】

図17は、本明細書で説明する態様による、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)において実行可能な例示的な方法1700のフローチャートである。一態様では、デバイスは、図15の例示的なデバイス1500と同様であり得る。デバイスは、ネットワークサービスを提供するネットワークアクセスノードの能力を

識別する情報を取得し得る1702。情報は、任意の適切な方法で受信され得る。たとえば、情報は、ネットワークアクセスノード(たとえば、eNB)から広告の形式で受信され得る。広告は、オーバージエアブロードキャストを介してネットワーク能力を広告する(たとえば、システム情報ブロック(SIB)において提示される情報を介して広告する)ことができる。別の例として、情報は、アクセスネットワーククエリプロトコル(ANQP)またはサービスクエリプロトコル(SQP)クエリに対する応答において受信され得る。ネットワーク能力は、たとえば、ネットワークアクセスノードによって提供されるネットワークサービスを含み得る。

【０２２２】

デバイスはネットワークアクセスノードから、ネットワークサービスを提供するネットワークアクセスノードの権限を検証するために、許可情報を取得し得る1704。一態様では、許可情報は、許可証明の形式をとり得る。許可サーバ(またはローカル許可サーバ)は、ネットワークアクセスノードに許可証明を送っていることがある。デバイスは、たとえば、ネットワークアクセスノードがネットワークサービスを提供することを許可されていることを検証するために、許可情報を送る要求をネットワークアクセスノードに送ることによって、許可情報を取得し得る。

【０２２３】

デバイスは、ネットワークアクセスノードおよび/またはネットワークサービスを提供するネットワークアクセスノードの権限を確認するために、許可情報を確認し得る1706。いくつかの態様では、許可情報は、許可証明を確認することによって確認され得る。いくつかの態様では、許可サーバが許可証明を発信した場合、許可証明は、許可サーバの公開鍵を使用して確認され得る。いくつかの態様では、ローカル許可サーバが許可証明を発信した場合、許可証明は、ローカル許可サーバの公開鍵を使用して確認され得る。デバイスは、許可情報の確認が成功したかどうかを判断し得る1708。許可情報の確認が成功したとデバイスが判断した場合、デバイスは、ネットワークサービスを使用し得る1710。許可情報の確認が成功しなかったとデバイスが判断した場合、デバイスは、ネットワークサービスを使用し得ない1712。

【０２２４】

図18は、本明細書で説明する態様による、ネットワークノード(たとえば、ネットワークアクセスノード、eNB、MME、S-GW、P-GW)において実行可能な例示的な方法1800のフローチャートである。一態様では、ネットワークノードは、図15の例示的なデバイス1500と同様であり得る。ネットワークノードはデバイスから、ネットワークサービスを使用する要求を取得することができる1802。ネットワークノードはデバイスから、許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を取得することもできる1804。

【０２２５】

ネットワークノードは、デバイスの権限の証拠を確認し得る1806。すなわち、ネットワークノードは、許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を確認し得る。ネットワークノードは、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限を確認するために、デバイスの権限の証拠を確認し得る。選択的にアクティブ化される特徴の第1のセットは、ネットワークサービスを使用するためにデバイスによって必要とされ得る。いくつかの態様では、デバイスの権限の証拠は、許可証明を確認することによって確認され得る。いくつかの態様では、許可サーバが許可証明を発信した場合、許可証明は、許可サーバの公開鍵を使用して確認され得る。いくつかの態様では、ローカル許可サーバが許可証明を発信した場合、許可証明は、ローカル許可サーバの公開鍵を使用して確認され得る。

【０２２６】

ネットワークノードは、ネットワークサービスを使用するためにデバイスによって必要とされる特徴を別個に識別し、その後、選択的にアクティブ化される特徴の第1のセット

を、ネットワークサービスを使用するためにデバイスによって必要とされる別個に識別される特徴と比較し得る。ネットワークノードは、別個に識別される特徴が選択的にアクティブ化される特徴の第1のセットと合致する場合に、デバイスがネットワークサービスを使用することが可能であると判断し得る。

【０２２７】

したがって、ネットワークノードは、ネットワークサービスを使用するためにデバイスによって必要とされる選択的にアクティブ化される特徴の第2のセットを識別し得る1808。一態様によれば、ネットワークノードは、許可サーバ(もしくはローカル許可サーバ)によって維持される許可された選択的にアクティブ化される特徴のモデル固有のリスト、許可サーバ(もしくはローカル許可サーバ)によって維持される許可された選択的にアクティブ化される特徴のデバイス固有のリスト、または許可サーバ(もしくはローカル許可サーバ)によって維持される許可された選択的にアクティブ化される特徴のモデル固有およびデバイス固有のリストから特徴を取得または導出することによって、選択的にアクティブ化される特徴の第2のセットを識別し得る。別の態様によれば、ネットワークノードは、許可サーバ(もしくはローカル許可サーバ)によって維持されるライセンス可能な選択的にアクティブ化される特徴のモデル固有のリスト、許可サーバ(もしくはローカル許可サーバ)によって維持されるライセンス可能な選択的にアクティブ化される特徴のデバイス固有のリスト、または許可サーバ(もしくはローカル許可サーバ)によって維持されるライセンス可能な選択的にアクティブ化される特徴のモデル固有およびデバイス固有のリストから特徴を取得または導出することによって、選択的にアクティブ化される特徴の第2のセットを識別し得る。

【０２２８】

ネットワークノードは、デバイスの権限の証拠を確認し、選択的にアクティブ化される特徴の第2のセットが選択的にアクティブ化される特徴の第1のセットに含まれるかどうかを判断した結果に基づいて、要求への応答を送り得る1810。ネットワークノードによって別個に識別される特徴(すなわち、選択的にアクティブ化される特徴の第2のセット)が、デバイスにおいてアクティブ化されることを許可された選択的にアクティブ化される特徴の第1のセットに含まれるか、またはかかる第1のセットのサブセットであり、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠が正常に検証された場合、ネットワークサービスを使用する要求への応答は、デバイスがネットワークサービスを使用することを許されていることを示し得る。

【０２２９】

一方、選択的にアクティブ化される特徴の第2のセットが選択的にアクティブ化される特徴の第1のセットに含まれない場合、またはデバイスの権限の証拠が正常に確認されなかった場合、ネットワークノードは、ネットワークサービスを使用する要求を無視することができ、またはデバイスがネットワークサービスを使用することを許されていないことを示す応答を送ることができる。

【０２３０】

いくつかの態様によれば、ネットワークノードは、ネットワークアクセスノード(たとえば、eNB)、モビリティ管理エンティティ、および/またはゲートウェイデバイスであり得る。

【０２３１】

一態様では、選択的にアクティブ化される特徴の第1のセットは、第1の選択的にアクティブ化される特徴を含み、デバイスの権限の証拠は、許可サーバにおいて発生する。デバイスの権限の証拠は、許可サーバの秘密鍵により署名された、第1の選択的にアクティブ化される特徴のリスティングを含むことができる。一例では、本方法は、許可サーバの公開鍵を使用して、第1の選択的にアクティブ化される特徴のリスティングを確認することによって、デバイスの権限の証拠を確認するステップをさらに含むことができる。

【０２３２】

一態様では、デバイスの権限の証拠は、許可サーバにおいて発生し、ネットワークノー

ドにおいて、デバイスから取得され得る。別の態様では、デバイスの権限の証拠は、許可サーバにおいて発生し、ネットワークノードにおいて、ホーム加入者サーバ(HSS)から、デバイスの能力プロファイルの形式で取得され得る。別の態様では、デバイスの権限の証拠は、認証および鍵一致(AKA)プロセス中にデバイスから取得される。いくつかの態様では、デバイスの権限の証拠は、許可証明を表すデータであり得る。さらに他の態様では、デバイスの権限の証拠は、デバイスが選択的にアクティブ化される特徴の第1のセットをアクティブ化することを許可されていることを示す許可合意を表すデータであり得る。

【０２３３】

一例では、選択的にアクティブ化される特徴の第2のセットを識別するステップは、許可サーバによって維持される許可された選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、ネットワークサービスを使用するためにデバイスによって必要とされる選択的にアクティブ化される特徴をネットワークノードが導出するステップを含むことができる。別の例では、選択的にアクティブ化される特徴の第2のセットを識別するステップは、許可サーバによって維持されるライセンス可能な選択的にアクティブ化される特徴のモデル固有および/またはデバイス固有のリストから、ネットワークサービスを使用するためにデバイスによって必要とされる選択的にアクティブ化される特徴をネットワークノードが導出するステップを含むことができる。

【０２３４】

一態様では、本方法は、デバイスの権限の証拠とともに含まれるデバイスの公開鍵に対応する秘密鍵をデバイスが保有していることを検証するステップをさらに含むことができ、要求への応答を送るステップは、検証の結果にさらに基づき得る。

