(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2022-92060
(P2022-92060A)
(43)公開日　令和4年6月21日(2022.6.21)

(51)国際特許分類　FI
H04W 8/26 (2009.01)　H04W 8/26
H04W 12/06 (2021.01)　H04W 12/06
H04W 12/69 (2021.01)　H04W 12/69
H04W 12/041 (2021.01)　H04W 12/041

審査請求　有　請求項の数　1　ＯＬ　（全20頁）

(21)出願番号　特願2022-67702(P2022-67702)
(22)出願日　令和4年4月15日(2022.4.15)
(62)分割の表示　特願2020-554296(P2020-554296)の分割
原出願日　平成31年4月4日(2019.4.4)
(31)優先権主張番号　201841013099
(32)優先日　平成30年4月5日(2018.4.5)
(33)優先権主張国・地域又は機関
インド(IN)

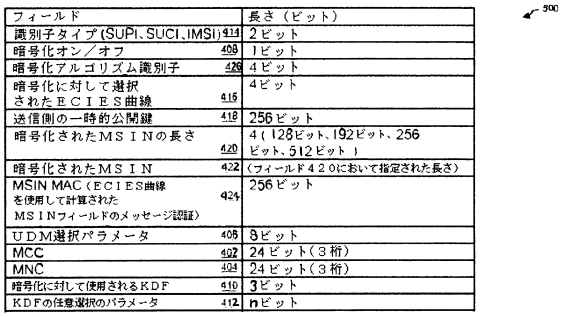
（特許庁注：以下のものは登録商標）
１．３ＧＰＰ
２．ＦＲＡＭ

(71)出願人　515076873
ノキア テクノロジーズ オサケユイチア
フィンランド国，０２６１０ エスプー，カラカーリ ７
(74)代理人　100094569
弁理士　田中 伸一郎
(74)代理人　100103610
弁理士　▲吉▼田 和彦
(74)代理人　100109070
弁理士　須田 洋之
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100086771
弁理士　西島 孝喜
(74)代理人　100109335

最終頁に続く

(54)【発明の名称】　通信システムにおける統合サブスクリプション識別子管理

(57)【要約】
【課題】通信システムにおける所与のユーザ機器において、統合サブスクリプション識別子データ構造が構築される。
【解決手段】統合サブスクリプション識別子データ構造は、２つ以上のサブスクリプション識別子タイプの選択された１つ、及び選択されたサブスクリプション識別子タイプと関連付けられた選択可能パラメータについての情報を指定する複数のフィールドを含み、統合サブスクリプション識別子データ構造における情報は、選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいて、通信システムと関連付けられた１つ以上のネットワークにアクセスするために所与のユーザ機器によって使用可能である。
【選択図】図５



【特許請求の範囲】
【請求項１】
無線通信システム（１００、２００）に対するユーザ機器（１０２、２０２）であって、
前記無線通信システム（１００、２００）における前記ユーザ機器（１０２、２０２）において、統合サブスクリプション識別子データ構造を構築することと、
前記統合サブスクリプション識別子データ構造（４００、６００）を記憶することであって、前記統合サブスクリプション識別子データ構造（４００、６００）は、選択されたサブスクリプション識別子タイプと関連付けられた２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の選択された１つを指定する複数のフィールド（４０２～４２６、６０２～６１６）を備える、前記記憶することと、
前記選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいて、前記無線通信システム（１００、２００）と関連付けられた１つ以上のネットワークにアクセスするために、前記統合サブスクリプション識別子データ構造（４００、６００）における２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の前記選択された１つを使用することと、
を実行するように構成されたプロセッサ（２１２）及びメモリ（２１６）を備える、
前記ユーザ機器（１０２、２０２）。
【請求項２】
前記複数のフィールド（４０２～４２６、６０２～６１６）は、サブスクリプション識別子タイプフィールド（４１４、６０８）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項３】
サブスクリプション識別子タイプは、秘匿化サブスクリプション識別子（ＳＵＣＩ）、加入者永久識別子（ＳＵＰＩ）、及び国際移動局識別子（ＩＭＳＩ）を備えるグループから選択可能である、請求項２に記載のユーザ機器（１０２、２０２）。
【請求項４】
前記複数のフィールド（４０２～４２６、６０２～６１６）は、ネットワークエンティティ選択パラメータフィールド（４０６、６０６）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項５】
ネットワークエンティティ（１０４、２０４）は、統合データ管理、ＵＤＭ、機能及び認証サーバ機能、ＡＵＳＦのうちの１つ以上を実行する、請求項４に記載のユーザ機器（１０２、２０２）。
【請求項６】
前記複数のフィールド（４０２～４２６）は、暗号化オン／オフフィールド（４０８）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項７】
前記複数のフィールド（４０２～４２６）は、暗号化アルゴリズム識別子フィールド（４２６）を備える、請求項６に記載のユーザ機器（１０２、２０２）。
【請求項８】
前記複数のフィールド（４０２～４２６）は、鍵導出関数フィールド（４１０）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項９】
前記複数のフィールド（４０２～４２６）は、鍵導出関数パラメータフィールド（４１２）を備える、請求項８に記載のユーザ機器（１０２、２０２）。
【請求項１０】
前記複数のフィールド（４０２～４２６、６０２～６１６）は、モバイル国コードフィールド（４０２、６０２）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項１１】
前記複数のフィールド（４０２～４２６、６０２～６１６）は、モバイルネットワークコ

ードフィールド（４０４、６０４）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項１２】
前記複数のフィールド（４０２～４２６）は、楕円曲線統合暗号化スキームから選択された曲線を指定するフィールド（４１６）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項１３】
前記複数のフィールド（４０２～４２６）は、一時的公開鍵ペアフィールド（４１８）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項１４】
前記複数のフィールド（４０２～４２６、６０２～６１６）は、暗号化移動局識別番号、ＭＳＩＮ、フィールドの長さを指定するフィールド（４２０、６１０）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項１５】
前記複数のフィールド（４０２～４２６、６０２～６１６）は、暗号化ＭＳＩＮフィールド（４２２、６１２）を備える、請求項１４に記載のユーザ機器（１０２、２０２）。
【請求項１６】
前記複数のフィールド（４０２～４２６、６０２～６１６）は、ＭＳＩＮメッセージ認証コードフィールド（４２４、６１４）を備える、請求項１４に記載のユーザ機器（１０２、２０２）。
【請求項１７】
前記無線通信システム（１００、２００）は、５Ｇシステムを備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項１８】
前記無線通信システム（１００、２００）と関連付けられた前記１つ以上のネットワークへのアクセスを取得するよう、前記無線通信システム（１００、２００）における少なくとも１つのネットワークエンティティ（１０４、２０４）に前記統合サブスクリプション識別子データ構造（４００、６００）を送信することを更に備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項１９】
前記複数のフィールド（６０２～６１６）は、プロファイル選択フィールド（６１６）を備える、請求項１に記載のユーザ機器（１０２、２０２）。
【請求項２０】
前記プロファイル選択フィールド（６１６）は、前記ユーザ機器（１０２、２０２）が、前記選択されたサブスクリプション識別子フィールド（３００、３１０、３２０）と関連付けられた１つ以上の選択可能パラメータに対して事前に確立された値を使用するよう、前記無線通信システム（１００、２００）と関連付けられた前記１つ以上のネットワークにおける１つ以上のネットワークエンティティに通知することを可能にする、請求項１９に記載のユーザ機器（１０２、２０２）。
【請求項２１】
前記無線通信システム（１００、２００）と関連付けられた前記１つ以上のネットワークへのアクセスを取得するよう、前記無線通信システム（１００、２００）における前記１つ以上のネットワークエンティティのうちの少なくとも１つに、前記プロファイル選択フィールド（６１６）及び減少したフィールドのセットを有する前記統合サブスクリプション識別子データ構造（６００）を送信することを更に備える、請求項２０に記載のユーザ機器（１０２、２０２）。
【請求項２２】
無線通信システム（１００、２００）におけるユーザ機器（１０２、２０２）において、
統合サブスクリプション識別子データ構造（４００、６００）を構築することと、
前記統合サブスクリプション識別子データ構造（４００、６００）を記憶することであっ

て、前記統合サブスクリプション識別子データ構造（４００、６００）は、選択されたサブスクリプション識別子タイプと関連付けられた２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の選択された１つを指定する複数のフィールド（４０２～４２６、６０２～６１６）を備える、前記記憶することと、
前記選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいて、前記無線通信システム（１００、２００）と関連付けられた１つ以上のネットワークにアクセスするために、前記統合サブスクリプション識別子データ構造（４００、６００）における２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の前記選択された１つを使用することと、
を備える、方法。

