(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7298718号
(P7298718)

(45)発行日　令和5年6月27日(2023.6.27)

(24)登録日　令和5年6月19日(2023.6.19)

(51)国際特許分類		FI		
H04W 12/06 (2021.01)		H04W	12/06	
H04W 8/18 (2009.01)		H04W	8/18	
H04W 88/06 (2009.01)		H04W	88/06	
H04W 12/45 (2021.01)		H04W	12/45	
H04W 48/16 (2009.01)		H04W	48/16	131

請求項の数　10　（全35頁）

(21)出願番号　特願2021-572688(P2021-572688)
(86)(22)出願日　令和2年5月26日(2020.5.26)
(65)公表番号　特表2022-536125(P2022-536125A)
(43)公表日　令和4年8月12日(2022.8.12)
(86)国際出願番号　PCT/JP2020/020690
(87)国際公開番号　WO2020/250664
(87)国際公開日　令和2年12月17日(2020.12.17)
審査請求日　令和3年12月7日(2021.12.7)
(31)優先権主張番号　201941023422
(32)優先日　令和1年6月13日(2019.6.13)
(33)優先権主張国・地域又は機関
インド(IN)
前置審査

(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　サシ ニベディャ パラムバス
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　ラジェンドラン ロヒニ
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　吉澤 敬人
ドイツ連邦共和国、６９１１５ ハイデルベルク、クアフェアステンアンラーゲ３６、エヌイーシー ヨーロッパ リミテ

最終頁に続く

(54)【発明の名称】　ユーザ機器、方法、及びプログラム

(57)【特許請求の範囲】

【請求項１】

ユーザ機器（ＵＥ）であって、

少なくとも１つのプロセッサと、

前記少なくとも１つのプロセッサと動作可能に結合された少なくとも１つのメモリと、を備え、

前記少なくとも１つのプロセッサは、

ノーマルネットワークオペレーション用の認証を実行するために使用される第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションと、

ＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行するために使用される第２のＵＳＩＭアプリケーションと、を備え、

前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、

前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含み、

前記プロセッサは、登録要求メッセージを前記ノーマルネットワークと前記ＮＰＮに１つずつ送信することによって登録手順を実行し、前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションの両方をそれぞれ登録するように構成され、

前記プロセッサは、さらに、前記ユーザ機器がメインでチューンするプライマリネットワークを管理するローカルコンフィグレーションを有するように構成され、
前記ローカルコンフィグレーションは、所定のユーザアプリケーションによって上書きされる、
ユーザ機器。
【請求項２】
前記第１のセキュリティクレデンシャルのセットは、第１のパーマネントキー、前記ノーマルネットワークオペレーション用に割り当てられた第１のＰＬＭＮ（Ｐｕｂｌｉｃ Ｌａｎｄ Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋ）ＩＤ、および第１のＩＭＳＩ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｍｏｂｉｌｅ Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｉｄｅｎｔｉｔｙ）を含み、
前記第２のセキュリティクレデンシャルのセットは、第２のパーマネントキー、ＩＯＰＳ（Ｉｓｏｌａｔｅｄ ＥＵＴＲＡＮ Ｏｐｅｒａｔｉｏｎ ｆｏｒ Ｐｕｂｌｉｃ Ｓａｆｅｔｙ）ネットワークオペレーション用に割り当てられた第２のＰＬＭＮ ＩＤ、および第２のＩＭＳＩを含む、
請求項１に記載のユーザ機器。
【請求項３】
前記第１のセキュリティクレデンシャルのセットは、他のローミングネットワーク用のＰＬＭＮ ＩＤを含み、
前記第２のセキュリティクレデンシャルのセットは、前記ＮＰＮに専用である、
請求項２に記載のユーザ機器。
【請求項４】
前記プロセッサは、存在する全てのＵＳＩＭ ＡＩＤ（Ａｐｐｌｉｃａｔｉｏｎ ＩＤｅｎｔｉｔｙ）の第３のストレージを備え、
前記第３のストレージは、前記第１のＵＳＩＭアプリケーションの第１のＡＩＤと前記第２のＵＳＩＭアプリケーションの第２のＡＩＤを含む、
請求項１から３のいずれか一項に記載のユーザ機器。
【請求項５】
前記プロセッサは、存在する全てのＵＳＩＭ ＡＩＤ（Ａｐｐｌｉｃａｔｉｏｎ ＩＤｅｎｔｉｔｙ）の第３のストレージを備え、
前記第３のストレージは、前記第１のＵＳＩＭアプリケーションの第１のＡＩＤと前記第２のＵＳＩＭアプリケーションの第２のＡＩＤを含み、
前記プロセッサは、
前記第１のＡＩＤのための前記第１のＵＳＩＭアプリケーションをアクティベートし、前記第１のＡＩＤにリンクされた前記第１のＰＬＭＮ ＩＤを保存し、
前記第２のＡＩＤのための前記第２のＵＳＩＭアプリケーションをアクティベートし、前記第２のＡＩＤにリンクされた前記第２のＰＬＭＮ ＩＤを保存する、
ように構成される、請求項２、または、３に記載のユーザ機器。
【請求項６】
前記プロセッサは、
前記第１のＰＬＭＮ ＩＤまたは前記第２のＰＬＭＮ ＩＤの一方を使用して、ネットワークへのアタッチを試み、
前記第１のＰＬＭＮ ＩＤまたは前記第２のＰＬＭＮ ＩＤの前記一方が現在アクティブなＵＳＩＭアプリケーションと一致しない場合は、現在アクティブなＵＳＩＭアプリケーションを非アクティベートし、
前記第１のＰＬＭＮ ＩＤと前記第２のＰＬＭＮ ＩＤの他方に対応する別のＵＳＩＭアプリケーションをアクティベートする、
ように構成される、請求項２、３、または、５に記載のユーザ機器。
【請求項７】
前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションは同じネットワークにアソシエートされ、

前記ユーザ機器は、複数のＮＰＮにアクセスするようにサブスクライブされる、
請求項１から６のいずれか一項に記載のユーザ機器。
【請求項８】
前記プロセッサは、
前記第１のＵＳＩＭアプリケーションまたは前記第２のＵＳＩＭアプリケーションの一方が前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションの他方よりも優先される優先順位を有し、
前記優先順位に基づいて、ノーマル基地局とスタンドアロンＮＰＮ基地局のどちらにチューンするかを決定する、
ように構成される、請求項１から７のいずれか一項に記載のユーザ機器。
【請求項９】
ユーザ機器（ＵＥ）のための方法であって、
第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションを使用してノーマルネットワークオペレーション用の認証を実行し、
第２のＵＳＩＭアプリケーションを使用してＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行し、
前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、
前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含み、
前記方法は、登録要求メッセージを前記ノーマルネットワークと前記ＮＰＮに１つずつ送信することによって登録手順を実行し、前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションの両方をそれぞれ登録し、
前記ユーザ機器は、前記ユーザ機器がメインでチューンするプライマリネットワークを管理するローカルコンフィグレーションを有し、
前記ローカルコンフィグレーションは、所定のユーザアプリケーションによって上書きされる、
方法。
【請求項１０】
ユーザ機器（ＵＥ）のための方法をコンピュータに実行させるプログラムであって、
前記方法は、
第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションを使用してノーマルネットワークオペレーション用の認証を実行し、
第２のＵＳＩＭアプリケーションを使用してＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行し、
前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、
前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含み、
前記方法は、登録要求メッセージを前記ノーマルネットワークと前記ＮＰＮに１つずつ送信することによって登録手順を実行し、前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションの両方をそれぞれ登録し、
前記ユーザ機器は、前記ユーザ機器がメインでチューンするプライマリネットワークを管理するローカルコンフィグレーションを有し、
前記ローカルコンフィグレーションは、所定のユーザアプリケーションによって上書きされる、

プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、非パブリックネットワークのためのクレデンシャルストレージ及びクレデンシャルの選択に関する。
【背景技術】
【０００２】
５Ｇシステムは、物理的および仮想的な非パブリックネットワークの両方が可能なＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）をサポートする。３ＧＰＰ ＴＳ ２２．２６１（非特許文献３）で示されているさまざまな展開の可能性では、「具体的には、完全にスタンドアロンのネットワークとして展開されるか、ＰＬＭＮによってホストされるか、ＰＬＭＮのスライスとして提供される可能性がある」と述べられている。３ＧＰＰ ＳＡ２の検討は完了しており、多くのソリューションでは、ＵＥが複数のＮＰＮへのサブスクリプション関連データを保持できると想定される。３ＧＰＰ ＳＡ３では、サブスクリプション識別子は常にＵＳＩＭに保存されることが定義されている。一方、これはＮＰＮでは厳密には必要ない場合がある。ＮＰＮサービスがＵＳＩＭを発行したＰＬＭＮによって提供されている場合、ＮＰＮの標準化された部分がクレデンシャルストレージのためにＵＳＩＭ（または組み込みＳＩＭ－ｅＵＩＣＣ）を使用する可能性がある。ＵＥは、ＵＳＩＭを有するＭＥとして定義され、ＵＳＩＭには１つのサブスクリプションのクレデンシャルが含まれる。ＮＰＮでは、１つのＵＥに複数のサブスクリプションが存在することは、対処する必要のある新しい側面である。
【０００３】
したがって、本開示は、ＮＰＮに接続する場合にＵＥが複数のサブスクリプションを処理する方法に関する。各サブスクリプション関連データは、各ＵＳＩＭまたはｅＵＳＩＭに保存でき、ＭＥは、マルチＳＩＭ ＵＥ（ｍｕｌｔｉ－ＳＩＭ ＵＥ）デバイスとしても知られる複数のＵＳＩＭ（ｍｕｌｔｉｐｌｅ ＵＳＩＭ）とインターワーク可能である。複数のサブスクリプション関連データは、ＵＳＩＭまたはｅＵＳＩＭに保存できる。
【先行技術文献】
【非特許文献】
【０００４】
【文献】３ＧＰＰ ＴＲ ２１．９０５,“Ｖｏｃａｂｕｌａｒｙ ｆｏｒ ３ＧＰＰ Ｓｐｅｃｉｆｉｃａｔｉｏｎｓ”,Ｖ１５．０．０(２０１８－０３)
３ＧＰＰ ＴＳ ３３．５０１,“Ｓｅｃｕｒｉｔｙ ａｒｃｈｉｔｅｃｔｕｒｅ ａｎｄ ｐｒｏｃｅｄｕｒｅｓ ｆｏｒ ５Ｇ ｓｙｓｔｅｍ”,Ｖ１５．２．０(２０１８－０９)
３ＧＰＰ ＴＳ ２２．２６１,“Ｓｅｒｖｉｃｅ ｒｅｑｕｉｒｅｍｅｎｔｓ ｆｏｒ ｔｈｅ ５Ｇ ｓｙｓｔｅｍ”,Ｖ１６．５．０(２０１８－０９)
３ＧＰＰ ＴＲ ２３．７３４,“Ｓｔｕｄｙ ｏｎ ５ＧＳ Ｅｎｈａｎｃｅｄ ｓｕｐｐｏｒｔ ｏｆ Ｖｅｒｔｉｃａｌ ａｎｄ ＬＡＮ Ｓｅｒｖｉｃｅｓ”,Ｖ１．０．０(２０１８－１２)
３ＧＰＰ ＴＳ ３３．４０１,“３ＧＰＰ Ｓｙｓｔｅｍ Ａｒｃｈｉｔｅｃｔｕｒｅ Ｅｖｏｌｕｔｉｏｎ (ＳＡＥ); Ｓｅｃｕｒｉｔｙ ａｒｃｈｉｔｅｃｔｕｒｅ”,Ｖ１５．７．０(２０１９－０３),Ｒｅｌ－１５
３ＧＰＰ ＴＲ ３３．８９７,“Ｓｔｕｄｙ ｏｎ ｉｓｏｌａｔｅｄ Ｅｖｏｌｖｅｄ Ｕｎｉｖｅｒｓａｌ Ｔｅｒｒｅｓｔｒｉａｌ Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ (Ｅ－ＵＴＲＡＮ) ｏｐｅｒａｔｉｏｎ ｆｏｒ ｐｕｂｌｉｃ ｓａｆｅｔｙ”,Ｖ１３．１．０(２０１６－０３),Ｒｅｌ－１３
３ＧＰＰ ＴＳ ３１．１０２,“Ｃｈａｒａｃｔｅｒｉｓｔｉｃｓ ｏｆ ｔｈｅ Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ (ＵＳＩＭ) ａｐｐｌｉｃａｔｉｏｎ”,Ｖ１５．５．０(２０１９－０３),Ｒｅｌ－１５
３ＧＰＰ ＴＳ ３１．１０１,“ＵＩＣＣ－ｔｅｒｍｉｎａｌ ｉｎｔｅｒｆａｃｅ; Ｐｈｙ

sical and Logical characteristics”,V15.1.0(2018-10),Rel-15
3GPP TR 33.819,“Study on security enhancement of 5GS for vertical and LAN services”,V0.3.0(2019-03),Rel-16
3GPP TS 23.501,“System Architecture of 5G System”,V16.0.2(2019-04),Rel-16
RFC 7542,“The Network Access Identifier”(2015-05)
3GPP TS 23.003,“Numbering, Addressing and Identification”,V15.6.0(2018-12),Rel-15
3GPP TS 23.401,“General Packet Radio Service(GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network(E-UTRAN) access”,V16.2.0(2019-03),Rel-16

【発明の概要】
【発明が解決しようとする課題】
【０００５】
メインの問題提示：
クレデンシャルストレージ：
－ＵＥのクレデンシャルストレージは、ＵＥのサブスクリプションクレデンシャルを安全に保存するＵＳＩＭまたはｅＵＳＩＭに配置される。
－ＮＰＮでは、サブスクリプションの数を１つのＵＥのために１より多くすることができ、オペレータのサブスクリプションと特定のＮＰＮサブスクリプションを含めることができる。
－しかし、いつでもアクティブにできるのは１つのＵＳＩＭまたはｅＵＳＩＭのみであり、異なるＮＰＮサブスクリプションのためにクレデンシャルを使用したい場合、ＵＥはＵＳＩＭを切り替える必要がある。
【０００６】
クレデンシャルストレージの切り替え：
関連技術では、ＵＥがアクティブなクレデンシャルストレージまたはＵＳＩＭを切り替えることができるＩＯＰＳ（Ｉｓｏｌａｔｅｄ Ｏｐｅｒａｔｉｏｎｓ ｆｏｒ Ｐｕｂｌｉｃ Ｓａｆｅｔｙ）のためのセキュリティメカニズムが存在する。しかし、このメカニズムは２つのＵＳＩＭでのみ動作し、それ以上では動作しない。例えば、ＮＰＮがＰＬＭＮによって提供されている場合、１つ以上のＮＰＮが同じＰＬＭＮ ＩＤを共有できるため、このメカニズムでは、ＰＬＭＮ ＩＤを使用して、ＮＰＮでは動作しないＵＳＩＭを切り替える。したがって、複数のＮＰＮサブスクリプションを有するＵＥは、ＮＰＮサブスクリプション間を切り替え可能とする必要がある。
【０００７】
さらに、３ＧＰＰ ＴＳ ２３．５０１（非特許文献１０）によれば、ＵＥは、ＮＧ－ＲＡＮがブロードキャストするブロードキャストシステム情報内のネットワーク識別子（Ｎｅｔｗｏｒｋ ｉｄｅｎｔｉｆｉｅｒ：ＮＩＤ）情報をリッスンし、どのＮＰＮサブスクリプションを選択するかを決定することができる。しかし、規格で定義されている明確なＭＥメカニズムは存在しない。
【０００８】
サブの問題提示１：
－複数のＮＰＮが同じＰＬＭＮ ＩＤを有する可能性があり、ＵＥを複数のＮＰＮに同時に接続できるという事実がある場合、ＵＥはＮＰＮへの認証のために正しいクレデンシャルセットまたはＵＳＩＭ（またはｅＵＳＩＭ）をどのように選択できるか。
【０００９】