【０２３５】

いくつかの態様では、本方法は、デバイスの完全性情報を受信するステップをさらに含み得る。そのような態様では、要求への応答は、完全性情報が容認できるかどうかを判断することにさらに基づき得る。いくつかの態様によれば、デバイス能力プロファイルは、セキュアなブートプロセス、認証されたブートプロセス、またはセキュアで認証されたブートプロセス中に作成されたデバイス完全性情報を含み得る。一例では、デバイス完全性情報は、デバイスの許可回路/機能/モジュールの完全性を証明し得る。

【０２３６】

いくつかの態様では、デバイスの権限の証拠は、許可サーバ、ローカル許可サーバ、または許可サーバおよびローカル許可サーバにおいて発生している(たとえば、最初に取得されている、最初に導出されている)ことがある。許可サーバおよびローカル許可サーバは、許可、認証、およびアカウンティング(AAA)サーバとは異なり得る。許可サーバおよびローカル許可サーバは、ホーム加入者サーバ(HSS)とは異なり得る。

【０２３７】

いくつかの態様によれば、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠は、選択的にアクティブ化される特徴の各々に関して、選択的にアクティブ化される特徴をアクティブ化する許可が満了する日を含む。

【０２３８】

一態様では、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠は、ネットワークノードによってデバイスから適切な時間に取得され得る。一例として、デバイスの権限の証拠は、デバイスがネットワークに接続したときにデバイスから取得され得る。別の例として、デバイスの権限の証拠は、特徴アクティブ化プロセス中に許可サーバまたはローカル許可サーバから取得され得る。

【０２３９】

一例では、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠は、ホーム加入者サーバ(HSS)に送られ得る。いくつかの実装形態では、デバイスの選択的にアクティブ化される特徴の許可ステータス(たとえば、選択的にアクティブ化される特徴が許可およびアクティブ化されるかどうかを示すステータス)がHSSに送られ得る。デバイスの権限の証拠、デバイスの選択的にアクティブ化される特

徴の許可ステータス、またはデバイスの権限の証拠およびデバイスの選択的にアクティブ化される特徴の許可ステータスは、デバイスの能力プロファイルを更新するために使用されてよく、能力プロファイルはHSSに記憶され得る。

【０２４０】

一態様では、HSSからデバイスの能力プロファイルを取得することは、ネットワークノード(たとえば、eNB、MME、S-GW、P-GW)が、ネットワークノードが別の形式の証拠を取得する必要なく、デバイスが選択的にアクティブ化される特徴を使用する許可を確認することを可能にし得る(たとえば、ネットワークノードがデバイスから、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を取得する必要性を除去し得る)。

【０２４１】

いくつかの実装形態では、ネットワークノードは、デバイスの能力プロファイルに基づいてデバイスコンテキスト(たとえば、UEコンテキスト)を作成および/または変更することができる。いくつかの態様によれば、HSSは、デバイスにおいてアクティブ化されることを許可された選択的にアクティブ化される特徴を識別する情報要素を送り得る。一態様では、情報要素は、デバイスの能力プロファイルを含むことができる。HSSは、ネットワークノードに情報要素を送り得る。いくつかの態様によれば、ネットワークノードは、HSSに記憶されたデバイスの能力プロファイルの変更に基づいて、選択的にアクティブ化される特徴をアクティブ化および/または非アクティブ化し得る。選択的にアクティブ化される特徴は、ネットワークノードの選択的にアクティブ化される特徴であり得る。HSSに記憶されたデバイスの能力プロファイルの変更に基づく選択的にアクティブ化される特徴のアクティブ化および/または非アクティブ化は、デバイスコンテキスト(たとえば、UEコンテキスト)を作成および/または変更することを容易にし得る。

【０２４２】

図19は、本明細書で説明する態様による、ネットワークノード(たとえば、ネットワークアクセスノード、eNB、MME、S-GW、P-GW)において実行可能な別の例示的な方法1900のフローチャートである。一態様では、ネットワークノードは、図15の例示的なデバイス1500と同様であり得る。ネットワークノードはデバイスから、ネットワークサービスを使用する要求を取得することができる1902。ネットワークノードはまた、許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を取得することができる1904。

【０２４３】

ネットワークノードは、デバイスの権限の証拠を確認し得る1906。いくつかの態様では、デバイスの権限の証拠は、許可証明を確認することによって確認され得る。いくつかの態様では、許可サーバが許可証明を発信した場合、許可証明は、許可サーバの公開鍵を使用して確認され得る。いくつかの態様では、ローカル許可サーバが許可証明を発信した場合、許可証明は、ローカル許可サーバの公開鍵を使用して確認され得る。

【０２４４】

ネットワークノードはまた、(デバイスの権限の証拠を送った)デバイスが、権限の証拠とともに含まれるデバイスの公開鍵に対応する秘密鍵を保有していることを検証し得る1908。このようにして、ネットワークノードは、権限の証拠を送ったデバイスが、権限の証拠において識別されるデバイスであることを検証することができる。いくつかの態様では、デバイスが、権限の証拠とともに含まれるデバイスの公開鍵に対応する秘密鍵を保有していることを検証することは、権限の証拠とともに含まれるデバイスの公開鍵を使用して、(デバイスの秘密鍵によりデバイスによって行われた)デバイスの署名を確認することを伴うことができる。

【０２４５】

ネットワークノードは、デバイスの権限の証拠の確認およびデバイスの検証が成功したかどうかを判断し得る1910。デバイスの権限の証拠の確認、デバイスの検証、またはデバイスの権限の証拠の確認とデバイスの検証の両方が成功しなかったとネットワークノード

が判断した場合、ネットワークノードは、ネットワークサービスを使用する要求を無視することができ、またはネットワークサービスを使用する要求を拒否する応答を送ることができる1912。

【０２４６】

デバイスの権限の証拠の確認とデバイスの検証の両方が成功したとネットワークノードが判断した場合、ネットワークノードは、ネットワークサービスを使用するためにデバイスによって必要とされる特徴を識別し得る1914。一例では、ネットワークノードは、別個に識別を行い得る。

【０２４７】

デバイスにおいてアクティブ化されることを許可された選択的にアクティブ化される特徴の第1のセットのリスティングが、デバイスの権限の証拠から取得され得る。ネットワークノードは、権限の証拠に記載された選択的にアクティブ化される特徴を、ネットワークサービスを使用するためにデバイスによって必要とされる識別される特徴と比較し得る1916。

【０２４８】

デバイスの権限の証拠に含まれる選択的にアクティブ化される特徴が、ネットワークノードによって識別される特徴と合致するかどうかについて判断が行われ得る1918。次いで、判断に基づく応答が送られ得る。特徴が合致するとき、ネットワークノードは、ネットワークサービスを使用する要求を承認する応答を送り得る1920。特徴が合致しないとき、ネットワークノードは、ネットワークサービスを使用する要求を無視すること、またはネットワークサービスを使用する要求を拒否する応答を送ることのいずれかができる1922。

【０２４９】

例示的なホーム加入者サーバ(HSS)

図20は、本明細書で説明する態様による、許可合意の検証および実施をサポートするように構成された例示的なホーム加入者サーバ(HSS)2000を示すブロック図である。一例では、例示的なHSS2000は、ネットワーク通信回路2002、処理回路2004、およびメモリ回路/記憶デバイス(本明細書ではメモリ回路2006と呼ばれる)を含み得る。ネットワーク通信回路2002、処理回路2004、およびメモリ回路2006は、データおよび命令の交換のための通信バス2008に結合され得る。

【０２５０】

ネットワーク通信回路2002は、入力/出力動作のための第1の入力/出力回路/機能/モジュール2010を含み得る。当業者なら諒解するように、ネットワーク通信回路2002とともに他の回路/機能/モジュールが含まれることがある。

【０２５１】

処理回路2004は、許可合意の確認および/または実施をサポートするように構成された、1つまたは複数のプロセッサ、特定用途向けプロセッサ、ハードウェアおよび/またはソフトウェアモジュールなどを含むか、または実装するように構成され得る。処理回路2004は、HSSの機能を実施するためのHSS動作回路/機能/モジュール2012を含むように構成され得る。処理回路2004はまた、許可機能回路/機能モジュール2014を含むように構成され得る。当業者なら諒解するように、処理回路2004とともに他の回路/機能/モジュールが含まれることがある。

【０２５２】

メモリ回路2006は、複数のデバイスに関する、サブスクリプションプロファイル2016および能力プロファイル2017を記憶するための記憶空間を含むように構成され得る。メモリ回路2006はまた、HSS動作命令2018、および本明細書では許可命令2020と呼ばれる許可回路/機能/モジュール命令を含むように構成され得る。当業者なら諒解するように、メモリ回路2006に他の命令およびデータの記憶のためのロケーションが含まれることがある。