【請求項２３】
実行可能プログラムコードがその中に具現化された非一時的コンピュータ可読記憶媒体であって、前記実行可能プログラムコードは、プロセッサ（２１２）によって実行されるとき、前記プロセッサ（２１２）に、
無線通信システム（１００、２００）におけるユーザ機器（１０２、２０２）において、統合サブスクリプション識別子データ構造（４００、６００）を構築することと、
前記統合サブスクリプション識別子データ構造（４００、６００）を記憶することであって、前記統合サブスクリプション識別子データ構造（４００、６００）は、選択されたサブスクリプション識別子タイプと関連付けられた２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の選択された１つを指定する複数のフィールド（４０２～４２６、６０２～６１６）を備える、前記記憶することと、
前記選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいて、前記無線通信システム（１００、２００）と関連付けられた１つ以上のネットワークにアクセスするために、前記統合サブスクリプション識別子データ構造（４００、６００）における２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の前記選択された１つを使用することと、
を実行させる、前記非一時的コンピュータ可読記憶媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本分野は概して、通信システムに関し、より具体的には、排他的ではないが、そのようなシステム内でのユーザサブスクリプション識別子管理に関する。

【背景技術】
【０００２】
このセクションは、発明のより良好な理解を促進することを支援することができる態様を導入する。したがって、このセクションの記載は、この観点で読み取られるべきであり、従来技術にあるもの、または従来技術にないものについての了承として理解されるべきではない。

【０００３】
ロングタームエボリューション（ＬＴＥ）技術としても知られている第４世代（４Ｇ）無線モバイル通信技術は、特に人間の対話のための高データレートによる高容量モバイルマルチメディアを提供するよう設計されてきた。次世代または第５世代（５Ｇ）技術は、人間の対話のためだけでなく、いわゆるモノのインターネット（ＩｏＴ）ネットワークにおけるマシンタイプ通信のためにも使用されることを意図している。

【０００４】
５Ｇネットワークは、大規模ＩｏＴサービス（例えば、非常に多くの制限された容量のデバイス）及びミッションクリティカルなＩｏＴサービス（例えば、高信頼性を必要とする）を可能にすることを意図しており、レガシーモバイル通信サービスに対する改善は、モバイルデバイスに対して改善した無線インターネットアクセスを提供する拡張モバイルブロードバンド（ｅＭＢＢ）サービスの形式でサポートされる。

【０００５】
例示的な通信システムでは、モバイル端末（加入者）などのユーザ機器（５Ｇネットワークにおける５Ｇ　ＵＥ、またはより広義にはＵＥ）は、５Ｇネットワークにおいて、エアインタフェースを通じてｇＮＢと称される基地局またはアクセスポイントと通信する。アクセスポイント（例えば、ｇＮＢ）は、通信システムのアクセスネットワークの例示的な部分である。例えば、５Ｇネットワークでは、アクセスネットワークは、５Ｇシステムと称され、「Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｓｅｒｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍ　Ａｓｐｅｃｔｓ；Ｓｙｓｔｅｍ　Ａｒｃｈｉｔｅｃｔｕｒｅ　ｆｏｒ　ｔｈｅ　５Ｇ　Ｓｙｓｔｅｍ」と題する、３ＧＰＰ　Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ（ＴＳ）２３．５０１、Ｖ１５．０．０に記載されており、その開示は参照によりその全体が本明細書に組み込まれる。概して、アクセスポイント（例えば、ｇＮＢ）は、ＵＥに対してコアネットワーク（ＣＮ）へのアクセスを提供し、ＣＮは次いで、ＵＥに対して、他のＵＥへのアクセス及び／またはパケットデータネットワーク（例えば、インターネット）などのデータネットワークへのアクセスを提供する。更に、５Ｇネットワークアクセス手順は、「Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｓｅｒｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍ　Ａｓｐｅｃｔｓ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ　ａｎｄ　Ｐｒｏｃｅｄｕｒｅｓ　ｆｏｒ　ｔｈｅ　５Ｇ　Ｓｙｓｔｅｍ」と題する、３ＧＰＰ　Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ（ＴＳ）２３．５０２、ＶＩ５．１．０に記載されており、その開示は参照によりその全体が本明細書に組み込まれる。また更に、「Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｓｅｒｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍ　Ａｓｐｅｃｔｓ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ　ａｎｄ　Ｐｒｏｃｅｄｕｒｅｓ　ｆｏｒ　ｔｈｅ　５Ｇ　Ｓｙｓｔｅｍ」と題する、３ＧＰＰ　Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ（ＴＳ）３３．５０１、Ｖ０．７．０には、５Ｇネットワークと関連付けられたセキュリティ管理の詳細が更に記載されており、その開示は参照によりその全体が本明細書に組み込まれる。
【０００６】
５Ｇネットワークでは、５Ｇ互換ＵＥは、３ＧＰＰ　ＴＳ　２３．５０２において説明される登録要求手順の間に、３ＧＰＰ　ＴＳ　３３．５０１において説明される秘匿化サブスクリプション識別子（Ｃｏｎｃｅａｌｅｄ　Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｉｄｅｎｔｉｆｉｅｒ（ＳＵＣＩ））を含んでもよい。ＳＵＣＩは、加入者永久識別子（Ｓｕｂｓｃｒｉｂｅｒ　Ｐｅｒｍａｎｅｎｔ　Ｉｄｅｎｔｉｆｉｅｒ（ＳＵＰＩ））の秘匿化（暗号化）された形式である。レガシー４Ｇ（ＬＴＥ）ネットワークでは、使用されるサブスクリプション識別子は、「Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｃｏｒｅ　Ｎｅｔｗｏｒｋ　ａｎｄ　Ｔｅｒｍｉｎａｌｓ；Ｎｕｍｂｅｒｉｎｇ、Ａｄｄｒｅｓｓｉｎｇ　ａｎｄ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ」と題する、３ＧＰＰ　Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ（ＴＳ）２３．００３、Ｖ１５．３．０において定義された国際移動局識別子（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｍｏｂｉｌｅ　Ｓｔａｔｉｏｎ　Ｉｄｅｎｔｉｆｉｅｒ（ＩＭＳＩ））であり、その開示は参照によりその全体が本明細書に組み込まれる。そのようなサブスクリプション識別子の管理は、大きな課題を提示することがある。
【０００７】
３ＧＰＰ；Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｃｏｒｅ　Ｎｅｔｗｏｒｋ　ａｎｄ　Ｔｅｒｍｉｎａｌｓ；Ｎｏｎ－Ａｃｃｅｓｓ－Ｓｔｒａｔｕｍ（ＮＡＳ）　ｐｒｏｔｏｃｏｌ　ｆｏｒ　５Ｇ　Ｓｙｓｔｅｍｓ（５ＧＳ）；Ｓｔａｇｅ　３（Ｒｅｌｅａｓｅ　１５）は、ユーザ機器が既存の識別子タイプの中で特定のタイプのモバイル識別子を要求及び取得する方法を開示している。
【０００８】
国際公開第ＷＯ２０１４／０５３１９７Ａ１号公報は、ポリシー制御の方法を開示し、更に、複数の加入者に適用されるユーザコミュニティプロファイルのサポートを可能にする

拡張された装置を開示している。更に、ユーザコミュニティプロファイルから派生し、好ましくは、第１のユーザに対してセッションを確立するときに導入される、コミュニティポリシー及び課金ルールの生成及び実施が開示されている。複数のユーザの後続のユーザに対して確立されることになるセッションは、先述のコミュニティポリシーにより実施されることがあり、課金ルールは、個々の基準に対してそれらを扱う必要がなく有効にされることがある。

【０００９】

３ＧＰＰ；２３．５０１：ＳＵＰＩ ｔｅｒｍｉｎｏｌｏｇｙ ｃｏｒｒｅｃｔｉｏｎ；３ＧＰＰ ｄｒａｆｔは、５Ｇシステムにおいてグローバルに一意な５Ｇ加入者永久識別子（ＳＵＰＩ）を各々の加入者に割り当てることができるような、「加入者永久識別子」を開示している。

