

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7066746号

(P7066746)

(45)発行日 令和4年5月13日(2022.5.13)

(24)登録日 令和4年5月2日(2022.5.2)

(51)国際特許分類

F I

H 0 4 W 12/02 (2009.01)

H 0 4 W 12/02

H 0 4 W 60/00 (2009.01)

H 0 4 W 60/00

請求項の数 29 (全24頁)

(21)出願番号 特願2019-560230(P2019-560230)
 (86)(22)出願日 平成30年4月30日(2018.4.30)
 (65)公表番号 特表2020-523812(P2020-523812 A)
 (43)公表日 令和2年8月6日(2020.8.6)
 (86)国際出願番号 PCT/US2018/030143
 (87)国際公開番号 WO2018/204235
 (87)国際公開日 平成30年11月8日(2018.11.8)
 審査請求日 令和1年12月20日(2019.12.20)
 (31)優先権主張番号 15/794,856
 (32)優先日 平成29年10月26日(2017.10.26)
 (33)優先権主張国・地域又は機関 米国(US)
 (31)優先権主張番号 62/502,266
 (32)優先日 平成29年5月5日(2017.5.5)
 最終頁に続く

(73)特許権者 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, 0 2 6 1 0 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】 認証要求を制御するためのプライバシーインジケータ

(57)【特許請求の範囲】

【請求項1】

通信ネットワークにおける要素または機能において、前記通信ネットワークのユーザ機器から、1つ以上のプライバシーインジケータを備えるメッセージを受信することと、1つ以上のプライバシーインジケータに基づいてメッセージを処理するための1つ以上のプライバシーフィーチャを決定することと、

を備え、

前記メッセージは、前記ユーザ機器に関連付けられた前記通信ネットワークのサブスクライバに関するサブスクリプション識別子を備える登録要求を備え、前記1つ以上のプライバシーインジケータが、前記登録要求における前記サブスクリプション識別子がプライバシー保護されているかどうかを指示するフィールドを備える、方法。

【請求項2】

プライバシー保護されている前記サブスクリプション識別子が、前記サブスクライバの永続サブスクリプション識別子の少なくとも一部分を備える、請求項1に記載の方法。

【請求項3】

前記1つ以上のプライバシーインジケータに基づいて前記メッセージを処理するための、前記1つ以上のプライバシーフィーチャを決定することが、前記サブスクリプション識別子がプライバシー保護されていることを指示する前記フィールドに応答して、前記登録要求における前記サブスクリプション識別子からプライバシー保護を取り除くことを備える、請求項1に記載の方法。

【請求項 4】

前記通信ネットワークにおける前記要素または機能が、前記サブスクリプション識別子を利用して、前記登録要求をホームサブスクリバサーバ（HSS）またはユーザデータ管理（UDM）機能にマップするサーバ位置特定機能（SLF）を備える、請求項 3 に記載の方法。

【請求項 5】

前記プライバシー保護されている識別子は、前記通信ネットワークにおける前記サブスクリバのホームネットワークオペレータの公開鍵を利用して暗号化されている、請求項 1 に記載の方法。

【請求項 6】

前記 1 つ以上のプライバシーインジケータは、前記メッセージを暗号化するために使用される暗号化アルゴリズムに少なくとも部分的に基づく暗黙のプライバシーインジケータを含む、請求項 1 に記載の方法。

【請求項 7】

前記登録要求は、第 2 のタイプの無線アクセスネットワークを介して前記ユーザ機器を第 1 のタイプのコアネットワークに登録する要求を含む、請求項 1 に記載の方法。

【請求項 8】

前記第 1 のタイプの前記コアネットワークは、4G コアネットワークを含み、前記第 2 のタイプの前記無線アクセスネットワークは、5G 無線アクセスネットワークを含む、請求項 7 に記載の方法。

【請求項 9】

前記フィールドが第 1 の値を含む場合、前記フィールドは前記登録要求における前記サブスクリプション識別子がプライバシー保護されていないことを指示し、
前記フィールドが第 2 の値を含む場合、前記フィールドは前記登録要求における前記サブスクリプション識別子がプライバシー保護されていることを指示する、請求項 1 に記載の方法。

【請求項 10】

前記通信ネットワークは、第 5 世代（5G）システムを含む、請求項 1 に記載の方法。

【請求項 11】

メモリに動作可能に結合され、請求項 1 の方法をおこなうように構成されたプロセッサを備える、装置。

【請求項 12】

通信ネットワークにおける要素または機能において、前記通信ネットワークによってサポートされる 1 つ以上のプライバシーフィーチャ及び前記通信ネットワークが動作している関連領域の 1 つ以上のプライバシー規制を決定し、前記 1 つ以上のプライバシーフィーチャは前記通信ネットワークにおける前記要素または機能が登録要求におけるプライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかの指示を含むものであることと、

前記通信ネットワークにおける前記要素または機能において、前記決定された 1 つ以上のプライバシーフィーチャ及び前記 1 つ以上のプライバシー規制に基づいて選択された、1 つ以上の他のプライバシーインジケータを備えるブロードキャストメッセージを生成し、前記 1 つ以上のプライバシーインジケータは前記通信ネットワークが前記プライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかを指示するフィールドを含むものであることと、