サブの問題提示２：
　ＵＥのために複数のサブスクリプション関連データがある場合に、これらのサブスクリプションのコールイベントが同時に発生すると、ＵＥはどのように応答するか：
　－ＵＥによって提供される複数のサブスクリプションの間には適切な区別が必要である。つまり、ＵＥがＵＳＩＭ－１サブスクリプションとＵＳＩＭ－２サブスクリプションを有する場合、要求が送信されるサブスクリプションのために対応する応答を受信する必要がある。
【００１０】
　この問題は、ＵＥがネットワークにアタッチされ、特定のサービスを持つスライスにアタッチされている場合に適用される。スライスがＮＰＮ用であるとすると、両方のネットワーク上のイベントを処理する必要がある。
【００１１】
サブの問題提示３：
　複数のＮＰＮサブスクリプションクレデンシャルストレージ
　－非パブリックネットワークに接続するときにＵＥのために複数のサブスクリプションがある場合、クレデンシャル、非パブリックネットワークにアソシエートされたＮＩＤ、およびその他のサブスクリプション関連データをネットワークのどこかに保存する必要がある。ＵＤＭが適切なストレージの場所であるかどうかは不明である。
　－クレデンシャル、非パブリックネットワークにアソシエートされたＮＩＤ、およびその他のサブスクリプション関連データがネットワークの他の場所に保存されている場合、これらの情報がどのように取得され、ネットワーク内のどの要素によって取得されるかが問題となる。
【００１２】
　上記の全てにおいて、クレデンシャルは通常、ロングターム識別子（ｌｏｎｇ ｔｅｒｍ ｉｄｅｎｔｉｆｉｅｒ）とロングタームキー（ｌｏｎｇ ｔｅｒｍ ｋｅｙ）の組み合わせを意味する。例えば、ＩＭＳＩと秘密鍵を合わせてクレデンシャルと呼ぶ。同様に、公開鍵と識別子で構成される証明書（ｃｅｒｔｉｆｉｃａｔｅ）もクレデンシャルとすることができる。クレデンシャルの他の例には、ユーザ名とパスワード、ＱＲコード（登録商標）、共有秘密鍵、公開鍵、ホームネットワーク公開鍵、ＮＰＮネットワーク公開鍵などが含まれる。また、場合によっては、クレデンシャルが複数のデバイスで共有される場合に、グループクレデンシャルが使用でき、認証を実行する個々のデバイスではなく、グループのために参照できる。
【００１３】
　これら全てのタイプのクレデンシャルは、ＭＥまたはＵＩＣＣに保存できる。それらがＵＩＣＣまたはｅＵＩＣＣに保存されている場合、標準的なストレージは、ＵＳＩＭまたはｅＵＳＩＭを使用するためのものである。
【００１４】
　上記の問題に鑑みて、本開示は、様々な問題のうちの少なくとも１つを解決するための解決策を提供することを目的とする。
【課題を解決するための手段】
【００１５】
　１つの開示に係るユーザ機器（ＵＥ）は、少なくとも１つのプロセッサと、前記少なくとも１つのプロセッサと動作可能に結合された少なくとも１つのメモリと、を備える。前記少なくとも１つのプロセッサは、ノーマルネットワークオペレーション用の認証を実行するために使用される第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションと、ＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行するために使用される第２のＵＳＩＭアプリケーションと、を備える。前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、前記第２のＵＳＩＭアプリケーション

は、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含む。

【００１６】

１つの開示に係るネットワークシステムは、ユーザ機器（ＵＥ）とコアネットワークとを備える。前記ユーザ機器は、少なくとも１つのプロセッサと、前記少なくとも１つのプロセッサと動作可能に結合された少なくとも１つのメモリと、を備える。前記少なくとも１つのプロセッサは、ノーマルネットワークオペレーション用の認証を実行するために使用される第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションと、ＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行するために使用される第２のＵＳＩＭアプリケーションと、を備える。前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含む。

【００１７】

１つの開示に係るユーザ機器（ＵＥ）のための方法は、第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションを使用してノーマルネットワークオペレーション用の認証を実行し、第２のＵＳＩＭアプリケーションを使用してＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行する。前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含む。

【図面の簡単な説明】

【００１８】

【図１】図１は、第１の態様に係るＵＳＩＭアプリケーションがアクティベートされた場合の動作を示している。

【図２】図２は、第１の態様に係る別のＵＳＩＭアプリケーションがアクティベートされた場合の動作を示している。

【図３】図３は、第１の態様に係る両方のＵＳＩＭアプリケーションがアクティベートされた場合の動作を示している。

【図４】図４は、第３の態様に係る非スタンドアロンＮＰＮアクセスクレデンシャルを有するｅＵＩＣＣの概略構成を示している。

【図５】図５は、第３の態様に係るスタンドアロンＮＰＮアクセスクレデンシャルを有するｅＵＩＣＣの概略構成を示している。

【図６】図６は、ＵＥの概略的なブロック図を示している。

【図７】図７は、（Ｒ）ＡＮの概略的なブロック図を示している。

【図８】図８は、コアネットワークノードの概略的なブロック図を示している。

【発明を実施するための形態】

【００１９】

１．略語

本明細書の目的のため、３ＧＰＰ ＴＲ ２１．９０５（非特許文献１）および以下に記載されている略語が適用される。本明細書で定義されている略語は、もしあれば３ＧＰＰ ＴＲ ２１．９０５（非特許文献１）における同じ略語の定義よりも優先される。

５ＧＣ　　５Ｇ Ｃｏｒｅ Ｎｅｔｗｏｒｋ

５ＧＳ　　５Ｇ Ｓｙｓｔｅｍ

５Ｇ－ＡＮ　　５Ｇ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ

５Ｇ－ＧＵＴＩ　５Ｇ Ｇｌｏｂａｌｌｙ Ｕｎｉｑｕｅ Ｔｅｍｐｏｒａｒｙ Ｉｄｅｎ

tifier
5GS－TMSI 5G S－Temporary Mobile Subscription Identifier
AMF Access and Mobility Management Function
AN Access Node
AID Application Identifier
AS Access Stratum
AUSF Authentication Server Function
CP Control Plane
CM Connection Management
CAG Closed Access Group
DL Downlink
DN Data Network
DNAI DN Access Identifier
DNN Data Network Name
EPS Evolved Packet System
EPC Evolved Packet Core
FQDN Fully Qualified Domain Name
GPSI Generic Public Subscription Identifier
GUAMI Globally Unique AMF Identifier
HR Home Routed(roaming)
IMSI International Mobile Subscription Identity
IOPS Isolated EUTRAN Operation for Public Safety
I－RNTI I－Radio Network Temporary Identifier
KDF Key Derivation Function
LADN Local Area Data Network
LBO Local Break Out(roaming)
LMF Location Management Function
LRF Location Retrieval Function
MAC Medium Access Control
MME Mobility Management Entity
N3IWF Non－3GPP Inter Working Function
NAI Network Access Identifier
NAS Non－Access Stratum
NEF Network Exposure Function
NF Network Function
NG－RAN NextGenerationRadioAccessNetwork
NID Network identifier
NPN Non－Public Network
NPN ID Non－Public Network Identifier
なお、本開示におけるＮＰＮＩＤは、ＴＳ ２３．５０１（非特許文献１０）におけるＮＩＤと等しい。
NR New Radio
NRF Network Repository Function
NSI ID Network Slice Instance Identifier

ＮＳＳＡＩ　Ｎｅｔｗｏｒｋ Ｓｌｉｃｅ Ｓｅｌｅｃｔｉｏｎ Ａｓｓｉｓｔａｎｃｅ Ｉｎｆｏｒｍａｔｉｏｎ
ＮＳＳＦ　Ｎｅｔｗｏｒｋ Ｓｌｉｃｅ Ｓｅｌｅｃｔｉｏｎ Ｆｕｎｃｔｉｏｎ
ＮＳＳＰ　Ｎｅｔｗｏｒｋ Ｓｌｉｃｅ Ｓｅｌｅｃｔｉｏｎ Ｐｏｌｉｃｙ
ＰＣＦ　Ｐｏｌｉｃｙ Ｃｏｎｔｒｏｌ Ｆｕｎｃｔｉｏｎ
ＰＥＩ　Ｐｅｒｍａｎｅｎｔ Ｅｑｕｉｐｍｅｎｔ Ｉｄｅｎｔｉｆｉｅｒ
ＰＥＲ　Ｐａｃｋｅｔ Ｅｒｒｏｒ Ｒａｔｅ
ＰＬＭＮ　Ｐｕｂｌｉｃ Ｌａｎｄ Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋ
ＰＳＡ　ＰＤＵ Ｓｅｓｓｉｏｎ Ａｎｃｈｏｒ
ＱＦＩ　ＱｏＳ Ｆｌｏｗ Ｉｄｅｎｔｉｆｉｅｒ
ＱｏＥ　Ｑｕａｌｉｔｙ ｏｆ Ｅｘｐｅｒｉｅｎｃｅ
(Ｒ)ＡＮ　(Ｒａｄｉｏ) Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ
ＲＲＣ　Ｒａｄｉｏ Ｒｅｓｏｕｒｃｅ Ｃｏｎｔｒｏｌ
ＳＡ ＮＲ　Ｓｔａｎｄａｌｏｎｅ Ｎｅｗ Ｒａｄｉｏ
ＳＢＡ　Ｓｅｒｖｉｃｅ Ｂａｓｅｄ Ａｒｃｈｉｔｅｃｔｕｒｅ
ＳＢＩ　Ｓｅｒｖｉｃｅ Ｂａｓｅｄ Ｉｎｔｅｒｆａｃｅ
ＳＤ　Ｓｌｉｃｅ Ｄｉｆｆｅｒｅｎｔｉａｔｏｒ
ＳＥＡＦ　ＳＥＣＵＲＩＴＹ Ａｎｃｈｏｒ Ｆｕｎｃｔｉｏｎａｌｉｔｙ
ＳＩＢ　Ｓｙｓｔｅｍ Ｉｎｆｏｒｍａｔｉｏｎ Ｂｒｏａｄｃａｓｔ
ＳＩＤＦ　Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｉｄｅｎｔｉｆｉｅｒ Ｄｅ－ｃｏｎｃｅａｌｉｎｇ Ｆｕｎｃｔｉｏｎ
ＳＭＦ　Ｓｅｓｓｉｏｎ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ
Ｓ－ＮＳＳＡＩ　Ｓｉｎｇｌｅ Ｎｅｔｗｏｒｋ Ｓｌｉｃｅ Ｓｅｌｅｃｔｉｏｎ Ａｓｓｉｓｔａｎｃｅ Ｉｎｆｏｒｍａｔｉｏｎ
ＳＰ　Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ
ＳＳＣ　Ｓｅｓｓｉｏｎ ａｎｄ Ｓｅｒｖｉｃｅ Ｃｏｎｔｉｎｕｉｔｙ
ＳＳＴ　Ｓｌｉｃｅ／Ｓｅｒｖｉｃｅ Ｔｙｐｅ
ＳＵＣＩ　Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｃｏｎｃｅａｌｅｄ Ｉｄｅｎｔｉｆｉｅｒ
ＳＵＰＩ　Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｐｅｒｍａｎｅｎｔ Ｉｄｅｎｔｉｆｉｅｒ
ＵＩＣＣ　Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ
ＵＳＩＭ　Ｕｓｅｒ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ
ＵＤＳＦ　Ｕｎｓｔｒｕｃｔｕｒｅｄ Ｄａｔａ Ｓｔｏｒａｇｅ Ｆｕｎｃｔｉｏｎ
ＵＤＭ　Ｕｎｉｆｉｅｄ Ｄａｔａ Ｍａｎａｇｅｍｅｎｔ
ＵＰＦ　Ｕｓｅｒ Ｐｌａｎｅ Ｆｕｎｃｔｉｏｎ
ＵＤＲ　Ｕｎｉｆｉｅｄ Ｄａｔａ Ｒｅｐｏｓｉｔｏｒｙ
ＵＲＳＰ　ＵＥ Ｒｏｕｔｅ Ｓｅｌｅｃｔｉｏｎ Ｐｏｌｉｃｙ

【００２０】

２．定義

本明細書の目的のため、ＴＲ ２１．９０５（非特許文献１）および以下に記載されている用語と定義が適用される。本明細書で定義されている用語は、もしあればＴＲ ２１．９０５（非特許文献１）における同じ用語の定義よりも優先される。

【００２１】

３．関連技術に関する情報

－ＴＳ ２３．５０１（非特許文献１０）“Ｓｙｓｔｅｍ ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ｔｈｅ ５Ｇ”の関連技術：

－非パブリックネットワークのサポート－ＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）は、非パブリックの使用のためにデプロイされた５ＧＳである（ＴＳ ２２．２６１（非特許文献３）参照）。ＮＰＮは、次のようにデプロイできる：

－ＳＮＰＮ（Ｓｔａｎｄ－ａｌｏｎｅ Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）、つまりＮＰＮオペレータによって運用され、ＰＬＭＮによって提供されるネットワーク機能

に依存しない、または、
　－パブリックネットワーク統合ＮＰＮ（Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ Ｉｎｔｅｇｒａｔｅｄ ＮＰＮ）、つまり、ＰＬＭＮのサポートでデプロイされた非パブリックネットワーク。
【００２２】
　－パブリックネットワーク統合ＮＰＮは、ネットワークスライシングを使用し有効にできる（ＴＳ ２３．５０１（非特許文献１０）の付録Ｄで定義される）。認可（ａｕｔｈｏｒｉｚｅ）されていないＵＥがパブリックネットワーク統合ＮＰＮにアクセスしようとすることを防ぐために、ＣＡＧ（Ｃｌｏｓｅｄ Ａｃｃｅｓｓ Ｇｒｏｕｐ）機能を追加で使用できる。
【００２３】
　－スタンドアロン非パブリックネットワークの識別子（Ｉｄｅｎｔｉｆｉｅｒｓ ｆｏｒ Ｓｔａｎｄ－ａｌｏｎｅ ｎｏｎ－ｐｕｂｌｉｃ ｎｅｔｗｏｒｋｓ）
　－ＰＬＭＮ ＩＤとＮＩＤ（Ｎｅｔｗｏｒｋ ｉｄｅｎｔｉｆｉｅｒ）の組み合わせにより、ＳＮＰＮが識別される。
　－ＳＮＰＮのために使用されるＰＬＭＮ ＩＤは、ユニークである必要はない。プライベートネットワークで使用するために予約されているＰＬＭＮ ＩＤは、例えばＩＴＵによって割り当てられたＭＣＣ（ｍｏｂｉｌｅ ｃｏｕｎｔｒｙ ｃｏｄｅ）９９９に基づいており、非パブリックネットワークのために使用できる。
【００２４】
　－ＮＩＤ（Ｎｅｔｗｏｒｋ Ｉｄｅｎｔｉｆｉｅｒ）は、次の２つの割り当てモデルをサポートする必要がある：
　－ローカルに管理されるＮＩＤは、デプロイメントタイムにＳＮＰＮによって個別に選択されると想定される（したがって、ユニークではない場合がある）
　－ユニバーサルに管理されるＮＩＤは、グローバルにユニークであると想定される。
【００２５】
　－オプションのヒューマンリーダブルネットワークネーム（ｈｕｍａｎ－ｒｅａｄａｂｌｅ ｎｅｔｗｏｒｋ ｎａｍｅ）は、手動のＳＮＰＮ選択の間にＳＮＰＮを識別することを助ける。
【００２６】
　－ブロードキャストシステム情報（Ｂｒｏａｄｃａｓｔ ｓｙｓｔｅｍ ｉｎｆｏｒｍａｔｉｏｎ）からのサポート
【００２７】
　－ＳＮＰＮへのアクセスを提供するＮＧ－ＲＡＮノードは、次の情報をブロードキャストする：
　－１つまたは複数のＰＬＭＮ ＩＤ
　－ＮＧ－ＲＡＮがアクセスを提供する非パブリックネットワークを識別するＰＬＭＮ ＩＤごとのＮＩＤのリスト
　－オプションで、ＮＩＤごとのヒューマンリーダブルネットワークネーム。
【００２８】
　－ＳＮＰＮのためのＵＥコンフィグレーションとサブスクリプションアスペクト
【００２９】
　－ＳＮＰＮ－ｅｎａｂｌｅｄ ＵＥ（ＳＮＰＮ可能ＵＥ）は、ＰＬＭＮ ＩＤとＮＩＤの組み合わせによって識別される１つまたは複数のＳＮＰＮのためのサブスクライバー識別子（ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｆｉｅｒ）とクレデンシャルで構成（ｃｏｎｆｉｇｕｒｅ）される。
【００３０】
　－ＳＮＰＮのサブスクライバーは、ＴＳ ２３．００３（非特許文献１２）２８．２．２節で定義されているＮＡＩ ＲＦＣ ７５４２（非特許文献１１）ベースのユーザ識別子（ｕｓｅｒ ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）を使用して、ＮＡＩ（Ｎｅｔｗｏｒｋ Ａｃｃ