【０２５３】

ネットワーク通信回路2002、処理回路2004、メモリ回路2006、および例示的なHSS2000の他の構成要素(図示せず)の間の通信は、通信バス2008などを経由してよい。

【０２５４】
ホーム加入者サーバにおいて実行可能な例示的な方法
図21は、本明細書で説明する態様による、デバイス(たとえば、チップ構成要素、クライアントデバイス、ネットワークノード)の1つまたは複数の選択的にアクティブ化される特徴のセットを使用する許可を確認することに関係する、サーバ(たとえば、HSS)において実行可能な例示的な方法2100を示す。サーバは、たとえば、図20の例示的なHSS2000と同様であり得る。
【０２５５】
例示的な方法2100では、サーバ(たとえば、HSS)は、デバイスの選択的にアクティブ化される特徴の第1のリスト(たとえば、デバイスの取得された能力プロファイル)を取得し得る2102。
【０２５６】
デバイスの許可ステータスの変更に関する情報は、デバイスの能力の変更に関する情報と見なされ得る。デバイスの許可ステータスの変更に関する情報は、デバイスの選択的にアクティブ化される特徴のセットにおける少なくとも1つの選択的にアクティブ化される特徴の許可ステータスの変更に関係し得る。
【０２５７】
サーバ(たとえば、HSS)は、第1のリストに基づいて、サーバ(たとえば、HSS)に記憶された、デバイスの選択的にアクティブ化される特徴の第2のリストを更新することができる2104。第2のリストは、デバイスの記憶された能力プロファイルと呼ばれ得る。一態様によれば、サーバ(たとえば、HSS)に記憶された第2のリストは、デバイスのサブスクリプションプロファイルに関連付けられ得る。HSSに記憶された、デバイスの選択的にアクティブ化される特徴の第2のリストの更新は、第2のリストにおける少なくとも1つの選択的にアクティブ化される特徴の許可ステータスの変更を反映し得る。
【０２５８】
一態様では、選択的にアクティブ化される特徴の第1のリストは、許可サーバにおいて発生し得、許可サーバの秘密鍵により署名され得る。そのような態様によれば、本方法はまた、許可サーバの公開鍵を使用して、選択的にアクティブ化される特徴の第1のリストを確認するステップを含み得る。
【０２５９】
サーバ(たとえば、HSS)は、デバイスの能力に関するクエリを取得し得る。サーバ(たとえば、HSS)は、本明細書で説明する態様によれば、デバイスの能力に関するクエリに応答して、デバイスの選択的にアクティブ化される特徴の第2のリストを含む能力プロファイルを送り得る2106。
【０２６０】
一例によれば、HSSは、初期接続手順中にデバイスの能力に関するクエリを取得し得る。クエリは、MMEから取得され得る。HSSは、クエリに応答して、第2のリストを含む能力プロファイルをMMEに送り得る。能力プロファイルは、デバイスのサブスクリプションプロファイルに関連付けられ得る。
【０２６１】
代替的に、HSSは、HSSに記憶された情報の特定の要素を求める要求を取得し得る。情報の要素は、デバイスの能力に関係し得る。情報の要素は、デバイスの選択的にアクティブ化される特徴の第2のリストにおいて(たとえば、デバイスの記憶された能力プロファイルにおいて)識別される1つまたは複数の選択的にアクティブ化される特徴に関係し得る。
【０２６２】
初期接続手順の例を使用して、HSSは、第2のデバイス(たとえば、MME)が第1のデバイス上ですでに許可/アクティブ化されている選択的にアクティブ化される特徴を実装または補完するように様々な特徴を構成することができるように、第1のデバイス(たとえば、チップ構成要素、クライアントデバイス)の能力プロファイルを第2のデバイス(たとえば、MME)に送り得る。

【０２６３】
第2のデバイス(たとえば、MME)は、第1の許可サーバによって署名された、第1のデバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用する第1のデバイスの権限の証拠(たとえば、許可証明の形式をとる許可情報)を第2のデバイス(たとえば、MME)が第1のデバイスから取得する必要なしに、1つまたは複数の選択的にアクティブ化される特徴を使用する第1のデバイスの権利を確認し得る。第1のデバイスの権限の証拠は、選択的にアクティブ化される特徴のセットを使用する第1のデバイスの権利を確認するために第2のデバイス(たとえば、MME)によって必要とされ得る。代替態様では、証拠は、第2のデバイス(たとえば、MME)によってHSSから取得され、第1のデバイスからの入力なしにネットワークに対して構成され得る。したがって、たとえば、HSSから、たとえば、強化型アクセスネットワーククエリプロトコルまたはサービスクエリプロトコルを使用して取得され得る、能力プロファイル、および/またはデバイスの能力に関係し得る情報の要素を使用することで、MMEによる許可合意の確認および実施を円滑にする/その速度を上げる/その効率性を改善することができる。
【０２６４】
図示および説明した特定の実装形態は例にすぎず、本明細書で別段に規定されない限り、本開示を実装するための唯一の方法として解釈されるべきでない。本開示の様々な例が多数の他の解決策によって実施され得ることが、当業者には容易に明らかである。
【０２６５】
本明細書で説明し、図面に示した、構成要素、動作、特徴、および/または機能のうちの1つまたは複数は、単一の構成要素、動作、特徴、または機能に再構成および/または結合されてよく、いくつかの構成要素、動作、特徴、または機能に含まれてもよい。本開示から逸脱することなく、さらなる要素、構成要素、動作、および/または機能も追加されてよい。本明細書で説明するアルゴリズムはまた、ソフトウェアにおいて効率的に実装されてもよく、かつ/またはハードウェアに組み込まれてもよい。
【０２６６】
説明では、不要な詳細で本開示を不明瞭にしないように、要素、回路、機能、およびモジュールが、ブロック図の形式で示され得る。逆に、図示および説明した特定の実装形態は例にすぎず、本明細書で別段に規定されない限り、本開示を実装するための唯一の方法として解釈されるべきではない。さらに、ブロック定義、および様々なブロック間の論理の分割は、特定の実装形態の例である。ほとんどの部分について、タイミング問題などに関する詳細は、そのような詳細が本開示の完全な理解を得るために必要ではなく、関連分野における当業者の能力の範囲内である場合、省略されている。
【０２６７】
また、例は、フローチャート、フロー図、構造図、またはブロック図として描かれるプロセスとして説明され得る点に留意されたい。フローチャートでは動作を順次プロセスとして説明する場合があるが、動作の多くは、並列または同時に実行され得る。加えて、動作の順序は並べ替えられてよい。プロセスは、その動作が完了したとき、終了する。プロセスは、メソッド、関数、プロシージャ、サブルーチン、サブプログラムなどに対応し得る。プロセスが関数に対応するとき、その終了は呼出し関数またはメイン関数への関数のリターンに対応する。
【０２６８】
情報および信号が、様々な異なる技術および技法のいずれかを使用して表され得ることを、当業者は諒解されよう。たとえば、この説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表され得る。いくつかの図面は、提示および説明を明快にするために、信号を単一の信号として示すことがある。信号が信号のバスを表してよく、バスが様々なビット幅を有してよく、本開示が、単一のデータ信号を含む任意の数のデータ信号上に実装されてよいことが当業者によって理解されよう。

【０２６９】
本明細書で「第1の」、「第2の」などの呼称を使用した要素へのいかなる言及も、それらの要素の数量または順序の限定が明示的に述べられていない限り、そのような限定をしないことを理解されたい。むしろ、呼称は、本明細書では、2つ以上の要素または要素の例同士を区別する好都合な方法として使用される場合がある。したがって、第1の要素および第2の要素への言及は、2つの要素だけがそこで採用され得ること、または何らかの形で第1の要素が第2の要素に先行するべきであることを意味しない。追加として、別段に述べられていない限り、要素のセットは1つまたは複数の要素を備え得る。さらに、単数形で使用される単語が複数形を含み、複数形で使用される単語が単数形を含むことを理解されたい。

【０２７０】
さらに、記憶媒体は、読取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、磁気ディスク記憶媒体、光学記憶媒体、フラッシュメモリデバイスならびに/または他の機械可読媒体、プロセッサ可読媒体、処理回路可読媒体、および/もしくは情報を記憶するためのコンピュータ可読媒体を含む、データを記憶するための1つまたは複数のデバイスを表す場合がある。「機械可読媒体」、「プロセッサ可読媒体」、「処理回路可読媒体」、および/または「コンピュータ可読媒体」という用語は、限定はしないが、ポータブルまたは固定記憶デバイス、光記憶デバイス、ならびに命令および/またはデータを記憶し、含み、または搬送することが可能な様々な他の媒体などの非一時的媒体を含み得る。したがって、本明細書で説明する様々な方法は、機械可読媒体、プロセッサ可読媒体、処理回路可読媒体、および/またはコンピュータ可読媒体に記憶され、1つまたは複数のプロセッサ、処理回路、機械、および/またはデバイスによって実行され得る命令および/またはデータによって完全にまたは部分的に実装され得る。

