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

特許第6555258号
(P6555258)

(45)発行日　令和1年8月7日(2019.8.7)　(24)登録日　令和1年7月19日(2019.7.19)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
H04W 92/18	(2009.01)	H04W	92/18	
H04W 12/04	(2009.01)	H04W	12/04	
H04M 3/42	(2006.01)	H04M	3/42	A

請求項の数 14　(全 27 頁)

(21)出願番号　特願2016-526370 (P2016-526370)
(86)(22)出願日　平成26年8月27日 (2014.8.27)
(65)公表番号　特表2016-538771 (P2016-538771A)
(43)公表日　平成28年12月8日 (2016.12.8)
(86)国際出願番号　PCT/JP2014/004393
(87)国際公開番号　WO2015/063991
(87)国際公開日　平成27年5月7日 (2015.5.7)
審査請求日　平成29年7月4日 (2017.7.4)
(31)優先権主張番号　特願2013-225200 (P2013-225200)
(32)優先日　平成25年10月30日 (2013.10.30)
(33)優先権主張国・地域又は機関
日本国(JP)
(31)優先権主張番号　特願2013-226681 (P2013-226681)
(32)優先日　平成25年10月31日 (2013.10.31)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103894
弁理士　家入　健
(72)発明者　ジャン　シャオウェイ
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　プラサド　アナンド　ラガワ
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】移動通信システム、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ、UE及び方法

(57)【特許請求の範囲】
【請求項１】
Ｐｒｏｘｉｍｉｔｙ　Ｓｅｒｖｉｃｅｓ（ＰｒｏＳｅ）をサポートする第１のＵＥ（Ｕｓｅｒ　Ｅｑｕｉｐｍｅｎｔ）と、
前記ＰｒｏＳｅをサポートする第２のＵＥと、
ＰＣ３インタフェースを介して前記第１のＵＥと通信する第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎと、
前記ＰＣ３インタフェースを介して前記第２のＵＥと通信する第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎと、を備え、
前記第１のＵＥは、セキュリティ構成要素を得るため、前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに第１の信号を送り、
前記第１のＵＥは、前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから第１のセキュリティ鍵情報を含む第２の信号を受信し、
前記第２のＵＥは、前記セキュリティ構成要素を得るため、前記第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに第３の信号を送り、
前記第２のＵＥは、前記第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから、前記第１のセキュリティ鍵情報と異なる第２のセキュリティ鍵情報を含む第４の信号を受信する、
移動通信システム。
【請求項２】
前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎと前記第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ

は、ＰＣ２インタフェースを介してＰｒｏＳｅアプリケーションサーバと通信する、請求項１に記載の移動通信システム。
【請求項３】
前記第１のＵＥと前記第２のＵＥは、前記第１のセキュリティ鍵情報及び第２のセキュリティ鍵情報に基づき保護され、ＰＣ５インタフェースによる一対一通信を行う、請求項１に記載の移動通信システム。
【請求項４】
移動通信システムに用いられるＰｒｏＳｅ（Ｐｒｏｘｉｍｉｔｙ　Ｓｅｒｖｉｃｅｓ）Ｆｕｎｃｔｉｏｎであって、
ＰＣ３インタフェースを介して前記ＰｒｏＳｅをサポートする第１のＵＥ（Ｕｓｅｒ　Ｅｑｕｉｐｍｅｎｔ）から、セキュリティ構成要素を得るため第１の信号を受信する第１の受信手段と、
前記ＰＣ３インタフェースを介して前記第１のＵＥに、第１のセキュリティ鍵情報を含む第２の信号を送信する第１の送信手段と、
ＰＣ３インタフェースを介して前記ＰｒｏＳｅをサポートする第２のＵＥから、前記セキュリティ構成要素を得るため第３の信号を受信する第２の受信手段と、
前記ＰＣ３インタフェースを介して前記第２のＵＥに、前記第１のセキュリティ鍵情報と異なる第２のセキュリティ鍵情報を含む第４の信号を送信する第２の送信手段と、を有するＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ。
【請求項５】
前記ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎは、ＰＣ２インタフェースを介してＰｒｏＳｅアプリケーションサーバと通信する、請求項４に記載のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ。
【請求項６】
前記第１のＵＥと前記第２のＵＥは、前記第１のセキュリティ鍵情報及び第２のセキュリティ鍵情報に基づき保護され、ＰＣ５インタフェースによる一対一通信を行う、請求項４に記載のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ。
【請求項７】
移動通信システムに用いられるＰｒｏＳｅ（Ｐｒｏｘｉｍｉｔｙ　Ｓｅｒｖｉｃｅｓ）をサポートする複数のＵＥ（Ｕｓｅｒ　Ｅｑｕｉｐｍｅｎｔ）であって、
第１のＵＥは、
ＰＣ３インタフェースを介して第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに、セキュリティ構成要素を得るため第１の信号を送信する第１の送信手段と、
前記ＰＣ３インタフェースを介して前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから、第１のセキュリティ鍵情報を含む第２の信号を受信する第１の受信手段と、を有し、
第２のＵＥは、
前記ＰＣ３インタフェースを介して第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに、前記セキュリティ構成要素を得るため第３の信号を送信する第２の送信手段と、
前記ＰＣ３インタフェースを介して前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから、前記第１のセキュリティ鍵情報と異なる第２のセキュリティ鍵情報を含む第４の信号を受信する第２の受信手段と、を有するＵＥ。
【請求項８】
前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎと前記第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎは、ＰＣ２インタフェースを介してＰｒｏＳｅアプリケーションサーバと通信する、請求項７に記載のＵＥ。
【請求項９】
前記第１のＵＥと前記第２のＵＥは、前記第１のセキュリティ鍵情報及び第２のセキュリティ鍵情報に基づき保護され、ＰＣ５インタフェースによる一対一通信を行う、請求項７に記載のＵＥ。
【請求項１０】
Ｐｒｏｘｉｍｉｔｙ　Ｓｅｒｖｉｃｅｓ（ＰｒｏＳｅ）をサポートする第１のＵＥ（Ｕ

ｓｅｒ　Ｅｑｕｉｐｍｅｎｔ）と、前記ＰｒｏＳｅをサポートする第２のＵＥと、ＰＣ３インタフェースを介して前記第１のＵＥと通信する第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎと、前記ＰＣ３インタフェースを介して前記第２のＵＥと通信する第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎと、を含む移動通信システムの通信方法であって、

前記第１のＵＥは、セキュリティ構成要素を得るため、前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに第１の信号を送り、

前記第１のＵＥは、前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから第１のセキュリティ鍵情報を含む第２の信号を受信し、

前記第２のＵＥは、前記セキュリティ構成要素を得るため、前記第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに第３の信号を送り、

前記第２のＵＥは、前記第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから前記第１のセキュリティ鍵情報と異なる第２のセキュリティ鍵情報を含む第４の信号を受信する、

移動通信システムの通信方法。

【請求項１１】

前記移動通信システムは、前記第１のＵＥと前記第２のＵＥの間のＤｉｓｃｏｖｅｒｙに用いられる、請求項１０に記載の方法。

【請求項１２】

前記第１のＵＥと前記第２のＵＥは、前記第１のセキュリティ鍵情報及び第２のセキュリティ鍵情報に基づき保護され、ＰＣ５インタフェースによる一対一通信を行う、請求項１０に記載の方法。

【請求項１３】

移動通信システムに用いられるＰｒｏＳｅ（Ｐｒｏｘｉｍｉｔｙ　Ｓｅｒｖｉｃｅｓ）Ｆｕｎｃｔｉｏｎの方法であって、

ＰＣ３インタフェースを介して前記ＰｒｏＳｅをサポートする第１のＵＥ（Ｕｓｅｒ　Ｅｑｕｉｐｍｅｎｔ）から、セキュリティ構成要素を得るため第１の信号を受信し、

前記ＰＣ３インタフェースを介して前記第１のＵＥに、第１のセキュリティ鍵情報を含む第２の信号を送信し、

ＰＣ３インタフェースを介して前記ＰｒｏＳｅをサポートする第２のＵＥから、前記セキュリティ構成要素を得るため第３の信号を受信し、

前記ＰＣ３インタフェースを介して前記第２のＵＥに、前記第１のセキュリティ鍵情報と異なる第２のセキュリティ鍵情報を含む第４の信号を送信する、

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎの方法。

【請求項１４】

移動通信システムに用いられるＰｒｏＳｅ（Ｐｒｏｘｉｍｉｔｙ　Ｓｅｒｖｉｃｅｓ）をサポートする複数のＵＥ（Ｕｓｅｒ　Ｅｑｕｉｐｍｅｎｔ）の方法であって、

第１のＵＥは、

ＰＣ３インタフェースを介して第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに、セキュリティ構成要素を得るため第１の信号を送信し、

前記ＰＣ３インタフェースを介して前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから、第１のセキュリティ鍵情報を含む第２の信号を受信し、

第２のＵＥは、

前記ＰＣ３インタフェースを介して第２のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに、前記セキュリティ構成要素を得るため第３の信号を送信し、

前記ＰＣ３インタフェースを介して前記第１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから、前記第１のセキュリティ鍵情報と異なる第２のセキュリティ鍵情報を含む第４の信号を受信する、

ＵＥの方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ＰｒｏＳｅ（Ｐｒｏｘｉｍｉｔｙ ｂａｓｅｄ Ｓｅｒｖｉｃｅｓ）のための装置、システムおよび方法に関する。特に、本発明は、ＰｒｏＳｅでダイレクト通信のためのセキュリティに関するものであり、ダイレクト通信を許可されたネットワークに関する。また、本発明は、ＰＫＩ（Ｐｕｂｌｉｃ－Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）を用いた近接ダイレクト通信に関し、一対一のダイレクト通信のみならず、一対多のダイレクト通信にも関する。

【背景技術】

【０００２】

ダイレクト通信は、３ＧＰＰ（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ）で検討されている（非特許文献１及び２参照）。

【０００３】

ダイレクト通信のための重要な問題は、インタフェースＰＣ５を保護することである。最小限の信号で、インタフェースＰＣ５をどのように保護するか、及び信頼のソースからセキュリティコンテキスト（例えば鍵配布、割り当て、更新含む）をどのように確立するかは、重要な問題である。

【０００４】

インタフェースＰＣ５は、ＵＥがその上ダイレクト通信をできるようなＵＥ（複数のユーザ機器）間のベースポイントであることに留意されたい。インタフェースＰＣ５は、ＰｒｏＳｅのｄｉｓｃｏｖｅｒｙ、ダイレクト通信、ＵＥリレーの制御とユーザプレーンのために使用される。ＵＥダイレクト通信は、直接またはＬＴＥ－Ｕｕを介して実行することができる。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】3GPP TR 33.cde, "Study on security issues to support Proximity Services (Release 12)", V0.2.0, 2013-07, Clauses 5.4, 5.5 and 6.3, pp. 11, 12 and 13-20

【非特許文献２】3GPP TR 23.703, "Study on architecture enhancements to support Proximity Services（ＰｒｏＳｅ）(Release 12)", V0.4.1, 2013-06, Clauses 5.4, 5.12 and 6.2, pp. 13, 17, 18 and 62-82

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、本出願の発明者は、３ＧＰＰ ＳＡ３（セキュリティワーキンググループ）内の現在の解決方法は、以下の欠点を有することを見出した。