【００１０】

３ＧＰＰ；ＳＡ ＷＧ３；ＬＳ ｏｎ Ｓｅｃｕｒｉｔｙ ａｓｐｅｃｔｓ ｏｆ ＥＣＩＥＳ ｆｏｒ ｃｏｎｃｅａｌｉｎｇ ＩＭＳＩ ｏｒ ＳＵＰＩは、次世代のモバイルネットワーク（５Ｇと称される）を開示している。グローバルに一意な５Ｇサブスクリプション永久識別子を表すために使用されることが提案されている、ＳＵＰＩ（サブスクリプション永久識別子）と称される新たな且つ一般的な用語が開示されている。Ｄ４は更に、ＥＣＩＥＳ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｉｎｔｅｇｒａｔｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｃｈｅｍｅ（楕円曲線統合暗号化スキーム））によって、５ＧにおいてＩＭＳＩまたはＳＵＰＩをオーバージエアで秘匿化することを提案している。

【発明の概要】

【００１１】

例示的な実施形態は、通信システムにおいてサブスクリプション識別子を管理する改善された技術を提供する。

【００１２】

例えば、１つの例示的な実施形態では、方法は、以下のステップを含む。通信システムにおける所与のユーザ機器において、統合サブスクリプション識別子データ構造が構築される。統合サブスクリプション識別子データ構造は、２つ以上のサブスクリプション識別子タイプの選択された１つ、及び選択されたサブスクリプション識別子タイプと関連付けられた選択可能パラメータについての情報を指定する複数のフィールドを含み、統合サブスクリプション識別子データ構造における情報は、選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいて、通信システムと関連付けられた１つ以上のネットワークにアクセスするよう所与のユーザ機器によって使用可能である。

【００１３】

更なる例示的な実施形態は、プロセッサによって実行されるとき、プロセッサに上記ステップを実行させる、実行可能プログラムコードがその中に具現化された非一時的コンピュータ可読記憶媒体の形態で提供される。また更なる例示的な実施形態は、上記ステップを実行するように構成されたプロセッサ及びメモリを有する装置を含む。

【００１４】

有利なことに、異なる認証シナリオの間、所与のユーザ機器は、所与の認証シナリオのための適切なサブスクリプション識別子（例えば、ＳＵＰＩ、ＳＵＣＩ、またはＩＭＳＩ）及び関連するパラメータを提供するために、統合サブスクリプション識別子データ構造を利用する。

【００１５】

本明細書で説明される実施形態のそれらの及び他の特徴及び利点は、添付図面及び以下の詳細な説明からより明らかになるであろう。

【図面の簡単な説明】

【００１６】

【図１】１つ以上の例示的な実施形態が実施され得る、通信システムを示す。

【図２】１つ以上の例示的な実施形態が実施され得る、認証手順の間の加入者識別子管理

を提供するユーザ機器及びネットワーク要素／機能を示す。
【図３】Ａは、１つ以上の例示的な実施形態が実施され得る、ＩＭＳＩフォーマットを示す。Ｂは、１つ以上の例示的な実施形態が実施され得る、ＳＵＰＩフォーマットを示す。Ｃは、１つ以上の例示的な実施形態が実施され得る、ＳＵＣＩフォーマットを示す。
【図４】例示的な実施形態に従った、統合サブスクリプション識別子フォーマットを示す。
【図５】例示的な実施形態に従った、統合サブスクリプション識別子フォーマットの例示的なフィールド長を示す。
【図６】別の例示的な実施形態に従った、統合サブスクリプション識別子フォーマットを示す。
【図７】例示的な実施形態に従った、統合サブスクリプション識別子フォーマットを利用するユーザ機器方式を示す。
【図８】例示的な実施形態に従った、統合サブスクリプション識別子フォーマットを利用するネットワークエンティティ方式を示す。
【発明を実施するための形態】
【００１７】
通信システムにおける認証手順及び他の手順の間のサブスクリプション識別子管理を提供する例示的な通信システム及び関連する技術と共に実施形態が本明細書で示される。しかしながら、特許請求の範囲は、開示される特定のタイプの通信システム及び／または処理に限定されないことが理解されるべきである。実施形態は、代替的な処理及び操作を使用して、多種多様な他のタイプの通信システムにおいて実装されてもよい。例えば、３ＧＰＰ次世代システム（５Ｇ）などの３ＧＰＰシステム要素を利用する無線セルラシステムのコンテキストにおいて示されるが、開示される実施形態は、様々な他のタイプの通信システムに直接的な様式で適合されてもよい。
【００１８】
５Ｇ通信システム環境において実装される例示的な実施形態に従って、１つ以上の３ＧＰＰ技術仕様（ＴＳ）及び技術報告（ＴＲ）、例えば、上記参照された３ＧＰＰ　ＴＳ　２３．００３、２３．５０１、２３．５０２、及び３３．５０１は、本発明の解決策の一部と相互作用することができるネットワーク要素／機能及び／または操作の更なる説明を提供することができる。他の３ＧＰＰ　ＴＳ／ＴＲドキュメントは、当業者が実現する他の従来の詳細を提供することができる。しかしながら、５Ｇ関連３ＧＰＰ標準に良好に適合されると共に、実施形態は、いずれかの特定の標準に必ずしも限定されない。
【００１９】
例示的な実施形態は、５Ｇネットワークと関連付けられたサブスクリプション識別子管理に関連する。そのような例示的な実施形態を説明する前に、５Ｇネットワークの主要な構成要素の全体的な説明が図１及び図２のコンテキストにおいて以下で説明される。
【００２０】
図１は、例示的な実施形態が実装される通信システム１００を示す。通信システム１００に示される要素は、システム内で提供される主要な機能、例えば、ＵＥアクセス機能、モビリティ管理機能、認証機能、サービングゲートウェイ機能などを表すことを意図していることが理解されよう。そのようにして、図１に示されるブロックは、それらの主要な機能を提供する５Ｇネットワークにおける特定の要素を指す。しかしながら、表される主要な機能のいくつかまたは全てを実装するために、他のネットワーク要素が使用されてもよい。また、５Ｇネットワークの全ての機能が図１に記述されるわけではないことが理解されよう。むしろ、例示的な実施形態の説明を容易にする機能が表される。後続の図は、いくつかの追加の要素／機能を記述することができる。
【００２１】
したがって、示されるように、通信システム１００は、エアインタフェース１０３を介してアクセスポイント（ｇＮＢ）１０４と通信するユーザ機器（ＵＥ）１０２を含む。ＵＥ１０２は、移動局であってもよく、そのような移動局は、例として、携帯電話、コンピュ

ータ、または任意の他のタイプの通信デバイスを含んでもよい。したがって、本明細書で使用される用語「ユーザ機器」は、様々な異なるタイプの移動局、加入者ステーション、またはより一般的に、ラップトップもしくはスマートフォンなどの他の機器に挿入されたデータカードの組み合わせなどの例を含む通信デバイスを包含するように、広義に解釈されることを意図している。そのような通信デバイスは、アクセス端末と一般的に称されるデバイスを包含することも意図している。

【００２２】

一実施形態では、ＵＥ１０２は、ユニバーサル集積回路カード（ＵＩＣＣ）部分及びモバイル機器（ＭＥ）部分から構成される。ＵＩＣＣは、ＵＥのユーザ依存部分であり、少なくとも１つのユニバーサル加入者識別モジュール（ＵＳＩＭ）及び適切なアプリケーションソフトウェアを含む。ＵＳＩＭは、ネットワークにアクセスする加入者を識別及び認証するために使用される、永久的なサブスクリプション識別子及びその関連する鍵を安全に記憶する。ＭＥは、ＵＥのユーザ独立部分であり、端末機器（ＴＥ）機能及び様々なモバイル端末（ＭＴ）機能を含む。

【００２３】

アクセスポイント１０４は、通信システム１００のアクセスネットワークの例示的な部分である。そのようなアクセスネットワークは、例えば、複数の基地局及び１つ以上の関連する無線ネットワーク制御機能を有する５Ｇシステムを含んでもよい。基地局及び無線ネットワーク制御機能は、論理的に別個のエンティティであってもよいが、所与の実施形態では、例えば、基地局ルータまたはフェムトセルアクセスポイントなどの同一の物理ネットワーク要素に実装されてもよい。