ｅｓｓ Ｉｄｅｎｔｉｆｉｅｒ）の形式をとるネットワーク特有の識別子（ｎｅｔｗｏｒｋ－ｓｐｅｃｉｆｉｃ ｉｄｅｎｔｉｆｉｅｒ）を含むＳＵＰＩによって識別される。ＮＡＩのレルム（ｒｅａｌｍ）部分には、ＳＮＰＮのＮＩＤが含まれる場合がある。

【００３１】

－ＳＮＰＮ－ｅｎａｂｌｅｄ ＵＥは、ＳＮＰＮアクセスモードをサポートする。ＵＥがＳＮＰＮアクセスモードで動作するように設定されている場合、ＵＥはＵｕを介したＳＮＰＮ（ＳＮＰＮ ｏｖｅｒ Ｕｕ）のみを選択及び登録する。

【００３２】

－ＵＥがＳＮＰＮアクセスモードで動作するように設定されていない場合、ＳＮＰＮ－ｅｎａｂｌｅｄ（ＳＮＰＮ可能）であっても、ＵＥはＳＮＰＮを選択及び登録しない。

【００３３】

－ＳＮＰＮアクセスモードにおけるネットワーク選択

－ＳＮＰＮアクセスモードで動作しているＵＥは、ブロードキャストシステム情報から利用可能なＰＬＭＮ ＩＤと利用可能なＮＩＤのリストを読み取り、ネットワーク選択の間にそれらを考慮する。

－自動ネットワーク選択の場合、ＵＥは、ＵＥがＳＵＰＩとクレデンシャルを有するＰＬＭＮ ＩＤとＮＩＤによって識別される利用可能なＳＮＰＮを選択し登録を試みる。ＵＥがＳＵＰＩとクレデンシャルを有する複数のＳＮＰＮが利用可能な場合、ＳＮＰＮを選択し登録を試みるための優先順位は、ＵＥの実装に基づいている。

－手動ネットワーク選択の場合、ＳＮＰＮアクセスモードで動作するＵＥは、ＵＥがＳＵＰＩとクレデンシャルを有する利用可能なＳＮＰＮのＮＩＤのリスト及び関連するヒューマンリーダブルネーム（利用可能な場合）をユーザに提供する。

－ＵＥがＳＮＰＮへの初期登録（Ｉｎｉｔｉａｌ Ｒｅｇｉｓｔｒａｔｉｏｎ）を実行する場合、ＵＥは選択されたＮＩＤ及び対応するＰＬＭＮ ＩＤをＮＧ－ＲＡＮにインジケートする必要がある。ＮＧ－ＲＡＮは、選択されたＰＬＭＮ ＩＤ及びＮＩＤをＡＭＦに通知する必要がある。

【００３４】

－ネットワークアクセス制御

－ＵＥがＰＬＭＮ ＩＤ及びローカルに管理されたＮＩＤにより識別されるＳＮＰＮで登録（ｒｅｇｉｓｔｒａｔｉｏｎ）またはサービス要求手順（ｓｅｒｖｉｃｅ ｒｅｑｕｅｓｔ ｐｒｏｃｅｄｕｒｅ）を実行し、ＵＥのためのサブスクリプションがない場合、ＡＭＦは、ＵＥが同じＳＮＰＮを自動的に選択及び登録することを一時的に防ぐため、適切な原因コード（ｃａｕｓｅ ｃｏｄｅ）を用いてＵＥを拒否（ｒｅｊｅｃｔ）する必要がある。

－ＵＥがＰＬＭＮ ＩＤ及びユニバーサルに管理されたＮＩＤにより識別されるＳＮＰＮで登録またはサービス要求手順を実行し、ＵＥのサブスクリプションがない場合、ＡＭＦは、ＵＥが同じＳＮＰＮを自動的に選択及び登録することを永続的に防ぐため、適切な原因コードを用いてＵＥを拒否する必要がある。

【００３５】

－ネットワークの輻輳／過負荷の場合に認可（ａｕｔｈｏｒｉｚｅ）されたＵＥのためのＳＮＰＮへのアクセスを防ぐために、ユニファイドアクセス制御情報（ｕｎｉｆｉｅｄ ａｃｃｅｓｓ ｃｏｎｔｒｏｌ ｉｎｆｏｒｍａｔｉｏｎ）は、非パブリックネットワークごとに構成（ｃｏｎｆｉｇｕｒｅ）される（つまり、ＵＥが所定の非パブリックネットワークのために有するサブスクリプション情報の一部として）。

【００３６】

－ＳＮＰＮアクセスモードにおけるセル（再）選択（Ｃｅｌｌ （ｒｅ－）ｓｅｌｅｃｔｉｏｎ）

－ＳＮＰＮアクセスモードで動作しているＵＥは、選択したＳＮＰＮのＰＬＭＮ ＩＤ及びＮＩＤの両方をブロードキャストするセル及びネットワークのみを選択する。

【００３７】

－スタンドアロン非パブリックネットワークを介したＰＬＭＮサービスへのアクセス
－ＰＬＭＮサービスへアクセスするために、ＳＮＰＮに正常に登録されたＳＮＰＮアクセスモードのＵＥは、ＴＳ ２３．５０１（非特許文献１０）の４．２．８節で指定されているものと同じアーキテクチャ原理に従い、（そのＰＬＭＮのクレデンシャルを使用して）ＰＬＭＮを用いてＳＮＰＮを介して別の登録を実行でき、ＳＮＰＮは「信頼できない非３ＧＰＰアクセス（Ｕｎｔｒｕｓｔｅｄ ｎｏｎ－３ＧＰＰ ａｃｃｅｓｓ）」の役割を果たす。

【００３８】

－ＰＬＭＮを介したスタンドアロン非パブリックネットワークサービスへのアクセス
－ＳＮＰＮサービスへアクセスするために、ＰＬＭＮに正常に登録されたＵＥは、ＴＳ ２３．５０１（非特許文献１０）の４．２．８節で指定されているものと同じアーキテクチャ原理に従って、（そのＳＮＰＮのクレデンシャルを使用して）ＳＮＰＮを用いてＰＬＭＮを介して別の登録を実行でき、ＰＬＭＮは「信頼できない非３ＧＰＰアクセス（Ｕｎｔｒｕｓｔｅｄ ｎｏｎ－３ＧＰＰ ａｃｃｅｓｓ）」の役割を果たす。

【００３９】

－パブリックネットワーク統合ＮＰＮ（Ｐｕｂｌｉｃ ｎｅｔｗｏｒｋ ｉｎｔｅｇｒａｔｅｄ ＮＰＮ）
－パブリックネットワーク統合ＮＰＮは、例えば、専用のＤＮＮを使用するか、または、ＮＰＮのために割り当てられた１つ（または複数）のネットワークスライスインスタンスを使用することにより、ＰＬＭＮを介して利用可能になるＮＰＮである。ＴＳ ２３．５０１（非特許文献１０）の５．１５節に記載されているように、既存のネットワークスライシング機能が適用される。ＮＰＮがＰＬＭＮを介して利用可能になると、ＵＥはＰＬＭＮのサブスクリプションを有する。
－ＴＳ ２３．５０１（非特許文献１０）の付録Ｄは、ＰＬＭＮのネットワークスライスとして非パブリックネットワークをサポートする際に考慮すべき追加の考慮事項を提供する。
－ネットワークスライシングでは、ＵＥがＮＰＮのために割り当てられたネットワークスライスの使用が許可されていないエリアで、ＵＥがネットワークにアクセスしようとする可能性を防ぐことができないため、オプションで、ネットワークスライシングに加えてクローズドアクセスグループ（Ｃｌｏｓｅｄ Ａｃｃｅｓｓ Ｇｒｏｕｐ）を使用して、アクセス制御を適用できる。
－クローズドアクセスグループは、ＣＡＧにアソシエートされた１つ以上のＣＡＧセルへのアクセスを許可されているサブスクライバーのグループを識別する。
－ＣＡＧは、アソシエートされたセルを介してＮＰＮにアクセスすることを許可されていないＵＥが、アソシエートされたセルを自動的に選択及びアクセスすることを防ぐため、パブリックネットワーク統合ＮＰＮに使用される。
－識別（ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）には以下が必要である。
－ＣＡＧは、ＰＬＭＮ ＩＤのスコープ内でユニークとなるＣＡＧ識別子（ＣＡＧ Ｉｄｅｎｔｉｆｉｅｒ）によって識別される。
－ＣＡＧセルは、ＰＬＭＮごとに１つまたは複数のＣＡＧ識別子をブロードキャストする。

【００４０】

－ＴＲ２３．７３４（非特許文献４）“Ｓｔｕｄｙ ｏｎ ５ＧＳ Ｅｎｈａｎｃｅｄ ｓｕｐｐｏｒｔ ｏｆ Ｖｅｒｔｉｃａｌ ａｎｄ ＬＡＮ Ｓｅｒｖｉｃｅｓ”の関連技術：
－ソリューション＃１：非パブリックネットワークの識別、選択、およびアクセス制御では、次のように述べられている：
－ＵＥは、ＰＬＭＮ ＩＤとＮＰＮ ＩＤに基づいてセル選択を行う。
－ＵＥは、サブスクリプションのあるＮＰＮにのみ登録を試み、複数のサブスクリプションと複数のネットワークが利用可能な場合に優先メカニズム（ｐｒｉｏｒｉｔｙ ｍｅｃｈａｎｉｓｍ）を使用する必要がある。

【００４１】
－ソリューション＃２：クローズドアクセスグループでは次のように述べられている：
－サブスクリプションは、ＵＥがアクセスしたいくつかのＣＡＧ ＩＤを含む必要がある。
【００４２】
－ソリューション＃３：非パブリックネットワークの識別、選択、およびアクセス制御では次のように述べられている：
－複数のＮＰＮが１つのＮＰＮ ＩＤを共有するシナリオを示す。サブスクリプションはＳＰ ＩＤによって識別される。
－ＲＡＮは、ＰＬＭＮ ＩＤ、ＮＰＮ ＩＤ、およびＳＰ ＩＤをブロードキャストする。
－Ｅｑｕｉｖａｌｅｎｔ Ｈｏｍｅ ＰＬＭＮリストを使用してＳＰ－ＩＤを選択する。
【００４３】
－ソリューション＃５：アクセス制御のソリューションでは次のように述べられている：
－アクセス制御を実施できるように、サブスクリプションを識別する必要性がある。
－非パブリックネットワークサブスクリプションを識別する方法を記述する明確なテキスト要素が必要であると述べてられている。
【００４４】
－ＴＳ ３３．４０１（非特許文献５）の関連技術：
－ＩＯＰＳ（Ｉｓｏｌａｔｅｄ Ｅ－ＵＴＲＡＮ Ｏｐｅｒａｔｉｏｎ ｆｏｒ Ｐｕｂｌｉｃ Ｓａｆｅｔｙ）は、バックホール通信が失われた後、ＩＯＰＳ－ｃａｐａｂｌｅ ｅＮＢ（または接続されたＩＯＰＳ－ｃａｐａｂｌｅ ｅＮＢのセット）を介して、パブリックセーフティユーザのための通信のレベルを維持する機能を提供する。
【００４５】
－Ｉｓｏｌａｔｅｄ Ｅ－ＵＴＲＡＮオペレーションモード（Ｉｓｏｌａｔｅｄ Ｅ－ＵＴＲＡＮ ｍｏｄｅ ｏｆ ｏｐｅｒａｔｉｏｎ）は、Ｎｏｍａｄｉｃ ＥＰＳデプロイメントの形成、つまり、１つ以上のスタンドアロンＩＯＰＳ－ｃａｐａｂｌｅ ｅＮＢのデプロイメント、バックホール通信なしのサービング無線アクセスネットワークの作成、およびローカルＩＰ接続とノーマルＥＰＳインフラストラクチャが利用できない場合のパブリックセーフティユーザへのサービスの提供に適用できる。
【００４６】
－パブリックセーフティネットワークオペレータは、ＰＬＭＮアイデンティティ（ＰＬＭＮ Ｉｄｅｎｔｉｔｙ）を、ＩＯＰＳモードで動作しているときにｅＮＢによってシステム情報（Ｓｙｓｔｅｍ Ｉｎｆｏｒｍａｔｉｏｎ）でブロードキャストされるＩＯＰＳオペレーションモードに専用とする。認可（ａｕｔｈｏｒｉｚｅ）されたＩＯＰＳ－ｅｎａｂｌｅｄ ＵＥ（ＩＯＰＳ可能ＵＥ）のみが、ＩＯＰＳ ＰＬＭＮとしてインジケートされるＰＬＭＮにアクセスできる。
【００４７】
－この仕様で説明されているセキュリティ機能及び手順を使用して、ローカルＥＰＣアプローチに基づいて、ＩＯＰＳネットワークのためのセキュリティソリューションを提供できる。
【００４８】
－ＩＯＰＳのサポートがノーマルオペレーションのセキュリティを損なうことがないようにするために、ＩＯＰＳモードで動作している場合、ＡＫＡ手順（３ＧＰＰ ＴＳ ３３．４０１（非特許文献５）の６．１項で説明されている）は、ＩＯＰＳ－ｅｎａｂｌｅｄ ＵＥに存在するＵＩＣＣでのＩＯＰＳオペレーションのための専用のＵＳＩＭアプリケーションと、（ローカルＥＰＣに含まれる）ローカルＨＳＳとの間で実行される。同じことが、バックホール通信が失われ、ＩＯＰＳ－ｅｎａｂｌｅｄ ＵＥの集団に対してＩｓｏｌａｔｅｄ Ｅ－ＵＴＲＡＮオペレーションをサポートするためにＩＯＰＳ－ｃａｐａｂｌｅ ｅＮＢが移行した場合にも適用される。
【００４９】

－ＩＯＰＳオペレーションのための専用のＵＳＩＭアプリケーションは、「ノーマル」オペレーションのために使用されるものとは区別された別のセキュリティクレデンシャルのセットを使用する。これらのクレデンシャルは、ＩＯＰＳオペレーションの開始前にローカルＨＳＳとＵＩＣＣにおいて構成（ｃｏｎｆｉｇｕｒｅ）される。

【００５０】

－ＩＯＰＳ－ｅｎａｂｌｅｄ ＵＥにおいて、ＩＯＰＳオペレーションのための専用のＵＳＩＭアプリケーションは、少なくとも次のものを含む区別されたセキュリティクレデンシャルのセットを有する：

－パーマネントキー（ｐｅｒｍａｎｅｎｔ ｋｅｙ）Ｋ（ＩＯＰＳオペレーションのためにユニークに割り当てられる）。

－ＩＯＰＳネットワークオペレーションのために割り当てられたＰＬＭＮアイデンティティ（ＰＬＭＮ ｉｄｅｎｔｉｔｙ）。

－ＩＭＳＩ（ＩＯＰＳオペレーションのためにユニークに割り当てられる）。

－１１または１５のアクセスクラスステータス（Ａｃｃｅｓｓ Ｃｌａｓｓ ｓｔａｔｕｓ）（地域／国の規制要件およびオペレータポリシーに従う）。

【００５１】

－これらのクレデンシャルは、パブリックセーフティ当局（Ｐｕｂｌｉｃ Ｓａｆｅｔｙ ａｕｔｈｏｒｉｔｙ）が、バックホール通信が失われた場合にＵＥにサービスを提供することを要求する、ＩＯＰＳオペレーションをサポートするローカルＥＰＣ内の全てのローカルＨＳＳで提供（ｐｒｏｖｉｓｉｏｎ）される。

【００５２】

－ローカルＨＳＳに設定されたＩＯＰＳネットワークセキュリティクレデンシャルのストレージは、ＩＯＰＳネットワークにおけるオペレーションのために認可（ａｕｔｈｏｒｉｚｅ）されたＵＥに対してのみ実行される。アドミニストレーティブプロビジョニングは、ローカルＥＰＣ内のローカルＨＳＳで全ての認可されたＵＥのためのセキュリティクレデンシャルを最新に維持するために使用される。更新は、「ノーマル」ネットワークにおけるＥＰＣとｅＮＢの間にすでに存在するセキュリティコンテキスト内で提供される。

【００５３】

－このソリューションは、ＩＯＰＳネットワークのための整合性と機密性を提供し、この仕様で定義されている手順との共通性を維持する。さらに、このアプローチは、３ＧＰＰ ＴＳ ２３．４０１（非特許文献１３）で定義されているＩＯＰＳのための実装および展開ガイドライン（ｔｈｅ ｉｍｐｌｅｍｅｎｔａｔｉｏｎ ａｎｄ ｄｅｐｌｏｙｍｅｎｔ ｇｕｉｄｅｌｉｎｅｓ ｆｏｒ ＩＯＰＳ）に沿っている。