１）ＭＭＥ（Ｍｏｂｉｌｉｔｙ Ｍａｎａｇｅｍｅｎｔ Ｅｎｔｉｔｙ）への影響：ＭＭＥは、鍵データの割り当てを含むダイレクト通信手順に関与している必要がある。

２）キー割り当て手順は、ＵＥが信号を作成するだけでなく、同時に１対１の通信が発生するときにも、ＵＥが別のＵＥとダイレクト通信することを望むたびに発生する。

したがって、この解決策は、効率的ではない。

【０００７】

従って、本発明の目的は、ＰｒｏＳｅでダイレクト通信のセキュリティを効果的に確保するための解決策を提供することである。

【課題を解決するための手段】

【０００８】

上記課題を解決するために、本発明の第１の実施態様に係るＵＥは、ＵＥを正常にノードに登録する場合に、ノードからルート鍵を取得する手段と、前記ノードは、ＵＥを、ＵＥと、ＵＥに近接し、且つＵＥと通信することが許可されている一つ以上の異なるＵＥとの間のダイレクト通信をサポートし、ルート鍵のいずれかを使用することによって、異なるＵＥのいずれかと安全にダイレクト通信を行うための一組のセッション鍵を配布するた

めの配布手段と、を備える。
【０００９】
本発明の第２の実施態様に係るノードは、互いに近接しているＵＥ間のダイレクト通信をサポートし、相互に通信することを許可する。
このノードは、ＵＥがサーバに正常に登録された場合に、サーバからルート鍵を取得するための取得手段と、ここで、ルート鍵は、安全にダイレクト通信を行うための一組のセッション鍵を配布するために、前記ＵＥの一つのために用いられ、サーバは、ルート鍵を管理し、前記ＵＥの一つにルート鍵を分配するための分配手段と、を備える。
【００１０】
本発明の第３の実施態様に係るサーバは、少なくとも一つの別のＵＥと、安全にダイレクト通信を行うための一組のセッション鍵を配布するために各ＵＥのルート鍵を格納するためのストレージ手段と、ここで、前記ＵＥは、少なくとも一つの別のＵＥと互いに近接しており、ノードにルート鍵を送信することで、ノードからの要求に応答する応答手段と、ここで、前記ノードはＵＥの間のダイレクト通信をサポートする、を備える。
【００１１】
本発明の第４の実施態様に係る通信システムは、互いに近接しており、互いにダイレクト通信を行うことが許可された複数のＵＥと、ダイレクト通信をサポートするノードと、
別のＵＥの少なくとも一つと安全にダイレクト通信を行うための一組のセッション鍵を配布するために各ＵＥのルート鍵を管理するサーバとを備える。
各ＵＥをノードに正常に登録する場合、前記ノードは、サーバからルート鍵を取得して、各ＵＥに、取得したルート鍵を配布する。
前記各ＵＥは、配布されたルート鍵のいずれかを使用してセッション鍵を配布する。
【００１２】
本発明の第５の実施態様に係る方法は、ＵＥのための制御の方法である。
この方法は、各ＵＥをノードに正常に登録する場合、ノードからルート鍵を取得し、ここで、前記ノードは、ＵＥと、且つＵＥと通信することが許可されている一つ以上の異なるＵＥとの間のダイレクト通信をサポートし、ルート鍵のいずれかを使用することによって、異なるＵＥのいずれかと安全にダイレクト通信を行うためのセッション鍵を配布する、ことを含む。
【００１３】
本発明の第６の実施態様に係る方法は、互いに近接し、且つ相互に通信することが許可されたＵＥ間のダイレクト通信をサポートするノードの動作を制御する方法である。
この方法は、ＵＥのいずれかをノードに正常に登録する場合に、サーバからルート鍵を取得し、前記ＵＥのいずれかに使用されるルート鍵は、少なくともう一方のＵＥと安全に、ダイレクト通信を行うための一組のセッション鍵を配布するために用いられ、前記サーバは、ルート鍵を管理し、前記ＵＥのいずれかにルート鍵を配布することを含む。
【００１４】
本発明の第７の実施態様に係る方法は、サーバの動作を制御する方法である。
この方法は、少なくともひとつの別のＵＥと、安全にダイレクト通信を行うための、一組のセッション鍵を配布するために、各ＵＥのルート鍵を格納し、前記ＵＥは、互いに近接し、相互に通信を許可し、ノードにルート鍵を送信することで、ノードからの要求に応答し、ノードは、ＵＥの間のダイレクト通信をサポートすることを含む。
【００１５】
本発明の第８の実施態様に係るＵＥは、ＵＥを正常にノードに登録する場合に、ＵＥの公開鍵を登録するための、且つ１つまたはそれ以上の異なるＵＥの公開鍵を取得するための、第１の手段と、ここで、異なるＵＥがＵＥに近接している場合に、異なるＵＥは、ＵＥとダイレクト通信を行うことが許可され、ノードは、ダイレクト通信をサポートし、
異なるＵＥ間で第１のＵＥの公開鍵を用いて、第１のＵＥからの要求がＵＥとダイレクト通信を行うことであると確認するための第２の手段と、ここで、要求は、第１のＵＥの秘密鍵で保護される、を備える。

【００１６】
本発明の第９の実施態様に係るＵＥは、ＵＥを正常にノードに登録する場合にＵＥの公開鍵を登録し、且つ１つまたはそれ以上の異なるＵＥの公開鍵を取得するための、第１の手段であり、ここで、異なるＵＥがＵＥに近接している場合に、異なるＵＥは、ＵＥとダイレクト通信を行うことが許可され、ノードは、ダイレクト通信をサポートし、異なるＵＥ間で第１のＵＥの公開鍵を用いて、最初の要求に対する応答がＵＥと一対一でダイレクト通信を行うため、第１のＵＥを要求する保護された第１の要求への応答を確認するための第２の手段と、ここで、要求は、第１のＵＥの秘密鍵で保護されている、を備える。
【００１７】
本発明の第１０の実施態様に係るノードは、互いに近接し、且つ相互に通信を許可されたＵＥの間のダイレクト通信をサポートし、ノードである。
このノードは、正常にノードにＵＥの一つを登録する場合に、前記ＵＥのいずれかから公開鍵を受信するための受信手段と、正常な登録への応答として、前記ＵＥのいずれかに、他のＵＥの公開鍵を送信するための送信手段と、を備える。
公開鍵は、ダイレクト通信の要求を少なくとも確認するために、各ＵＥに使用される。
【００１８】
本発明の第１１の実施態様に係るサーバは、ＵＥが互いに近接している場合、互いにダイレクト通信を行うことが許可されたＵＥの公開鍵を格納するための格納手段と、ここで、公開鍵は、ダイレクト通信をサポートするノードにより登録されており、ノードに格納された公開鍵を送信して、ノードからの要求に応答するための応答手段と、を備える。
公開鍵は、少なくともダイレクト通信の要求を確認するために、各ＵＥに使用される。
【００１９】
本発明の第１２の実施態様に係る通信システムは、ＵＥが相互に近接しているときに、互いにダイレクト通信を行うことが許可されている複数のＵＥと、ダイレクト通信をサポートするノードと、を備える。
各ＵＥをノードに正常に登録した場合に、前記各ＵＥは、ノードを介してＵＥの公開鍵を共有し、公開鍵のいずれかを使用してダイレクト通信するための要求を少なくとも確認する。
前記ノードは、各ＵＥをノードに登録する場合、各ＵＥからの公開鍵のそれぞれを受信し、正常な登録への応答として、各ＵＥに、異なるＵＥの公開鍵を送信する。
【００２０】
本発明の第１３の実施態様に係る方法は、ＵＥの動作を制御する方法である。
この方法は、ＵＥをノードに正常に登録する場合に、ＵＥの公開鍵を登録し、且つ１つまたは複数の異なるＵＥの公開鍵を取得し、ここで、別のＵＥがＵＥと近接している場合に、別のＵＥは、ＵＥとダイレクト通信を行うことが許可されており、ノードは、ダイレクト通信をサポートし、異なるＵＥ間で第１のＵＥの公開鍵を用いて、ＵＥとダイレクト通信を行うための第１のＵＥからの要求を確認し、要求は、第１のＵＥの秘密鍵で保護されている、ことを含む。
【００２１】
本発明の第１４の実施態様に係る方法は、ＵＥの動作を制御する方法である。
この方法は、ＵＥをノードに正常に登録する場合に、ＵＥの公開鍵を登録し、且つ１つまたは複数の異なるＵＥの公開鍵を取得し、ここで、別のＵＥがＵＥと近接している場合に、別のＵＥは、ＵＥとダイレクト通信を行うことが許可されており、ノードは、ダイレクト通信をサポートし、異なるＵＥ間で第１のＵＥの公開鍵を用いて、ＵＥとダイレクト通信を行うための第１のＵＥからの保護された要求に対する応答を確認し、応答は、第１のＵＥの秘密鍵で保護されている、ことを含む。
【００２２】
本発明の第１５の実施態様に係る方法は、互いに通信することができ、互いに近接しているＵＥの間のダイレクト通信をサポートするノードを制御する方法である。
この方法は、ＵＥの一つをノードに正常に登録する場合に、前記ＵＥのいずれかから公

開鍵を受信し、正常な登録への応答として、他のＵＥの公開鍵を、前記ＵＥのいずれかに、送信する、ことを含む。
公開鍵は、ダイレクト通信のために少なくとも要求を確認するために、各ＵＥのために使用される。
【００２３】
本発明の第１６の実施態様に係る方法は、サーバの動作を制御する方法である。この方法は、ＵＥが相互に近接し、互いにダイレクト通信を行うことが許可されている場合、ＵＥの公開鍵を格納し、公開鍵は、ダイレクト通信をサポートするノードにより登録され、ノードに格納されている公開鍵を送信することで、ノードからの要求に応じる、ことを含む。公開鍵は、少なくともダイレクト通信のための要求を確認するために、各ＵＥのために使用される。
【発明の効果】
【００２４】
本発明によれば、上記課題を解決するために、そしてＰｒｏＳｅでダイレクト通信のセキュリティを効果的に確保するための解決策を提供することができる。
【００２５】
例えば、第１から７のいずれかの実施態様によれば、以下の効果を得ることができる。
１）集中的なルート鍵管理で、同期の問題を防ぐ。
２）ＵＥが、ダイレクト通信サービスを必要とする度のルートの割り当てを減らす。
【図面の簡単な説明】
【００２６】
【図１】図１は、本発明の第１の実施の形態にかかる通信システムの構成例を示すブロック図である。
【図２】図２は、第１の例示的な実施形態にかかる通信システムのルート鍵を割り当てるための動作の一例を示すシーケンス図である。
【図３】図３は、第１の例示的な実施形態にかかる通信システムのルート鍵を割り当てるための動作の他の例を示すシーケンス図である。
【図４】図４は、第１の例示的な実施形態にかかる通信システムのセッション鍵を配布するための動作の一例を示すシーケンス図である。
【図５】図５は、第１の例示的な実施形態にかかる通信システムにおいて、セッション鍵を配布するための動作の他の例を示すシーケンス図である。
【図６】図６は、第１の例示的な実施形態にかかるＵＥの構成例を示すブロック図である。
【図７】図７は、第１の例示的な実施形態にかかるノードの構成例を示すブロック図である。
【図８】図８は、第１の例示的な実施形態にかかるサーバの構成例を示すブロック図である。
【図９】図９は、本発明の第２の実施の形態にかかる通信システムの構成例を示すブロック図である。
【図１０】図１０は、実施の形態２にかかる通信システムにおいて、ＵＥを登録するための動作の一例を示すシーケンス図である。
【図１１】図１１は、実施の形態２にかかる通信システムにおいて、一対一のダイレクト通信のためのセッション鍵を配布するための動作の一例を示すシーケンス図である。
【図１２】図１２は、第２の実施の形態にかかる通信システムにおける一対多のダイレクト通信のためのセッション鍵を配布するための動作の一例を示すシーケンス図である。
【図１３】図１３は、第２の実施形態にかかるＵＥの構成例を示すブロック図である。
【図１４】図１４は、第２の実施形態にかかるノードの構成例を示すブロック図である。
【図１５】図１５は、第２の実施形態にかかるサーバの構成例を示すブロック図である。
【発明を実施するための形態】
【００２７】