【００２４】

この例示的な実施形態におけるアクセスポイント１０４は、モビリティ管理機能１０６に動作可能に結合される。５Ｇネットワークでは、モビリティ管理機能は、アクセス及びモビリティ管理機能（ＡＭＦ）によって実装される。セキュリティアンカー機能（ＳＥＡＦ）も、ＵＥがモビリティ管理機能と安全に接続することを可能にするようＡＭＦにより実装されてもよい。本明細書で使用されるモビリティ管理機能は、他のネットワーク動作の中で、（アクセスポイント１０４を介した）ＵＥとのアクセス及びモビリティ（認証／承認を含む）動作を管理し、またはそうでなければ参加する通信システムのコアネットワーク（ＣＮ）部分における要素または機能（すなわち、エンティティ）である。ＡＭＦは、また、本明細書でより一般的に、アクセス及びモビリティ管理エンティティと称されてもよい。

【００２５】

この例示的な実施形態におけるＡＭＦ１０６は、ホーム加入者機能１０８、すなわち、加入者のホームネットワークに存在する１つ以上の機能に動作可能に結合される。示されるように、それらの機能のいくつかは、統合データ管理（ＵＤＭ）機能と共に認証サーバ機能（ＡＵＳＦ）を含む。ＡＵＳＦ及びＵＤＭ（４Ｇホーム加入者サーバまたはＨＳＳに従って別個にまたは集合的に）は、本明細書でより一般的に、認証エンティティとも称されてもよい。加えて、ホーム加入者機能は、それらに限定されないが、ネットワークスライス選択機能（ＮＳＳＦ）、ネットワーク公開機能（ＮＥＦ）、ネットワークリポジトリ機能（ＮＲＦ）、ポリシー制御機能（ＰＣＦ）、及びアプリケーション機能（ＡＦ）を含んでもよい。

【００２６】

アクセスポイント１０４はまた、ユーザプレーン機能（ＵＰＦ）１１２に動作可能に結合された、サービングゲートウェイ機能、すなわち、セッション管理機能（ＳＭＦ）１１０に動作可能に結合される。ＵＰＦ１１２は、パケットデータネットワーク、例えば、インターネット１１４に動作可能に結合される。そのようなネットワーク要素の更なる典型的な動作及び機能は、それらが例示的な実施形態の焦点ではなく、適切な３ＧＰＰ　５Ｇドキュメントにおいて発見することができるので、ここでは説明されない。

【００２７】

システム要素のこの特定の配置は、例示にすぎず、他の実施形態での通信システムを実装するために追加的または代替的な要素の他のタイプおよび配置が使用されてもよいことが認識されよう。例えば、他の実施形態では、システム１００は、本明細書で明確に示されない他の要素／機能を含んでもよい。

【００２８】

したがって、図１の配置は、無線セルラシステムの一実施例の構成にすぎず、システム要素の多数の代替的な構成が使用されてもよい。例えば、単一の要素／機能のみが図１の実施形態に示されたが、これは、説明の簡易化及び明確さのためであるにすぎない。もちろん、所与の代替的な実施形態は、より多くの数のそのようなシステム要素と共に、従来のシステムの実装態様と共通して関連付けられたタイプの追加の要素または代替的な要素を含んでもよい。

【００２９】

図１はまた、システム要素を単一の機能的ブロックとして示すが、５Ｇネットワークを構成する様々なサブネットワークがいわゆるネットワークスライスに区画化されることにも留意されよう。ネットワークスライス（ネットワーク区画）は、共通物理インフラストラクチャ上でのネットワーク機能仮想化（ＮＦＶ）を使用した各々の対応するサービスタイプに対する一連のネットワーク機能（ＮＦ）セット（すなわち、機能チェーン）を含む。ネットワークスライスは、所与のサービス、例えば、ｅＭＢＢサービス、大規模ＩｏＴサービス、及びミッションクリティカルＩｏＴサービスに対して必要に応じてインスタンス化される。よって、ネットワークスライスまたは機能は、そのネットワークスライスまたは機能のインスタンスが作成されるときにインスタンス化される。いくつかの実施形態では、これは、下層にある物理インフラストラクチャの１つ以上のホストデバイス上でネットワークスライスまたは機能をインストールすること、またはそうでなければ稼働させることを伴う。ＵＥ１０２は、ｇＮＢ１０４を介してそれらのサービスのうちの１つ以上にアクセスするように構成される。

【００３０】

図２は、例示的な実施形態においてサブスクリプション識別子管理を認証手順の一部として提供するユーザ機器２０２及びネットワーク要素／機能２０４を含む通信システム２００の一部のブロック図である。一実施形態では、ネットワーク要素／機能２０４は、ＵＤＭ（上記説明されたような）であってもよい。しかしながら、ネットワーク要素／機能２０４は、サブスクリプション識別子管理及び本明細書で説明される他の認証技術を提供するように構成可能である任意のネットワーク要素／機能を表すことができることが認識されよう。

【００３１】

ユーザ機器２０２は、メモリ２１６及びインタフェース回路２１０に結合されたプロセッサ２１２を含む。ユーザ機器２０２のプロセッサ２１２は、プロセッサによって実行される少なくともソフトウェアの形態で実装することができる、認証処理モジュール２１４を含む。処理モジュール２１４は、サブスクリプション識別子管理、並びに後続の図及び本明細書におけるその他の箇所と関連して説明される他の関連する技術を実行する。ユーザ機器２０２のメモリ２１６は、サブスクリプション識別子管理及び他の動作の間に生成され、またはそうでなければ使用されるデータを記憶するサブスクリプション識別子管理データ記憶モジュール２１８を含む。

【００３２】

ネットワーク要素／機能２０４は、メモリ２２６及びインタフェース回路２２０に結合されたプロセッサ２２２を含む。ネットワーク要素／機能２０４のプロセッサ２２２は、プロセッサ２２２によって実行される少なくともソフトウェアの形態で実装することができる、認証処理モジュール２２４を含む。処理モジュール２２４は、ＵＥ２０２によって提供されるサブスクリプション識別子を使用した認証技術、並びに後続の図及び本明細書におけるその他の箇所と関連して説明される他の技術を実行する。ネットワーク要素／機能２０４のメモリ２２６は、認証動作及び他の動作の間に生成され、またはそうでなければ

使用されたデータを記憶する認証処理データ記憶モジュール２２８を含む。
【００３３】
ユーザ機器２０２及びネットワーク要素／機能２０４のそれぞれのプロセッサ２１２及び２２２は、例えば、マイクロプロセッサ、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）、デジタルシグナルプロセッサ（ＤＳＰ）、または他のタイプの処理デバイスもしくは集積回路と共に、そのような要素の一部または組み合わせを含んでもよい。そのような集積回路デバイスと共に、それらの一部または組み合わせは、その用語が本明細書で使用されるように、「回路」の例である。例示的な実施形態を実装することにおいて、ハードウェア及び関連するソフトウェアまたはファームウェアの多種多様な他の配置が使用されてもよい。
【００３４】
ユーザ機器２０２及びネットワーク要素／機能２０４のそれぞれのメモリ２１６及び２２６は、本明細書で説明される機能性の少なくとも一部を実装するよう、それぞれのプロセッサ２１２及び２２２によって実行される１つ以上のソフトウェアプログラムを記憶するために使用されてもよい。例えば、サブスクリプション識別子管理動作、並びに後続の図及び本明細書におけるその他の箇所と関連して説明される他の認証機能性は、プロセッサ２１２及び２２２によって実行されるソフトウェアコードを使用した直接的な様式で実装されてもよい。
【００３５】
したがって、メモリ２１６または２２６の所与の１つは、本明細書でより一般的にコンピュータプログラム製品と称されるもの、または更により一般的にそこで具体化された実行可能プログラムコードを有するプロセッサ可読記憶媒体と称されるものの例として見なされてもよい。プロセッサ可読記憶媒体の他の例は、任意の組み合わせでのディスクまたは他のタイプの磁気媒体もしくは光学媒体を含んでもよい。例示的な実施形態は、そのようなコンピュータプログラム製品または他のプロセッサ可読記憶媒体を含む製品を含むことができる。
【００３６】
メモリ２１６または２２６はより具体的に、例えば、スタティックＲＡＭ（ＳＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、または他のタイプの揮発性もしくは不揮発性電子メモリなどの電子的ランダムアクセスメモリ（ＲＡＭ）を含んでもよい。後者は、例えば、フラッシュメモリ、磁気ＲＡＭ（ＭＲＡＭ）、相変化ＲＡＭ（ＰＣ－ＲＡＭ）、強誘電体ＲＡＭ（ＦＲＡＭ）などの不揮発性メモリを含んでもよい。本明細書で使用される用語「メモリ」は、広義に解釈されることを意図しており、加えてまたは代わりに、例えば、リードオンリメモリ（ＲＯＭ）、ディスクベースメモリ、または他のタイプの記憶装置と共に、そのようなデバイスの一部または組み合わせを包含してもよい。
【００３７】
ユーザ機器２０２及びネットワーク要素／機能２０４のそれぞれのインタフェース回路２１０及び２２０は、関連するシステム要素が本明細書で説明される様式において相互に通信することを可能にする送受信機または他の通信ハードウェアもしくはファームウェアを例示的に含む。
【００３８】
ユーザ機器２０２は、それらのインタフェース回路２１０及び２２０のそれぞれを介してネットワーク要素／機能２０４と通信するよう構成され、その逆もまた可能であることが図２から明らかである。ネットワーク要素／機能２０４がＵＤＭである場合、ユーザ機器及びＵＤＭは、ｇＮＢ１０４及びＡＭＦ１０６を介して（図１に示すようにように）動作可能に結合され、ｇＮＢ１０４及びＡＭＦ１０６を介して通信する。この通信は、ユーザ機器２０２がネットワーク要素／機能２０４にデータを送信すること、及びネットワーク要素／機能２０４がユーザ機器２０２にデータを送信することを伴う。しかしながら、代替的な実施形態では、より多くのまたはより少ないネットワーク要素（ｇＮＢ及びＡＭＦに加えてまたはそれらに代えて）が、ネットワーク要素／機能２０２及び２０４の間で動