前記通信ネットワークにおける前記要素または機能から前記通信ネットワークの複数のユーザ機器に向けて、前記 1 つ以上のプライバシーインジケータを備える前記生成されたブロードキャストメッセージを送信することと、

前記生成されたブロードキャストメッセージに応答して、前記通信ネットワークにおける前記要素または機能において、前記複数のユーザ機器の少なくとも一部から、それぞれのプライバシー保護されたサブスクリプション識別子を含む 1 つ以上の登録要求を受信するこ

10

20

30

40

50

とと、

前記 1 つ以上の登録要求を処理してそれぞれのサブスクリプション識別子を決定することと、

前記 1 つ以上の登録要求を提供する先の、1 つ以上のホームサブスクリバサーバ（H S S）または 1 つ以上のユーザデータ管理（U D M）機能を識別することと、
を備える、方法。

【請求項 1 3】

前記生成されたブロードキャストメッセージはマスタ情報ブロックを有するシステム情報メッセージ及び 1 つ以上のシステム情報ブロックを含み、前記 1 つ以上のプライバシーインジケータは、前記システム情報メッセージに追加される、請求項 1 2 に記載の方法。

10

【請求項 1 4】

通信ネットワークの装置であって、前記装置はメモリと動作可能に結合したプロセッサを含み、前記プロセッサは、少なくとも、

前記装置において、前記通信ネットワークによってサポートされる 1 つ以上のプライバシーフィーチャ及び前記通信ネットワークが動作している関連領域の 1 つ以上のプライバシー規制を決定し、前記 1 つ以上のプライバシーフィーチャは前記装置が登録要求におけるプライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかの指示を含むものであることと、

前記通信ネットワークにおける前記装置において、前記決定された 1 つ以上のプライバシーフィーチャ及び前記 1 つ以上のプライバシー規制に基づいて選択された、1 つ以上の他のプライバシーインジケータを備えるブロードキャストメッセージを生成し、前記 1 つ以上のプライバシーインジケータは前記通信ネットワークが前記プライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかを指示するフィールドを含むものであることと、

20

前記通信ネットワークにおける前記装置から前記通信ネットワークの複数のユーザ機器に向けて、前記 1 つ以上のプライバシーインジケータを備える前記生成されたブロードキャストメッセージを送信することと、

前記生成されたブロードキャストメッセージに応答して、前記装置において、前記複数のユーザ機器の少なくとも一部から、それぞれのプライバシー保護されたサブスクリプション識別子を含む 1 つ以上の登録要求を受信することと、

30

前記 1 つ以上の登録要求を処理してそれぞれのサブスクリプション識別子を決定することと、

前記 1 つ以上の登録要求を提供する先の、1 つ以上のホームサブスクリバサーバ（H S S）または 1 つ以上のユーザデータ管理（U D M）機能を識別することと、
を実行するように構成された、装置。

【請求項 1 5】

前記生成されたブロードキャストメッセージはマスタ情報ブロックを有するシステム情報メッセージ及び 1 つ以上のシステム情報ブロックを含み、前記 1 つ以上のプライバシーインジケータは、前記システム情報メッセージに追加される、請求項 1 4 に記載の装置。

【請求項 1 6】

40

通信ネットワークにおける要素または機能から、前記通信ネットワークのユーザ機器において、前記通信ネットワークの 1 つ以上のプライバシーフィーチャ及び前記通信ネットワークの 1 つ以上のプライバシー規制の指示を備えるブロードキャストメッセージを受信することと、

前記通信ネットワークの前記ユーザ機器において、少なくとも前記指示に基づいて、メッセージを処理するための前記 1 つ以上のプライバシーフィーチャを決定し、前記メッセージは前記ユーザ機器に関連する前記通信ネットワークのサブスクリバのためのサブスクリプション識別子を含む登録要求を含むものであることと、

前記決定された 1 つ以上のプライバシーフィーチャに基づいて 1 つ以上のプライバシーインジケータを前記メッセージに追加し、前記 1 つ以上のプライバシーインジケータは、前記登録

50

要求における前記サブスクリプション識別子がプライバシー保護されているかどうかを指示するフィールドを含むものであることと、

前記ユーザ機器から前記通信ネットワークにおける要素または機能に、1つ以上のプライバシーインジケータを有する前記メッセージを送信することと、

を備え、

前記1つ以上のプライバシーフィーチャは、プライバシー保護されたサブスクリプション識別子を取り扱うための前記通信ネットワークにおけるネットワークエンティティの能力を含むものである、方法。

【請求項17】

装置であって、前記装置はメモリと動作可能に結合したプロセッサを含み、前記プロセッサは、少なくとも、

通信ネットワークにおける要素または機能から、前記通信ネットワークの1つ以上のプライバシーフィーチャ及び前記通信ネットワークの1つ以上のプライバシー規制の指示を備えるブロードキャストメッセージを受信することと、