以下、本発明にかかるＵＥ、ノード及びサーバと、これらのＵＥ、ノード及びサーバが適用される通信システムの、第１及び第２の実施形態を、添付の図面とともに説明する。

【００２８】

＜第１の実施の形態＞

図１は、Ｐｒｏｘｉｍｉｔｙサービスのための通信システムの構成例を示している。Ｐｒｏｘｉｍｉｔｙサービスは、商業／社会的な利用や公共の安全使用の両方のために、近接しているＵＥ間のｄｉｓｃｏｖｅｒｙと通信を制御するオペレータネットワークを提供する。ＰｒｏＳｅサービスは、ネットワークカバレッジの有無にかかわらずＵＥに提供されるべきであることが要求される。

【００２９】

図１に示すように、本実施の形態にかかる通信システムは、複数のＵＥ１０＿１～１０＿ｍ（以下ではまとめて符号１０で参照され得る）、一つ以上のＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ ２０＿１～２０＿ｎ（以下ではまとめて符号２０によって参照され得る）、Ｅ－ＵＴＲＡＮ（Ｅｖｏｌｖｅｄ Ｕｎｉｖｅｒｓａｌ Ｔｅｒｒｅｓｔｒｉａｌ Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ）３０、ＥＰＣ（Ｅｖｏｌｖｅｄ Ｐａｃｋｅｔ Ｃｏｒｅ）４０、及びＰｒｏＳｅＡＰＰ（アプリケーション）サーバ５０を含む。

【００３０】

ＵＥ１０は、Ｅ－ＵＴＲＡＮ３０を介して（すなわち、インタフェースＬＴＥ－Ｕｕ及びＳ１を介して）ＥＰＣ４０にアタッチし、これによって、典型的なＵＥとして機能する。また、ＵＥ１０は、上記インタフェースＰＣ５を使用し、これによってＰｒｏＳｅ通信を行う。ＰｒｏＳｅ通信に先立って、ＵＥ１０は、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０に登録されている。ＵＥ１０＿１～１０＿ｍは、同じＰｒｏＳｅ Ｆｕｎｃｔｉｏｎまたは互いに異なるＰｒｏＳｅ Ｆｕｎｃｔｉｏｎに登録することができることに留意されたい。また、ＵＥ１０＿１～１０＿ｍのいくつかは、同じＰｒｏＳｅ Ｆｕｎｃｔｉｏｎに登録することができる。

【００３１】

ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０はＵＥ１０＿１～１０＿ｍ間のＰｒｏＳｅ通信をサポートするノードである。ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０は、特定のネットワークノードに従属したノードまたは独立したノードのいずれかであってもよく、ＥＰＣ４０の内または外に存在してもよい。ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０は、インタフェースＰＣ３を介してＵＥ１０と通信を行う。また、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０は、インタフェースＰＣ４を介してＥＰＣ４０と通信する。また、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０＿１～２０＿ｎは、インタフェースＰＣ６を介して相互に通信することができる。

【００３２】

インタフェースＰＣ３は、ＵＥ１０とＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０との間のリファレンスポイントであることに留意されたい。インタフェースＰＣ３は、ＵＥ１０とＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０との間の相互作用を定義するために使用される。例えば、ＰｒｏＳｅのｄｉｓｃｏｖｅｒｙと通信するように構成するために使用してもよい。さらに、インタフェースＰＣ４は、ＥＰＣ４０及びＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０との間のベースポイントである。インタフェースＰＣ４は、ＥＰＣ４０及びＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０との間の相互作用を定義するために使用される。ＵＥ１０＿１～１０＿ｍ間の１対１の通信経路を設定するとき、またはリアルタイムでセッション管理やモビリティ管理のためのＰｒｏＳｅサービス（承認）を確認するときに可能なユースケースであってもよい。また、インタフェースＰＣ６はＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ２０＿１～２０＿ｎ間のベースポイントである。インタフェースＰＣ６は、異なるＰＬＭＮ（Ｐｕｂｌｉｃ Ｌａｎｄ Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋｓ）に加入し、ユーザ間のＰｒｏＳｅのｄｉｓｃｏｖｅｒｙなどの機能のために使用してもよい。

【００３３】

Ｅ－ＵＴＲＡＮ３０は、１つまたは複数のｅＮＢ（ｅｖｏｌｖｅｄ Ｎｏｄｅ Ｂｓ）（図示せず）によって形成される。ＥＰＣ４０は、ネットワークノード、ＵＥ１０＿１～

１０＿ｍのモビリティを管理するＭＭＥ（モビリティ管理エンティティ）等を含む。ＰｒｏＳｅＡＰＰサーバ５０は、インタフェースＳＧＩを通じてＥＰＣ４０と通信することができる。また、ＰｒｏＳｅＡＰＰサーバ５０は、インタフェースＰＣ１を介してＵＥ１０と通信することができ、且つインタフェースＰＣ２を通じてＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０と通信することができる。インタフェースＰＣ１がＵＥ１０＿１～１０＿ｍでのＰｒｏＳｅのアプリとＰｒｏＳｅＡＰＰサーバ５０との間のリファレンスポイントであることに留意されたい。インタフェースＰＣ１は、アプリケーションレベルのシグナリングの要件を定義するために使用される。一方、インタフェースＰＣ２は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０とＰｒｏＳｅＡＰＰサーバ５０との間のリファレンスポイントである。インタフェースＰＣ２はＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０を介して、３ＧＰＰ　ＥＰＳ（Ｅｖｏｌｖｅｄ　Ｐａｃｋｅｔ　Ｓｙｓｔｅｍ）によって提供され、ＰｒｏＳｅＡＰＰサーバ５０とＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎの間の相互作用を定義するために使用される。一つの例では、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０でＰｒｏＳｅデータベース用のアプリケーションデータの更新のためであってもよい。別の例では、３ＧＰＰの機能とアプリケーションデータ、例えば名前の変換、の間のインターワーキングでＰｒｏＳｅＡＰＰサーバ５０により使用のためのデータであってもよい。ＰｒｏＳｅＡＰＰサーバ５０は、ＥＰＣ４０の内または外に存在してもよい。

【００３４】

図示は省略するが、通信システムは、信頼できるサードパーティによって運営されるサーバを含む。以下の説明では、このサーバは、単に「第三の（サード）パーティ」と呼び、符号６０で参照される。一般的に、サードパーティ６０は、後述するルート鍵を管理する。

【００３５】

次に、本実施の形態の動作例を図２～５を参照して詳細に説明する。なお、ＵＥ１０、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０、及びサードパーティ６０の構成例は、図５～８を参照して後述する。

【００３６】

この例示的な実施形態では、ルート鍵を配布、更新及び割り当てるために、サードパーティ６０を使用することを提案している。ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０は、ダイレクト通信をサポートしており、登録時にＵＥ１０にすべてのルート鍵を割り当てる。セッション鍵は、ルート鍵を使用してＵＥ１０側に配布される。例えば、セッション鍵は、直接ＵＥ１０＿１～１０＿ｍとの間で転送されるメッセージを保護するための機密性と完全性のキーの一組である。

【００３７】

＜ルート鍵を割り当てるための操作＞

ルート鍵割り当てのために提案された２つのオプションがある。

【００３８】

オプション１：ルート鍵が所定のＵＥに関連している

ルート鍵は、登録時に割り当て／配布される。ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０は、ＵＥ１０＿１が通信を許可しているＵＥのリストを持っていると仮定し、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０は、信頼できるサードパーティ６０から、ＵＥ１０＿１のためのすべてのルート鍵を求めることができる。サードパーティ６０は、鍵配布と割り当てを担当している。ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１～２０＿ｎには、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１～２０＿ｎの間で動機を必要としないように登録されたＵＥ１０＿１～１０＿ｍのために、サードパーティ６０からルート鍵を取得することができる。各ルート鍵はユニークなＫＳＩ（Ｋｅｙ　Ｓｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）によって識別される。ダイレクト通信が発生すると、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０はＫＳＩを使用するかをＵＥ１０＿１～１０＿ｍに指示することができ、またはＵＥ１０＿１～１０＿ｍに交渉することができる。

【００３９】

具体的には、図２に示すように、ＵＥ１０＿１はＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１（ステップＳ１１）で登録する。

【００４０】

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１は、ルート鍵（ステップＳ１２）を管理し、サードパーティ６０にＵＥ１０＿１のルート鍵要求を送信する。

【００４１】

サードパーティ６０は、ＵＥ１０＿１のルート鍵でＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１に応答する。各ルート鍵はユニークなＫＳＩとＵＥに関連しており、ＵＥ１０＿１は、ＰｒｏＳｅサービス（ステップＳ１３）を持つことが許可される。

【００４２】

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１は、ＵＥのＩＤおよびＫＳＩを含むルート鍵を、ＵＥ１０＿１に配布する（ステップＳ１４）。

【００４３】

ステップＳ１１～Ｓ１４と同様の手順が、ＵＥ１０＿２とＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿２との間で行われる（ステップＳ１５～Ｓ１８）。

【００４４】

オプション２：ルート鍵プール

オプション１と同様に、ＵＥは、各キーはそれを識別するためのユニークなＫＳＩを持っているキー・プールを取得することができる。

ＵＥ１０＿１が、ダイレクト通信のためのセッション鍵を必要とするとき、ネットワーク（ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ）は、使用するキーを指示し、また、同じセッション鍵を配布することができるようにＵＥ１０＿１とＵＥ１０＿２に同じパラメータを与えることができる。

【００４５】

オプション１と比べての違いは、ここでのルート鍵は、任意のＵＥに関連していないということである。したがって、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０は、同じルート鍵が異なるＵＥに再利用されないことを確実にする必要がある。

【００４６】

具体的には、図３に示すように、ＵＥ１０＿１はＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１（ステップＳ２１）で登録する。

【００４７】

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１は、ルート鍵（ステップＳ２２）を管理し、サードパーティ６０にＵＥ１０＿１のリクエストルート鍵を送信する。

【００４８】

サードパーティ６０は、ルート鍵の束を含むルート鍵プールでＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１に応答する。各キーは、ユニークなＫＳＩに関係している（ステップＳ２３）。

【００４９】

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１はＫＳＩでＵＥ１０＿１にルート鍵を配布している（ステップＳ２４）。

【００５０】

ステップＳ２１～Ｓ２４と同様の手順が、ＵＥ１０＿２とＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿２との間で行われる（ステップＳ２５～Ｓ２８）。

【００５１】

このオプション２によれば、オプション１と比べてＵＥへのシグナリングの量を低減することができる。ルート鍵は、任意のＵＥに関係しない、したがって、ＵＥに送信するルート鍵の数は、オプション１よりも小さくすることができる。また、ルート鍵を格納するためにＵＥにリソースを削減することも可能である。