【０２７１】
さらに、態様は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、またはそれらの任意の組合せによって実装されてよい。ソフトウェア、ファームウェア、ミドルウェア、またはマイクロコードにおいて実装されるとき、タスクを実行するためのプログラムコードまたはコードセグメントは、記憶媒体または他のストレージなどの機械可読媒体に記憶され得る。処理回路は、タスクを実行し得る。コードセグメントは、プロセス、プロシージャ、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、または命令、データ構造、もしくはプログラムステートメントの任意の組合せを表してよい。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容を渡すこと、転送すること、または送信することによって、別のコードセグメントまたはハードウェア回路に結合されてよい。情報、データ、引数、パラメータ、またはメモリ内容などは、メモリ共有、メッセージパッシング、トークンパッシング、ネットワーク送信などを含む任意の適切な手段を介して渡され、転送され、または送信されてよい。

【０２７２】
本明細書で開示する例に関して説明する様々な例示的な論理ブロック、要素、回路、モジュール、機能、および/または構成要素は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理構成要素、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明する機能を実行するように設計されたそれらの任意の組合せで実装または実行され得る。汎用プロセッサは、マイクロプロセッサであってもよいが、代替として、汎用プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってもよい。プロセッサはまた、コンピューティング構成要素の組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、いくつかのマイクロプロセッサ、DSPコアと連係した1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装されてもよい。本明細書で説明する態様を実行するために構成された汎用プロセッサは、そのような態様を実行するための専用プロ

セッサと見なされる。同様に、汎用コンピュータは、本明細書で説明する態様を実行するために構成されるとき、専用コンピュータと見なされる。

【０２７３】

本明細書で開示する例に関して説明する方法またはアルゴリズムは、処理ユニット、プログラミング命令、または他の指示の形態で、直接ハードウェアに、プロセッサによって実行可能なソフトウェアモジュールに、または両方の組合せに含まれてよく、単一のデバイスに含まれるかまたは複数のデバイスにわたって分散されることがある。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当業者が認識している任意の他の形態の記憶媒体に存在してよい。記憶媒体は、プロセッサが記憶媒体から情報を読み取ることができ、記憶媒体に情報を書き込むことができるように、プロセッサに結合されてよい。代替形態において、記憶媒体はプロセッサと一体である場合がある。

【０２７４】

本明細書で説明する例に関して説明する様々な例示的な論理ブロック、回路、機能、モジュール、およびアルゴリズムは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装されてもよいことを当業者はさらに諒解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的な要素、構成要素、ブロック、回路、機能、モジュール、およびアルゴリズムについて、概してそれらの機能に関して上記で説明してきた。そのような機能がハードウェアとして実装されるか、ソフトウェアとして実装されるか、それともそれらの組合せとして実装されるかは、具体的な適用例およびシステム全体に課された設計選択に依存する。

【０２７５】

本明細書で説明する本開示の様々な特徴は、本開示から逸脱することなく様々なシステムにおいて実装され得る。上記の態様は例にすぎず、本開示を限定するものとして解釈されるべきではないことに留意されたい。本開示の教示の例の説明は例示的であることが意図され、特許請求の範囲を限定することは意図されない。したがって、本教示は、他のタイプの装置に容易に適用されてよく、多くの代替形態、変更形態、および変形形態が当業者には明らかであろう。

【符号の説明】

【０２７６】

100　システム
102　デバイスA、デバイス
104　デバイスB、デバイス
106　デバイスC、デバイス
108　許可回路/機能/モジュール、許可回路/機能/モジュールA、許可機能
110　選択的にアクティブ化される特徴の第1のセット、選択的にアクティブ化される特徴のセット
112　許可回路/機能/モジュール、許可回路/機能/モジュールB、許可機能
114　選択的にアクティブ化される特徴の第2のセット、選択的にアクティブ化される特徴のセット
116　許可回路/機能/モジュール、許可回路/機能/モジュールC、許可機能
118　選択的にアクティブ化される特徴の第3のセット、選択的にアクティブ化される特徴のセット
120　許可合意
122　許可証明
124　許可ファイル
126　許可サーバ
128　ローカル許可サーバ
200　動作環境
202　第1のデバイス

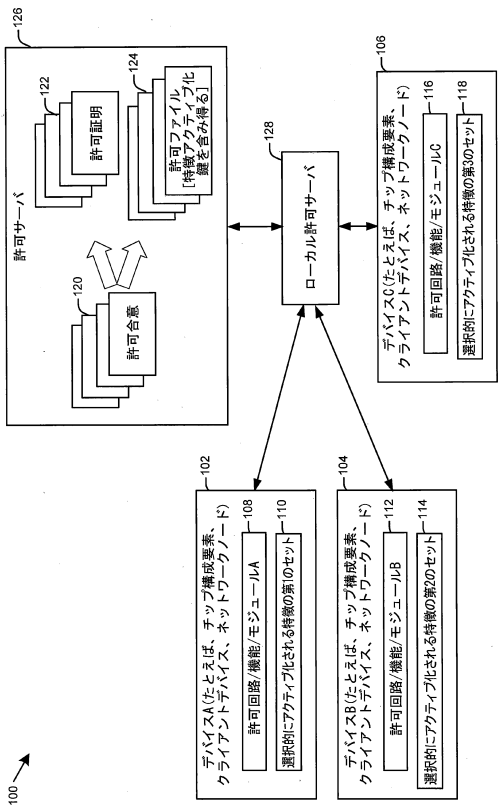
203 第1の許可機能
204 第2のデバイス
205 第2の許可機能
206 第3のデバイス
207 第3の許可機能
210 無線アクセスネットワーク(RAN)
212 コアネットワーク
214 モビリティ管理エンティティ(MME)
216 ホーム加入者サーバ/許可、認証、およびアカウンティングサーバ(HSS/AAA)
218 サービングゲートウェイデバイス(S-GW)
220 パケットデータネットワークゲートウェイデバイス(P-GW)
222 ローカル許可サーバ
228 アプリケーションサーバ
230 アプリケーションサーバ
232 パケットデータネットワーク(PDN)
234 許可サーバ
300 システム
302 デバイス
304 許可機能
305 セキュア動作環境
306 ローカル許可サーバ
308 許可サーバ
310 セキュア記憶回路
312 データ記憶デバイス
314 処理回路
316 秘密鍵
318 特徴アクティブ化鍵
320 選択的にアクティブ化される特徴
322 特徴および許可パラメータのリスト
323 許可証明
324 許可ファイル
325 通信バス
326 ネットワーク通信回路
328 データ記憶デバイス
330 許可合意
332 デバイスのための鍵記憶、鍵記憶
334 特徴アクティブ化鍵
336 許可パラメータ
338 通信バス
340 処理回路
342 ネットワーク通信回路
400 リスト
402 合意の日
404 デバイスの所有者の識別子
406 デバイスの製造業者またはOEMの識別子
408 デバイスの識別子
410 許可された特徴のリスト
412 許可合意の存続期間
414 特徴の使用に対する制限
416 特徴の使用に対する料金

500 リスト
502 合意の開始日
504 合意の終了日
506 デバイスの識別子
508 許可された特徴のリスト
510 特徴の使用に対する制限
512 デバイスの公開鍵の識別子
514 デバイスの製造業者またはOEMの識別子
516 特徴の使用に対する料金
600 リスティング
602 許可合意の開始日
604 許可合意の終了日
606 デバイスの識別子
608 許可されたサービスのリスト
610 許可された特徴のリスト
612 デバイスの製造業者またはOEMの識別子
614 特徴の使用に対する料金
800 フロー図
900 フロー図
1000 許可サーバ
1002 ネットワーク通信回路
1004 処理回路
1006 メモリ回路
1008 通信バス
1010 入力/出力モジュール/回路/機能
1012 許可合意管理回路/機能/モジュール
1014 特徴アクティブ化鍵導出回路/機能/モジュール
1016 許可パラメータ導出回路/機能/モジュール
1018 許可証明導出回路/機能/モジュール
1020 許可合意管理命令
1022 特徴アクティブ化鍵導出命令
1024 許可パラメータ導出命令
1026 許可証明導出命令
1030 特徴アクティブ化鍵記憶
1032 許可パラメータ記憶
1034 公開鍵記憶
1036 許可証明記憶
1100 ローカル許可サーバ
1102 ネットワーク通信回路
1104 処理回路
1106 メモリ回路
1108 通信バス
1110 入力/出力モジュール/回路/機能
1112 許可合意管理回路/機能/モジュール
1114 特徴アクティブ化鍵導出回路/機能/モジュール
1116 許可パラメータ導出回路/機能/モジュール
1118 許可証明導出回路/機能/モジュール
1120 許可合意管理命令
1122 特徴アクティブ化鍵導出命令
1124 許可パラメータ導出命令