作可能に結合されてもよい。本明細書で使用される用語「データ」は、それらに限定されないが、メッセージ、識別子、鍵、インジケータ、ユーザデータ、制御データなどを含む、ユーザ機器と１つ以上のネットワーク要素／機能との間で送信することができるあらゆるタイプの情報を包含するように広義に解釈されることを意図している。

【００３９】

図２に示される特定の配置の構成要素は例にすぎず、他の実施形態では多数の代替的な構成が使用されてもよいことが認識されよう。例えば、追加の構成要素または代替的な構成要素を組み込み、他の通信プロトコルをサポートするよう、任意の所与のネットワーク要素／機能が構成されてもよい。

【００４０】

他のシステム要素（それに限定されないが、図１に示された他の要素など）は各々、プロセッサ、メモリ、及びネットワークインタフェースなどの構成要素を含むようにも構成されてもよい。それらの要素は、別個のスタンドアロン処理プラットフォーム上に実装される必要はないが、代わりに、例えば、単一の共通処理プラットフォームの異なる機能的部分を表す。

【００４１】

上記説明された一般的概念を仮定して、サブスクリプション識別子管理の問題に対処する例示的な実施形態がここで説明される。

【００４２】

上記言及されたように、レガシー４Ｇ（ＬＴＥ）通信システムでは、永久的なサブスクリプション識別子は典型的には、ＵＥの国際移動局識別子（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｍｏｂｉｌｅ Ｓｔａｔｉｏｎ Ｉｄｅｎｔｉｆｉｅｒ）、すなわち、ＩＭＳＩである。上記参照された３ＧＰＰ ＴＳ ２３．００３において定義されるように、ＩＭＳＩは、モバイル国コード（ＭＣＣ）、モバイルネットワークコード（ＭＮＣ）、及び移動局識別番号（ＭＳＩＮ）から構成される。典型的には、サブスクリプション識別子が保護される必要がある場合、ＩＭＳＩのＭＳＩＮ部分のみが暗号化される必要がある。ＭＮＣ及びＭＣＣ部分は、正確なホームネットワークに経路指定するためにサービングネットワークによって使用される、ルーティング情報を提供する。５Ｇ通信システムでは、永久的なサブスクリプション識別子は、加入者永久識別子（Ｓｕｂｓｃｒｉｂｅｒ Ｐｅｒｍａｎｅｎｔ Ｉｄｅｎｔｉｆｉｅｒ）、すなわち、ＳＵＰＩと称される。ＩＭＳＩと同様に、ＳＵＰＩは、加入者を一意に識別するためにＭＳＩＮを利用してもよい。ＳＵＰＩのＭＳＩＮが暗号化されるとき、それは、サブスクリプション秘匿化識別子（Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｃｏｎｃｅａｌｅｄ Ｉｄｅｎｔｉｆｉｅｒ）、すなわち、ＳＵＣＩと称される。

【００４３】

しかしながら、異なる動作シナリオでは、ＵＥは、サブスクリプション識別子をＳＵＣＩ、ＳＵＰＩ、またはＩＭＳＩとして表す必要がある場合があることが本明細書で理解される。それらの問題及び他のサブスクリプション識別子管理の問題に対処するために、例示的な実施形態は、サブスクリプション識別子に対する統合された表現構造を提案する。

【００４４】

より具体的には、例示的な実施形態は、ＵＥによってネットワークに送信される登録要求メッセージ、並びに５Ｇネットワークにおける ＵＥ認証手順において適切なサブスクリプション識別子表現、すなわち、ＳＵＰＩもしくはその暗号化された形態のＳＵＣＩ、または更にはＩＭＳＩを使用する課題に対処する（同一または類似の統合データ構造がネットワークエンティティの間で交換されてもよいことに留意されたい）。例えば、５Ｇ認証及び鍵合意（ＡＫＡ）手順（例えば、上記参照された３ＧＰＰ ＴＳ ３３．５０１を参照）を実行する間にＵＥは、３つの異なるフォーマットＳＵＣＩ、ＳＵＰＩ、またはＩＭＳＩにおいてサブスクリプション識別子を提示する必要がある場合がある。認証手順が拡張可能認証プロトコル（ＥＡＰ）ＡＫＡ’手順（例えば、上記参照された３ＧＰＰ ＴＳ ３３．５０１を参照）を使用している場合、次いで、表現は、Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ（ＩＥＴＦ）Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍ

ｍｅｎｔ（ＲＦＣ）７５４２、「Ｔｈｅ　Ｎｅｔｗｏｒｋ　Ａｃｃｅｓｓ　Ｉｄｅｎｔｉｆｉｅｒ」、２０１５年５月において定義されるように、ネットワークアクセス識別子（ＮＡＩ）フォーマット、すなわち「ｊｏｅ＠ｅｘａｍｐｌｅ．ｃｏｍ」を使用し、その開示は参照によりその全体が本明細書に組み込まれる。

【００４５】

異なるサブスクリプション識別子フォーマットの課題は、上記参照されたＴＳ　３３．５０１においても、いかなる他のステージ３の仕様においても対処されない。「Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ　Ｇｒｏｕｐ　Ｓｅｒｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍ　Ａｓｐｅｃｔｓ；３ＧＰＰ　Ｓｙｓｔｅｍ　Ａｒｃｈｉｔｅｃｔｕｒｅ　Ｅｖｏｌｕｔｉｏｎ（ＳＡＥ）；Ｓｙｓｔｅｍ　ａｒｃｈｉｔｅｃｔｕｒｅ」と題する３ＧＰＰ　Ｔｅｃｈｎｉｃａｌ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ（ＴＳ）３３．４０１、Ｖ１５．３．０では、ＩＭＳＩの使用法のみが定義されており、その開示は参照によりその全体が本明細書に組み込まれる。

【００４６】

図３Ａは、１つ以上の例示的な実施形態を実装することができる、ＩＭＳＩフォーマット３００を示す。示されるように、フォーマット３００は、固定された１５桁の長さを含み、３桁のモバイル国コード（ＭＣＣ）、３桁のモバイルネットワークコード（ＭＮＣ）、及び９桁の移動局識別番号（ＭＳＩＮ）から構成される。いくつかのケースでは、ＭＮＣは、２桁であってもよく、ＭＳＩＮは、１０桁であってもよい。ＩＭＳＩに関する更なる詳細は、上記参照された３ＧＰＰ　ＴＳ　２３．００３において定義される。

【００４７】

上記説明されたように、認証手順がＥＡＰ－ＡＫＡ’手順またはＥＡＰトランスポートレイヤセキュリティ（ＴＬＳ）手順（各々が上記参照された３ＧＰＰ　ＴＳ　３３．５０１において定義される）を使用している場合、次いで、サブスクリプション識別子表現は、ＮＡＩフォーマットを使用する。ＲＦＣ７５４２は、３ＧＰＰについて、「ユーザ名」部分は、デバイス固有情報から導出された一意な識別子であり、「レルム（ｒｅａｌｍ）」部分は、ホームネットワークとそれに続くベース文字列「３ｇｐｐｎｅｔｗｏｒｋ．ｏｒｇ」に関する情報から構成される。例えば、ＮＡＩフォーマットにおけるサブスクリプション識別子は、以下のように表されてもよい。