【００５２】

対照的に、オプション１によれば、オプション２と比較してＰｒｏＳｅ　Ｆｕｎｃｔｉ

ｏｎの負荷を軽減することができる。ルート鍵は一対一でＵＥに割り当てられ、したがって、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎが同じルート鍵は、異なるＵＥのために再使用されないことを保証する必要がないからである。

【００５３】

＜セッション鍵を配布するための操作＞

セッション鍵配布および割り当てのために提案された２つのオプションがある。

【００５４】

オプション１：ＵＥが自律的にセッション鍵を配布する

ダイレクト通信を開始するＵＥ１０＿１１は、単純にセッション鍵を配布し、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに送信し、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎは他のＵＥに送信する。

【００５５】

あるいは、図４に示すように、ＵＥ１０＿１は、ＵＥ１０＿２にダイレクト通信要求を送信する（ステップＳ３１）。

【００５６】

図２に示すように、各ルート鍵が所定のＵＥに関連している場合には、ＵＥ１０＿１及び１０＿２は、ネットワークの任意の命令を受けることなく、セッション鍵を配布するために使用される同一のルート鍵を識別することができる。したがって、ＵＥ１０＿１及び１０＿２は、識別されたルート鍵からセッション鍵を別々に配布する（ステップＳ３２）。

【００５７】

その後、ＵＥ１０＿１とＵＥ１０＿２は、セッション鍵を使用したセキュリティ保護でダイレクト通信を開始する（ステップＳ３３）。

【００５８】

オプション２：ＵＥはＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎによって指示されたＫＳＩに基づいてセッション鍵を配布

このオプションは、図３に示すようにルート鍵プールが割り当てられている場合に適している。

【００５９】

図５に示すように、ＵＥ１０＿１は、ＵＥ１０＿２（ＵＥ１０＿１がダイレクト通信サービスを望むＵＥ）のＩＤでダイレクト通信要求をＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１に送信する（ステップＳ４１）。

【００６０】

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１は、ＵＥ１０＿１が、ＵＥ１０＿２とのダイレクト通信をすることが許可されているかどうかの認証を行う（ステップＳ４２）。

【００６１】

正常に許可されている場合、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１は、ＵＥ１０＿１にルート鍵ＫＳＩを示す（ステップＳ４３）。

【００６２】

また、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿１は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０＿２を介してＵＥ１０＿２にルート鍵ＫＳＩを示す（ステップＳ４４）。

【００６３】

ＵＥ１０＿１とＵＥ１０＿２はＫＳＩで示されるルート鍵からセッション鍵を別々に配布する（ステップＳ４５）。

【００６４】

その後、ＵＥ１０＿１とＵＥ１０＿２は、セッション鍵を使用するセキュリティ保護でダイレクト通信を開始する（ステップＳ４６）。

【００６５】

次に、本実施形態にかかるＵＥ１０、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ（ノード）２０、及びサードパーティ（サーバ）６０の構成例を図６～８を用いて説明する。

【００６６】

図６に示すように、ＵＥ１０は、取得部１１及び配布部１２を含む。ＵＥ１０をＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０に正常に登録する場合、取得部１１は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０からルート鍵を取得する。配布部１２は、取得したルート鍵を使用してセッション鍵を配布する。図２に示すように、各ルート鍵が所定のＵＥに関連している場合、配布部１２は、セッション鍵を配布する場合に、ＵＥ１０がダイレクト通信を望むＵＥに対応するルート鍵を使用する。一方、図３に示すようにルート鍵プールが割り当てられている場合、配布部１２は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０から受信したＫＳＩによって示されたルート鍵を使用する。これらのユニット１１及び１２は、相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット１１及び１２は、例えば、インタフェースＰＣ５を介して別のＵＥとダイレクト通信を行う送受信機、インタフェースＰＣ３を通じてＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０と通信を行う送受信機、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）のような送受信機を制御するコントローラによって構成することができる。

【００６７】

図７に示すように、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０は、取得部２１と、分配器２２を含む。取得部２１は、ＵＥ１０をＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０に正常に登録する場合、サードパーティ６０からのルート鍵を取得する。分配部２２は、ＵＥ１０に取得されたルート鍵を配布する。図３に示すように、ルート鍵プールが割り当てられている場合、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０は、指示部２３を含む。指示部２３は、ルート鍵のＫＳＩがＵＥ１０により使用されることを、ＵＥ１０に指示する。これらのユニット２１～２３は、相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット２１～２３は、例えば、インタフェースＰＣ３を介してＵＥ１０と通信を行う送受信機、及びこの送受信機を制御するＣＰＵのようなコントローラで構成することができる。

【００６８】

図８に示すように、サードパーティ６０は、記憶部６１及び応答部６２を含む。記憶部６１は、ルート鍵を格納する。応答部６２は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０にルート鍵を送信し、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０からの要求に応答する。これらのユニット６１及び６２は相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット６１および６２は、例えば、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ２０と通信を行う送受信機、及びこのような送受信機を制御するＣＰＵ等のコントローラで構成することができる。

【００６９】

＜第２の実施の形態＞

図９は、Ｐｒｏｘｉｍｉｔｙサービスのための通信システムの構成例を示している。Ｐｒｏｘｉｍｉｔｙサービスは、商業／社会的な利用や公共の安全使用の両方のために、近接しているＵＥ間のｄｉｓｃｏｖｅｒｙと通信を制御するオペレータネットワークを提供する。ＰｒｏＳｅサービスは、ネットワークカバレッジの有無にかかわらずＵＥに提供されるべきであることが要求される。

【００７０】

図９に示すように、本実施の形態にかかる通信システムは、複数のＵＥ１１０＿１～１１０＿ｍ（以下ではまとめて符号１１０で参照され得る）、一つ以上のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１～１２０＿ｎ（以下ではまとめて符号１２０で参照され得る）、Ｅ－ＵＴＲＡＮ（Ｅｖｏｌｖｅｄ　Ｕｎｉｖｅｒｓａｌ　Ｔｅｒｒｅｓｔｒｉａｌ　Ｒａｄｉｏ　Ａｃｃｅｓｓ　Ｎｅｔｗｏｒｋ）１３０、ＥＰＣ（Ｅｖｏｌｖｅｄ　Ｐａｃｋｅｔ　Ｃｏｒｅ）１４０、及びＰｒｏＳｅＡＰＰ（アプリケーション）サーバ１５０を含む。

【００７１】

ＵＥ１１０は、Ｅ－ＵＴＲＡＮ１３０を介して（すなわち、インタフェースＬＴＥ－Ｕｕ及びＳ１を介して）ＥＰＣ１４０にアタッチし、これによって、典型的なＵＥとして機

能する。また、ＵＥ１１０は、上記インタフェースＰＣ５を使用し、これによってＰｒｏＳｅ通信を行う。ＰｒｏＳｅ通信に先立って、ＵＥ１１０は、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０に登録されている。ＵＥ１１０＿１～１１０＿mは、同じＰｒｏＳｅ Ｆｕｎｃｔｉｏｎまたは互いに異なるＰｒｏＳｅ Ｆｕｎｃｔｉｏｎに登録することができることに留意されたい。また、ＵＥ１１０＿１～１１０＿mのいくつかは、同じＰｒｏＳｅ Ｆｕｎｃｔｉｏｎに登録することができる。

【００７２】

ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０はＵＥ１１０＿１～１０＿m間のＰｒｏＳｅ通信をサポートするノードである。ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０は、特定のネットワークノードに従属したノードまたは独立したノードのいずれかであってもよく、ＥＰＣ１４０の内または外に存在してもよい。ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０は、インタフェースＰＣ３を介してＵＥ１１０と通信を行う。また、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０は、インタフェースＰＣ４を介してＥＰＣ１４０と通信する。また、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０＿１～２０＿nは、インタフェースＰＣ６を介して相互に通信することができる。

【００７３】

インタフェースＰＣ３は、ＵＥ１１０とＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０との間のリファレンスポイントであることに留意されたい。インタフェースＰＣ３は、ＵＥ１１０とＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０との間の相互作用を定義するために使用される。例えば、ＰｒｏＳｅのｄｉｓｃｏｖｅｒｙと通信するように構成するために使用してもよい。さらに、インタフェースＰＣ４は、ＥＰＣ１４０及びＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０との間のベースポイントである。インタフェースＰＣ４は、ＥＰＣ１４０及びＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０との間の相互作用を定義するために使用される。ＵＥ１１０＿１～１０＿m間の１対１の通信経路を設定するとき、またはリアルタイムでセッション管理やモビリティ管理のためのＰｒｏＳｅサービス（承認）を確認するときに可能なユースケースであってもよい。また、インタフェースＰＣ６はＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０＿１～２０＿n間のベースポイントである。インタフェースＰＣ６は、異なるＰＬＭＮ（Ｐｕｂｌｉｃ Ｌａｎｄ Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋｓ）に加入し、ユーザ間のＰｒｏＳｅのｄｉｓｃｏｖｅｒｙなどの Ｆｕｎｃｔｉｏｎのために使用してもよい。

【００７４】

Ｅ－ＵＴＲＡＮ１３０は、１つまたは複数のｅＮＢ（ｅｖｏｌｖｅｄ Ｎｏｄｅ Ｂｓ）（図示せず）によって形成される。ＥＰＣ１４０は、ネットワークノード、ＵＥ１１０＿１～１０＿mのモビリティを管理するＭＭＥ（モビリティ管理エンティティ）等を含む。ＰｒｏＳｅＡＰＰサーバ１５０は、インタフェースＳＧＩを通じてＥＰＣ１４０と通信することができる。また、ＰｒｏＳｅＡＰＰサーバ１５０は、インタフェースＰＣ１を介してＵＥ１１０と通信することができ、且つインタフェースＰＣ２を通じてＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０と通信することができる。インタフェースＰＣ１がＵＥ１１０＿１～１０＿mでのＰｒｏＳｅのアプリとＰｒｏＳｅＡＰＰサーバ１５０との間のリファレンスポイントであることに留意されたい。インタフェースＰＣ１は、アプリケーションレベルのシグナリングの要件を定義するために使用される。一方、インタフェースＰＣ２は、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０とＰｒｏＳｅＡＰＰサーバ１５０との間のリファレンスポイントである。インタフェースＰＣ２はＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０を介して、３ＧＰＰ ＥＰＳ（Ｅｖｏｌｖｅｄ Ｐａｃｋｅｔ Ｓｙｓｔｅｍ）によって提供され、ＰｒｏＳｅＡＰＰサーバ１５０とＰｒｏＳｅ Ｆｕｎｃｔｉｏｎの間の相互作用を定義するために使用される。一つの例では、ＰｒｏＳｅ Ｆｕｎｃｔｉｏｎ１２０でＰｒｏＳｅデータベース用のアプリケーションデータの更新のためであってもよい。別の例では、３ＧＰＰの機能 とアプリケーションデータ、例えば名前の変換、の間のインターワーキングでＰｒｏＳｅＡＰＰサーバ１５０により使用のためのデータであってもよい。ＰｒｏＳｅＡＰＰサーバ１５０は、ＥＰＣ１４０の内または外に存在してもよい。