【００５４】

－ＴＲ ３３．８１９（非特許文献９）の関連技術：

－重要な問題（Ｋｅｙ Ｉｓｓｕｅ）＃２．３：ＮＰＮおよびＰＬＭＮを用いた認証（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）及び認可（ａｕｔｈｏｒｉｚａｔｉｏｎ）のための独立したクレデンシャル

－この重要な問題は、ＵＥがＮＰＮを介してＰＬＭＮから提供されるサービスにアクセスして取得する必要がある場合、またはその逆の場合の認証及び認可のためのクレデンシャルのサポートに関連する。

－３ＧＰＰ ＴＲ ２３．７３４（非特許文献４）で締結されたソリューションにより、非パブリックネットワークを介してＰＬＭＮサービスにアクセスするために、ＵＥは非パブリックネットワークを介してＩＰ接続（ＩＰ ｃｏｎｎｅｃｔｉｖｉｔｙ）を取得し、ＰＬＭＮによって提供されるＮ３ＩＷＦを検出し、Ｎ３ＩＷＦを介してＰＬＭＮへの接続を確立する。ＵＥが従う、またはその逆の同様の手順では、ＰＬＭＮを介して非パブリックネットワークサービスにアクセスする。ＰＬＭＮ及び非パブリックネットワークは、ＵＥが同時に接続される異なるネットワークである。

－ＰＬＭＮネットワークの場合、５Ｇ ＡＫＡおよびＥＡＰ－ＡＫＡ’がサポートされる認証方法である。５Ｇシステムを使用する非パブリックネットワーク（プライベートネ

ットワーク）の場合、サポートされる認証方法は、５Ｇ ＡＫＡ、ＥＡＰ－ＡＫＡ'、および３ＧＰＰ ＴＳ ３３．５０１（非特許文献２）のＥＡＰフレームワーク内の追加方法である。ＵＥおよび非パブリックネットワークは、ＮＰＮオペレータポリシーに基づいて、プライマリ認証のために使用される（ＥＡＰフレームワークを介した）認証方法に対応するセキュリティクレデンシャルを所有している必要がある。

【００５５】

４． 提案される態様

４．１ 第１の態様

－ＵＥは、ＵＳＩＭアプリケーションを含むＵＩＣＣを有するＭＥとして定義され、ＵＳＩＭアプリケーションは１つのサブスクリプションのためのクレデンシャルを含む。非パブリックネットワーク（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）では、ＵＥに複数のサブスクリプションが存在することが、対処する必要のある新しい側面である。

【００５６】

－本開示では、非パブリックネットワークサブスクリプションのための、専用のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）またはＮＳＩＭ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションを備えることが提案される。これは、ＮＰＮクレデンシャルが管理され、オペレータクレデンシャルとは区別されたストレージに保存（ｓｔｏｒｅ）されることを意味する。場合によっては、例えば、ＵＥがプライベートデプロイメントにのみ接続することを意図しており、パブリックデプロイメントに決して接続することがない場合など、オペレータクレデンシャルが存在しないことがある。

【００５７】

－３ＧＰＰ ＴＳ ２３．５０１（非特許文献１０）によると、非パブリックネットワークへのアクセスを提供するために、次の情報がｇＮＢによってシステム情報ブロック（Ｓｙｓｔｅｍ Ｉｎｆｏｒｍａｔｉｏｎ Ｂｌｏｃｋ）でブロードキャストされる：

－（プライベートネットワーク用にＩＴＵによって割り当てられた）ＭＣＣ ９９９と、非パブリックネットワークの一部としてネットワークを識別するために３ＧＰＰによって定義されたＭＮＣで構成される１つまたは複数のＰＬＭＮ ＩＤ。

－ＮＧ－ＲＡＮがアクセスを提供する非パブリックネットワークを識別するＰＬＭＮ ＩＤごとのＮＩＤのリスト。

【００５８】

－ＵＥにおけるＮＰＮクレデンシャルストレージ：

－ＵＥは複数のＮＰＮにサブスクライブできる。したがって、ＵＥに複数のＮＰＮクレデンシャルを保存する必要がある。本態様では、ＮＰＮクレデンシャルを保存するための組み込みＵＩＣＣ（ｅｍｂｅｄｄｅｄ ＵＩＣＣ：ｅＵＩＣＣ）を有することも提案される。組み込みＵＳＩＭ（ｅＵＩＣＣ）は、複数のプロファイルをダウンロードし保存できる。各プロファイルは、ＵＩＣＣにおける伝統的なＵＳＩＭアプリケーションに保存されているはずのオペレータとサブスクライバーのデータで構成される。

【００５９】

－ネットワーク及びＵＳＩＭ選択：

－ｇＮＢによってブロードキャストされたシステム情報（Ｓｙｓｔｅｍ ｉｎｆｏｒｍａｔｉｏｎ）で受信された情報に基づいて、ＵＥはＰＬＭＮごとのＮＰＮ－ＩＤのリストをブロードキャストするｇＮＢ間のネットワーク選択（ｎｅｔｗｏｒｋ ｓｅｌｅｃｔｉｏｎ）を実行する。

【００６０】

－ＵＥは、同じＮＰＮ－ＩＤをブロードキャストするｇＮＢ間のセル（再）選択（ｃｅｌｌ （ｒｅ－）ｓｅｌｅｃｔｉｏｎ）を実行する。

【００６１】

－ＵＥは、任意の特定の非パブリックネットワークに接続する必要がある場合に、適切なＵＳＩＭ／ＮＳＩＭアプリケーションをアクティベートする。ＵＥは、ＵＥがサブス

クライバー識別子（ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｆｉｅｒ）とクレデンシャルを有する非パブリックネットワークを、自動的に選択し登録を試みる。複数のＮＰＮサブスクリプションが存在する場合、つまりＵＥが複数の非パブリックネットワークにアクセスするためにサブスクライブされている場合、ＵＥは、ＴＳ ２３．５０１（非特許文献１０）５．３０．２．４節に記載されているように、非パブリックネットワークを選択し登録を試みるための優先順位に従う必要がある。

【００６２】

－単一のＩＭＳＩを複数の秘密鍵（ｓｅｃｒｅｔ ｋｅｙ）またはアルゴリズムに結び付ける（ｃｏｎｎｅｃｔ）ことはできないため、ＮＰＮ専用のＵＳＩＭ／ＮＳＩＭアプリケーションは、ＮＰＮ専用のＩＭＳＩ（ＮＰＮ ＩＤ）、ロングタームキー（Ｌｏｎｇ ｔｅｒｍ ｋｅｙ）（K_{NPN}）、アソシエートさているＰＬＭＮ ＩＤ、および結び付けられている認証アルゴリズムの１つのタイプを有してもよい。ＮＰＮクレデンシャルストレージは、ＮＰＮ ＩＤを公開鍵（ｐｕｂｌｉｃ ｋｅｙ）で暗号化するために、ＮＰＮ ＩＤに関連する公開鍵を保存してもよい。ただし、公開鍵は、ＭＥに保存してもよい。

【００６３】

－本態様では、ＳＵＣＩにおいて「ネットワークサブスクリプションタイプ（Ｎｅｔｗｏｒｋ Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｔｙｐｅ）」を追加することも提案される。ネットワークサブスクリプションタイプは、ＵＥ／ユーザが非パブリックネットワークまたはＰＬＭＮネットワークのサブスクリプションを有するかどうかを表示（ｄｅｎｏｔｅ）する。

１．このケースでＰＬＭＮがＮＰＮサービスを提供する場合、ＭＮＣはＰＬＭＮネットワークを表示してもよいが、サブスクリプションはＰＬＭＮによってホストされるＮＰＮ用となる。ＭＮＣのみでは、ネットワークにアソシエートされているＵＥのサブスクリプションタイプをインジケートするために十分ではない。

２．ＰＬＭＮとサブスクライブされている全てのＮＰＮの両方について、ＵＥが単一のＳＵＰＩを有している場合、ＮＰＮがＵＥのＰＬＭＮ特有のＳＵＰＩ（ＰＬＭＮ ｓｐｅｃｉｆｉｃ ＳＵＰＩ）を知る必要があり得るため、プライバシーの問題が生じる。

【００６４】

－また、ネットワークサブスクリプションタイプは、さまざまな非パブリックネットワークに関する識別情報（ｉｄｅｎｔｉｆｉｃａｔｉｏｎ ｉｎｆｏｒｍａｔｉｏｎ）を含む。したがって、ネットワークサブスクリプションタイプは、アクセス可能なＮＰＮネットワークを識別するためのパラメータとして使用できる。

【００６５】

－非パブリックネットワーク選択のために次の２つのオプションが可能である：

－オプション１：ＵＥが非パブリックネットワークへのアクセスを提供するためにｇＮＢからブロードキャストされたシステム情報ブロック（Ｓｙｓｔｅｍ Ｉｎｆｏｒｍａｔｉｏｎ Ｂｌｏｃｋ）を受信した場合、ＵＥはサブスクライバー識別子（ｓｕｂｓｃｒｉｂｅｒ ｉｄｅｎｔｉｆｉｅｒ）とクレデンシャルを受信した専用のＵＳＩＭアプリケーションをアクティベートしてもよい。これを行うために、ＵＥは、ＰＬＭＮ ＩＤとＮＰＮ ＩＤの組み合わせのリストと、複数のＮＰＮがある場合にアクティベートされる適切なＵＳＩＭ／ＮＳＩＭを保持する必要がある。ブロードキャストを受信すると、まず、ＵＥは、非パブリックネットワーク（ＭＣＣ ９９９）をインジケートするインジケータのためにＰＬＭＮ ＩＤを確認する；次に、ＵＥは、ｅＵＩＣＣをアクティベートする；最後に、ＵＥは、ＮＰＮ－ＩＤをｅＵＩＣＣにあるクレデンシャルのリストと比較し、特定のネットワークのために使用するクレデンシャルを選択する。１つのクレデンシャルのみがある場合、ＵＥの比較は単純なｔｒｕｅ／ｆａｌｓｅになり、その後、ＵＥはｅＵＩＣＣにおいてこのＮＰＮのクレデンシャルがある（ない）と判断してもよい。ＵＥが複数のＵＳＩＭ／ＮＳＩＭをＰＬＭＮ ＩＤとＮＰＮ ＩＤの組み合わせにアソシエートできると判断した場合、ＵＥは、識別された全てのＵＳＩＭ／ＮＳＩＭについて、ユーザアイデンティティ（ｕｓｅｒ ｉｄｅｎｔｉｔｙ）すなわちＳＵＰＩまたはＳＵＣＩを有する登録要求メッセージ（ｒｅｇｉｓｔｒａｔｉｏｎ ｒｅｑｕｅｓｔ ｍｅｓｓａｇｅ）を、非パブリックネッ

トワークへ１つずつ送信することによって、登録手順（ｒｅｇｉｓｔｒａｔｉｏｎ ｐｒｏｃｅｄｕｒｅ）を実行する。

【００６６】

－オプション２：ＮＰＮ－ｅｎａｂｌｅｄ ＵＥは、専用のＮＩＤと、ＮＰＮ専用のＵＳＩＭアプリケーション（ＮＳＩＭアプリケーション）で構成されるアソシエートされたＰＬＭＮ ＩＤを有する。手動で選択する場合、ＮＰＮ－ｅｎａｂｌｅｄ ＵＥは、利用可能なＮＩＤおよびアソシエートされたＰＬＭＮに関する情報を表示でき、複数のＮＰＮサブスクリプションがある場合にユーザが適切なＮＰＮ専用のＵＳＩＭアプリケーションをアクティベートすることを支援する。ユーザプリファレンスに応じて、ユーザはいつでも手動でＵＳＩＭアプリケーションの切り替えを実行できる。アクティベートされた専用のＮＰＮ ＵＳＩＭアプリケーションを有する、認可（ａｕｔｈｏｒｉｚｅ）されたＮＰＮ－ｅｎａｂｌｅｄ ＵＥが、ＮＰＮを選択した場合、ＮＰＮ－ｅｎａｂｌｅｄ ＵＥは、専用のＰＬＭＮ ＩＤを選択し、特定の非パブリックネットワークにアタッチし、ＴＲ ３３．８１９（非特許文献９）で指定されているセキュリティ手順とアクティブなＮＰＮ ＵＳＩＭアプリケーションからのセキュリティクレデンシャルを使用して認証される。

【００６７】

－ケースＩ：１つのＵＳＩＭのみがアクティブモードにできる場合

図１は、（ＰＬＭＮサービス用の）ＵＳＩＭアプリケーション１がアクティベートされた場合の動作を示している。図１に示されるように、ネットワークシステム１００は、ＵＥ１１０、ノーマルＢＳ１２０、スタンドアロンＮＰＮ１３０、および５Ｇコアネットワーク１４０を含む。ＵＥは、ＵＳＩＭアプリケーション１およびＵＳＩＭアプリケーション２を含む。ケースIでは、ＵＳＩＭアプリケーション１とＵＳＩＭアプリケーション２のうちの１つをアクティベートできる。図１では、ＵＳＩＭアプリケーション１がアクティベートされている。５Ｇコアネットワーク１４０は、ＵＤＭ１４１、ＮＰＮ ＵＤＭ１４２、および（複数のＮＰＮ ＩＤのための）クレデンシャルストア１４３を含む。

【００６８】

図１では、（ＰＬＭＮ専用の）ＵＳＩＭアプリケーション１を使用して、「ノーマル」ネットワークオペレーションのための認証（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を実行する。ＵＳＩＭアプリケーション１は、少なくとも次のものを含む：

－パーマネントキー（ｐｅｒｍａｎｅｎｔ ｋｅｙ）Ｋ１（Ｋ）

－「ノーマル」ネットワークオペレーションのために割り当てられたＰＬＭＮ ＩＤ１（ＰＬＭＮ ＩＤ）

－ＩＭＳＩ１（ＩＭＳＩ）

【００６９】

さらに、Ｋ１、ＰＬＭＮ ＩＤ１、およびＩＭＳＩ１は、５Ｇコアネットワーク１４０のＵＤＭ １４１で提供（ｐｒｏｖｉｓｉｏｎ）され、ＴＳ ３３．５０１（非特許文献２）で現在指定されているようにＵＥ１１０とネットワーク間の認証に使用される必要がある。

【００７０】

図２は、（ＮＰＮサービス用の）ＵＳＩＭアプリケーション２がアクティベートされた場合の動作を示している。

【００７１】

図２では、（ＮＰＮ専用の）ＵＳＩＭアプリケーション２を使用して、ＮＰＮのための認証を実行する。ＵＳＩＭアプリケーション２は、少なくとも次のものを含む：

－パーマネントキーＫ２（K_{NPN}）

－ＩＯＰＳネットワークオペレーションのために割り当てられたＰＬＭＮ ＩＤ２（$PLMN\ ID_{NPN}$）

－ＩＭＳＩ２（$IMSI_{NPN}$）

【００７２】

さらに、Ｋ２、ＰＬＭＮ ＩＤ２、およびＩＭＳＩ２は、ＮＰＮオペレーションをサポートするためにＮＰＮ ＵＤＭ１４２（ＵＤＭ ｃｌｏｕｄ）または外部クレデンシャルスト