少なくとも前記指示に基づいて、メッセージを処理するための前記1つ以上のプライバシーフィーチャを決定し、前記メッセージは前記装置に関連する前記通信ネットワークのサブスクライバのためのサブスクリプション識別子を含む登録要求を含むものであることと、前記決定された1つ以上のプライバシーフィーチャに基づいて1つ以上のプライバシーインジケータを前記メッセージに追加し、前記1つ以上のプライバシーインジケータは、前記登録要求における前記サブスクリプション識別子がプライバシー保護されているかどうかを指示するフィールドを含むものであることと、

前記装置から前記通信ネットワークにおける要素または機能に、前記1つ以上のプライバシーインジケータを有する前記メッセージを送信することと、

を実行するよう構成され、

前記1つ以上のプライバシーフィーチャは、プライバシー保護されたサブスクリプション識別子を取り扱うための前記通信ネットワークにおけるネットワークエンティティの能力を含むものである、装置。

【請求項18】

通信ネットワークのユーザ機器において、前記通信ネットワークにおける要素または機能から、1つ以上のプライバシーインジケータを備えるブロードキャストメッセージを受信し、前記1つ以上のプライバシーインジケータが、前記通信ネットワークにおける前記要素または機能がプライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかを指示するフィールドを備えていることと、

前記ブロードキャストメッセージにおける前記1つ以上のプライバシーインジケータに少なくとも基づいて、前記通信ネットワークによってサポートされる1つ以上のプライバシーフィーチャ及び前記通信ネットワークが動作している関連領域の1つ以上のプライバシー規制を決定し、前記1つ以上のプライバシーフィーチャは、プライバシー保護されたサブスクリプション識別子を取り扱うための前記通信ネットワークの能力を含むものであることと、前記通信ネットワークがプライバシー保護されたサブスクリプション識別子を取り扱うように構成されている場合に、前記ユーザ機器に関連する前記通信ネットワークのサブスクライバのためのサブスクリプション識別子を含む登録要求を含むメッセージに、前記登録要求における前記サブスクリプション識別子はプライバシー保護されているという指示を追加することと、

前記通信ネットワークがプライバシー保護されたサブスクリプション識別子を取り扱うように構成されていない場合に、前記ユーザ機器に関連する前記通信ネットワークの前記サブスクライバのための前記サブスクリプション識別子を含む前記登録要求を含む前記メッセージに、前記登録要求における前記サブスクリプション識別子はプライバシー保護されていないという指示を追加することと、

前記ユーザ機器から前記通信ネットワークにおけるネットワークエンティティに前記メッセージを送信することと、

10

20

30

40

50

を備える、方法。

【請求項 19】

前記 1 つ以上のプライバシーインジケータが前記通信ネットワークはプライバシー保護されたサブスクリプション識別子を取り扱うように構成されていないことを指示する場合、プライバシー保護されたサブスクリプション識別子を含む前記登録要求を前記通信ネットワークにおける前記ネットワークエンティティに送信することを控えること、

をさらに備える、請求項 18 に記載の方法。

【請求項 20】

前記 1 つ以上のプライバシーインジケータに基づいて前記ユーザ機器が前記ユーザ機器に関連する前記通信ネットワークのサブスクライバの真の識別の要求に応答することを禁止すること、

をさらに備える、請求項 18 に記載の方法。

【請求項 21】

前記サブスクライバの前記真の識別の前記要求は、国際移動体加入者識別番号 (IMSI) ページング要求を含む、

請求項 20 に記載の方法。

【請求項 22】

装置であって、前記装置はメモリと動作可能に結合したプロセッサを含み、前記プロセッサは、少なくとも、

通信ネットワークにおける要素または機能から、1 つ以上のプライバシーインジケータを備えるブロードキャストメッセージを受信し、前記 1 つ以上のプライバシーインジケータが、前記通信ネットワークにおける前記要素または機能がプライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかを指示するフィールドを備えていることと、

前記ブロードキャストメッセージにおける前記 1 つ以上のプライバシーインジケータに少なくとも基づいて、前記通信ネットワークによってサポートされる 1 つ以上のプライバシーフィーチャ及び前記通信ネットワークが動作している関連領域の 1 つ以上のプライバシー規制を決定し、前記 1 つ以上のプライバシーフィーチャは、プライバシー保護されたサブスクリプション識別子を取り扱うための前記通信ネットワークの能力を含むものであることと、

前記通信ネットワークがプライバシー保護されたサブスクリプション識別子を取り扱うように構成されている場合に、前記装置に関連する前記通信ネットワークのサブスクライバのためのサブスクリプション識別子を含む登録要求を含むメッセージに、前記登録要求におけるサブスクリプション識別子はプライバシー保護されているという指示を追加することと、前記通信ネットワークがプライバシー保護されたサブスクリプション識別子を取り扱うように構成されていない場合に、前記装置に関連する前記通信ネットワークの前記サブスクライバのための前記サブスクリプション識別子を含む前記登録要求を含む前記メッセージに、前記登録要求における前記サブスクリプション識別子はプライバシー保護されていないという指示を追加することと、