【００７５】
図示は省略するが、通信システムは、信頼できるサードパーティによって運営されるサーバを含む。以下の説明では、このサーバは、単に「第三の（サード）パーティ」と呼び、符号１６０で参照される。一般的に、サードパーティ１６０は、後述するルート鍵を管理する。
【００７６】
次に、本実施の形態の動作例を図１０～１２を参照して詳細に説明する。なお、ＵＥ１１０、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０、及びサードパーティ１６０の構成例は、図１３～１５を参照して後述する。
【００７７】
この例示的な実施形態は、ダイレクト通信のためのＰＫＩを使用することを提案している。ＵＥ１１０＿１～１１０＿ｍは、登録手続きにおいて自分の公開鍵を登録し、その間に他のＵＥの公開鍵を取得することができる。ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０は、ＵＥ１１０にダイレクト通信を許可する要求で、ＵＥの公開鍵を供給することのみを、ＵＥ１１０に保証する。ＵＥ１１０＿１～１１０＿ｍは、ダイレクト通信を開始するためのセッション鍵を配布することができるように他の端末に確認するために、公開鍵を使用する。例えば、セッション鍵は、直接ＵＥ１１０＿１～１０＿ｍとの間で転送されるメッセージを保護するための機密性と完全性のキーの一組である。
【００７８】
以下に、鍵配布するためのオプションを提案する。
【００７９】
１．１対１のダイレクト通信のためのＰＫＩ：
ＵＥ１１０＿１～１１０＿ｍは、登録時に自分の公開鍵を提供し、正常に登録された他のＵＥの公開鍵を受け取る。例えば、ＵＥ１１０＿１は、秘密鍵でダイレクト通信要求を保護する。ダイレクト通信要求を受信したＵＥ１１０＿２は、ＵＥ１の公開鍵で確認することができる。ＵＥ１１０＿２は、ＵＥ１１０＿１へのセッション鍵配布のためのデータを送ることができ、それらはダイレクト通信の保護のために同じ鍵を配布することができる。ＵＥ１１０＿１は、ＵＥ２の公開鍵で、ＵＥ１１０＿２から送信されたメッセージを確認でき、したがって、それらは相互に認証することができる。
【００８０】
セッション鍵の配布は、
１）鮮度を保つために、予めＵＥの一つによって提供された鍵データを入力としてＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎから取得されたルート鍵を使用ことができ、そして
２）また、計算及び秘密鍵を共有するための鍵交換スキーム（例えばＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換スキーム）を使用ことができる。
【００８１】
具体的には、図１０に示すように、ＵＥ１１０＿１は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１への登録時に、公開鍵を登録する（ステップＳ１１１）。
【００８２】
ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１は、ＵＥ１１０＿１の公開鍵をサードパーティ１６０に登録する（ステップＳ１１２）。
【００８３】
サードパーティ１６０は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１に許可リストを送信する。許可リストには、ＵＥ１１０＿１とダイレクト通信が許可されたＵＥのＩＤと、このＵＥの関連する公開鍵が含まれている（ステップＳ１１３）。
【００８４】
ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１は、ＵＥ１１０＿１に許可リストを転送する（ステップＳ１１４）。
【００８５】
ステップＳ１１１～Ｓ１１４と同様の手順が、ＵＥ１１０＿２で実行される（ステップ

Ｓ１１５～Ｓ１１８）。
【００８６】
図１１に示すように、ダイレクト通信を開始したとき、ＵＥ１１０＿１は、ＵＥ１１０＿２のＩＤで、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１にダイレクト通信要求、ＵＥ１１０＿１の公開鍵ＫＳＩを送信する。メッセージは、ＵＥ１１０＿１の秘密鍵を用いて保護することができる。メッセージは、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１によって、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿２に転送される（ステップＳ１２１）。
【００８７】
ＫＳＩの使用は、複数の公開鍵がＵＥ１１０＿１に割り当てられる場合に適していることに留意されたい。ＵＥ１１０＿２は、ＵＥ１１０＿１によって使用される秘密鍵に対応する公開鍵の一つを識別するためにＫＳＩを参照することができる。
【００８８】
ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿２のサポートにより、ＵＥ１１０＿１が、ＵＥ１１０＿２とのダイレクト通信サービスを実行できるかどうかの承認行う（ステップＳ１２２）。
【００８９】
正常に承認された場合、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿２は、ＵＥ１１０＿２にダイレクト通信要求を転送する（ステップＳ１２３）。
【００９０】
ＵＥが通信可能範囲外にあるときにダイレクト通信が発生した場合、ダイレクト通信要求がＵＥ１１０＿１からＵＥ１１０＿２に直接行き、及び上記のステップＳ１２２が省略されることに留意されたい。
【００９１】
ＵＥ１１０＿２は、ＵＥ１１０＿１の公開鍵でメッセージの整合性チェックを実行することができる（ステップＳ１２４）。
【００９２】
整合性が正常にチェックされると、ＵＥ１１０＿２は、上記のようにセッション鍵を配布する（ステップＳ１２５）。
【００９３】
ＵＥ１１０＿２は、セッション鍵を配布するためのデータでダイレクト通信応答をＵＥ１１０＿１に送信する。あるいは、ＵＥ１１０＿２は、ダイレクト通信応答で配布されたセッション鍵を含んでいる。メッセージは、ＵＥ１１０＿２の秘密鍵で保護されている（ステップＳ１２６）。
【００９４】
ＵＥ１１０＿１は、ＵＥ１１０＿２の公開鍵を使用してメッセージの整合性チェックを実行する（ステップＳ１２７）。
【００９５】
整合性が正常にチェックされると、ＵＥ１１０＿１は、データからセッション鍵を配布する。（ステップＳ１２８）。ステップＳ１２６で、ＵＥ１１０＿１が、ＵＥ１１０＿２からのセッション鍵を受信した場合、ステップＳ１２８はスキップされる。あるいは、ＵＥ１１０＿１は、ＵＥ１１０＿２の公開鍵を使用してダイレクト通信応答からセッション鍵を抽出する。
【００９６】
その後、ダイレクト通信は、ＵＥ１１０＿１とＵＥ１１０＿２が共有するセッション鍵によってセキュリティ保護を開始する（ステップＳ１２９）。
【００９７】
２．１対多のダイレクト通信のためのＰＫＩ：
登録手順は、図１０に示したものと同様である。
【００９８】
ＵＥ１１０＿１は、秘密鍵でダイレクト通信要求を保護する。

他のＵＥ（例えばＵＥ１１０＿２、ＵＥ１１０＿３）は、ＵＥ１の公開鍵で確認することができる。

【００９９】

一方、このオプションでは、ＵＥ１１０＿１は、１対多のダイレクト通信のためのセッション鍵を配布し、安全なインタフェースＰＣ３上でのダイレクト通信要求とともにセッション鍵をＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０に送信する。ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０は、ＵＥ１１０＿２とＵＥ１１０＿３にセッション鍵を送信する。ＵＥ１１０＿２またはＵＥ１１０＿３が異なるＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに登録されている場合、ＵＥ１１０＿１のＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎは、ＵＥ１１０＿２／１１０＿３が提供するＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎにセッション鍵を転送する。セッション鍵の配布は、ＵＥ１１０＿１の秘密鍵または任意のＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）鍵を入力に使用できる。

【０１００】

具体的には、図１２に示すように、ＵＥ１１０＿１は、ダイレクト通信のためにセッション鍵を配布する（ステップＳ１３１）。

【０１０１】

ＵＥ１１０＿１は、対象のＵＥ（例えばＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿２と、ＵＥ１１０＿２及び１１０＿３）に提供するＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎに転送することができるＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１、にダイレクト通信要求を送信する。このメッセージには、ＵＥ１１０＿１の秘密鍵で保護された、対象のＵＥのＩＤ及びＵＥ１１０＿１の公開鍵ＫＳＩを含んでいる。ＵＥ１１０＿１は、メッセージにセッション鍵を含む（ステップＳ１３２）。

【０１０２】

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿１と１２０＿２は、ＵＥ１１０＿１は、対象のＵＥ１１０＿２と１１０＿３と１対多のダイレクト通信ができるかどうかについての承認を行う（ステップＳ１３３）。

【０１０３】

ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０＿２は、ＵＥ１１０＿２と１１０＿３にダイレクト通信要求を転送する（ステップＳ１３４）。

【０１０４】

各ＵＥ１１０＿２と１１０＿３は、ＵＥ１１０＿１の公開鍵でメッセージの整合性をチェックする（ステップＳ１３５）。

【０１０５】

各ＵＥ１１０＿２と１１０＿３は、受信したセッション鍵で保護されたダイレクト通信応答をＵＥ１１０＿１に送信する（ステップＳ１３６）。その後、ダイレクト通信は、ＵＥ１１０＿１～１１０＿３で共有されたセッション鍵によるセキュリティ保護で開始する。

【０１０６】

３．ＰＫＩセッション鍵を使用せずに一対多方向通信

１対多の通信がＵＥ１から他への唯一の方法である場合を考えると、ＵＥ１１０＿１は、単純に秘密鍵で他のＵＥへのダイレクト通信を保護する。ＵＥ１１０＿からメッセージを受信することを承認されている他のＵＥは、ＵＥ１１０＿１の公開鍵を得ることができ、したがって、ＵＥ１１０＿１から送信されたメッセージを確認し、読むことができる。

ネットワーク（例えばＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ）は、承認されていないＵＥは、ＵＥ１１０＿１の秘密鍵を取得できないよう確実にし、この秘密鍵は他のＵＥに送信すべきではない。

【０１０７】

したがって、（非特許文献２の５．１２項で要求されるように）ＰｒｏＳｅグループ通信の送信を聞くことにより、非メンバーを防ぐことができる。

【０１０８】

４．入力としての１対多公開鍵のためのＰＫＩ使用：
ＵＥ１１０＿１～１１０＿ｍは、セッション鍵を配布し、鍵配布のための入力は、１）ＵＥ１１０＿１の秘密鍵、２）ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０から受信した鍵配布データである。ＵＥ１１０＿１秘密鍵と鍵配布データに必要なことは、承認されたＵＥに提供されていることのみである。

【０１０９】
ＵＥ１１０＿１が、同じセッション鍵を持つようにするには：
Ａ）ＵＥ１１０＿１は、同じセッション鍵でセッションを配布することができるように、公開鍵を保持し、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０から鍵配布データを受信する。
Ｂ）ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０は、ＵＥ１１０＿１の公開鍵とキー配布材料の両方を知っているので、鍵を配布することができる。
ｃ）ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０は、ＵＥ１１０＿１が同じセッション鍵を配布するための秘密鍵で使用することできるは鍵配布データを提供する。

【０１１０】
このことは、ＵＥ１１０＿１及び他のＵＥ鍵への配布データが何らかの関係を持っている必要がある。

【０１１１】
次に、本実施形態のＵＥ１１０、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ（ノード）１２０およびサードパーティ（サーバ）１６０の構成例を、図１３～１５を参照して説明する。

【０１１２】
図１３で示したように、ＵＥ１１０は、登録／検索部１１１および検証部１１２を含む。　登録／検索部１１１は、図１０に示すプロセスまたはそれと同等のプロセスを実行する。検証部１１２は、図１１及び１２に示すプロセスまたはそれとプロセスの処理を実行する。これらのユニット１１１および１１２は、相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット１１１及び１１２は、例えば、インタフェースＰＣ５を介して別のＵＥとダイレクト通信を行う送受信機、インタフェースＰＣ３を通じてＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０と通信を行う送受信機、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）のような送受信機を制御するコントローラによって構成することができる。