ア１４３で提供される必要がある。
【００７３】
－ＵＳＩＭアプリケーション１は、「ノーマル」ネットワークオペレーションおよびその他のローミングネットワークのためのＰＬＭＮ ＩＤを含む。ＵＳＩＭアプリケーション２は、専用のＮＰＮ特有のクレデンシャル（ＮＰＮ－ｓｐｅｃｉｆｉｃ ｃｒｅｄｅｎｔｉａｌ）を含む。
【００７４】
－ＵＥ１１０が初期化され、ＵＩＣＣインタラクション（ｉｎｔｅｒａｃｔｉｏｎ）を有する場合、ＵＥ１１０は、存在する全てのＵＳＩＭ ＡＩＤ（Ａｐｐｌｉｃａｔｉｏｎ ＩＤｅｎｔｉｔｙ）のローカルストアを作成できる。
【００７５】
－各ＵＳＩＭ ＡＩＤについて、ＵＥ１１０は、次に、ＵＳＩＭアプリケーションをアクティベートし、各ＡＩＤにリンクされたＰＬＭＮアイデンティティを再びローカルに保存することができる。
【００７６】
－ＵＥ１１０がアタッチを試み、ＰＬＭＮ ＩＤが現在アクティブなＵＳＩＭアプリケーションと一致しない場合、ＵＥ１１０は現在のＵＳＩＭアプリケーションを非アクティベート（ｄｅ－ａｃｔｉｖａｔｅ）し、次に他のＵＳＩＭアプリケーションをアクティベートできる（ＰＬＭＮが他のＡＩＤのために保存されたＰＬＭＮと一致すると想定する）。
【００７７】
－ＵＳＩＭアプリケーション１とＵＳＩＭアプリケーション２の両方が同じネットワークオペレータにアソシエートされる。１つのＵＥは、複数のＮＰＮにアクセスするようにサブスクライブされてもよい。したがって、次のオプションを使用することを提案する：
－オプション１：５Ｇコアネットワーク１４０は、複数のＮＰＮクレデンシャルを保存（ｓｔｏｒｅ）および保持（ｍａｉｎｔａｉｎ）するために使用できる外部クレデンシャルストア１４３（ＵＤＭ ｃｌｏｕｄ）を保持できる。
－オプション２：各非パブリックネットワークは、ＮＰＮ関連のクレデンシャルのストレージのための自身専用のＮＰＮ ＵＤＭを有する。
【００７８】
－ＵＥ１１０が、図１および図２におけるノーマルＢＳおよびスタンドアロンＮＰＮの両方を同時にリッスン（ｌｉｓｔｅｎ）できる場合、ＵＥローカルコンフィグレーションは、ＵＳＩＭアプリケーションが他のＵＳＩＭアプリケーションよりも優先される優先順位を有してもよい。その優先順位に基づいて、ＵＥ１１０は、どのＲＡＮにチューン（ｔｕｎｅ）するかを決定してもよい。
【００７９】
－ケースＩＩ：両方のＵＳＩＭアプリケーションがアクティベートされる場合
ケースＩＩでは、ＵＳＩＭアプリケーション１とＵＳＩＭアプリケーション２の両方をアクティベートできる。図３は、両方のＵＳＩＭアプリケーションが同時にアクティベートされた場合の動作を示している。
【００８０】
－ノーマルネットワークオペレーション：ＵＥのＵＳＩＭアプリケーション１がノーマルオペレーションのためにアクティベートされ、非パブリックネットワークのための専用のＵＳＩＭアプリケーション２も同時にアクティベートされる。両方のＵＳＩＭアプリケーションは、それぞれのＵＤＭで構成（ｃｏｎｆｉｇｕｒｅ）されたセキュリティクレデンシャルのセットを含む。
【００８１】
－ＵＥ１１０が、図３におけるノーマルＢＳ１２０とスタンドアロンＮＰＮ１３０の両方を同時にリッスンできる場合、ＵＥ１１０は、ユーザアイデンティティすなわちＳＵＰＩまたはＳＵＣＩを有する登録要求メッセージを、ノーマルＢＳ１２０および非パブリックネットワークへ１つずつ送信することによって、登録手順を実行し、ＵＳＩＭアプリケ

ーション１とＵＳＩＭアプリケーション２の両方をそれぞれ登録する。このケースでは、単一のレシーバーＵＥ１１０は、ＵＥ１１０がメインでチューンするプライマリＲＡＮを管理するローカルコンフィグレーションを有する。いくつかのユーザアプリケーションは、そのローカルコンフィグレーションを上書きしてもよい。例えば、ＵＳＩＭアプリケーション２がＵＳＩＭアプリケーション１よりも優先度が高いためにＵＥ１１０がスタンドアロンＮＰＮ１３０にチューンする場合、ＵＳＩＭアプリケーション１におけるエマージェンシーコールアプリケーションは、ＵＥ１１０にノーマルＢＳ１２０へチューンするよう強制し、ＵＳＩＭアプリケーション１でエマージェンシーコールを進めることができる。これは、エマージェンシーコールがスタンドアロンＮＰＮ１３０でサポートされていない可能性があるために発生し得る。

【００８２】

４．２　第２の態様

本態様では、オペレータがＮＰＮとＰＬＭＮの両方のクレデンシャルを管理すると想定する。この目的のためにＩＯＰＳと同様のメカニズムを使用することを提案する。これにより、クレデンシャル管理が容易になり、ロバストネスを実現できる。解決すべき問題の１つは、このケースのＵＥがプライバシーの目的のために適切なホームネットワーク公開鍵を選択（ｐｉｃｋ）する方法と、ＵＥがＮＰＮアクセスのための追加の鍵を導出（ｄｅｒｉｖｅ）するかどうかを選択する方法である。

【００８３】

ここの前提では、ＵＥが１つのＵＳＩＭのみを有し、このＵＳＩＭが１つのクレデンシャルのみを含む。

【００８４】

ネットワークアーキテクチャは、ネットワークに２つのＵＤＭが含まれていることを意味するケースＩＩの図３のようになる。１つはＮＰＮに専用であり、もう１つはＰＬＭＮに専用である。ＰＬＭＮにおけるＵＤＭはメインＵＤＭであり、プライベートネットワークにおけるＵＤＭはスレーブＵＤＭである。

【００８５】

スレーブＵＤＭは次のように入力（ｐｏｐｕｌａｔｅ）される：

－スレーブＵＤＭは、メインＵＤＭから、プライベートネットワークへのアタッチが許可されているサブスクライバーのためのクレデンシャルを受信する。サブスクライバーごとに、スレーブＵＤＭはＩＭＳＩまたはＳＵＰＩと秘密鍵Ｋ'を受信する。Ｋ'は、次のような鍵分離メカニズム（ｋｅｙ ｓｅｐａｒａｔｉｏｎ ｍｅｃｈａｎｉｓｍ）を使用することにより、メインＵＤＭにおける秘密鍵Ｋから導出される：

－Ｋ'＝ＫＤＦ（Ｋ，ＮＰＮ ＩＤ）

【００８６】

ここで、ＫＤＦはＨＭＡＣ－ＳＨＡ２５６などの暗号学的ハッシュ関数（ｃｒｙｐｔｏｇｒａｐｈｉｃ ｈａｓｈ ｆｕｎｃｔｉｏｎ）であり、ＮＰＮ ＩＤは電波を介してブロードキャストされるＮＰＮの識別子とすることができる。このメカニズムは、ＴＳ ３３．５０１（非特許文献２）でｋｅｙ ｓｅｐａｒａｔｉｏｎ ｕｎｄｅｒ ＩＯＰＳとして知られている。

【００８７】

スレーブＵＤＭには、オンデマンドでクレデンシャルを入力してもよいし、事前に入力してもよい。

【００８８】

スレーブＵＤＭにおけるＳＩＤＦは、自身の公開鍵と秘密鍵のペアを含む。スレーブＵＤＭは、ＵＥ上のＵＳＩＭをこの公開鍵で更新できるようにするため、この公開鍵をメインＵＤＭに送信してもよい。スレーブＵＤＭは、ＮＰＮを識別できるようにするため、ＲＡＮで使用されるインジケータを受信する。このようなインジケータは、ＰＬＭＮ ＩＤ、アクセスクラス制限（Ａｃｃｅｓｓ Ｃｌａｓｓ ｂａｒｒｉｎｇ）、クローズドアクセスグループ（Ｃｌｏｓｅｄ Ａｃｃｅｓｓ Ｇｒｏｕｐ）、鍵分離インジケータ（ｋｅｙ ｓｅ

ｐａｒａｔｉｏｎ ｉｎｄｉｃａｔｏｒ）などを含む。
【００８９】
ＵＥは次のように構成（ｃｏｎｆｉｇｕｒｅ）される：
－ＵＥは、秘密鍵Ｋと、ＩＭＳＩまたはＳＵＰＩを有する。また、ＵＥは、「ｅｑｕｉｖａｌｅｎｔ ＰＬＭＮ ＩＤ」のリストも有する。このリストは、このサブスクリプションも有効なプライベートネットワークによって使用されるＰＬＭＮ ＩＤとＮＩＤを含む。このリストは、「鍵分離」インジケータを含んでもよい。これにより、ＵＥは、この特定のＰＬＭＮ ＩＤについて、鍵分離がＮＰＮアクセスに適用されていることを認識できる。このリストは、ネットワークが実際にＮＰＮである、またはネットワークが個別のストレージを有することを示すインジケータを含んでもよい。
【００９０】
－ＵＥは、ホームネットワーク公開鍵のストレージも有する。この鍵は、登録要求で送信される前にＩＭＳＩ／ＳＵＰＩを暗号化することにより、ＩＳＭＩをプライバシー保護するために使用される。暗号化されたＳＵＰＩは、ＴＳ ３３．５０１（非特許文献２）ではＳＵＣＩとも呼ばれる。ホームネットワーク公開鍵に加えて、ＵＥはネットワークから「ＮＰＮネットワーク公開鍵」も受信する。「ＮＰＮネットワーク公開鍵」は、ＵＥが「鍵分離」を適用するネットワークまたは「ＮＰＮ」としてインジケートされるネットワークを選択するたびに使用される。さらに、ＵＥは、鍵またはｅｑｕｉｖａｌｅｎｔ ＰＬＭＮ ＩＤと共に適切なＮＰＮ ＩＤを保存してもよい。これにより、ＵＥは、サブスクリプションを有するＮＰＮシステム情報ブロードキャスト（Ｓｙｓｔｅｍ Ｉｎｆｏｒｍａｔｉｏｎ Ｂｒｏａｄｃａｓｔ：ＳＩＢ）を受信するたびに、ストレージから正しい公開鍵を取得（ｒｅｔｒｉｅｖｅ）することができる。ＮＰＮネットワーク公開鍵と一緒に保存される別のパラメータは、ＮＰＮタイプオブアクセス（ＮＰＮ ｔｙｐｅ ｏｆ ａｃｃｅｓｓ）をインジケートするために公開ネットワークによって使用されるクローズドアクセスグループインジケータまたはアクセスクラス制限でもよい。
【００９１】
－クレデンシャルと公開鍵は、ＵＳＩＭ、ｅＵＳＩＭ、またはＭＥメモリに保存してもよい。
【００９２】
このケースにおける登録要求手順は次のように機能する：
－ＵＥが工場にあり、サブスクリプションのあるプライベートネットワークからＳＩＢを受信すると想定する。ＳＩＢは、アクセスクラス制限またはＣＡＧを含んでもよく、特定のパブリックネットワークのためのＰＬＭＮ ＩＤおよびＮＩＤを含んでもよい。また、ＳＩＢは、このネットワークのために鍵分離が使用されていることをインジケートするインジケータを含んでもよい。ＵＥは、ＳＩＢから関連情報（ＰＬＭＮ ＩＤやアクセスクラスなど）を読み取る。
【００９３】
－ＵＥは公開鍵ストレージを読み取り、ＳＩＢで受信した対応するＰＬＭＮ ＩＤまたはアクセスクラスまたは鍵分離インジケータを含むストレージから鍵を検索する。ＵＥは、正しい公開鍵を選択できるようにするため、対応するエレメントを検索する。
【００９４】
－公開鍵の選択の後、ＵＥはＳＵＰＩを公開鍵で暗号化し、暗号化されたＳＵＰＩ（ＳＵＣＩ）をｇＮＢへの登録要求メッセージに含める。
【００９５】
－ｇＮＢは、登録要求メッセージをスレーブＵＤＭに転送する。スレーブＵＤＭは、ＳＵＣＩを復号化してＳＵＰＩを取得し、ＵＥとの認証を開始（ｉｎｉｔｉａｔｅ）する。
【００９６】
ＵＥに適切な公開ネットワーク鍵がない場合が起こり得る。この問題を解決するために、ネットワークは暗号化されたＳＵＰＩの柔軟なルーティングを可能にする必要がある。そのためには、ストレージと上記の手順を次のように変更する必要がある：

【００９７】
－ＵＥはルーティングＩＤを保存し、ルーティングＩＤを各公開鍵にアソシエートする。このようなアソシエーションは、例えば、ルーティングＩＤ（またはルーティングＩＤへのポインタ）を各公開鍵と一緒に保存することによって実現してもよい。また、全てのルーティングＩＤが公開鍵にアソシエートされ、その逆も同様とするために、ルーティングＩＤと公開鍵のペアのリストを保持することにより実現してもよい。 また、ルーティングＩＤの代わりに公開鍵識別子（ｐｕｂｌｉｃ ｋｅｙ ｉｄｅｎｔｉｆｉｅｒ）を使用してもよい。
【００９８】
－ｅｑｕｉｖａｌｅｎｔ ＰＬＭＮ ＩＤのリストに、（例えば、鍵分離インジケータまたは明示的なＮＰＮインジケータを使用して）このネットワークがＮＰＮであることを示すインジケータが含まれている場合でも、ＵＥが特定のネットワークのための公開鍵を有していない場合はいつでも、ＵＥはデフォルトの公開鍵を使用し、登録要求メッセージでルーティングＩＤをオペレータのスレーブＵＤＭに設定する。
【００９９】
ＵＥは、暗号化されたＳＵＰＩとルーティングＩＤが設定された登録要求をオペレータのスレーブＵＤＭに送信し、ｇＮＢはそれをＡＭＦに転送する。ＡＭＦは、ルーティングＩＤに基づいてルーティングし、ＳＵＣＩをローカルＡＵＳＦ／ＵＤＭの代わりにオペレータのＡＵＳＦ／ＵＤＭに送信する。
【０１００】
４．３ 第３の態様
４．３．１ ＵＥ／ＭＥおよびネットワークにおけるＮＰＮクレデンシャルストレージ
－ＵＥがサブスクライブしている全ての非パブリックネットワークのためのユニークなクレデンシャルを保存する外部クレデンシャルストア（ＵＤＭ ｃｌｏｕｄ）インスタンスを有することが提案される。このストレージリポジトリは、ＵＤＭによりアクセス（ｒｅａｃｈ ｏｕｔ）され、要求を受信したクレデンシャルを取得（ｆｅｔｃｈ）できる。
【０１０１】
－この外部リポジトリはＮＰＮオーナーによってホストされ、ＮＰＮオーナーは複数のサブスクリプションを管理するアドミニストレータの役割が割り当てられてもよい。
【０１０２】
－ａｄｍｉｎ／ＮＰＮオーナーは、ユーザ／ＵＤＭに適切なサブスクリプションを割り当て、サブスクライブされたユーザによるクレデンシャルの使用をモニタしてもよい。
【０１０３】
－複数のサブスクライバーがサービスを要求しているときはいつでも、ＵＤＭは非パブリックネットワークへのＵＥの認証（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）と認可（ａｕｔｈｏｒｉｚａｔｉｏｎ）のために保存されたクレデンシャルを取得（ｒｅｔｒｉｅｖｅ）する必要がある。
【０１０４】
－また、ＵＥにｅＵＩＣＣを備えることも提案される。組み込みＳＩＭ（ｅｍｂｅｄｄｅｄ ＳＩＭ：ｅＵＩＣＣ）は複数のプロファイルを保存できるため、複数のサブスクリプションのためのＮＰＮクレデンシャルをｅＵＩＣＣに保存できる。
【０１０５】
－非スタンドアロンＮＰＮアクセス（ｎｏｎ－ｓｔａｎｄａｌｏｎｅ ＮＰＮ ａｃｃｅｓｓ）およびスタンドアロンＮＰＮアクセス（ｓｔａｎｄａｌｏｎｅ ＮＰＮ ａｃｃｅｓｓ）のための全体的なｅＵＩＣＣアーキテクチャを、それぞれ図４および図５に示す。図４は、非スタンドアロンＮＰＮアクセスクレデンシャルを有するｅＵＩＣＣの概略図である。図４では、ｅＵＩＣＣは非パブリックネットワークサブスクリプションのためのＮＰＮアクセスクレデンシャルを保存する。ｅＵＩＣＣは、非パブリックネットワークサブスクリプションのためのＵＳＩＭまたはＮＳＩＭアプリケーションを含む。ｅＵＩＣＣは、パブリックネットワークサブスクリプションのためのＵＴＭＳアクセスクレデンシャルを

保存する。ｅＵＩＣＣは、パブリックネットワークサブスクリプションのためのＵＳＩＭまたはＮＳＩＭアプリケーションを含む。ｅＵＩＣＣは、パブリックネットワークサブスクリプションのためのＩＭＳアクセスクレデンシャルを保存する。ｅＵＩＣＣは、パブリックネットワークサブスクリプションのためのＩＳＩＭ（ＩＭＳ ＳＩＭ）アプリケーションを含む。図５は、スタンドアロンＮＰＮアクセスクレデンシャルを有するｅＵＩＣＣの概略図である。図５では、ｅＵＩＣＣは非パブリックネットワークサブスクリプションのためのＮＰＮアクセスクレデンシャルを保存する。ｅＵＩＣＣは、非パブリックネットワークサブスクリプションのためのＮＳＩＭまたはＵＳＩＭアプリケーションを含む。