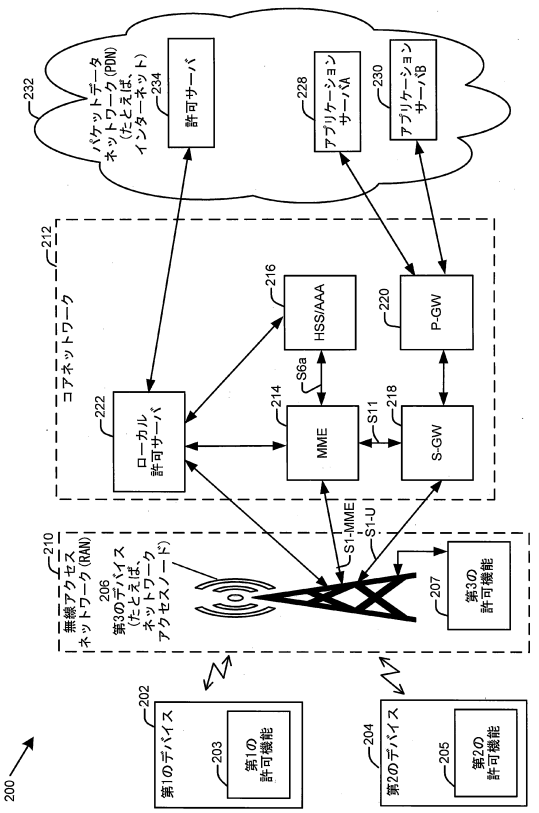
1126 許可証明導出命令
1130 特徴アクティブ化鍵記憶
1132 許可パラメータ記憶
1134 許可証明記憶
1136 公開鍵記憶
1138 特徴使用報告回路/機能/モジュール
1140 特徴使用報告命令
1200 呼フロー図
1202 デバイス
1204 ローカル許可サーバ
1206 許可サーバ
1214 リモート認証
1218 リモート認証
1219 リモート認証
1226 周期的報告
1228 周期的報告
1300 呼フロー図
1302 デバイス
1304 無線アクセスネットワーク(RAN)
1306 ネットワークノード
1308 HSS
1310 ローカル許可サーバ
1312 許可サーバ
1326 初期接続手順
1330 相互認証
1400 呼フロー図
1402 デバイス
1404 無線アクセスネットワーク(RAN)
1406 ネットワークノード
1412 接続要求
1414 要求
1418 相互認証
1420 確認
1422 検証
1424 応答
1432 確認
1434 検証
1500 デバイス
1502 ネットワーク通信回路
1504 処理回路
1506 メモリ回路
1508 通信バス
1510 第1の入力/出力回路/機能/モジュール
1511 第2の入力/出力回路/機能/モジュール
1512 許可機能回路/機能モジュール
1514 許可証明検証回路/機能モジュール
1516 許可パラメータ評価回路/機能モジュール
1518 特徴アクティブ化鍵抽出回路/機能モジュール
1520 許可命令
1522 許可証明検証命令

1524 許可パラメータ評価命令
1526 特徴アクティブ化鍵抽出命令
1528 セキュア記憶回路
1530 秘密鍵記憶
1532 特徴アクティブ化鍵記憶
1534 選択的にアクティブ化される特徴のリスティング
1536 デバイスの選択的にアクティブ化される特徴の各々に関する許可パラメータのリスティング
1600 方法
1700 方法
1800 方法
1900 方法
2000 ホーム加入者サーバ(HSS)
2002 ネットワーク通信回路
2004 処理回路
2006 メモリ回路
2008 通信バス
2010 第1の入力/出力回路/機能/モジュール
2012 HSS動作回路/機能/モジュール
2014 許可機能回路/機能モジュール
2016 サブスクリプションプロファイル
2017 能力プロファイル
2018 HSS動作命令
2020 許可命令
2100 方法

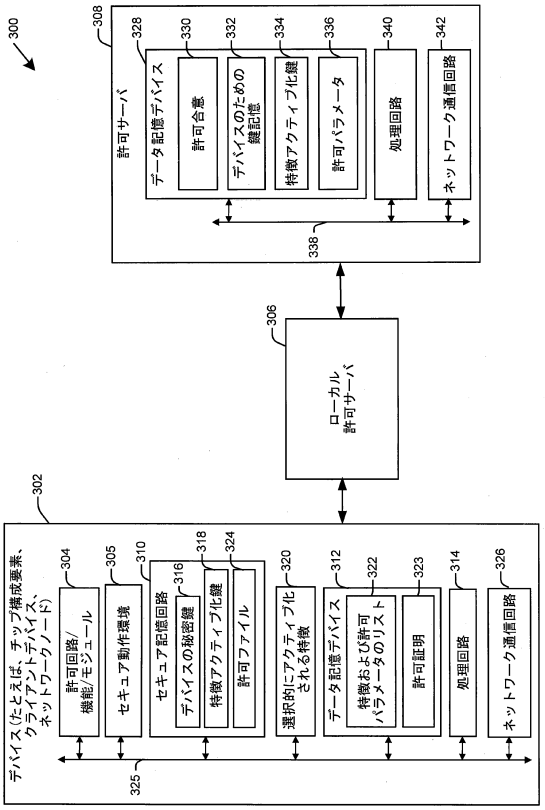
【図１】



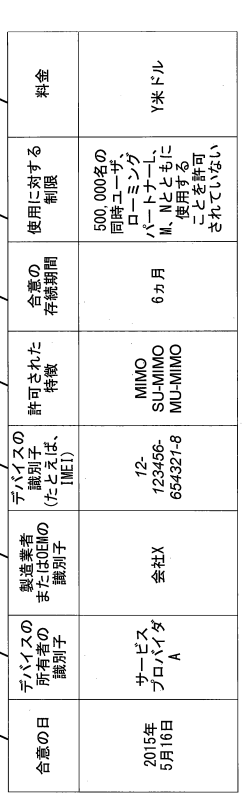
【図２】



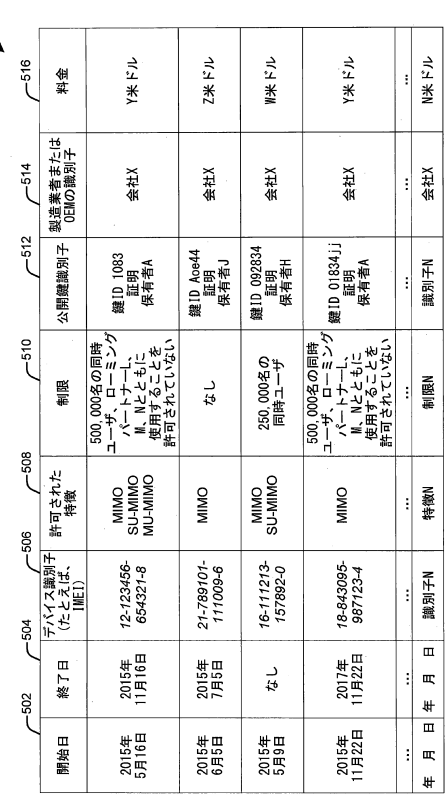
【図３】


300
308
許可サーバ
328
データ記憶デバイス
330
許可合意
332
デバイスのための鍵記憶
334
特徴アクティブ化鍵
336
許可パラメータ
340
処理回路
342
ネットワーク通信回路
338
306
ローカル許可サーバ
302
デバイス（たとえば、チップ構成要素、クライアントデバイス、ネットワークノード）
304
許可回路／機能／モジュール
305
セキュア動作環境
310
セキュア記憶回路
316
デバイスの秘密鍵
318
特徴アクティブ化鍵
324
許可ファイル
320
選択的にアクティブ化される特徴
312
データ記憶デバイス
322
特徴および許可パラメータのリスト
323
許可証明
314
処理回路
326
ネットワーク通信回路
325

【図４】


400
402 合意の日
404 デバイスの所有者の識別子
406 製造業者またはOEMの識別子
408 デバイスの識別子（たとえば、IMEI）
410 許可された特徴
412 合意の存続期間
414 使用に対する制限
416 料金
2015年5月16日
サービスプロバイダA
会社X
12-123456-654321-8
MIMO SU-MIMO MU-MIMO
6カ月
500,000名の同時ユーザ、パートナーL、M、Nとともに使用することを許可されていない
Y米ドル