前記装置から前記通信ネットワークにおけるネットワークエンティティに前記メッセージを送信することと、

を実行するように構成された、方法。

【請求項 23】

前記プロセッサは、少なくとも、

前記 1 つ以上のプライバシーインジケータが前記通信ネットワークはプライバシー保護されたサブスクリプション識別子を取り扱うように構成されていないことを指示する場合、プライバシー保護されたサブスクリプション識別子を含む前記登録要求を前記通信ネットワークにおける前記要素または機能に送信することを控えること、

を実行するようにさらに構成された、請求項 22 に記載の装置。

【請求項 24】

前記プロセッサは、少なくとも、

10

20

30

40

50

前記 1 つ以上のプライバシーインジケータに基づいて前記装置が前記装置に関連する前記通信ネットワークのサブスクリバの真の識別の要求に応答することを禁止すること、
を実行するようにさらに構成された、請求項 22 に記載の装置。

【請求項 25】

前記サブスクリバの前記真の識別の前記要求は、国際移動体加入者識別番号（IMSI）ページング要求を含む、
請求項 24 に記載の装置。

【請求項 26】

通信ネットワークのユーザ機器において、1 つ以上のプライバシーインジケータを含むメッセージを生成し、前記メッセージは前記ユーザ機器に関連する前記通信ネットワークのサブスクリバのためのサブスクリプション識別子を含む登録要求を含み、前記 1 つ以上のプライバシーインジケータは、前記登録要求における前記サブスクリプション識別子がプライバシー保護されているかどうかを指示するフィールドを含み、前記 1 つ以上のプライバシーインジケータは、前記メッセージを処理するための 1 つ以上のプライバシーフィーチャを指示するものであることと、
前記通信ネットワークにおけるネットワークエンティティに向けて、前記メッセージを送信することと、
を備える、方法。

【請求項 27】

装置であって、前記装置はメモリと動作可能に結合したプロセッサを含み、前記プロセッサは、少なくとも、
前記装置において、1 つ以上のプライバシーインジケータを含むメッセージを生成し、前記メッセージはユーザ機器に関連する通信ネットワークのサブスクリバのためのサブスクリプション識別子を含む登録要求を含み、前記 1 つ以上のプライバシーインジケータは、前記登録要求における前記サブスクリプション識別子がプライバシー保護されているかどうかを指示するフィールドを含み、前記 1 つ以上のプライバシーインジケータは、前記メッセージを処理するための 1 つ以上のプライバシーフィーチャを指示するものであることと、
前記通信ネットワークにおけるネットワークエンティティに向けて、前記メッセージを送信することと、
を実行するよう構成された、装置。

【請求項 28】

ユーザ機器において、通信ネットワークにおけるネットワークエンティティから 1 つ以上のプライバシーインジケータを含むブロードキャストメッセージを受信し、前記 1 つ以上のプライバシーインジケータは 1 つ以上のプライバシーフィーチャを指示し、前記 1 つ以上のプライバシーインジケータは、フィールドを含み、前記フィールドは前記ネットワークエンティティがプライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかを指示するものであることと、
前記ブロードキャストメッセージを受信したことに応答して、前記ユーザ機器から、前記ネットワークエンティティに向けて、1 つ以上のプライバシー保護されたサブスクリプション識別子を含む登録要求を送信することと、
を備える、方法。

【請求項 29】

装置であって、前記装置はメモリと動作可能に結合したプロセッサを含み、前記プロセッサは、少なくとも、
前記装置において、通信ネットワークにおけるネットワークエンティティから 1 つ以上のプライバシーインジケータを含むブロードキャストメッセージを受信し、前記 1 つ以上のプライバシーインジケータは 1 つ以上のプライバシーフィーチャを指示し、前記 1 つ以上のプライバシーインジケータは、フィールドを含み、前記フィールドは前記ネットワークエンティティがプライバシー保護されたサブスクリプション識別子を取り扱うように構成されているかどうかを指示するものであることと、

10

20

30

40

50

前記ブロードキャストメッセージを受信したことに応答して、前記装置から、前記ネットワークエンティティに向けて、1つ以上のプライバシー保護されたサブスクリプション識別子を含む登録要求を送信することと、
を実行するように構成された、装置。

【発明の詳細な説明】

【技術分野】

【0001】

本出願は、その開示が引用によりその全体が本明細書に組み込まれる、2017年5月5日に出願された、「Privacy Indicator for Controlling Authentication Requests」という名称の、米国整理番号第62/502,266号として識別される米国仮特許出願の優先権を主張するものである。

【0002】

本分野は、一般に、通信システムに関し、より詳細には、ただし、排他的にではなく、そのようなシステム内のセキュリティに関する。

【背景技術】

【0003】

本節は、本発明のより良い理解を容易にするために役立つことが可能な態様について紹介する。したがって、本節の記述は、この観点から読まれるべきであり、何が従来技術に含まれるか、または何が従来技術に含まれないかについての承認として理解されるべきではない。