【０１０６】

４．４　さらなる態様

ユーザ機器（Ｕｓｅｒ ｅｑｕｉｐｍｅｎｔ：ＵＥ）

図６は、ＵＥ３００の主要なコンポーネントを示すブロック図である。示されるように、ＵＥ３００は、１つまたは複数のアンテナ３０５を介して接続されたノードに信号を送信し、接続されたノードから信号を受信するように動作可能なトランシーバ回路３０４を含む。必ずしも図６に示されているわけではないが、ＵＥ３００はもちろん、伝統的なモバイルデバイス（ユーザインターフェース３０３など）の全ての通常の機能を有し、これは、必要に応じて、ハードウェア、ソフトウェア、およびファームウェアの任意の１つまたは任意の組み合わせによって提供されてもよい。ソフトウェアは、メモリ３０２にプレインストールされてもよいし、および／または、例えば、電気通信ネットワークを介して、またはリムーバブルデータストレージデバイス（ＲＭＤ）からダウンロードされてもよい。

【０１０７】

コントローラ３０１は、メモリ３０２に格納されたソフトウェアに従ってＵＥ３００の動作を制御する。例えば、コントローラ３０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）によって実現されてもよい。ソフトウェアは、とりわけ、オペレーティングシステム３０８と、少なくともトランシーバ制御モジュール３０７を有する通信制御モジュール３０６とを含む。通信制御モジュール３０６（そのトランシーバ制御サブモジュールを使用する）は、ＵＥ３００と他のノード（基地局／（Ｒ）ＡＮノード、ＭＭＥ、ＡＭＦ（および他のコアネットワークノード）など）との間のシグナリングおよびアップリンク／ダウンリンクデータパケットを処理（生成／送信／受信）する能力がある。そのようなシグナリングは、例えば、コネクションの確立およびメンテナンスに関連する適切にフォーマットされたシグナリングメッセージ（例えば、ＲＲＣメッセージ）、定期的ロケーション更新関連メッセージ（例えば、トラッキングエリア更新、ページングエリア更新、ロケーションエリア更新）などのＮＡＳメッセージを含んでもよい。

【０１０８】

(Ｒ)ＡＮノード

図７は、例示的な（Ｒ）ＡＮノード４００、例えば、基地局（ＬＴＥの「ｅＮＢ」、５Ｇの「ｇＮＢ」または「ｎｇＮＢ」）の主要なコンポーネントを示すブロック図である。示されるように、（Ｒ）ＡＮノード４００は、１つまたは複数のアンテナ４０５を介して接続されたＵＥに信号を送信し、接続されたＵＥから信号を受信し、ネットワークインターフェース４０３を介して（直接的または間接的のいずれか）他のネットワークノードに信号を送信し、他のネットワークノードから信号を受信するように動作可能なトランシーバ回路４０４を含む。コントローラ４０１は、メモリ４０２に格納されたソフトウェアに従って、（Ｒ）ＡＮノード４００の動作を制御する。例えば、コントローラ４０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）によって実現されてもよい。ソフトウェアは、メモリ４０２にプレインストールされてもよいし、および／または、例えば、電気通信ネットワークを介して、またはリムーバブルデータストレージデバイス（ＲＭＤ）からダウンロードされてもよい。ソフトウェアは、とりわけ、オペレーティングシステム４０８と、少なくともトランシーバ制御モジュール４０７を有する通信制御モジュール４０６とを含む。

【０１０９】
通信制御モジュール４０６（そのトランシーバ制御サブモジュールを使用する）は、（Ｒ）ＡＮノード４００と他のノード（ＵＥ、ＭＭＥ、ＡＭＦ（例えば、直接的または間接的に）など）との間のシグナリングを処理（生成／送信／受信）する能力がある。シグナリングは、例えば、無線コネクションおよびロケーション手順（特定のＵＥについて）に関連し、特に、コネクション確立およびメンテナンス（例えば、ＲＲＣコネクション確立および他のＲＲＣメッセージ）に関連する適切にフォーマットされたシグナリングメッセージ、定期的ロケーション関連メッセージ（例えば、トラッキングエリア更新、ページングエリア更新、ロケーションエリア更新）、Ｓ１ ＡＰメッセージおよびＮＧ ＡＰメッセージ（すなわち、Ｎ２リファレンスポイントによるメッセージ）などを含んでもよい。そのようなシグナリングは、例えば、送信ケースにおけるブロードキャスト情報（例えば、マスターの情報とシステム情報）を含んでもよい。
【０１１０】
コントローラ４０１はまた、実装されたとき、ＵＥモビリティ推定および／または移動軌道推定（ｍｏｖｉｎｇ ｔｒａｊｅｃｔｏｒｙ ｅｓｔｉｍａｔｉｏｎ）などの関連タスクを処理するように（ソフトウェアまたはハードウェアによって）構成される。
【０１１１】
コアネットワークノード
図８は、例示的なコアネットワークノード５００、例えば、ＡＭＦ、ＳＭＦ、ＳＥＡＦ、ＡＵＳＦ、ＵＰＦ、ＵＤＭ、ＡＲＰＦ、ＳＩＤＦ、ＰＣＦ、ＡＦなどの主要なコンポーネントを示すブロック図である。コアネットワークノードは５ＧＣに含まれる。示されるように、コアネットワークノード５００は、ネットワークインターフェース５０３を介して他のノード（ＵＥを含む）に信号を送信し、他のノードから信号を受信するように動作可能なトランシーバ回路５０４を含む。コントローラ５０１は、メモリ５０２に格納されたソフトウェアに従って、コアネットワークノード５００の動作を制御する。例えば、コントローラ５０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）によって実現されてもよい。ソフトウェアは、メモリ５０２にプレインストールされてもよいし、および／または、例えば、電気通信ネットワークを介して、またはリムーバブルデータストレージデバイス（ＲＭＤ）からダウンロードされてもよい。ソフトウェアは、とりわけ、オペレーティングシステム５０７と、少なくともトランシーバ制御モジュール５０６を有する通信制御モジュール５０５とを含む。
【０１１２】
通信制御モジュール５０５（そのトランシーバ制御サブモジュールを使用する）は、コアネットワークノード５００と、他のノード（ＵＥ、基地局／（Ｒ）ＡＮノード（例えば、「ｇＮＢ」または「ｅＮＢ）（直接的または間接的に）など」との間のシグナリングを処理（生成／送信／受信）する能力がある。そのようなシグナリングは、例えば、本明細書に記載の手順に関連する適切にフォーマットされたシグナリングメッセージ、例えば、ＵＥとの間でＮＡＳメッセージを伝達するためのＮＧ ＡＰメッセージ（すなわち、Ｎ２リファレンスポイントによるメッセージ）などを含んでもよい。
【０１１３】
ＡＭＦは、ＵＥベースの認証（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）、認可（ａｕｔｈｏｒｉｚａｔｉｏｎ）、およびモビリティ管理サービス（ｍｏｂｉｌｉｔｙ ｍａｎａｇｅｍｅｎｔ ｓｅｒｖｉｃｅ）を提供する。ＡＭＦは、セッション管理機能（Ｓｅｓｓｉｏｎ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ）にサービスを提供してもよい。また、サービス名ベースのインターフェース（Ｎａｍｅ ｏｆ ｓｅｒｖｉｃｅ ｂａｓｅｄ ｉｎｔｅｒｆａｃｅ）を介して、他のＡＭＦ、ポリシー制御機能（Ｐｏｌｉｃｙ Ｃｏｎｔｒｏｌ Ｆｕｎｃｔｉｏｎ）、ショートメッセージサービス機能（Ｓｈｏｒｔ Ｍｅｓｓａｇｅ Ｓｅｒｖｉｃｅ Ｆｕｎｃｔｉｏｎ）、ロケーション管理機能（Ｌｏｃａｔｉｏｎ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ）、ゲートウェイモバイルロケーションセンター（Ｇａｔｅｗａｙ Ｍｏｂｉｌｅ Ｌｏｃａｔｉｏｎ Ｃｅｎｔｒｅ）、およびＮＥＦにサービスを提供する。

主要なＡＭＦサービスのいくつかは、登録（ｒｅｇｉｓｔｒａｔｉｏｎ）、接続（ｃｏｎｎｅｃｔｉｏｎ）、到達可能性（ｒｅａｃｈａｂｉｌｉｔｙ）、およびモビリティの管理などを含む。また、ＡＭＦは、ＲＡＮコントロールプレーンインターフェース（ＲＡＮ ｃｏｎｔｒｏｌ－ｐｌａｎｅ ｉｎｔｅｒｆａｃｅ：Ｎ２）の終端ポイントとしても機能する。

【０１１４】

ＳＭＦは、ＵＥにＩＰアドレスを割り当てながら、ＵＥセッションの管理を処理する。また、ＳＭＦは、データ転送用のＵＰＦを選択し制御する。セッションごとのＳＭＦは、複数のセッションを持つＵＥに割り当てられてもよい。また、ＳＭＦは、ユーザプレーン機能（Ｕｓｅｒ Ｐｌａｎｅ Ｆｕｎｃｔｉｏｎ）とインタラクト（ｉｎｔｅｒａｃｔ）して、ユーザのパケットを効率的にルーティングする。

【０１１５】

ＳＥＡＦは、ＵＥとサービングネットワークがプライマリ認証のためのサブシークエント通信を保護するために使用できるユニファイドアンカーキー（ｕｎｉｆｉｅｄ ａｎｃｈｏｒ ｋｅｙ）ＫＳＥＡＦ（全てのアクセスに共通）を生成する。ＵＥが３ＧＰＰアクセス（ｖｉｓｉｔｅｄ ｎｅｔｗｏｒｋ）と非３ＧＰＰアクセス（ｈｏｍｅ ｎｅｔｗｏｒｋ）に接続されている場合、シナリオには２つのアンカーキーが存在する可能性がある。

【０１１６】

ＡＵＳＦコンポーネントは、３ＧＰＰアクセスおよび非３ＧＰＰアクセスネットワークの認証要求（ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｒｅｑｕｅｓｔ）を処理する。ＡＵＳＦコンポーネントは、ユーザ機器を認証するために、セキュリティアンカー機能（Ｓｅｃｕｒｉｔｙ Ａｎｃｈｏｒ Ｆｕｎｃｔｉｏｎ）とインタラクトする。ユニバーサルサブスクライバー識別モジュール（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｍｏｄｕｌｅ）の値のセットは、認証クレデンシャルリポジトリおよび処理機能（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｒｅｄｅｎｔｉａｌ Ｒｅｐｏｓｉｔｏｒｙ ａｎｄ Ｐｒｏｃｅｓｓｉｎｇ Ｆｕｎｃｔｉｏｎ）によって使用される。サブスクリプション識別子（ｓｕｂｓｃｒｉｐｔｉｏｎ ｉｄｅｎｔｉｆｉｅｒ）は、サブスクリプションをユニークに識別し、ＵＥと５Ｇコアネットワークを相互に認証するために使用される。ＡＵＳＦは、必要な認証および認可プロセス（ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ ａｕｔｈｏｒｉｚａｔｉｏｎ ｐｒｏｃｅｓｓｅｓ）を提供しながら、ユーザプレーンセキュリティの終端ポイントとして機能する。また、ネットワークスライシングセキュリティ（ｎｅｔｗｏｒｋ ｓｌｉｃｉｎｇ ｓｅｃｕｒｉｔｙ）とＥｎｈａｎｃｅｄ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｍｏｂｉｌｅ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｐｒｉｖａｃｙも処理する。

【０１１７】

ＵＰＦは、パケットのルーティングと転送、パケットの検査、およびＱｏＳ処理をサポートする。また、ＵＰＦは、データネットワークへの相互接続の外部ＰＤＵセッションポイントとしても機能し、イントラＲＡＴ（ｉｎｔｒａ－ＲＡＴ）およびインターＲＡＴ（ｉｎｔｅｒ－ＲＡＴ）モビリティのアンカーポイントとして機能する。これは重要な機能の１つであり、サブミリ秒以内にパケットを効率的に処理する必要がある。この機能の速度が低下すると、パケットの遅延が大幅に増加し、ユーザのエクスペリエンスの品質（ｑｕａｌｉｔｙ－ｏｆ－ｅｘｐｅｒｉｅｎｃｅ）が低下する。ＵＰＦは、セッション管理機能（Ｓｅｓｓｉｏｎ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ）のサービスを利用する。

【０１１８】

ＵＤＭは、ＡＭＦ、ＳＭＦ、ＳＭＳＦ、ＮＥＦ、およびＡＵＳＦにサービスを提供する。サービスは、サブスクリプションデータストレージ（Ｓｕｂｓｃｒｉｐｔｉｏｎ ｄａｔａ ｓｔｏｒａｇｅ）、ＡＵＳＦとコラボレーションしたコンテキストデータ管理サービス認証サービス（Ｃｏｎｔｅｘｔ ｄａｔａ ｍａｎａｇｅｍｅｎｔ ｓｅｒｖｉｃｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｓｅｒｖｉｃｅ）を含む。サブスクリプションデータ管理は、ＮＦ（ＡＭＦおよびＳＭＦ）によって使用され、ＵＤＭからコンシューマーＮＦに関連するＵＥのサブスクリプションデータを取得する。また、データ変更の通知をサブスクライブま

たはアンサブスクライブするために、コンシューマーＮＦによって使用される。ＵＤＭは、以前にサブスクライブしたコンシューマーＮＦ（ＡＭＦ、ＳＭＦ、ＳＭＳＦ）に、ＵＤＭがサブスクライブされたデータを変更することを決定した場合に通知サービスオペレーション（ｎｏｔｉｆｉｃａｔｉｏｎ ｓｅｒｖｉｃｅ ｏｐｅｒａｔｉｏｎ）によって通知を受け取るように提供する。

【０１１９】

ＡＲＰＦは、ＵＤＭとともに機能し、認証のためのＥＰＳ ＡＫＡまたはＥＡＰ－ＡＫＡにおけるキーＫなどのロングタームセキュリティクレデンシャルを保存する。ＡＲＰＦは、ロングタームセキュリティクレデンシャルを入力として使用して暗号化アルゴリズムを実行し、認証ベクトルを生成できる。

【０１２０】

ＰＣＦは、ユニファイドポリシーフレームワークをサポートすることにより、ネットワーク行動（ｎｅｔｗｏｒｋ ｂｅｈａｖｉｏｒ）を管理する。また、ＰＣＦは、コントロールプレーン機能（Ｃｏｎｔｒｏｌ Ｐｌａｎｅ ｆｕｎｃｔｉｏｎ）にポリシールールを提供する。例えば、ＰＣＦは、アクセスネットワークディスカバリー（Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ ｄｉｓｃｏｖｅｒｙ）および選択ポリシー（ｓｅｌｅｃｔｉｏｎ ｐｏｌｉｃｉｅｓ）およびＵＥルート選択ポリシー（ＵＥ Ｒｏｕｔｅ Ｓｅｌｅｃｔｉｏｎ Ｐｏｌｉｃｉｅｓ）のためのＵＥポリシー、ＡＭＦのためのポリシーに関連するアクセスおよびモビリティ管理（Ａｃｃｅｓｓ ａｎｄ Ｍｏｂｉｌｉｔｙ Ｍａｎａｇｅｍｅｎｔ）を提供する。

【０１２１】

ＡＦは、トラフィックルーティング、ＮＥＦへのアクセス、ポリシー制御のためのポリシーフレームワークとのインタラクションに対するアプリケーションインフルエンスを可能（ｅｎａｂｌｅ）にする。コア機能はアプリケーションレベルに開示されているため、この機能は信頼性とセキュリティに大きな影響を及ぼす。

【０１２２】

ＮＥＦは、監視、プロビジョニング、およびポリシー／課金（Ｃｈａｒｇｉｎｇ）をサポートするためのネットワークの外部開示ケイパビリティ機能（ｅｘｔｅｒｎａｌ ｅｘｐｏｓｕｒｅ ｃａｐａｂｉｌｉｔｉｅｓ ｏｆ ｎｅｔｗｏｒｋ ｆｕｎｃｔｉｏｎｓ）を可能にする。ネットワークケイパビリティ開示（ｎｅｔｗｏｒｋ ｃａｐａｂｉｌｉｔｙ ｅｘｐｏｓｕｒｅ）は、次のものを含む：

（ｉ）コアネットワークＮＦに対する外部および内部のネットワークイベントの開示。（ｉｉ）外部機能に対するプロビジョニングケイパビリティの開示。（ｉｉｉ）外部機能に対するポリシーおよび課金ケイパビリティの開示。（ｉｖ）分析のためのコアネットワーク内部ケイパビリティの開示。