【０１１３】
図１４に示すように、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０は、少なくとも、受信部１２１と、送信部１２２を含む。受信部１２１は、図１０に示すステップＳ１１１及びＳ１１５のプロセスまたはそれと同等のプロセスを実行する。送信ユニット１２２は、図１０に示すステップＳ１１４及びＳ１１８のプロセスまたはそれと同等のプロセスを実行する。また、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０はまた、登録部１２３および取得部１２４を含むことができる。登録部１２３は、図１０に示すステップＳ１１２及びＳ１１６のプロセスまたはそれと同等のプロセスを実行する。取得部１２４は、図１０に示すステップＳ１１３及びＳ１１７のプロセスまたはそれと同等のプロセスを実行する。これらのユニット１２１～１２４は、相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット１２１～１２４は、例えば、インタフェースＰＣ３を介してＵＥ１１０と通信を行う送受信機、サードパーティ１６０と通信を行う送受信機、及びこの送受信機を制御するＣＰＵのようなコントローラで構成することができる。

【０１１４】
図１５に示すように、サードパーティの１６０は、記憶部１６１及び応答部１６２を含む。記憶部１６１は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０によって登録されたルート鍵を格納する。応答装置１６２は、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０からの要求に応答し、格納されている公開鍵をＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０に送信する。これらのユニット１６１および１６２は相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット１６１と１６２は、例えば、ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ１２０と通信を行う送受信機、及びこのような送受信機を制御するＣＰＵ等のコントロー

ラで構成することができる。
【０１１５】
本発明は、上記実施の形態に限定されるものではなく、様々な修正は、特許請求の範囲の記載に基づいて当業者によってなされ得ることは明らかである。
【０１１６】
上記に開示された例示的な実施形態の全部または一部は、以下の付記を限定せずに説明するものである。
【０１１７】
（付記１）
ＵＥを正常にノードに登録する場合に、ノードからルート鍵を取得する手段と、前記ノードは、ＵＥを、ＵＥと、ＵＥに近接し、且つＵＥと通信することが許可されている一つ以上の異なるＵＥとの間のダイレクト通信をサポートし、
ルート鍵のいずれかを使用することによって、異なるＵＥのいずれかと安全にダイレクト通信を行うための一組のセッション鍵を配布するための配布手段と、を備えるＵＥ（ユーザ機器）。
【０１１８】
（付記２）
前記ルート鍵は、一対一の様式で異なるＵＥと関連づけされ、
前記配布手段は、セッション鍵を配布する場合に、前記異なるＵＥのいずれかに対応するルート鍵を使用するように構成されている、付記１に記載のＵＥ。
【０１１９】
（付記３）
前記ルート鍵が所定のＵＥと関連づけしていない鍵の束であり、
前記配布手段は、セッション鍵を配布する場合に、前記ノードに示されたルート鍵を使用するように構成されている、付記１に記載のＵＥ。
【０１２０】
（付記４）
ダイレクト通信がＰｒｏＳｅ（Proximity based Services）通信を含む付記１から３のいずれかに記載のＵＥ。
【０１２１】
（付記５）
互いに近接しているＵＥ間のダイレクト通信をサポートし、相互に通信することを許可するノードであって、
ＵＥがサーバに正常に登録された場合に、サーバからルート鍵を取得するための取得手段と、ここで、ルート鍵は、安全にダイレクト通信を行うための一組のセッション鍵を配布するために、前記ＵＥの一つのために用いられ、サーバは、ルート鍵を管理し、
前記ＵＥの一つにルート鍵を分配するための分配手段と、を備えるノード。
【０１２２】
（付記６）
ルート鍵は一対一の様式で互いに異なるＵＥに関連づけされる付記５に記載のノード。
【０１２３】
（付記７）
ルート鍵が所定のＵＥと関連づけしていないキーの束である場合、ルート鍵が、セッション鍵を配布するために使用される前記ＵＥのひとつに指示するための指示手段を更に備える。付記５に記載のノード。
【０１２４】
（付記８）
前記ダイレクト通信がＰｒｏＳｅ通信を含む付記４～７いずれかに記載のノード。
【０１２５】
（付記９）

少なくとも一つの別のＵＥと、安全にダイレクト通信を行うための一組のセッション鍵を配布するために各ＵＥのルート鍵を格納するためのストレージ手段と、ここで、前記ＵＥは、少なくとも一つの別のＵＥと互いに近接しており、
ノードにルート鍵を送信することで、ノードからの要求に応答する応答手段と、ここで、前記ノードはＵＥの間のダイレクト通信をサポートする、
を備えるサーバ。
【０１２６】
（付記１０）
ルート鍵は一対一の様式で互いに異なるＵＥに関連づけされる付記９に記載のサーバ。
【０１２７】
（付記１１）
ルート鍵が所定のＵＥと関連づけしていない鍵の束である、付記９に記載のサーバ。
【０１２８】
（付記１２）
ダイレクト通信がＰｒｏＳｅ通信を含む、付記９～１１のいずれかに記載のサーバ。
【０１２９】
（付記１３）
互いに近接しており、互いにダイレクト通信を行うことが許可された複数のＵＥと、
ダイレクト通信をサポートするノードと、
別のＵＥの少なくとも一つと安全にダイレクト通信を行うための一組のセッション鍵を配布するために各ＵＥのルート鍵を管理するサーバとを備え、
各ＵＥをノードに正常に登録する場合、前記ノードは、サーバからルート鍵を取得して、各ＵＥに、取得したルート鍵を配布し、
前記各ＵＥは、配布されたルート鍵のいずれかを使用してセッション鍵を配布する、通信システム。
【０１３０】
（付記１４）
ＵＥのための制御の方法であって、
各ＵＥをノードに正常に登録する場合、ノードからルート鍵を取得し、ここで、前記ノードは、ＵＥと、且つＵＥと通信することが許可されている一つ以上の異なるＵＥとの間のダイレクト通信をサポートし、
ルート鍵のいずれかを使用することによって、異なるＵＥのいずれかと安全にダイレクト通信を行うためのセッション鍵を配布する、方法。
【０１３１】
（付記１５）
互いに近接し、且つ相互に通信することが許可されたＵＥ間のダイレクト通信をサポートするノードの動作を制御する方法であって、
ＵＥのいずれかをノードに正常に登録する場合に、サーバからルート鍵を取得し、前記ＵＥのいずれかに使用されるルート鍵は、少なくともう一方のＵＥと安全に、ダイレクト通信を行うための一組のセッション鍵を配布するために用いられ、前記サーバは、ルート鍵を管理し、
前記ＵＥのいずれかにルート鍵を配布する、方法。
【０１３２】
（付記１６）
サーバの動作を制御する方法であって、
少なくともひとつの別のＵＥと、安全にダイレクト通信を行うための、一組のセッション鍵を配布するために、各ＵＥのルート鍵を格納し、前記ＵＥは、互いに近接し、相互に通信を許可されており、
ノードにルート鍵を送信することで、ノードからの要求に応答し、ノードは、ＵＥの間のダイレクト通信をサポートする方法。

【０１３３】
（付記１７）
ＵＥを正常にノードに登録する場合に、ＵＥの公開鍵を登録するための、且つ１つまたはそれ以上の異なるＵＥの公開鍵を取得するための、第１の手段と、ここで、異なるＵＥがＵＥに近接している場合に、異なるＵＥは、ＵＥとダイレクト通信を行うことが許可され、ノードは、ダイレクト通信をサポートし、
異なるＵＥ間で第１のＵＥの公開鍵を用いて、第１のＵＥからの要求がＵＥとダイレクト通信を行うことであると確認するための第２の手段と、ここで、要求は、第１のＵＥの秘密鍵で保護され、
を備えるＵＥ（ユーザ機器）。
【０１３４】
（付記１８）
前記要求は、第１のＵＥと一対一でダイレクト通信を行うようにＵＥに要求するものであり、
第２の手段は
正常に確認した場合に、安全に一対一でダイレクト通信を行うための一組のセッション鍵を配布し
ＵＥの秘密鍵を用いて要求に対する応答を保護し、応答は、セッション鍵またはセッション鍵を配布するための材料を含み、
第１のＵＥに応答を送信する、ように構成されている、付記１７に記載のＵＥ。
【０１３５】
（付記１９）
前記要求は、異なるＵＥのうちの別の１つまたは複数とともに１対多数のダイレクト通信を行うことをＵＥに要求するためのものであり、且つ安全に１対多数のダイレクト通信を行うための一組のセッション鍵を含み、
第２の手段は、要求からセッション鍵を抽出するように構成されている、付記１７に記載のＵＥ。
【０１３６】
（付記２０）
公開鍵は、複数のＵＥに割り当てられており、
第２の手段は、要求に含まれるインジケータに基づいて、確認のために使用される公開鍵のいずれかを識別するように構成されている、付記１７から１９のいずれかに記載のＵＥ。
【０１３７】
（付記２１）
ＵＥを正常にノードに登録する場合にＵＥの公開鍵を登録し、且つ１つまたはそれ以上の異なるＵＥの公開鍵を取得するための、第１の手段であって、ここで、異なるＵＥがＵＥに近接している場合に、異なるＵＥは、ＵＥとダイレクト通信を行うことが許可され、ノードは、ダイレクト通信をサポートし、
異なるＵＥ間で第１のＵＥの公開鍵を用いて、最初の要求に対する応答がＵＥと一対一でダイレクト通信を行うため、第１のＵＥを要求する保護された第１の要求への応答を確認するための第２の手段と、ここで、要求は、第１のＵＥの秘密鍵で保護されている、
を備えるＵＥ（ユーザ機器）。
【０１３８】
（付記２２）
前記応答は、安全に一対一のダイレクト通信を行うための第１の一組のセッション鍵または第１のセッション鍵を配布するためのデータを含み、
第２の手段は
正常に確認した場合に、応答から最初のセッション鍵や材料を抽出し、
データが抽出された場合に、データから第１のセッション鍵を配布するように構成され

ている、付記２１に記載のＵＥ。
【０１３９】
（付記２３）
第２の手段が
異なるＵＥの２つ以上と１対多数のダイレクト通信するために、１対多数のダイレクト通信を行うための一組の第２のセッション鍵を安全に配布し、
二つ以上の異なるＵＥに、一対多のダイレクト通信を行うことを要求する、第２の要求における第２のセッション鍵を含み、
ＵＥの秘密鍵で、第２の要求を保護し、
ノードを介して２つ以上の別のＵＥに第２の要求を送信する、ように構成されている、付記２１または２２に記載のＵＥ。
【０１４０】
（付記２４）
公開鍵は、複数のＵＥに割り当てられており、
第２の手段は、要求において、要求を保護するために使用されるＵＥの秘密鍵に対応する公開鍵のインジケータを含むように構成されている、付記２１から２３のいずれかに記載のＵＥ。
【０１４１】
（付記２５）
互いに近接し、且つ相互に通信を許可されたＵＥの間のダイレクト通信をサポートし、ノードであって、
正常にノードにＵＥの一つを登録する場合に、前記ＵＥのいずれかから公開鍵を受信するための受信手段と、
正常な登録への応答として、前記ＵＥのいずれかに、他のＵＥの公開鍵を送信するための送信手段と、を備え、
公開鍵は、ダイレクト通信の要求を少なくとも確認するために、各ＵＥに使用される、ノード。
【０１４２】
（付記２６）
サーバに前記ＵＥのいずれかの公開鍵を登録する登録手段と、
サーバから前記他のＵＥの公開鍵を取得する取得手段と、を更に備える付記２５に記載のノード。
【０１４３】
（付記２７）
ＵＥが互いに近接している場合、互いにダイレクト通信を行うことが許可されたＵＥの公開鍵を格納するための格納手段と、ここで、公開鍵は、ダイレクト通信をサポートするノードにより登録されており、
ノードに格納された公開鍵を送信して、ノードからの要求に応答するための応答手段と、を備え、
公開鍵は、少なくともダイレクト通信の要求を確認するために、各ＵＥに使用される、サーバ。
【０１４４】
（付記２８）
ＵＥが相互に近接しているときに、互いにダイレクト通信を行うことが許可されている複数のＵＥと、
ダイレクト通信をサポートするノードと、を備え、
各ＵＥをノードに正常に登録した場合に、前記各ＵＥは、ノードを介してＵＥの公開鍵を共有し、公開鍵のいずれかを使用してダイレクト通信するための要求を少なくとも確認し、
前記ノードは、各ＵＥをノードに登録する場合、各ＵＥからの公開鍵のそれぞれを受信