【0004】

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）無線モバイル遠隔通信技術が、特に人間との対話のために高いデータレートを有する高容量モバイルマルチメディアを提供すべく設計された。次世代技術、すなわち、第5世代（5G）技術は、人間との対話のためだけではなく、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型通信のためにも使用されることが意図される。

【0005】

5Gネットワークは、大量のIoTサービス（例えば、非常に大きい数の容量の限られたデバイス）およびミッションクリティカルなIoTサービス（例えば、高い信頼性を要求する）を可能にするように意図される一方で、レガシーモバイル通信サービスに優る改良が、モバイルデバイスに改良された無線インターネットアクセスを提供するように意図されたエンハンスドモバイルブロードバンド（eMBB）サービスの形態でサポートされる。

【0006】

例示的な通信システムにおいて、モバイル端末（サブスクライバ）などのユーザ機器（5Gネットワークにおける5G UE、またはより広くは、UE）が、5GネットワークにおいてgNB、もしくはLTEネットワークにおいてeNB（進化型ノードB）と呼ばれる基地局またはアクセスポイントと無線インターフェース上で通信する。アクセスポイント（例えば、gNB/eNB）は、例示的に、通信システムのアクセスネットワークの一部である。例えば、5Gネットワークにおいて、アクセスネットワークは5Gシステムと呼ばれ、その開示が引用によりその全体が本明細書に組み込まれる「Technical Specification Group Services and System Aspects; System Architecture for the 5G System」という名称の5G技術仕様書（TS）23.501、V0.4.0において説明される。LTEネットワークにおいて、アクセスネットワークは、進化型ユニバーサル地上無線アクセスネットワーク（E-UTRAN）である。一般に、アクセスポイント（例えば、gNB/eNB）は、コアネットワーク（CN）へのアクセスをUEに提供し、次に、CNが、他のUE、および/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UEに提供する。

【0007】

プライバシーは、任意の通信システムにおいて重要な考慮事項である。プライバシーは、その

10

20

30

40

50

開示が引用によりその全体が本明細書に組み込まれる「3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14)」という名称の5G技術報告書 (TR) 33.899、V1.1.0において広く対処される。詳細には、TR 33.899は、サブスクリプション (UE) プライバシを、5Gネットワークにおいて対処すべき最も重要なセキュリティ領域のうちの1つとして識別する。

【先行技術文献】

【非特許文献】

【0008】

【文献】5G技術仕様書 (TS) 23.501、V0.4.0、「Technical Specification Group Services and System Aspects; System Architecture for the 5G System」

5G技術報告書 (TR) 33.899、V1.1.0、「3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14)」

SA2 TS23.305

3GPP TS29.272 (Section 8:「User identity to HSS resolution」)、「3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 14)」

SA3 TS33.899

【発明の概要】

【課題を解決するための手段】

【0009】

例示的な実施形態が、通信システムにおいて認証要求を制御するための1つ以上のプライバシーインジケータを提供する。

【0010】

例えば、一実施形態において、方法が、通信ネットワークにおける要素または機能において、通信ネットワークのユーザ機器から、1つ以上のプライバシーインジケータを備えるメッセージを受信することと、1つ以上のプライバシーインジケータに基づいてメッセージを処理するための1つ以上のプライバシーフィーチャを決定することとを備える。

【0011】

メッセージは、ユーザ機器に関連付けられた通信ネットワークのサブスクリバに関するサブスクリプション識別子を備えるアタッチ要求を備えてよく、1つ以上のプライバシーインジケータは、アタッチ要求におけるサブスクリプション識別子がプライバシー保護されているかどうかを指示するフラグを備える。プライバシー保護されているサブスクリプション識別子は、サブスクリバの永続サブスクリプション識別子の少なくとも一部分を備えてよい。

【0012】

別の実施形態において、方法が、通信ネットワークにおける要素または機能において、通信ネットワークによってサポートされる1つ以上のプライバシーフィーチャを決定すること

10

20

30

40

50

と、通信ネットワークにおける要素または機能において、決定された1つ以上のプライバシーフィーチャに基づいて選択された1つ以上のプライバシーインジケータを備えるメッセージを生成することと、通信ネットワークにおける要素または機能から通信ネットワークのユーザ機器に、1つ以上のプライバシーインジケータを備える生成されたメッセージを送信することとを備える。

【0013】

1つ以上のプライバシーフィーチャは、プライバシー保護されているサブスクリプション識別子を取り扱うための、通信ネットワークにおける要素または機能の能力を備えてよい。

【0014】

別の実施形態において、方法が、通信ネットワークのユーザ機器において、メッセージを処理するための1つ以上のプライバシーフィーチャを決定することと、決定された1つ以上のプライバシーフィーチャに基づいて1つ以上のプライバシーインジケータをメッセージに追加することと、ユーザ機器から通信ネットワークにおける要素または機能に、1つ以上のプライバシーインジケータを有するメッセージを送信することとを備える。