【０１２３】

本開示におけるユーザ機器（Ｕｓｅｒ Ｅｑｕｉｐｍｅｎｔまたは「ＵＥ」、「モバイルステーション」、「モバイルデバイス」または「ワイヤレスデバイス」）は、ワイヤレスインターフェースを介してネットワークに接続されるエンティティである。

【０１２４】

以下の段落で説明するように、本明細書におけるＵＥは、専用の通信デバイスに限定されるものではなく、本明細書で説明されるＵＥとしての通信機能を有する任意のデバイスに適用できることに留意されたい。

【０１２５】

「ユーザ機器（Ｕｓｅｒ Ｅｑｕｉｐｍｅｎｔ）」または「ＵＥ」（３ＧＰＰで使用される用語として）、「モバイルステーション」、「モバイルデバイス」、および「ワイヤレスデバイス」という用語は、一般に互いに同義であることが意図されており、端末、携帯電話、スマートフォン、タブレット、セルラーＩｏＴデバイス、ＩｏＴデバイス、機械（ｍａｃｈｉｎｅｒｙ）など、スタンドアロンのモバイルステーションが含まれる。

【０１２６】

「ＵＥ」および「ワイヤレスデバイス」という用語はまた、長期間静止したままである

デバイスを含むことが理解される。

【０１２７】

ＵＥは、例えば、生産または製造のための機器のアイテム、および／またはエネルギー関連の機械のアイテム（例えば、次のような機器または機械：ボイラー、エンジン、タービン、ソーラーパネル、風力タービン、水力発電機、火力発電機、原子力発電機、バッテリー、原子力システムおよび／または関連機器、重電機械、真空ポンプを含むポンプ、コンプレッサー、ファン、ブロワー、オイル油圧機器、空気圧機器、金属加工機械、マニピュレーター、ロボットおよび／またはそれらのアプリケーションシステム、ツール、金型またはダイ、ロール、運搬機器、昇降機器、材料処理機器、繊維機器、縫製機器、印刷および／または関連機械、紙加工機械、化学機械、鉱業および／または建設機械および／または関連機器、農業、林業および／または漁業のための機械および／または器具、安全および／または環境保全機器、トラクター、精密ベアリング、チェーン、ギア、動力伝達機器、潤滑機器、バルブ、配管器具、および／または前述の機器または機械のアプリケーションシステムなど）でもよい。

【０１２８】

ＵＥは、例えば、輸送機器のアイテム（例えば、次のような輸送機器：車両（ｒｏｌｌｉｎｇ ｓｔｏｃｋ）、自動車、オートバイ、自転車、電車、バス、カート、人力車、船およびその他の船舶、航空機、ロケット、衛星、ドローン、気球など）でもよい。

【０１２９】

ＵＥは、例えば、情報通信機器のアイテム（例えば、次のような情報通信機器：電子コンピュータおよび関連機器、通信および関連機器、電子部品など）でもよい。

【０１３０】

ＵＥは、例えば、冷凍機、冷凍機適用製品、貿易および／またはサービス産業機器のアイテム、自動販売機、自動サービス機、事務機械または機器、家庭用電化製品および電子機器（例えば、次のような家電製品：オーディオ機器、ビデオ機器、拡声器、ラジオ、テレビ、電子レンジオーブン、炊飯器、コーヒーマシン、食器洗い機、洗濯機、乾燥機、電子ファンまたは関連機器、掃除機など）でもよい。

【０１３１】

ＵＥは、例えば、電気アプリケーションシステムまたは機器（例えば、次のような電気アプリケーションシステムまたは機器：Ｘ線システム、粒子加速器、放射性同位体機器、音波機器、電磁アプリケーション機器、電動アプリケーション機器など）でもよい。

【０１３２】

ＵＥは、例えば、電子ランプ、照明器具、測定機器、分析器、テスター、または測量または感知機器（例えば、煙探知器、人間警報センサー、モーションセンサー、ワイヤレスタグなどの測量または感知機器）、腕時計または時計、実験器具、光学機器、医療機器および／またはシステム、武器、刃物のアイテム、手工具などでもよい。

【０１３３】

ＵＥは、例えば、ワイヤレス実装パーソナルデジタルアシスタント（ｗｉｒｅｌｅｓｓ－ｅｑｕｉｐｐｅｄ ｐｅｒｓｏｎａｌ ｄｉｇｉｔａｌ ａｓｓｉｓｔａｎｔ）または関連機器（別の電子デバイス（例えば、パーソナルコンピュータ、電気測定機）への取り付けまたは挿入のために設計されたワイヤレスカードまたはモジュールなど）でもよい。

【０１３４】

ＵＥは、様々な有線および／または無線通信技術を使用して、「モノのインターネット（ｉｎｔｅｒｎｅｔ ｏｆ ｔｈｉｎｇｓ：ＩｏＴ）」に関して、以下に説明するアプリケーション、サービス、およびソリューションを提供するデバイスまたはシステムの一部でもよい。

【０１３５】

Ｉｎｔｅｒｎｅｔ ｏｆ Ｔｈｉｎｇｓデバイス（または「モノ：ｔｈｉｎｇｓ」）は、適切な電子機器、ソフトウェア、センサー、ネットワークコネクティビティなどが実装されてもよい。これらのデバイスは、相互に他の通信デバイスとデータを収集および交換で

きる。ＩｏＴデバイスは、内部メモリに保存されているソフトウェア命令に従って自動化された機器で構成されてもよい。ＩｏＴデバイスは、人間による管理やインタラクションを必要とせずに動作してもよい。ＩｏＴデバイスは、長期間、静止している、非アクティブのままでもよい。ＩｏＴデバイスは、（一般的に）固定された装置の一部として実装されてもよい。ＩｏＴデバイスは、非固定装置（車両など）に組み込まれてもよいし、モニタ／追跡する動物や人に取り付けられてもよい。

【０１３６】

ＩｏＴ技術は、データを送受信するために通信ネットワークに接続することができる任意の通信デバイスに実装することができ、そのような通信デバイスが人間の入力またはメモリに格納されたソフトウェア命令によって制御されるかどうかに関係ないことが理解される。

【０１３７】

ＩｏＴデバイスは、Ｍａｃｈｉｎｅ－Ｔｙｐｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎ（ＭＴＣ）デバイスまたはＭａｃｈｉｎｅ－ｔｏ－Ｍａｃｈｉｎｅ（Ｍ２Ｍ）通信デバイスまたはＮａｒｒｏｗ Ｂａｎｄ ＩｏＴ ＵＥ（ＮＢ－ＩｏＴ ＵＥ）と呼ばれる場合もある。ＵＥは、１つまたは複数のＩｏＴまたはＭＴＣアプリケーションをサポートし得ることが理解される。ＭＴＣアプリケーションのいくつかの例を次の表１に示す（出典：３ＧＰＰ ＴＳ ２２．３６８ Ｖ１３．１．０（２０１４－１２），Ａｎｎｅｘ Ｂ，その内容は参照により本明細書に組み込まれる）。このリストは完全なものではなく、マシンタイプ通信アプリケーションのいくつかの例を示すことを意図としている。

【０１３８】

【表１】

表１:マシンタイプ通信アプリケーションのいくつかの例

Service Area	**MTC applications**
Security	Surveillance systems Backup for landline Control of physical access (e.g. to buildings) Car/driver security
Tracking & Tracing	Fleet Management Order Management Pay as you drive Asset Tracking Navigation Traffic information Road tolling Road traffic optimisation/steering
Payment	Point of sales Vending machines Gaming machines
Health	Monitoring vital signs Supporting the aged or handicapped Web Access Telemedicine points Remote diagnostics
Remote Maintenance/Control	Sensors Lighting Pumps Valves Elevator control Vending machine control Vehicle diagnostics
Metering	Power Gas Water Heating Grid control Industrial metering
Consumer Devices	Digital photo frame Digital camera eBook

【０１３９】

アプリケーション、サービス、およびソリューションは、ＭＶＮＯ（Ｍｏｂｉｌｅ Ｖｉｒｔｕａｌ Ｎｅｔｗｏｒｋ Ｏｐｅｒａｔｏｒ）サービス、緊急無線通信システム、ＰＢＸ（Ｐｒｉｖａｔｅ Ｂｒａｎｃｈ ｅｘｃｈａｎｇｅ）システム、ＰＨＳ／デジタルコードレステレコミュニケーションシステム、ＰＯＳ（Ｐｏｉｎｔ ｏｆ ｓａｌｅ）システム、アドバタイズ通話システム、ＭＢＭＳ（Ｍｕｌｔｉｍｅｄｉａ Ｂｒｏａｄｃａｓｔ ａｎｄ Ｍｕｌｔｉｃａｓｔ Ｓｅｒｖｉｃｅ）、Ｖ２Ｘ（Ｖｅｈｉｃｌｅ ｔｏ Ｅｖｅｒｙｔｈｉｎｇ）システム、列車無線システム、位置関連サービス、災害／緊急無線通信サービス、コミュニティサービス、ビデオストリーミングサービス、フェムトセルアプリケーシ

ョンサービス、ＶｏＬＴＥ（Ｖｏｉｃｅ ｏｖｅｒ ＬＴＥ）サービス、チャージングサービス、ラジオオンデマンドサービス、ローミングサービス、アクティビティモニタリングサービス、通信事業者／通信ＮＷ選択サービス、機能制限サービス、ＰｏＣ（Ｐｒｏｏｆ ｏｆ Ｃｏｎｃｅｐｔ）サービス、個人情報管理サービス、アドホックネットワーク／ＤＴＮ（Ｄｅｌａｙ Ｔｏｌｅｒａｎｔ Ｎｅｔｗｏｒｋｉｎｇ）サービスなどでもよい。

【０１４０】

さらに、上記のＵＥカテゴリは、本明細書に記載されている技術的アイデアおよび例示的な態様の適用例にすぎない。言うまでもなく、これらの技術的アイデアおよび態様は、上記のＵＥに限定されず、それに様々な修正を加えることができる。

【０１４１】

当業者によって理解されるように、本開示は、方法およびシステムとして具体化されてもよい。したがって、本開示は、もっぱらハードウェアの態様、ソフトウェアの態様、またはソフトウェアとハードウェアの態様を組み合わせた態様の形態をとることができる。

【０１４２】

ブロック図の各ブロックは、コンピュータプログラム命令によって実装できることが理解される。これらのコンピュータプログラム命令は、汎用コンピュータ、専用コンピュータ、または他のプログラム可能なデータ処理装置のプロセッサに提供されて、装置を生成することができ、そのような命令は、コンピュータまたは他のプログラム可能なデータ処理装置のプロセッサを介して実行されることで、フローチャートおよび／またはブロック図のブロックで特定された機能／動作を実装するための手段を生成することができる。汎用プロセッサはマイクロプロセッサでもよいが、代替として、プロセッサは、任意の伝統的なプロセッサ、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もよい。プロセッサはまた、コンピューティングデバイス、例えば、複数のマイクロプロセッサ、１つまた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の組み合わせとして実装されてもよい。

【０１４３】

本明細書に開示される例に関連して説明される方法またはアルゴリズムは、ハードウェア、プロセッサによって実行されるソフトウェアモジュール、またはその２つの組み合わせで直接具体化されてもよい。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、または当技術分野で知られている他の形式の記憶媒体に存在してもよい。プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、記憶媒体は、プロセッサに結合されてもよい。あるいは、記憶媒体はプロセッサに統合されてもよい。プロセッサと記憶媒体はＡＳＩＣ内に存在してもよい。

【０１４４】

上記開示された例の説明は、当業者が本開示を実施または使用することを可能にするために提供される。これらの例に対する様々な変更は、当業者にとって容易に明らかであり、本明細書で定義される一般的な原理は、本開示の意図またはスコープから逸脱することなく、他の例に適用することができる。したがって、本開示は、本明細書に示される例に限定されることを意図するものではなく、本明細書に開示される原理および新規の特徴と一致する最も広いスコープが与えられる。

【０１４５】

本出願は、２０１９年６月１３日に出願されたインド特許出願第２０１９４１０２３４２２号に基づいており、優先権の利益を主張するものであり、本開示は、参照によりその全体が本明細書に組み込まれる。

【０１４６】

上記開示された例示的な実施形態の全部または一部は、以下の付記のように記載することができるが、これらに限定されない。

（付記１）

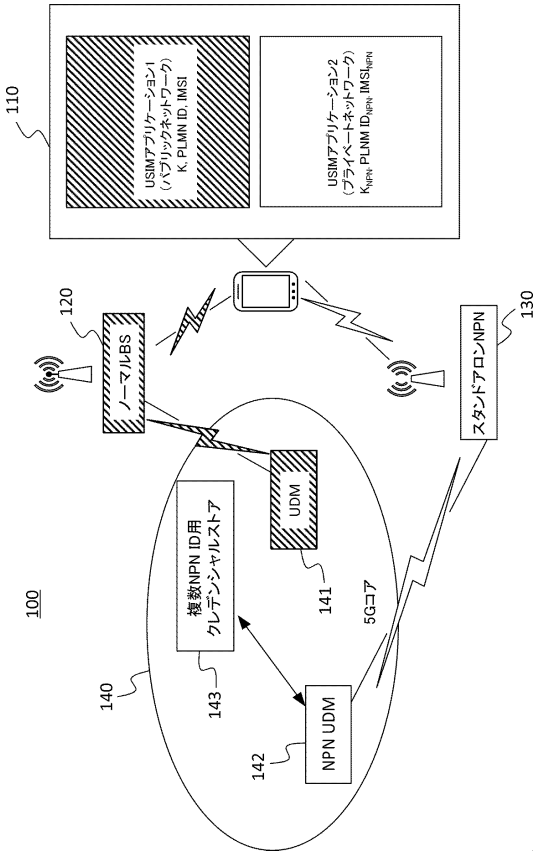
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサと動作可能に結合された少なくとも１つのメモリと、を備え、
前記少なくとも１つのプロセッサは、
ノーマルネットワークオペレーション用の認証を実行するために使用される第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションと、
ＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行するために使用される第２のＵＳＩＭアプリケーションと、を備え、
前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、
前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含む、
ユーザ機器（ＵＥ）。
（付記２）
前記第１のセキュリティクレデンシャルのセットは、第１のパーマネントキー、前記ノーマルネットワークオペレーション用に割り当てられた第１のＰＬＭＮ（Ｐｕｂｌｉｃ Ｌａｎｄ Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋ）ＩＤ、および第１のＩＭＳＩ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｍｏｂｉｌｅ Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｉｄｅｎｔｉｔｙ）を含み、
前記第２のセキュリティクレデンシャルのセットは、第２のパーマネントキー、ＩＯＰＳ（Ｉｓｏｌａｔｅｄ ＥＵＴＲＡＮ Ｏｐｅｒａｔｉｏｎ ｆｏｒ Ｐｕｂｌｉｃ Ｓａｆｅｔｙ）ネットワークオペレーション用に割り当てられた第２のＰＬＭＮ ＩＤ、および第２のＩＭＳＩを含む、
付記１に記載のユーザ機器。
（付記３）
前記第１のセキュリティクレデンシャルのセットは、他のローミングネットワーク用のＰＬＭＮ ＩＤを含み、
前記第２のセキュリティクレデンシャルのセットは、前記ＮＰＮに専用である、
付記２に記載のユーザ機器。
（付記４）
前記プロセッサは、存在する全てのＵＳＩＭ ＡＩＤ（Ａｐｐｌｉｃａｔｉｏｎ ＩＤｅｎｔｉｔｙ）の第３のストレージを備え、
前記第３のストレージは、前記第１のＵＳＩＭアプリケーションの第１のＡＩＤと前記第２のＵＳＩＭアプリケーションの第２のＡＩＤを含む、
付記１から３のいずれか一項に記載のユーザ機器。
（付記５）
前記プロセッサは、
前記第１のＡＩＤのための前記第１のＵＳＩＭアプリケーションをアクティベートし、前記第１のＡＩＤにリンクされた前記第１のＰＬＭＮ ＩＤを保存し、
前記第２のＡＩＤのための前記第２のＵＳＩＭアプリケーションをアクティベートし、前記第２のＡＩＤにリンクされた前記第２のＰＬＭＮ ＩＤを保存する、
ように構成される、付記４に記載のユーザ機器。
（付記６）
前記プロセッサは、
前記第１のＰＬＭＮ ＩＤまたは前記第２のＰＬＭＮ ＩＤの一方を使用して、ネットワークへのアタッチを試み、
前記第１のＰＬＭＮ ＩＤまたは前記第２のＰＬＭＮ ＩＤの前記一方が現在アクティブなＵＳＩＭアプリケーションと一致しない場合は、現在アクティブなＵＳＩＭアプリケーションを非アクティベートし、