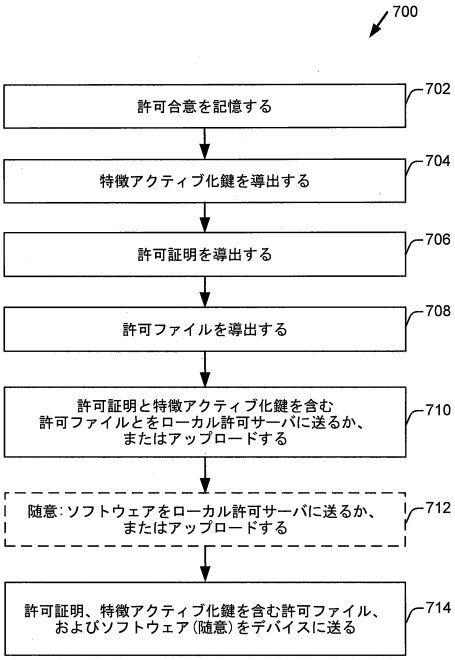
【図５】


500
502 開始日
504 終了日
506 デバイス識別子（たとえば、IMEI）
508 許可された特徴
510 制限
512 公開鍵識別子
514 製造業者またはOEMの識別子
516 料金
2015年5月16日
2015年11月16日
12-123456-654321-8
MIMO SU-MIMO MU-MIMO
500,000名の同時ユーザ、ローミングパートナーL、M、Nとともに使用することを許可されていない
鍵ID 1083 証明保有者A
会社X
Y米ドル
2015年6月5日
2015年7月5日
21-789101-111009-6
MIMO
なし
鍵ID Aoe44 証明保有者J
会社X
Z米ドル
2015年5月9日
なし
16-111213-157892-0
MIMO SU-MIMO
250,000名の同時ユーザ
鍵ID 092834 証明保有者H
会社X
W米ドル
2015年11月22日
2017年11月22日
18-843095-987123-4
MIMO
500,000名の同時ユーザ、ローミングパートナーL、M、Nとともに使用することを許可されていない
鍵ID 01834jj 証明保有者A
会社X
Y米ドル
年 月 日
識別子N
特徴N
制限N
識別子N
会社X
N米ドル

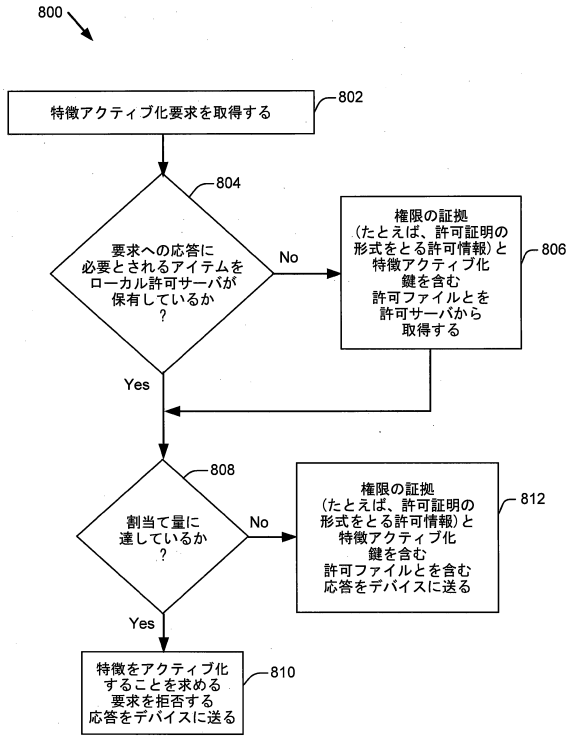
【図６】

600
602 開始日
604 終了日
606 デバイス識別子（たとえば、IMEI）
608 許可されたサービス
610 許可された特徴
612 製造業者またはOEMの識別子
614 料金
2015年5月16日
2015年11月16日
12-123456-654321-8
IPマルチメディアサブシステム（IMS）
MIMO SU-MIMO MU-MIMO
会社エンティティX
A米ドル
2015年6月5日
2015年7月5日
21-789101-111009-6
プッシュツートーク
MIMO
会社エンティティX
B米ドル
2015年5月9日
なし
16-1111213-157892-0
マルチメディアメッセージングサービス（MMS）
MIMO SU-MIMO
会社エンティティX
C米ドル
2015年11月22日
2017年11月22日
18-843095-987123-4
IMS
MIMO
会社エンティティX
D米ドル
2015年1月8日
2016年1月8日
21-481384-781543-1
MMS IMS
MIMO SU-MIMO MU-MIMO
会社エンティティZ
E米ドル
2015年3月25日
2015年6月25日
54-846291-264815-3
プッシュツートーク
MIMO
会社エンティティZ
F米ドル
2015年10月1日
2015年4月1日
11-864215-894572-0
発信者番号通知サービス
MIMO SU-MIMO
会社エンティティR
G米ドル
2015年6月1日
なし
83-249593-8273514
三者間会議通話
MIMO
会社エンティティL
H米ドル
開始日
終了日
識別子N
許可されたサービスN
許可された特徴N
会社エンティティX
I米ドル

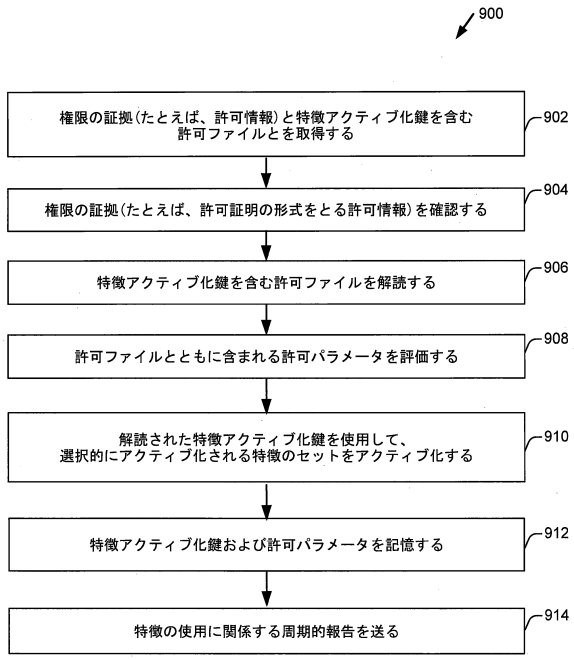
【図７】


700
許可合意を記憶する
702
特徴アクティブ化鍵を導出する
704
許可証明を導出する
706
許可ファイルを導出する
708
許可証明と特徴アクティブ化鍵を含む
許可ファイルとをローカル許可サーバに送るか、
またはアップロードする
710
随意：ソフトウェアをローカル許可サーバに送るか、
またはアップロードする
712
許可証明、特徴アクティブ化鍵を含む許可ファイル、
およびソフトウェア（随意）をデバイスに送る
714

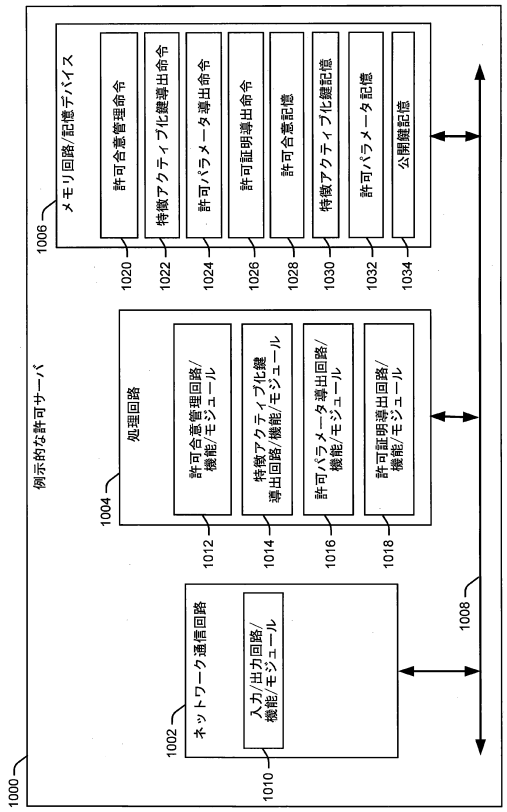
【図８】


800
特徴アクティブ化要求を取得する
802
804
要求への応答に
必要とされるアイテムを
ローカル許可サーバが
保有しているか
？
No
権限の証拠
（たとえば、許可証明の
形式をとる許可情報）と
特徴アクティブ化
鍵を含む
許可ファイルとを
許可サーバから
取得する
806
Yes
808
割当て量に
達しているか
？
No
権限の証拠
（たとえば、許可証明の
形式をとる許可情報）と
特徴アクティブ化
鍵を含む
許可ファイルとを含む
応答をデバイスに送る
812
Yes
特徴をアクティブ化
することを求める
要求を拒否する
応答をデバイスに送る
810