２３４１５０９９９９９９９９９＠ｉｍｓ．ｍｎｃ０１５．ｍｃｃ２３４．３ｇｐｐｎｅｔｗｏｒｋ．ｏｒｇ

【００４８】

したがって、ＥＡＰ－ＡＫＡ’手順について、ＵＥは、ＲＦＣ７５４２において指定されるようなＮＡＩフォーマットにおけるそのサブスクリプション識別子ＳＵＰＩまたはＳＵＣＩ、例えば、ＭＳＩＮ＠ｍｎｃ．ｍｃｃ．３ｇｐｐｎｅｔｗｏｒｋ．ｏｒｇを符号化する。

【００４９】

図３Ｂ及び図３Ｃはそれぞれ、１つ以上の例示的な実施形態を実装することができる、ＳＵＰＩフォーマット３１０及びＳＵＣＩフォーマット３２０を示す。この例では、ＳＵＰＩフォーマット３１０は、ＭＣＣフィールド（３桁）、並びにＭＮＣフィールド（３桁）、ＭＳＩＮ及びＵＤＭセレクタ（８ビット）を含む。ＳＵＣＩフォーマット３２０は、ＳＵＰＩフォーマット３１０の暗号化された形態であり、示されるように、ＭＣＣフィールド（３桁）、及びＭＮＣフィールド（３桁）、ＵＤＭセレクタフィールド、暗号化ＭＳＩＮ、並びに暗号化ＭＳＩＮを復号化するパラメータを含む。

【００５０】

３ＧＰＰ　ＳＡ３では、暗号化識別子をＳＵＣＩとして使用しながら、ＳＵＰＩのＭＳＩＮ部分を暗号化するために、少なくとも２つの楕円曲線、楕円曲線統合暗号化スキーム（ＥＣＩＥＳ）曲線Ａ及び曲線Ｂをサポートすることが合意されている。後続のリリースでは、３ＧＰＰは、曲線の楕円曲線暗号化（ＥＣＣ）ファミリからより多くのもしくはより少ない曲線を指定する可能性があり、またはＭＳＩＮを暗号化するためにプロプライエタ

リ曲線の使用を可能にする可能性がある。しかしながら、標準化スキームを使用することが好ましいと共に、ネットワークオペレータも、それ自体の特定の暗号化方法を使用することを決定することができることが理解される。更に、特に転換期では、ネットワークオペレータは、ＳＵＣＩに対してヌルスキームのみを使用するようデバイスを構成することができる。ヌルスキーム（ｎｕｌｌｓｃｈｅｍｅ）は、暗号化及び復号化の両方に適用される、入力と同一の出力を返すように実装される（すなわち、ＭＳＩＮが暗号化されない）。ヌルスキームは、ＳＵＣＩにおいてスキーム識別子によって示され、よって、同様の様式において統合サブスクリプション識別子フォーマットによって提示されてもよい。

【００５１】

秘匿化されたサブスクリプション識別子ＳＵＣＩがコアネットワークにおいてＵＥ（図１における１０２）とＵＤＭ（図１における１０８の一部）との間で交換されるので、ＵＤＭは、ＵＥがＭＳＩＮをどのように符号化したことを理解することが可能であるように構成される必要がある。よって、認証処理の間にＵＥとＵＤＭとの間で他のメッセージが交換されないので、符号化する方法は、符号化された出力自体とともに交換されたフォーマットの一部である必要がある。したがって、ＳＵＣＩを表すスキームは、複数のフィールドに適合するよう柔軟な表現をサポートする必要があり、各々のフィールドが複数のオプションをサポートするために十分に柔軟であることが理解される。

【００５２】

例示的な実施形態は、サブスクリプション識別子を表すよう統合された構造を提供することによって、上記課題及び他の課題に対処する。例えば、１つの例示的な実施形態における統合された構造は、ＳＵＣＩ、ＳＵＰＩ、及びＩＭＳＩなどのサブスクリプション識別子と共に、認証動作及び他の動作の間の各々の識別子の使用と関連付けられた様々なオプションを表すことができる。

【００５３】

図４は、例示的な実施形態に従った、統合サブスクリプション識別子フォーマット（データ構造）４００を示す。更に、図５は、図４の統合サブスクリプション識別子フォーマット４００に示される各々のフィールドについての例示的なフィールド長５００を示す。

【００５４】

示されるように、統合サブスクリプション識別子フォーマット４００は、以下のフィールドを含む（括弧内の例示的なフィールド長を有する）。

ＭＣＣフィールド４０２（２４ビット／３桁）、
ＭＮＣフィールド４０４（２４ビット／３桁）、
ＵＤＭ選択パラメータフィールド４０６（８ビット）、
暗号化オン／オフフィールド４０８（１ビット）、
ＫＤＦ（鍵導出関数）フィールド４１０（３ビット）、
ＫＤＦの任意選択のパラメータフィールド４１２（ｎビット／任意選択のパラメータに依存）、
識別子タイプＳＵＰＩ／ＳＵＣＩ／ＩＭＳＩフィールド４１４（２ビット）、
暗号化フィールド４１６（４ビット）に対して選択されたＥＣＩＥＳ曲線、
一時的公開鍵ペアフィールド４１８（２５６ビット）、
暗号化されたＭＳＩＮの長さフィールド４２０（４ビット／１２８、１９２、２５６、５１２ビット／ＭＳＩＮフォーマットに依存）、
ＭＳＩＮまたは暗号化されたＭＳＩＮフィールド４２２（フィールド４２０において指定された長さ）、
ＭＳＩＮ　ＭＡＣ（選択されたＥＣＩＥＳ曲線を使用して計算されたＭＳＩＮフィールドのメッセージ認証コード）フィールド４２４（２５６ビット）、及び
暗号化アルゴリズム識別子フィールド４２６（４ビット）

【００５５】

本明細書で説明されるフィールド長は、本質的に例示的であり、よって、限定することを意図していないことが認識されよう。ＵＥ及び５Ｇネットワークが機能する動作シナリオ

に応じて、フィールド長は、異なる値に設定されてもよい。代替的な実施形態では、１つ以上の他のフィールドがデータ構造に追加されてもよく、並びに／または上記フィールドのいくつかが削除されてもよく、及び／もしくは単純に使用されなくてもよいことも認識されよう。また、図４における構造フォーマット４００内のフィールドの位置付けは、本質的に例示的であり、よって、他の実施形態では、代替的なフィールド配列が考慮される。単に例として、データ構造の一部であり得る（または、ＵＤＭ選択もしくは他のフィールドにおいて示され得る）１つの追加のフィールドは、ネットワークスライス選択支援情報（ＮＳＳＡＩ）フィールドである。

【００５６】

いくつかの例示的な実施形態は、ＵＥが所与のＵＤＭ（または、１つ以上の他のネットワークエンティティ）に完全な統合サブスクリプション識別子データ構造（すなわち、図４における４００）を送信することをもたらすと共に、代替的な例示的な実施形態は、送信オーバヘッドを最小化するよう、例えば、ＫＤＦ、ＫＤＦの任意選択のパラメータ、選択された楕円曲線、暗号化アルゴリズム識別子などの多くの指標となるパラメータの搬送を回避する。そのようにして、代替的な例示的な統合サブスクリプション識別子データ構造６００が図６に記述される。示されるように、統合サブスクリプション識別子フォーマット６００は、以下のフィールドを含む（括弧内の例示的なフィールド長を有する）。