前記第１のＰＬＭＮ ＩＤと前記第２のＰＬＭＮ ＩＤの他方に対応する別のＵＳＩＭアプリケーションをアクティベートする、
ように構成される、付記２から５のいずれか一項に記載のユーザ機器。
（付記７）
前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションは同じネットワークにアソシエートされ、
前記ユーザ機器は、複数のＮＰＮにアクセスするようにサブスクライブされる、
付記１から６のいずれか一項に記載のユーザ機器。
（付記８）
前記プロセッサは、
前記第１のＵＳＩＭアプリケーションまたは前記第２のＵＳＩＭアプリケーションの一方が前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションの他方よりも優先される優先順位を有し、
前記優先順位に基づいて、ノーマル基地局とスタンドアロンＮＰＮ基地局のどちらにチューンするかを決定する、
ように構成される、付記１から７のいずれか一項に記載のユーザ機器。
（付記９）
前記プロセッサは、登録要求メッセージを前記ノーマルネットワークと前記ＮＰＮに１つずつ送信することによって登録手順を実行し、前記第１のＵＳＩＭアプリケーションと前記第２のＵＳＩＭアプリケーションの両方をそれぞれ登録するように構成されている、
付記１から８のいずれか一項に記載のユーザ機器。
（付記１０）
前記プロセッサは、前記ユーザ機器がメインでチューンするプライマリネットワークを管理するローカルコンフィグレーションを有するように構成される、
付記９に記載のユーザ機器。
（付記１１）
前記ローカルコンフィグレーションは、所定のユーザアプリケーションによって上書きされる、
付記１０に記載のユーザ機器。
（付記１２）
前記所定のユーザアプリケーションは、エマージェンシーコールアプリケーションを含む、
付記１１に記載のユーザ機器。
（付記１３）
ユーザ機器（ＵＥ）とコアネットワークとを備え、
前記ユーザ機器は、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサと動作可能に結合された少なくとも１つのメモリと、を備え、
前記少なくとも１つのプロセッサは、
ノーマルネットワークオペレーション用の認証を実行するために使用される第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションと、
ＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行するために使用される第２のＵＳＩＭアプリケーションと、を備え、
前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、
前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含む、

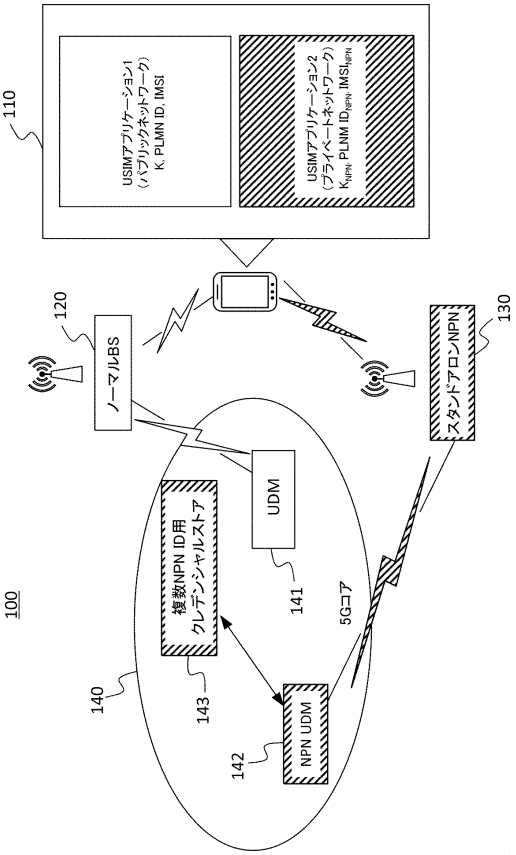
ネットワークシステム。
（付記１４）
ユーザ機器（ＵＥ）のための方法であって、
第１のＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）アプリケーションを使用してノーマルネットワークオペレーション用の認証を実行し、
第２のＵＳＩＭアプリケーションを使用してＮＰＮ（Ｎｏｎ－Ｐｕｂｌｉｃ Ｎｅｔｗｏｒｋ）用の認証を実行し、
前記第１のＵＳＩＭアプリケーションは、ＵＩＣＣ（Ｕｎｉｖｅｒｓａｌ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ Ｃａｒｄ）における第１のストレージに保存された第１のセキュリティクレデンシャルのセットを含み、
前記第２のＵＳＩＭアプリケーションは、前記ＵＩＣＣにおける第２のストレージに保存された第２のセキュリティクレデンシャルのセットを含む、
方法。
【符号の説明】
【０１４７】
１００　ネットワークシステム
１１０　ＵＥ
１２０　ノーマルＢＳ
１３０　スタンドアロンＮＰＮ
１４０　５Ｇコアネットワーク
１４１　ＵＤＭ
１４２　ＮＰＮ ＵＤＭ
１４３　クレデンシャルストア
３００　ＵＥ
３０１　コントローラ
３０２　メモリ
３０３　ユーザインターフェース
３０４　トランシーバ回路
３０５　アンテナ
３０６　通信制御モジュール
３０７　トランシーバ制御モジュール
３０８　オペレーティングシステム
４００　（Ｒ）ＡＮノード
４０１　コントローラ
４０２　メモリ
４０３　ネットワークインターフェース
４０４　トランシーバ回路
４０５　アンテナ
４０６　通信制御モジュール
４０７　トランシーバ制御モジュール
４０８　オペレーティングシステム
５００　コアネットワークノード
５０１　コントローラ
５０２　メモリ
５０３　ネットワークインターフェース
５０４　トランシーバ回路
５０５　通信制御モジュール
５０６　トランシーバ制御モジュール
５０７　オペレーティングシステム

【図面】

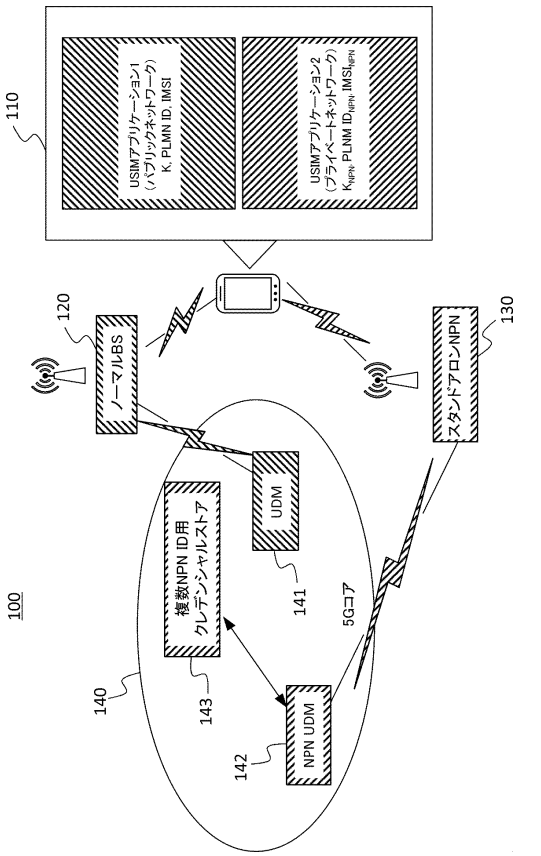
【図１】


110
USIMアプリケーション1
（パブリックネットワーク）
K, PLMN ID, IMSI
USIMアプリケーション2
（プライベートネットワーク）
K_{NPN}, PLNM ID_{NPN}, $IMSI_{NPN}$
120
ノーマルBS
130
スタンドアロンNPN
100
UDM
141
複数NPN ID用
クレデンシャルストア
143
5Gコア
140
142
NPN UDM

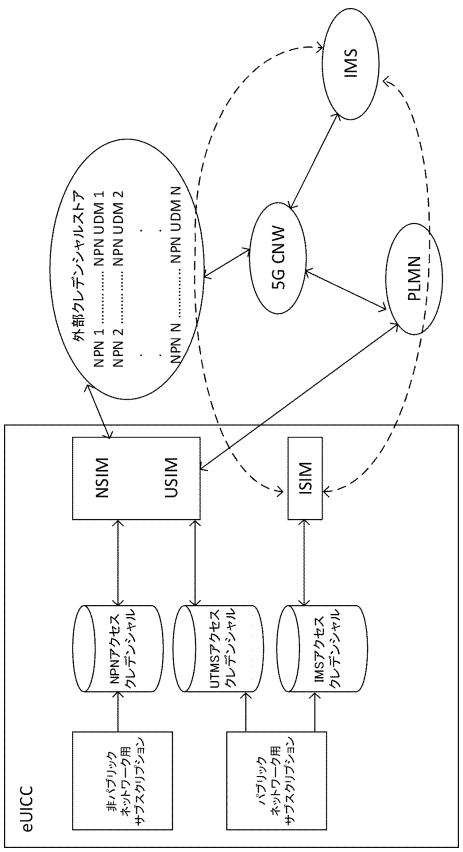
【図２】


110
USIMアプリケーション1
（パブリックネットワーク）
K, PLMN ID, IMSI
USIMアプリケーション2
（プライベートネットワーク）
K_{NPN}, PLNM ID_{NPN}, $IMSI_{NPN}$
120
ノーマルBS
130
スタンドアロンNPN
100
UDM
141
複数NPN ID用
クレデンシャルストア
143
5Gコア
140
142
NPN UDM

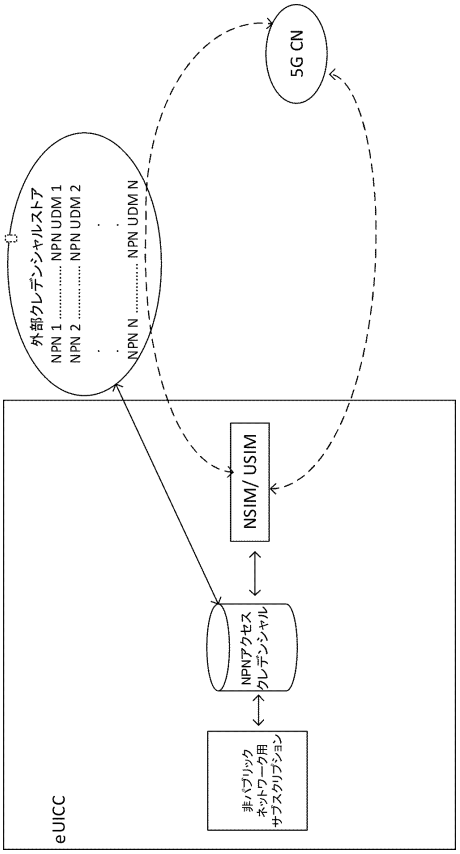
【図３】


110
USIMアプリケーション1
（パブリックネットワーク）
K, PLMN ID, IMSI
USIMアプリケーション2
（プライベートネットワーク）
K_{NPN}, PLNM ID_{NPN}, $IMSI_{NPN}$
120
ノーマルBS
130
スタンドアロンNPN
100
UDM
141
複数NPN ID用
クレデンシャルストア
143
5Gコア
140
142
NPN UDM

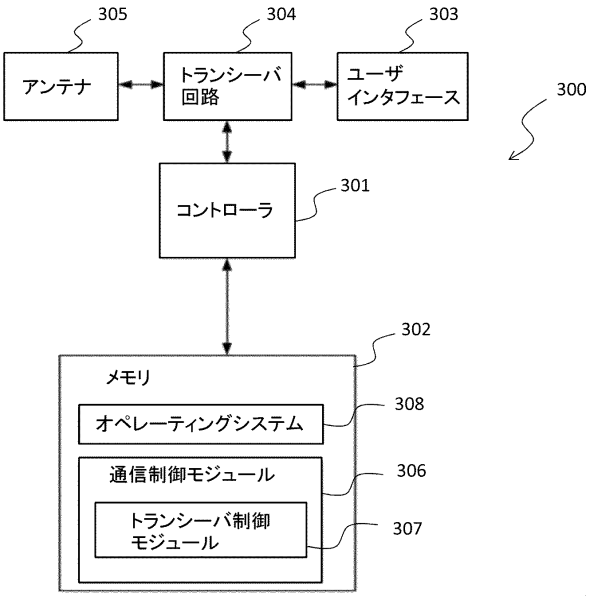
【図４】


IMS
5G CNW
PLMN
外部クレデンシャルストア
NPN 1 ..... NPN UDM 1
NPN 2 ..... NPN UDM 2
NPN N ..... NPN UDM N
NSIM
USIM
ISIM
NPNアクセス
クレデンシャル
UTMSアクセス
クレデンシャル
IMSアクセス
クレデンシャル
非パブリック
ネットワーク用
サブスクリプション
パブリック
ネットワーク用
サブスクリプション
eUICC

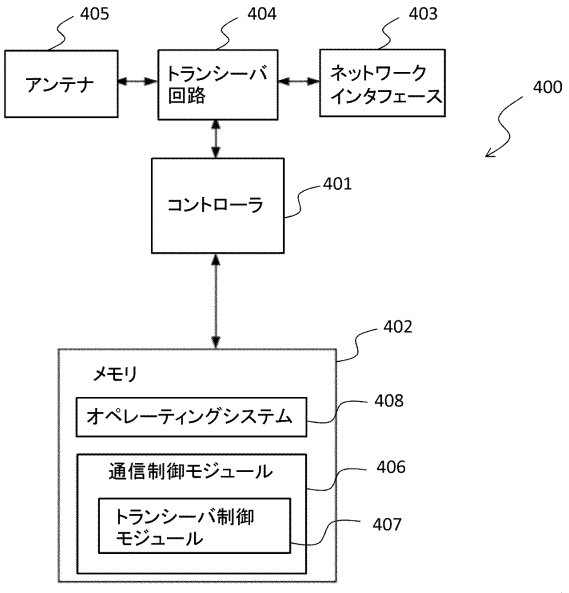
【図５】


5G CN
外部クレデンシャルストア
NPN 1 ..... NPN UDM 1
NPN 2 ..... NPN UDM 2
NPN N ..... NPN UDM N
NSIM/ USIM
NPNアクセス クレデンシャル
非パブリック ネットワーク用 サブスクリプション
eUICC

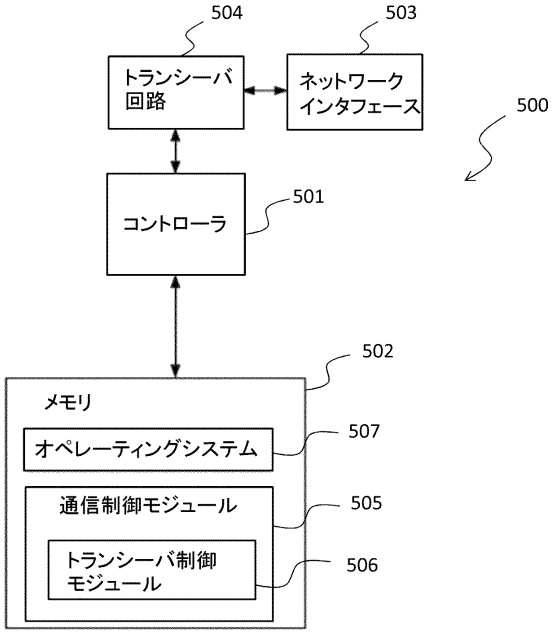
【図６】


305
304
303
アンテナ
トランシーバ 回路
ユーザ インタフェース
300
コントローラ
301
302
メモリ
オペレーティングシステム
308
通信制御モジュール
306
トランシーバ制御 モジュール
307

【図７】


405
404
403
アンテナ
トランシーバ 回路
ネットワーク インタフェース
400
コントローラ
401
402
メモリ
オペレーティングシステム
408
通信制御モジュール
406
トランシーバ制御 モジュール
407

【図８】


504
503
トランシーバ 回路
ネットワーク インタフェース
500
コントローラ
501
502
メモリ
オペレーティングシステム
507
通信制御モジュール
505
トランシーバ制御 モジュール
506

フロントページの続き

ッド内
(72)発明者　田村 利之
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　新井 寛

(56)参考文献　3GPP TR 33.897 V13.1.0，3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Security aspects (Release 13)，2016年03月17日，pp.14-16
3GPP TR 23.734 V16.2.0，3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services (Release 16)，2019年06月11日，p.14
3GPP TR 33.897 V1.0.0，3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Security aspects (Release 13)，2015年09月10日，pp.15-16

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４ －　７／２６
Ｈ０４Ｗ　４／００ －　９９／００
３ＧＰＰ　ＴＳＧ ＲＡＮ ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４