【0015】

メッセージは、ユーザ機器に関連付けられた通信ネットワークのサブスクライバに関するサブスクリプション識別子を備えるアタッチ要求を備えてよく、1つ以上のプライバシーインジケータは、アタッチ要求におけるサブスクリプション識別子がプライバシー保護されているかどうかを指示するフラグを備える。

【0016】

別の実施形態において、方法が、通信ネットワークのユーザ機器において、通信ネットワークにおける要素または機能から、1つ以上のプライバシーインジケータを備えるメッセージを受信することと、1つ以上のプライバシーインジケータを利用して通信ネットワークによってサポートされる1つ以上のプライバシーフィーチャを決定することとを備える。

【0017】

1つ以上のプライバシーインジケータは、通信ネットワークが、プライバシー保護されているサブスクリプション識別子を取り扱うために構成されているかどうかのインジケーションを備えてよい。方法は、1つ以上のプライバシーインジケータが、通信ネットワークがプライバシー保護されているサブスクリプション識別子を取り扱うために構成されていないことを指示することに応答して、通信ネットワークにおける要素または機能にアタッチ要求を送信するのを控えることをさらに含んでよい。

【0018】

本明細書において説明されるこれら、およびその他の技法は、様々な通信ネットワークに適用されることが可能であるが、これらは、5Gおよび次世代通信ネットワークに特に適する。

【0019】

本明細書において説明される実施形態のこれら、およびその他の特徴ならびに利点は、添付の図面、および以下の詳細な説明からより明白となる。

【図面の簡単な説明】

【0020】

【図1】例示的な実施形態における通信システムを示す図である。

【図2】例示的な実施形態におけるサーバ位置特定機能およびホームサブスクライバサーバをより詳細に示す図である。

【図3】例示的な実施形態におけるLTEネットワークのためのユーザ機器認証手続きに関するメッセージフローを示す図である。

【図4】例示的な実施形態における5Gネットワークのためのユーザ機器認証手続きに関するメッセージフローを示す図である。

【図5】例示的な実施形態における混成LTE/5Gネットワークのためのユーザ機器認証手続きに関するメッセージフローを示す図である。

【図6】別の例示的な実施形態における5Gネットワークのためのユーザ機器認証手続き

10

20

30

40

50

に関するメッセージフローを示す図である。

【図 7】例示的な実施形態における非 3 G P P アクセスおよび認証を介して 5 G ネットワークにアクセスするユーザ機器に関するメッセージフローを示す図である。

【発明を実施するための形態】

【0021】

実施形態は、ユーザのサブスクリプション識別のプライバシーを保護する状態で認証要求を管理するための、例示的な通信システムおよび関連付けられる技法と一緒に本明細書において例示される。しかし、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および／またはプロセスに限定されないことを理解されたい。実施形態は、代替のプロセスおよび動作を使用して、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ることが可能である。例えば、LTE 進化型パケットコア (EPC) および 3 G P P 次世代システム (5 G) などの 3 G P P 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例示されるものの、開示される実施形態は、WiMAX システムおよび Wi-Fi システムを含むが、これらには限定されない様々な他のタイプの通信システムに単純明快な状態で適合されることが可能である。

【0022】

前述したとおり、ユーザ機器とネットワークアクセスポイントとの間で無線インターフェース上で通信するとき、サブスクリプション識別子のプライバシーは、2 G / 3 G / 4 G ネットワークに関して重要な問題であった。5 G ネットワークにおいてこの重要な問題に対処する取り組みが行われてきた。競り下げ攻撃 (down bidding attack) (例えば、攻撃者が、ネットワークアクセスポイントと、より劣ったセキュリティ能力をネゴシエートするようにユーザ機器になりすます) が、より低世代のネットワークにアタッチするように 5 G UE を強制する可能性があることが不可避である場合でさえ、これらのプライバシー要求に対処する必要性があることが認識される。

【0023】

上記で参照された TR 33.899 は、無線インターフェース上でプライバシーを提供するいくつかのソリューションについて説明し、それは、以下の 3 つのソリューションクラス：

1) 対称暗号システムに基づくスードニム (pseudonym) ソリューション、これは、UE のホームネットワークのホームサブスクライバサーバ／機能に、変化するスードニムを UE の永続サブスクリプション識別子にマップすることを要求する；

2) ホームネットワークオペレータの公開鍵を使用する、UE の永続サブスクリプション識別子の暗号化；および

3) サービングネットワークオペレータの公開鍵を使用する、UE の永続サブスクリプション識別子の暗号化

に一般的にグループ化されることが可能である。

【0024】

一例において、国際移動体加入者識別番号 (IMSI) が、UE の永続サブスクリプション識別子 (サブスクライバ識別) であることに留意されたい。一実施形態において、IMSI は、固定の 15 桁長であり、3 桁のモバイル国コード (MCC) と、3 桁のモバイルネットワークコード (MNC) と、9 桁のモバイルステーション識別番号 (MSIN) である。