ＭＣＣフィールド６０２（２４ビット／３桁）、

ＭＮＣフィールド６０４（２４ビット／３桁）、

ＵＤＭ選択パラメータフィールド６０６（８ビット）、

識別子タイプＳＵＰＩ／ＳＵＣＩ／ＩＭＳＩフィールド６０８（２ビット）、

暗号化されたＭＳＩＮの長さフィールド６１０（４ビット／１２８、１９２、２５６、５１２ビット／ＭＳＩＮフォーマットに依存）、

ＭＳＩＮまたは暗号化されたＭＳＩＮフィールド６１２（フィールド６１０において指定された長さ）、

ＭＳＩＮ　ＭＡＣ（選択されたＥＣＩＥＳ曲線を使用して計算されたＭＳＩＮフィールドのメッセージ認証コード）フィールド６１４（２５６ビット）、及び

プロファイル選択フィールド６１６（４ビット）

【００５７】

本明細書で説明されるフィールド長は、本質的に例示的であり、よって、限定することを意図していないことが認識されよう。ＵＥ及び５Ｇネットワークが機能する動作シナリオに応じて、フィールド長は、異なる値に設定されてもよい。代替的な実施形態では、１つ以上の他のフィールドがデータ構造に追加されてもよく、並びに／または上記フィールドのいくつかが削除されてもよく、及び／もしくは単純に使用されなくてもよいことも認識されよう。また、図６における構造フォーマット６００内のフィールドの位置付けは、本質的に例示的であり、よって、他の実施形態では、代替的なフィールド配列が考慮される。単に例として、データ構造の一部であり得る（または、ＵＤＭ選択もしくは他のフィールドにおいて示され得る）１つの追加のフィールドは、ネットワークスライス選択支援情報（ＮＳＳＡＩ）フィールドである。

【００５８】

フィールド６０２～６１４は、データ構造４００におけるそれらの同じように命名された対応するものと同一の情報を提供する。しかしながら、データ構造６００は、プロファイル選択フィールド６１６を含む。ＵＥとＵＤＭとの間で統合サブスクリプション識別子表現フォーマットにおいて使用されることになる特定の標準プロファイルを事前に確立することが有益となり得ることが理解される。それらの合意されたプロファイルは、事前に設定された値として定義されてもよい（単に例として、暗号化フィールドに対して選択された４ビットのＥＣＩＥＳ曲線）。そのようなケースでは、プロファイルからの合意された値は、送信側ＵＥ及びＵＤＭによって使用され、それらのパラメータについての値の実際の交換を回避する。

【００５９】

例えば、統合サブスクリプション識別子データ構造のそのようなプロファイルベースの縮小されたフィールドバージョンでは、ＵＤＭは、「００１１」（４ビットである場合）の所与のプロファイル選択フィールドが、図６の縮小されたフィールドバージョンでは送信されない図４のフォーマットからのフィールドに対する特定の予め定められた設定に対応し、「１０１０」のプロファイル選択フィールドは、異なる予め定められた設定を意味する、などを知るように構成される。よって、ＵＤＭは、（ＵＥが異なる認証シナリオを選択するように構成されるので）ＵＥが送信する各々のとり得るプロファイルについてのデータ構造を事前に記憶する（または、リアルタイムで取得する）。

【００６０】

例示的な実施形態は、統合サブスクリプション識別子フォーマット４００及び６００と共に、代替的な変形をサポートするよう、全てのＵＥ（例えば、図１における１０２）、並びにそれらに限定されないが、ｇＮＢ（図１における１０４）、ＡＭＦ（図１における１０６の部分）、ＳＥＡＦ（図１における１０６の部分）、ＡＵＳＦ（図１における１０８の部分）、及びＵＤＭ（図１における１０８の部分）などのネットワーク要素／機能を提供する。

【００６１】

図７は、例示的な実施形態に従った、ＵＥの観点から統合サブスクリプション識別子フォーマット（例えば、図４のデータ構造４００または図６のデータ構造６００）を利用する方式７００を示す。

【００６２】

ステップ７０２では、ＵＥは、永久的なサブスクリプション識別子（ＳＵＰＩ）またはＩＭＳＩを維持する。

【００６３】

ステップ７０４では、ＵＥは、ＵＤＭの公開鍵と共に、それ自体の秘密鍵／公開鍵のペアを維持する。

【００６４】

ステップ７０６では、ＵＥは、ＭＳＩＮを暗号化するパラメータ（アルゴリズム、曲線など）を選択する。

【００６５】

ステップ７０８では、ＵＥは、識別子タイプ、暗号化アルゴリズム、曲線インジケータ、公開鍵、暗号化されたＭＳＩＮ、ＭＳＩＮ　ＭＡＣ、ＭＣＣ、ＭＮＣ、ＵＤＭセレクタ、ＫＤＦ、任意選択のＫＤＦパラメータなどを使用して、統合サブスクリプション識別子データ構造（例えば、図４における４００）を構築する。

【００６６】

ステップ７１０では、ＵＥは、ネットワークアクセス要求（例えば、登録要求）の間、選択されたＵＤＭに統合サブスクリプション識別子データ構造を送信する。一実施形態では、統合サブスクリプション識別子データ構造は、図４のデータ構造４００（すなわち、全てのフィールドを埋め込んだバージョン）であってもよく、代替的な実施形態では、統合サブスクリプション識別子データ構造は、図６のデータ構造６００（プロファイルベースの縮小されたフィールドバージョン）であってもよい。更なる代替的な実施形態では、統合サブスクリプション識別子データ構造の他の変形が送信されてもよい。ネットワークエンティティ（例えば、ＵＤＭ）はまた、そのような統合サブスクリプション識別子データ構造を構築し、またはそうでなければ取得／維持するように構成される。

【００６７】

図８は、例示的な実施形態に従った、ネットワークエンティティ（例えば、本明細書で説明されるネットワーク要素／機能のうちの１つ以上）の観点から統合サブスクリプション識別子フォーマット（例えば、図４のデータ構造４００または図６のデータ構造６００）を利用する方式８００を示す。

【００６８】

ステップ８０２では、ネットワークエンティティは、統合サブスクリプション識別子デー

タ構造を受信する。

【００６９】

ステップ８０４では、ネットワークエンティティは、必要に応じて統合サブスクリプション識別子データ構造を復号化する。

【００７０】

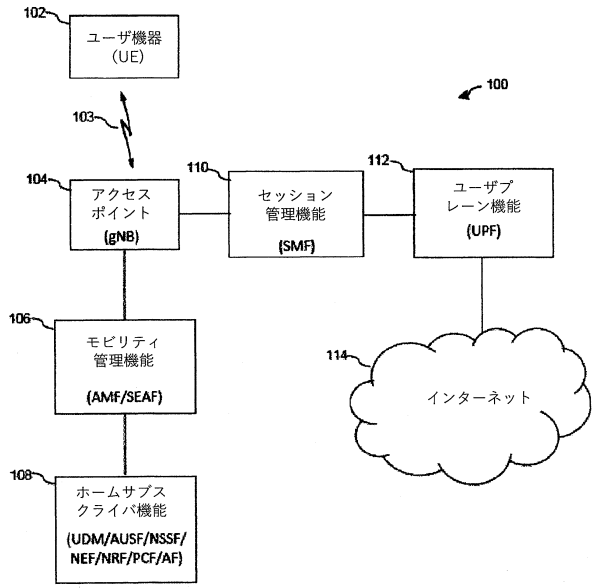
ステップ８０６では、ネットワーク要素は、受信されたデータ構造における選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいて、送信側ＵＥの認証を実行する。

【００７１】

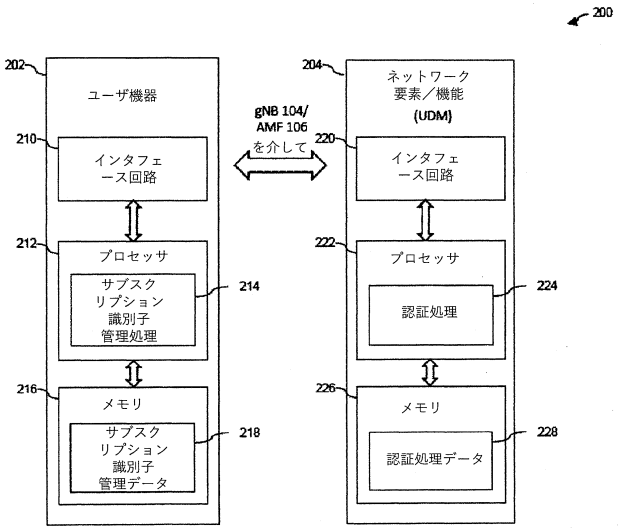
したがって、本明細書で説明される様々な実施形態は、例示的な実施例のみによって提示され、特許請求の範囲を限定するものとして解釈されるべきではないことが再度強調されるべきである。例えば、代替的な実施形態は、例示的な実施形態のコンテキストにおいて上記説明されたものとは異なる通信システム構成、ユーザ機器構成、基地局構成、鍵ペアのプロビジョニング及び使用プロセス、メッセージングプロトコル、並びにメッセージフォーマットを利用することができる。添付の特許請求の範囲内のそれらの及び多数の他の代替的な実施形態が当業者にとって容易に明らかであろう。