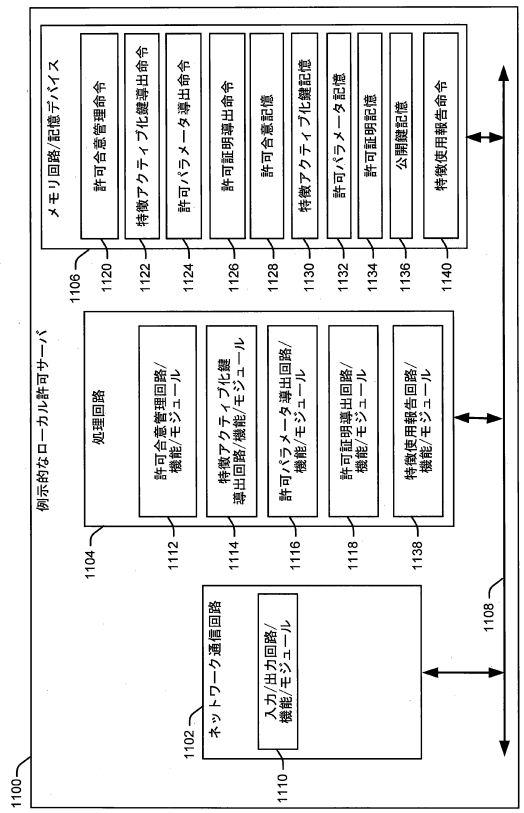
【図９】


900
権限の証拠（たとえば、許可情報）と特徴アクティブ化鍵を含む
許可ファイルとを取得する
902
権限の証拠（たとえば、許可証明の形式をとる許可情報）を確認する
904
特徴アクティブ化鍵を含む許可ファイルを解読する
906
許可ファイルとともに含まれる許可パラメータを評価する
908
解読された特徴アクティブ化鍵を使用して、
選択的にアクティブ化される特徴のセットをアクティブ化する
910
特徴アクティブ化鍵および許可パラメータを記憶する
912
特徴の使用に関係する周期的報告を送る
914

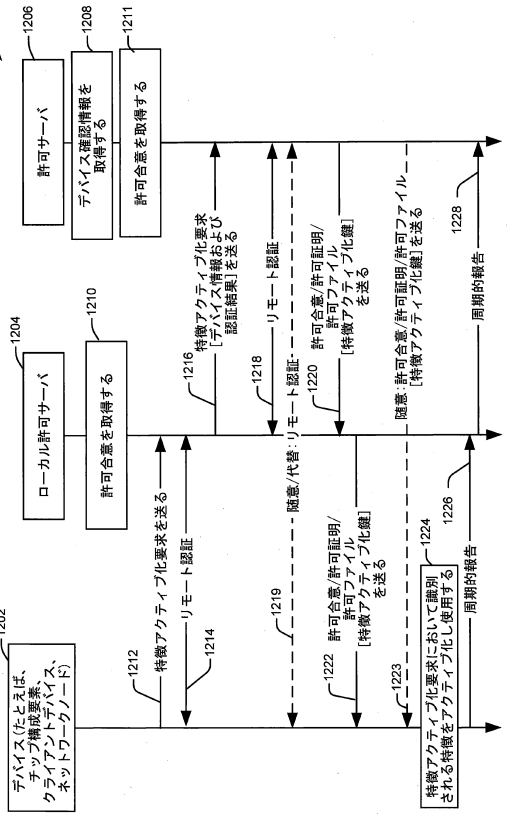
【図１０】


例示的な許可サーバ
1000
メモリ回路/記憶デバイス
1006
許可合意管理命令
1020
特徴アクティブ化鍵導出命令
1022
許可パラメータ導出命令
1024
許可証明導出命令
1026
許可合意記憶
1028
特徴アクティブ化鍵記憶
1030
許可パラメータ記憶
1032
公開鍵記憶
1034
処理回路
1004
許可合意管理回路/
機能/モジュール
1012
特徴アクティブ化鍵
導出回路/機能/モジュール
1014
許可パラメータ導出回路/
機能/モジュール
1016
許可証明導出回路/
機能/モジュール
1018
ネットワーク通信回路
1002
入力/出力回路/
機能/モジュール
1010
1008