し、正常な登録への応答として、各ＵＥに、異なるＵＥの公開鍵を送信する通信システム。

【０１４５】

（付記２９）

さらに公開鍵を管理するサーバを備え、

ノードは、各ＵＥの公開鍵をそれぞれサーバに登録し、サーバから異なるＵＥの公開鍵を取得し、

前記サーバは、ノードによって登録された公開鍵を格納し、ノードに格納されている公開鍵を送信して、ノードからの要求に応答する、付記２８に記載の通信システム。

【０１４６】

（付記３０）

ＵＥの動作を制御する方法であって、

ＵＥをノードに正常に登録する場合に、ＵＥの公開鍵を登録し、且つ１つまたは複数の異なるＵＥの公開鍵を取得し、ここで、別のＵＥがＵＥと近接している場合に、別のＵＥは、ＵＥとダイレクト通信を行うことが許可されており、ノードは、ダイレクト通信をサポートし、

異なるＵＥ間で第１のＵＥの公開鍵を用いて、ＵＥとダイレクト通信を行うための第１のＵＥからの要求を確認し、要求は、第１のＵＥの秘密鍵で保護されている、方法。

【０１４７】

（付記３１）

ＵＥの動作を制御する方法であって、

ＵＥをノードに正常に登録する場合に、ＵＥの公開鍵を登録し、且つ１つまたは複数の異なるＵＥの公開鍵を取得し、ここで、別のＵＥがＵＥと近接している場合に、別のＵＥは、ＵＥとダイレクト通信を行うことが許可されており、ノードは、ダイレクト通信をサポートし、

異なるＵＥ間で第１のＵＥの公開鍵を用いて、ＵＥとダイレクト通信を行うための第１のＵＥからの保護された要求に対する応答を確認し、応答は、第１のＵＥの秘密鍵で保護されている、方法。

【０１４８】

（付記３２）

互いに通信することができ、互いに近接しているＵＥの間のダイレクト通信をサポートするノードを制御する方法であって、

ＵＥの一つをノードに正常に登録する場合に、前記ＵＥのいずれかから公開鍵を受信し、

正常な登録への応答として、他のＵＥの公開鍵を、前記ＵＥのいずれかに、送信し、

公開鍵は、ダイレクト通信のために少なくとも要求を確認するために、各ＵＥのために使用される方法。

【０１４９】

（付記３３）

サーバの動作を制御する方法であって、

ＵＥが相互に近接し、互いにダイレクト通信を行うことが許可されている場合、ＵＥの公開鍵を格納し、公開鍵は、ダイレクト通信をサポートするノードにより登録され、

ノードに格納されている公開鍵を送信することで、ノードからの要求に応じ、

公開鍵は、少なくともダイレクト通信のための要求を確認するために、各ＵＥのために使用される。

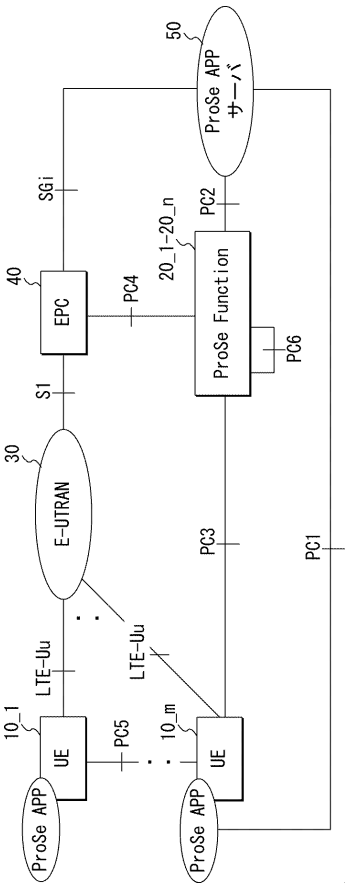
【０１５０】

この出願は、２０１３年１０月３０日に出願された日本出願特願２０１３－２２５２００及び２０１３年１０月３１日に出願された日本出願特願２０１３－２２６６８１を基礎とする優先権を主張し、その開示の全てをここに取り込む。

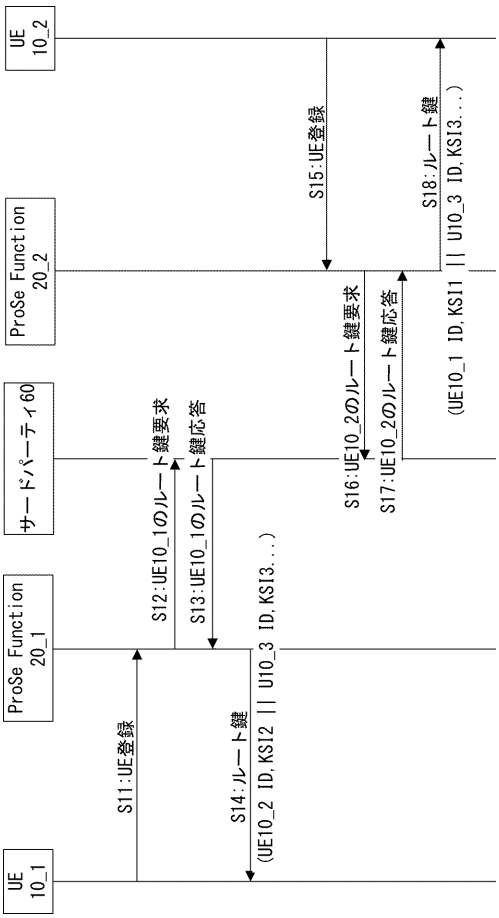
【符号の説明】

【０１５１】
１０、１０＿１－１０＿ｍ、１１０、１１０＿１－１１０＿ｍ　ＵＥ
１１、２１、１２４　取得部
１２　配布部
２０、２０＿１－２０＿ｎ、１２０、１２０＿１－１２０＿ｎ　ＰｒｏＳｅ　Ｆｕｎｃｔｉｏｎ
２２　分配部
２３　指示部
３０、１３０　Ｅ－ＵＴＲＡＮ
４０、１４０　ＥＰＣ
５０、１５０　ＰｒｏＳｅＡＰＰサーバ
６０、１６０　サードパーティ（サーバ）
６１、１６１　記憶部
６２、１６２　応答部
１１１　登録／検索部
１１２　検証部
１２１　受信部
１２２　伝送部
１２３　登録部

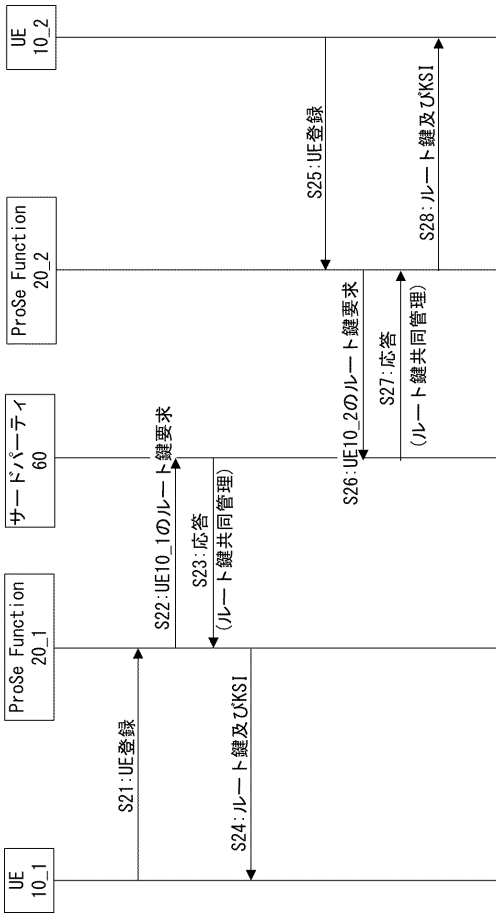
【図１】



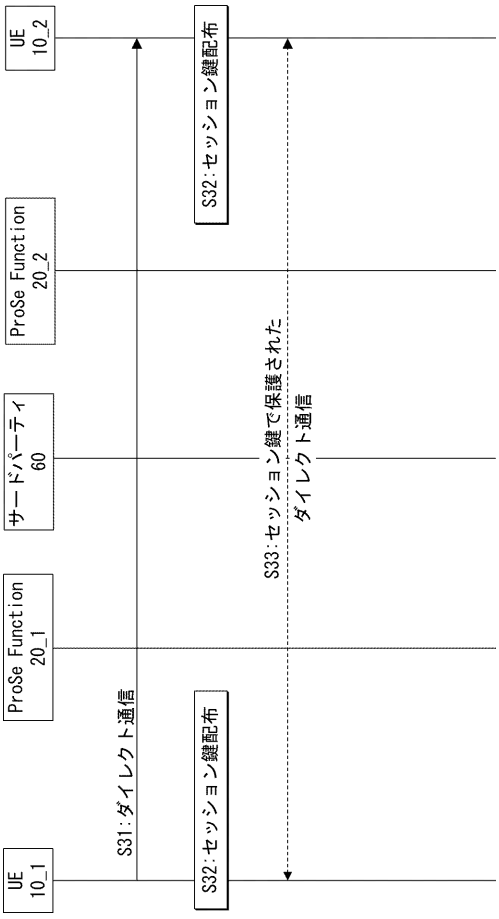
【図２】



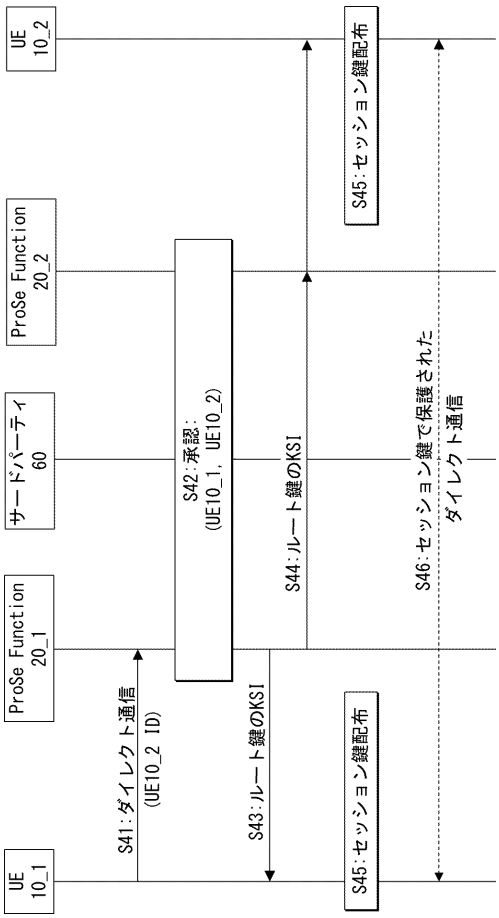
【図３】


UE 10_2
ProSe Function 20_2
サードパーティ 60
ProSe Function 20_1
UE 10_1
S21:UE登録
S22:UE10_1のルート鍵要求
S23:応答
(ルート鍵共同管理)
S24:ルート鍵及びKSI
S25:UE登録
S26:UE10_2のルート鍵要求
S27:応答
(ルート鍵共同管理)
S28:ルート鍵及びKSI