【0025】

また、LTE ネットワークにおいて、ホームサブスクライバサーバ／機能は、ホームサブスクライバサーバ (HSS) と呼ばれ、5 G ネットワークにおいて、それは、ユーザデータ管理 (UDM) と呼ばれ、これは、UDM 機能の一環として認証およびセキュリティ機能 (AUSF) と、認証クレデンシャルリポジトリおよび処理機能 (ARPF) とを備えてもよいことにも留意されたい。

【0026】

いくつかの例示的な実施形態は、第 2 のソリューションクラス (すなわち、ホームネットワーク公開鍵ベースのソリューション) の観点から本明細書において説明されるが、代替

10

20

30

40

50

の実施形態が、他の2つのソリューションクラスに関して実装され得る。その開示が引用によりその全体が本明細書に組み込まれる、SA2 TS23.502およびSA3 TS33.899を参照されたい。

【0027】

ホームネットワーク公開鍵ベースのソリューションにおいて、ホームオペレータは、その公開鍵を、すべてのホームネットワークサブスクリバに提供する。ホームネットワークサブスクリバは、サブスクリバ識別を暗号化するためにそれを使用し、サブスクリバ識別は、例として、IMSIのMSIN部分である。MNC+MCCが、正しいホームネットワークにルーティングするためにサービングネットワークによって必要とされるため、MSIN部分だけが暗号化される必要がある。ホームHSSだけが、公開鍵に対応する秘密鍵を所有するので、そのメッセージを復号することができる。ひとたびIMSIが識別されると、HSS/AuC（ここで、AuCは、HSSの認証センタ部分である）が、ユーザ（サブスクリバ）とHSS/AuCとの間の別個の共有されるルート鍵Kに基づいて、認証ベクトル（AV）を作成することになる。同様に、5Gネットワークにおいて、UDM/ARPFが、AUSFを介して要求されたAVを作成する。AUSFおよびUDMは、最適化の理由で並置され得る。

10

【0028】

オペレータは彼のネットワークにおいて、彼が異なるHSS/UDMにおいて別々のセットのユーザを管理することを可能にする、複数のHSSの実装を有してよい。複数のHSSのため、サーバ位置特定機能（SLF）が、HSSのセットの前方に実装されてよい。SLFは、サブスクリバ位置特定機能と呼ばれてもよいことに留意されたい。SLFは、MME/AMFから受信されたユーザに関する認証要求を分析し、それを正しいHSSにルーティングする。

20

【0029】

単に例として、SLFの動作は、その開示が引用によりその全体が本明細書に組み込まれる、「3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 14)」という名称の3GPP TS29.272 (Section 8: 「User identity to HSS resolution」) において説明される。SLFは、ローカルで保持されるサブスクリバプロファイルデータベースを使用してユーザ識別 (IMSI) ・ ツー ・ HSS 解決を提供し、選ばれたHSSに対するDiameterプロキシとして、ユーザ認証要求を収容するDiameterメッセージをルーティングする。5Gにおいて、5Gコアネットワークプロトコルが、Diameterとは異なる場合、例えばhttpプロキシを使用する等、同様の機能がやはり要求されることに留意されたい。以下の説明において、SLFは、5Gコアネットワークに関するプロトコル決定に依存して、4GによるDRA (Diameter Routing Agent) ベースのソリューション、または他の任意のプロキシ関連のソリューションの両方をカバーしていると想定される。

30

40

【0030】

ホームオペレータが、サブスクリバのセットをスプリットするためにSLFを使用する場合、SLFはまず、受信された識別子を評価する必要があることが、本明細書において認識される。このため、方法のうちの1つによって永続サブスクリバ識別（例えば、IMSI）が暗号化されている5Gネットワークにおいて、SLFは、IMSIのMSIN部分の復号を引き継ぐ必要があることになる。さらに、SLFは、すべてのサブスクリバのプロファイルのデータベースをルーティング情報と一緒に保つ必要があることになり、すなわち、プロファイルは、サブスクリバの永続識別（例えば、IMSI）をネット

50

ワークにおけるHSSのうちの1つにマップして、受信された（暗号化された）IMSIを復号した後に認証要求を転送しなければならない。したがって、暗号化されたIMSIの復号を、HSSにおいての代わりに、SLFにおいておこなうことが有利である。故に、HSSが秘密鍵を格納する代わりに、今や、SLFがネットワーク秘密鍵を格納し、使用する必要があることになる。SLFは、ホームオペレータのドメインに置かれ、信頼できるとみなされる。一般に、SLFは、大きいオペレータネットワークにおいて想定されることが可能である。SLFの使用は、5GネットワークにおけるHSS/UDMに関する新たなプライバシー管理を、無線インターフェース上のサブスクリプション識別子の保護のためにHSS/UDMがまったく変更されることがないところまで簡略化するが、SLFは、暗号化されたIMSI復号のさらなる機能をおこない、その後、IMSI・ツー・HSS解決をおこなう必要がある。