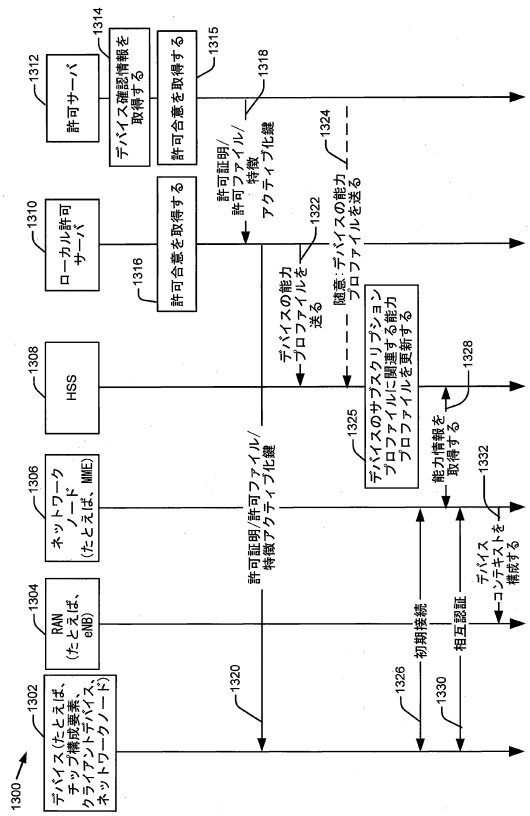
【図１１】



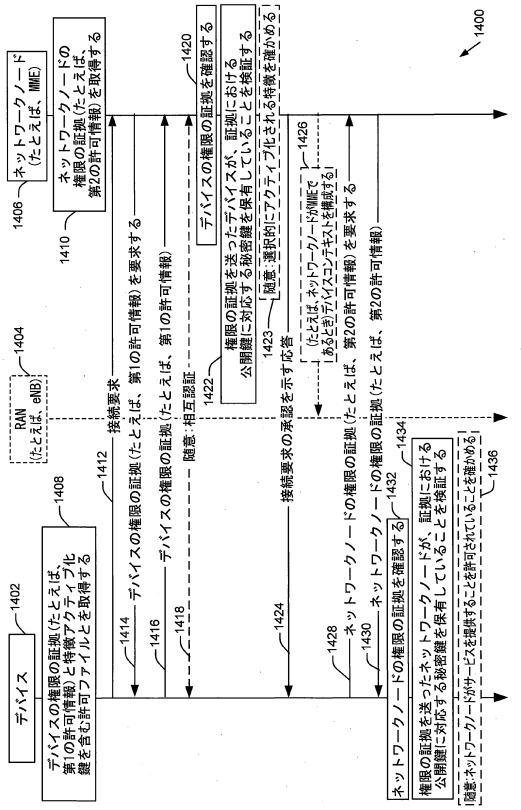
【図１２】



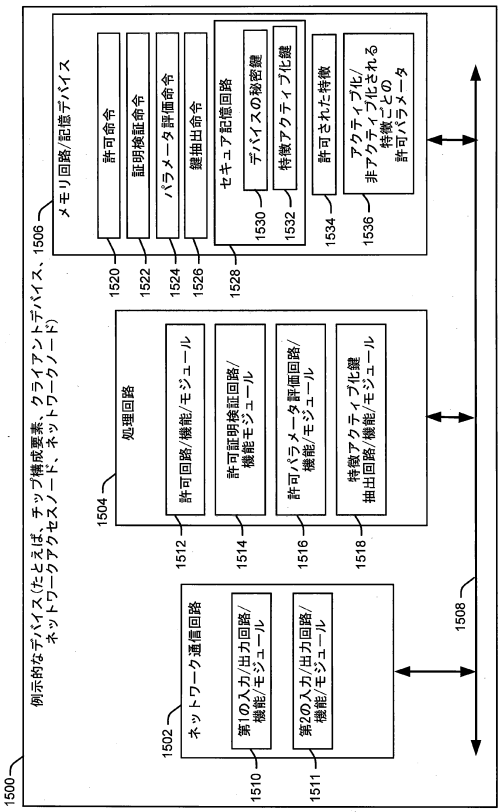
【図１３】



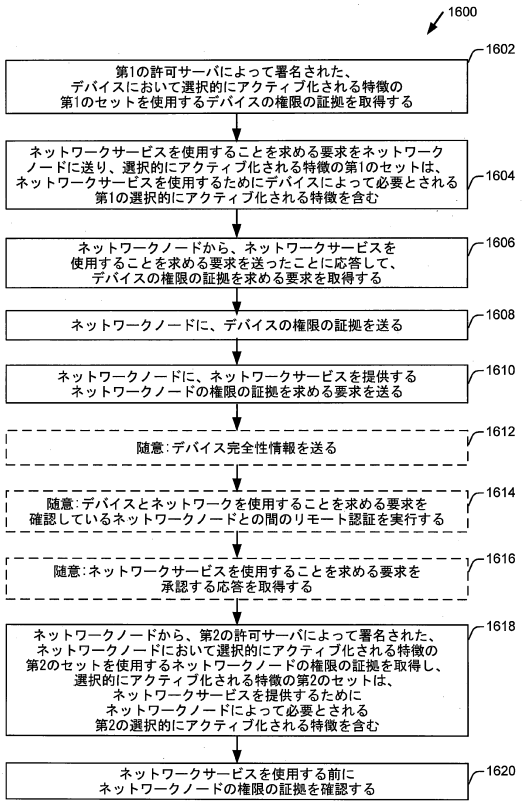
【図１４】



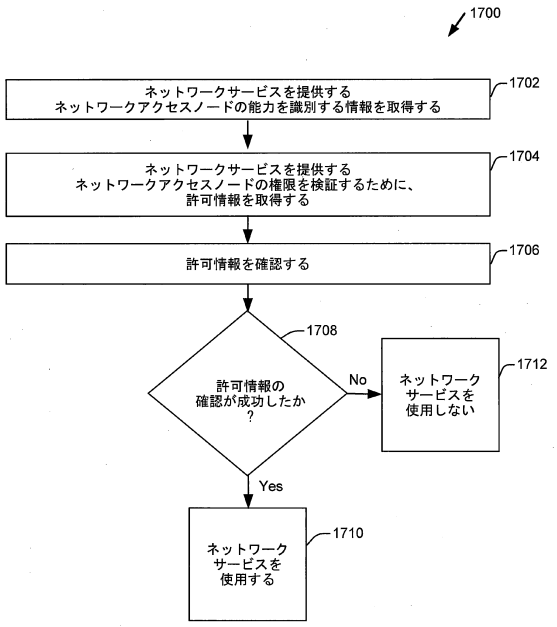
【図１５】



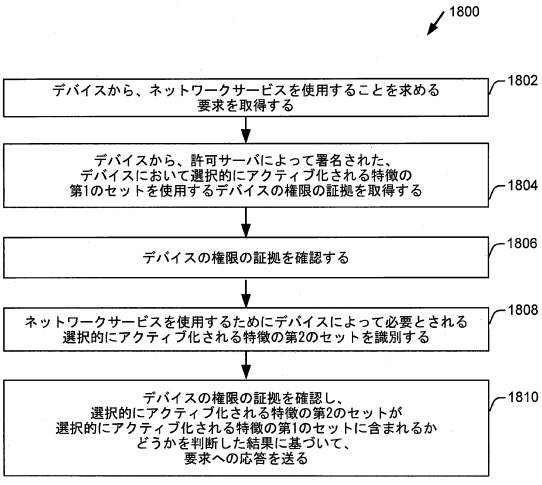
【図１６】



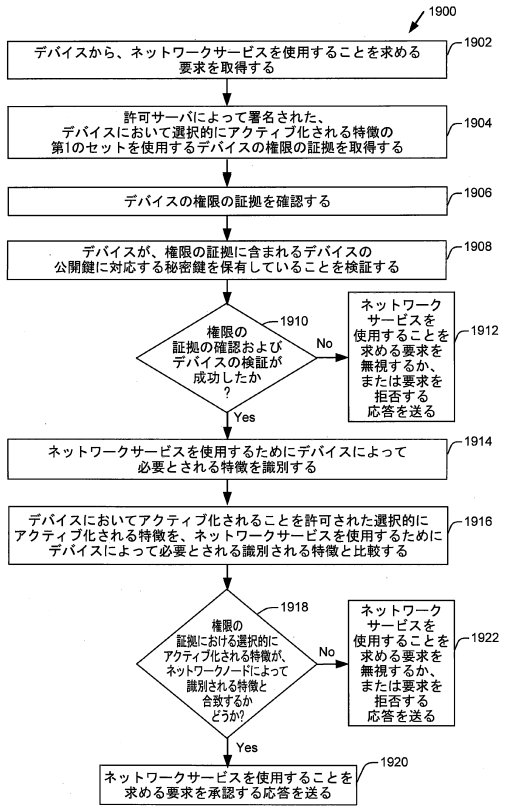
【図１７】



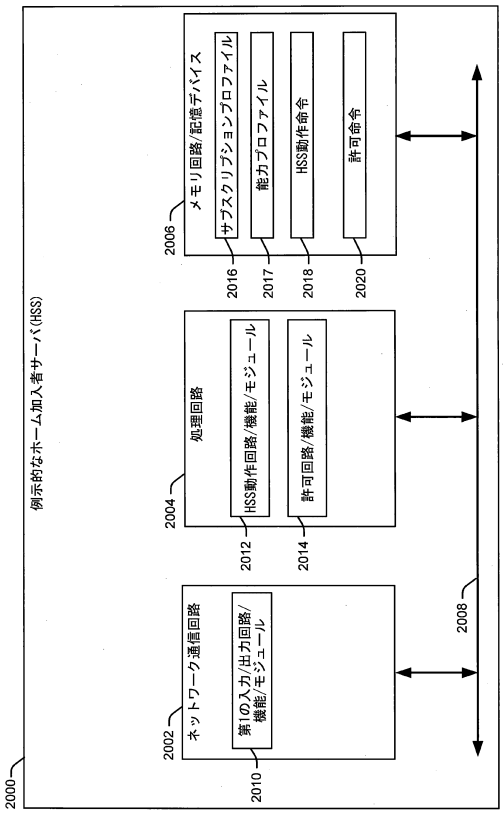
【図１８】



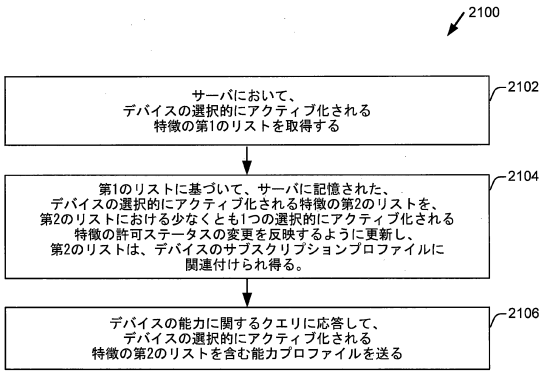
【図１９】


1900
デバイスから、ネットワークサービスを使用することを求める要求を取得する
1902
許可サーバによって署名された、デバイスにおいて選択的にアクティブ化される特徴の第1のセットを使用するデバイスの権限の証拠を取得する
1904
デバイスの権限の証拠を確認する
1906
デバイスが、権限の証拠に含まれるデバイスの公開鍵に対応する秘密鍵を保有していることを検証する
1908
権限の証拠の確認およびデバイスの検証が成功したか？
1910
No
ネットワークサービスを使用することを求める要求を無視するか、または要求を拒否する応答を送る
1912
Yes
ネットワークサービスを使用するためにデバイスによって必要とされる特徴を識別する
1914
デバイスにおいてアクティブ化されることを許可された選択的にアクティブ化される特徴を、ネットワークサービスを使用するためにデバイスによって必要とされる識別される特徴と比較する
1916
権限の証拠における選択的にアクティブ化される特徴が、ネットワークノードによって識別される特徴と合致するかどうか?
1918
No
ネットワークサービスを使用することを求める要求を無視するか、または要求を拒否する応答を送る
1922
Yes
ネットワークサービスを使用することを求める要求を承認する応答を送る
1920

【図２０】


例示的なホーム加入者サーバ(HSS)
2000
メモリ回路/記憶デバイス
2006
サブスクリプションプロファイル
2016
能力プロファイル
2017
HSS動作命令
2018
許可命令
2020
処理回路
2004
HSS動作回路/機能/モジュール
2012
許可回路/機能/モジュール
2014
ネットワーク通信回路
2002
第1の入力/出力回路/機能/モジュール
2010
2008

【図２１】


2100
サーバにおいて、デバイスの選択的にアクティブ化される特徴の第1のリストを取得する
2102
第1のリストに基づいて、サーバに記憶された、デバイスの選択的にアクティブ化される特徴の第2のリストを、第2のリストにおける少なくとも1つの選択的にアクティブ化される特徴の許可ステータスの変更を反映するように更新し、第2のリストは、デバイスのサブスクリプションプロファイルに関連付けられ得る。
2104
デバイスの能力に関するクエリに応答して、デバイスの選択的にアクティブ化される特徴の第2のリストを含む能力プロファイルを送る
2106

フロントページの続き

(72)発明者　ギャヴィン・バーナード・ホーン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ジョン・スミー
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ラジェシュ・パンカジュ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　トーマス・ラウズ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　児玉　崇晶

(56)参考文献　特表２０１２－５０２５８６（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１１３２５２（ＵＳ，Ａ１）
国際公開第２００４／０１９１８２（ＷＯ，Ａ２）
米国特許出願公開第２００５／００３９０６１（ＵＳ，Ａ１）
米国特許出願公開第２０１５／０１６９８４８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／１０
Ｇ０６Ｆ　２１／６４
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｗ　１２／０６