【図面】

【図１】



【図２】



【図３】

【図３Ａ】

300

IMSI		
MCC（３桁）	MNC（３桁）	MSIN（９桁）

【図３Ｂ】

310

SUPI			
MCC（３桁）	MNC（３桁）	UDM セレクタ（８ビット）	MSIN

【図３Ｃ】

320

SUCI			
MCC（３桁）	MNC（３桁）	UDM セレクタ	暗号化（MSIN）
暗号化ＭＳＩＮを復号化するパラメータ			

【図４】

400

サブスクリプション識別子(SUCI, SUPI, IMSI)		
MCC 402	MNC 404	UDM 選択パラメータ 406
暗号化オン／オフ 408	KDF 410	KDF の任意選択のパラメータ 412
識別子タイプ SUPI/SUCI/IMSI 414	暗号化に対して選択されたＥＣＩＥＳ曲線 416	一時的公開鍵ペア 418
暗号化されたＭＳＩＮの長さ 420	暗号化されたＭＳＩＮ 422	MSIN MAC 424
暗号化アルゴリズム識別子フィールド 426		

【図５】

500

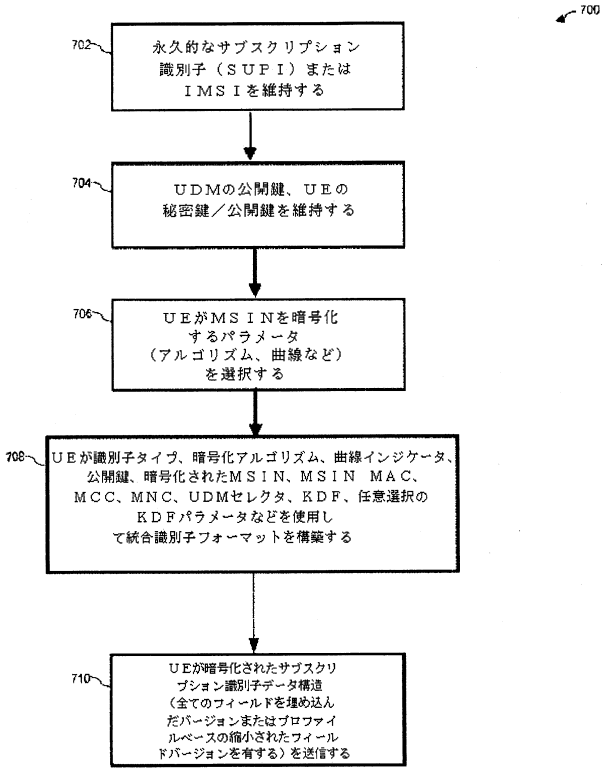
フィールド		長さ（ビット）
識別子タイプ(SUPI、SUCI、IMSI)	414	２ビット
暗号化オン／オフ	408	１ビット
暗号化アルゴリズム識別子	426	４ビット
暗号化に対して選択されたＥＣＩＥＳ曲線	416	４ビット
送信側の一時的公開鍵	418	256ビット
暗号化されたＭＳＩＮの長さ	420	４（128ビット、192ビット、256ビット、512ビット）
暗号化されたＭＳＩＮ	422	（フィールド４２０において指定された長さ）
MSIN MAC（ＥＣＩＥＳ曲線を使用して計算されたＭＳＩＮフィールドのメッセージ認証）	424	256ビット
ＵＤＭ選択パラメータ	406	８ビット
MCC	402	24ビット（３桁）
MNC	404	24ビット（３桁）
暗号化に対して使用されるＫＤＦ	410	３ビット
ＫＤＦの任意選択のパラメータ	412	ｎビット

【図６】

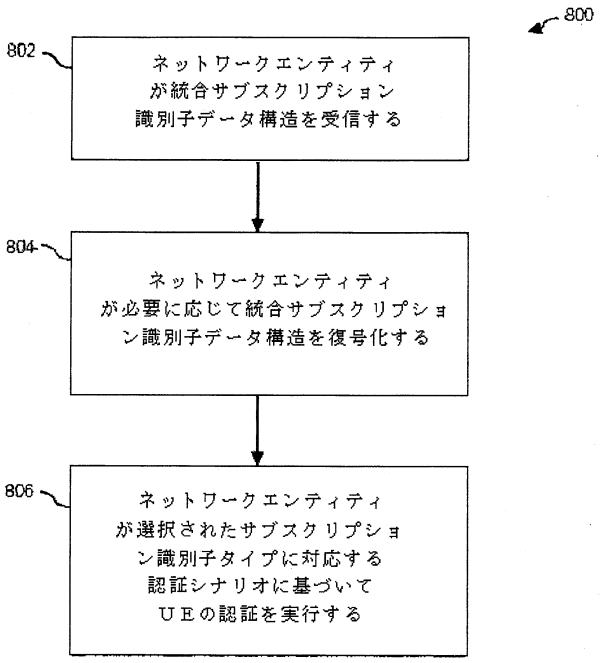
600

サブスクリプション識別子(SUCI, SUPI, IMSI)		
MCC 602	MNC 604	UDM 選択パラメータ 606
識別子タイプ SUPI/SUCI/IMSI 608	暗号化されたＭＳＩＮの長さ 610	暗号化されたMSIN 612
MSIN MAC 614	プロファイル選択 616	

【図７】


700
702
永久的なサブスクリプション識別子（ＳＵＰＩ）またはＩＭＳＩを維持する
704
ＵＤＭの公開鍵、ＵＥの秘密鍵／公開鍵を維持する
706
ＵＥがＭＳＩＮを暗号化するパラメータ（アルゴリズム、曲線など）を選択する
708
ＵＥが識別子タイプ、暗号化アルゴリズム、曲線インジケータ、公開鍵、暗号化されたＭＳＩＮ、ＭＳＩＮ ＭＡＣ、ＭＣＣ、ＭＮＣ、ＵＤＭセレクタ、ＫＤＦ、任意選択のＫＤＦパラメータなどを使用して統合識別子フォーマットを構築する
710
ＵＥが暗号化されたサブスクリプション識別子データ構造（全てのフィールドを埋め込んだバージョンまたはプロファイルベースの縮小されたフィールドバージョンを有する）を送信する

【図８】


800
802
ネットワークエンティティが統合サブスクリプション識別子データ構造を受信する
804
ネットワークエンティティが必要に応じて統合サブスクリプション識別子データ構造を復号化する
806
ネットワークエンティティが選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいてＵＥの認証を実行する

【手続補正書】
【提出日】令和4年5月13日(2022.5.13)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
無線通信システム（１００、２００）に対するユーザ機器（１０２、２０２）であって、
前記無線通信システム（１００、２００）における前記ユーザ機器（１０２、２０２）において、統合サブスクリプション識別子データ構造を構築することと、
前記統合サブスクリプション識別子データ構造（４００、６００）を記憶することであって、前記統合サブスクリプション識別子データ構造（４００、６００）は、選択されたサブスクリプション識別子タイプと関連付けられた２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の選択された１つを指定する複数のフィールド（４０２～４２６、６０２～６１６）を備える、前記記憶することと、
前記選択されたサブスクリプション識別子タイプに対応する認証シナリオに基づいて、前記無線通信システム（１００、２００）と関連付けられた１つ以上のネットワークにアクセスするために、前記統合サブスクリプション識別子データ構造（４００、６００）における２つ以上のサブスクリプション識別子フィールド（３００、３１０、３２０）の前記選択された１つを使用することと、
を実行するように構成されたプロセッサ（２１２）及びメモリ（２１６）を備える、
前記ユーザ機器（１０２、２０２）。

フロントページの続き

弁理士　上杉 浩
(74)代理人　100120525
弁理士　近藤 直樹
(74)代理人　100139712
弁理士　那須 威夫
(74)代理人　100158469
弁理士　大浦 博司
(72)発明者　ネア，スレッシュ
アメリカ合衆国，ニュージャージー州 ０７９８１，ホイッパニー，３３ ディアフィールド ロード
(72)発明者　ジェリチョウ，アンジャ
ドイツ国，８５５６７ グラーフィング，スデテンシュトラーセ ３４
(72)発明者　バイカムパディ，ナゲンドラ エス
インド国，バンガロール ５６０１０２，オフ サージャプラ メイン ロード，ハラル ロード，５９エー イーストウッド レイアウト
(72)発明者　ショイニアナキス，ディミトリオス
ドイツ国，８１５４１ ミュンヘン，ホヘンワルデクシュトラーセ ４７