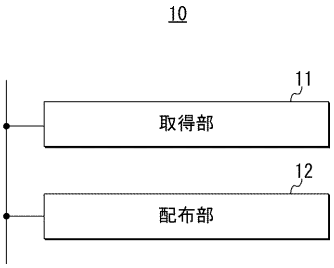
【図４】


UE 10_2
ProSe Function 20_2
サードパーティ 60
ProSe Function 20_1
UE 10_1
S31:ダイレクト通信
S32:セッション鍵配布
S32:セッション鍵配布
S33:セッション鍵で保護された
ダイレクト通信

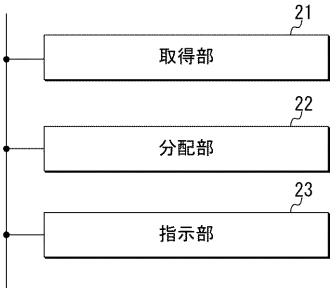
【図５】


UE 10_2
ProSe Function 20_2
サードパーティ 60
ProSe Function 20_1
UE 10_1
S41:ダイレクト通信
(UE10_2 ID)
S42:承認:
(UE10_1, UE10_2)
S43:ルート鍵のKSI
S44:ルート鍵のKSI
S45:セッション鍵配布
S45:セッション鍵配布
S46:セッション鍵で保護された
ダイレクト通信

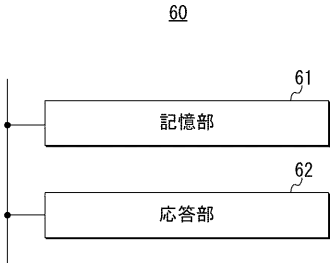
【図６】


10
11
取得部
12
配布部

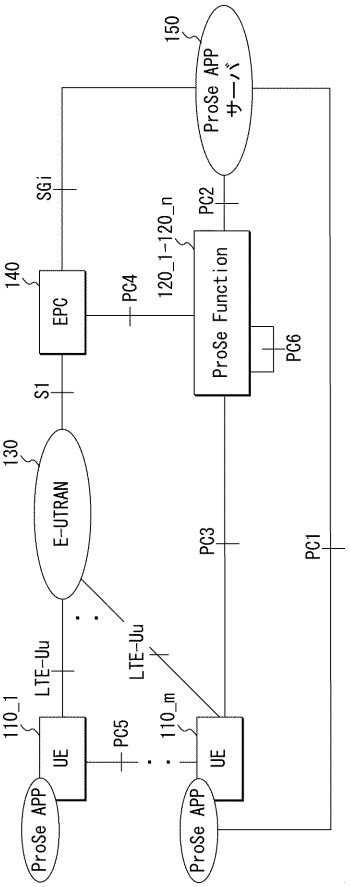
【図７】


20
21
取得部
22
分配部
23
指示部

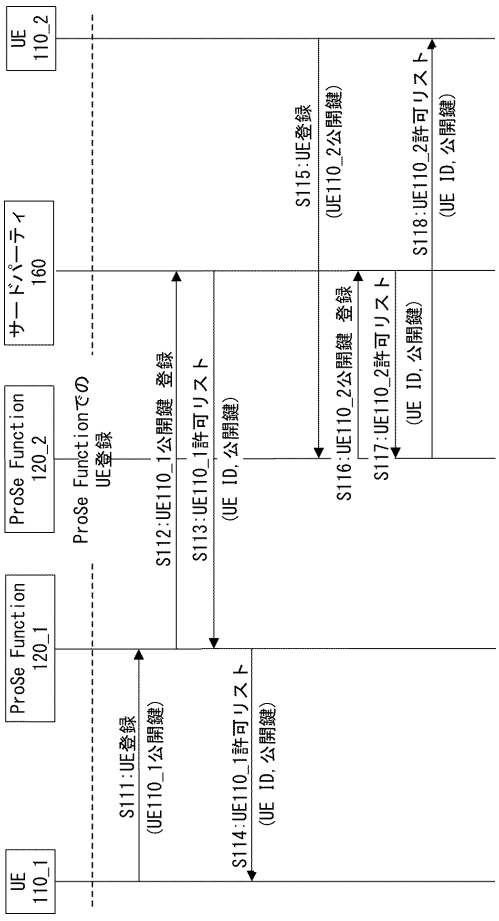
【図８】


60
61
記憶部
62
応答部

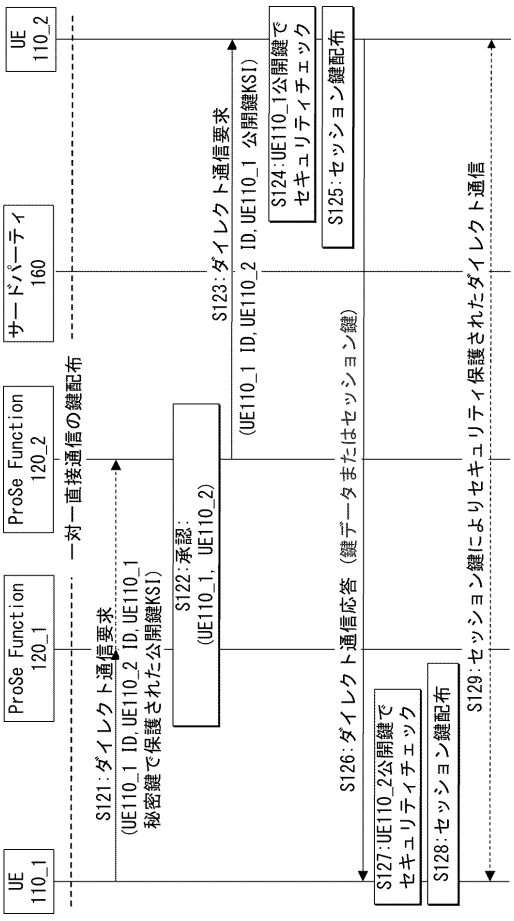
【図９】


150
ProSe APP サーバ
SGi
PC2
120_1-120_n
ProSe Function
PC6
140
EPC
PC4
S1
130
E-UTRAN
PC3
PC1
LTE-Uu
LTE-Uu
110_1
UE
PC5
110_m
UE
ProSe APP
ProSe APP

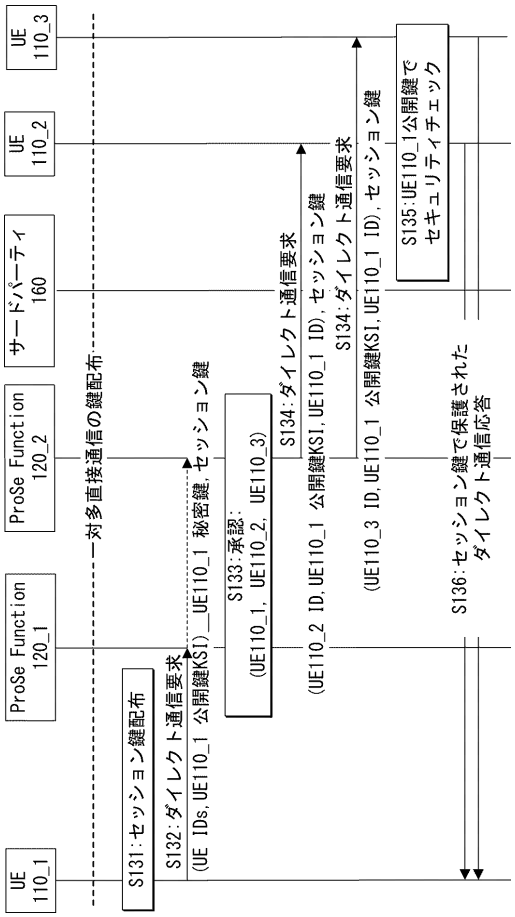
【図１０】


UE 110_1
ProSe Function 120_1
ProSe Function 120_2
サードパーティ 160
UE 110_2
ProSe Functionでの UE登録
S111:UE登録 (UE110_1公開鍵)
S112:UE110_1公開鍵 登録
S113:UE110_1許可リスト (UE ID, 公開鍵)
S114:UE110_1許可リスト (UE ID, 公開鍵)
S115:UE登録 (UE110_2公開鍵)
S116:UE110_2公開鍵 登録
S117:UE110_2許可リスト (UE ID, 公開鍵)
S118:UE110_2許可リスト (UE ID, 公開鍵)

【図１１】

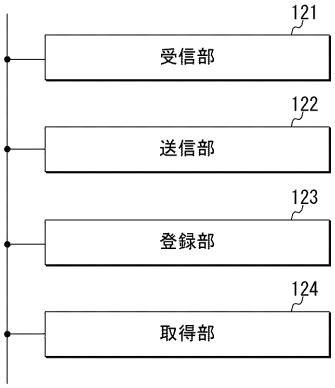

UE 110_1
ProSe Function 120_1
ProSe Function 120_2
サードパーティ 160
UE 110_2
一対一直接通信の鍵配布
S121:ダイレクト通信要求 (UE110_1 ID, UE110_2 ID, UE110_1 秘密鍵で保護された公開鍵(KSI))
S122:承認: (UE110_1, UE110_2)
S123:ダイレクト通信要求 (UE110_1 ID, UE110_2 ID, UE110_1 公開鍵(KSI))
S124:UE110_1公開鍵で セキュリティチェック
S125:セッション鍵配布
S126:ダイレクト通信応答 (鍵データまたはセッション鍵)
S127:UE110_2公開鍵で セキュリティチェック
S128:セッション鍵配布
S129:セッション鍵によりセキュリティ保護されたダイレクト通信

【図１２】

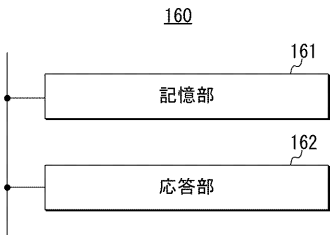


【図１３】

【図１４】



【図１５】



フロントページの続き

前置審査

(56)参考文献 特開２０１２－１３４７１０（ＪＰ，Ａ）
特開２０１０－２２６３３６（ＪＰ，Ａ）
特開２００４－３２８０９３（ＪＰ，Ａ）
国際公開第２０１３／１１８０９６（WO，Ａ１）
米国特許出願公開第２０１０／０２５７２５１（ＵＳ，Ａ１）
米国特許出願公開第２００６／０１５０２４１（ＵＳ，Ａ１）
米国特許出願公開第２０１０／０３２９４６５（ＵＳ，Ａ１）
Technical Specification Group Services and System AspectsStudy on security issues to support Proximity Services (Release 12)[online], 3GPP TSG-SA WG3#72 S3-130882, インターネット<URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_72_Qingdao/Docs/S3-130882.zip>, ２０１３年 7月１２日, ｐｐ. １－２１
Telecom Italia, Solution DX for network controlled ProSe discovery[online], 3GPP TSG-SA WG2#99 S2-133809, インターネット<URL:http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_99_Xiamen/Docs/S2-133809.zip>, ２０１３年 9月２７日, ｐｐ. １－１２

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｈ０４Ｍ ３／４２
Ｈ０４Ｗ １２／０４
Ｈ０４Ｗ ９２／１８