10

【0031】

したがって、本明細書において説明される例示的な実施形態は、HSS/UDMまたはSLFがどのように、新たに導入されたプライバシーフィーチャを、すなわち、受信されたアタッチ要求がまず復号される必要があることを、効率的に扱うことができるかという問題に対処する。このことがケアされない場合、HSS/UDMまたはSLFは、要求を受信して、それを処理しようと試みて、無用な計算リソースを浪費することになる。

【0032】

プライバシーは、国特有の規制に依存し、したがって、HSS/UDMまたはSLFは、認証ベクトルに関する要求の両方の事例を取り扱うように、すなわち、5G UEがプライバシーを適用していない場合に「通常の」アタッチ要求を処理するように、もしくは転送するように、または「プライバシー」アタッチ要求を処理するように実装される必要がある。

20

【0033】

第1の例示的な実施形態において、5G UEは、そのプライバシーを保護することを所望する場合、MSINが暗号化された形態で提供されることを指示するべく識別プライバシーフラグ（すなわち、プライバシーインジケータ）を追加する。

【0034】

プライバシーインジケータは、フラグまたはフィールドなどの「明示的」プライバシーインジケータであるに加えて、代替として、「暗黙の」プライバシーインジケータであることが可能であることを理解されたい。暗黙のプライバシーインジケータによって、プライバシーフィーチャが、メッセージを暗号化するために使用されるアルゴリズムを介してUEによってネットワーク要素／機能に伝えられることが意味される。このため、UEからメッセージを受信するネットワーク要素／機能は、メッセージが特定の暗号化アルゴリズムを用いて暗号化されているという事実によってプライバシーフィーチャについて知られる。また、このことは、NULL暗号化スキームにも当てはまる。NULL暗号化スキームにおいて、入力、出力と等しく、SUPI (Subscription Permanent Identifier of the UE) (UEのサブスクリプション永続識別子) は、暗号化されない、すなわち、フォーマット維持されるスキームである。このことを、SUPI (またはIMSI) が常時、暗号化されていると解釈することも可能であるが、プライバシーがまったく「オンにされていない」場合、NULL暗号化が使用される。このため、プライバシーインジケータは、使用されるアルゴリズムスキーム（例えば、NULL暗号化またはメッセージを実際に暗号化するアルゴリズム）に暗黙に存在することになる。

30

40

【0035】

HSSまたはSLFは、このプライバシーインジケータがなくても、要求を解決し、暗号化されている場合、復号を試みる最初の試行の後に見当がつくであろうことが示唆され得る。しかし、そのようなインジケーションを明示させる1つの重要な理由は、このことが、処理時間を節約し、要求される処理リソースがより少なくなるからである。このため、この第1の例示的な実施形態において、SLFは、このフラグを見ることによって処理について決定することができる。設定されていない場合、SLFは、提供されたIMSIが暗号化されていないものと想定し、IMSI・ツー・HSS解決を行い、正しいHSS/U

50

DMに転送する、すなわち、4G動作との互換性が保持される。フラグが設定されている場合、SLFは、提供されたIMSIが暗号化されていることを認識し、真の暗号化されていないIMSIを形成すべくネットワーク秘密鍵を使用してMSIN部分を復号し、IMSI・ツー・HSS解決をおこない、その後、正しいHSS/UDMに認証要求を転送する。SLFが使用されない場合、同一の原理が、HSS/UDMによって使用されることが可能である。すなわち、HSS/UDMは、5G UEがフラグを設定しているかどうかを確認し、次に、復号が必要とされるかどうかを決定しなければならない。

【0036】

この第1の例示的な実施形態は、5G RAN（無線アクセスネットワーク）を介して5Gコアネットワーク（CN）にアタッチする5G UEに適用されることが可能である。しかし、3GPPは、当面の配備シナリオとして、5G UEが、5G RANを介して4G CNにアタッチすべきことを識別している。UEがインジケータを設定する場合、4G CNは、識別プライバシーフラグまたは他のプライバシーインジケータを理解するように強化される必要があることになる。

【0037】

進化する4Gネットワークから5Gまでを有するオペレータに関するネットワークアーキテクチャの観点から、4Gと5Gのアクセスおよびコアネットワークはともに、相当な時間にわたってサポートされる必要がある。このことは、暗号化されたMSINを復号する新たな5G HSS機能をサポートしながら、現在の4G HSSがサポートされる必要があることを意味する。実施形態によれば、認証要求をHSSにルーティングする前に、暗号化されたMSINを識別すること、およびそれを復号することができるSLFを置くことが、オペレータネットワークにおける4Gおよび5Gコアの併存を管理するために役立つ。新たな識別5GプライバシーフィーチャをサポートするようにSLFを強化することは、HSSを強化することと比べて、より有利である。HSSが拡張された場合、複数のHSSを有する大きいネットワークにおいて、暗号化されたIMSIを復号する能力と一緒にすべてのHSSが更新される必要がある。このことは、単一の中央ノード（例えば、SLF）において問題を解決することと比べて、取り扱うのがより面倒であり得る。有利には、第1の例示的な実施形態では、5Gにおける（4Gへの）競り下げ攻撃は、同一のフィーチャが4Gにおいても配備されて、それによって、このフィーチャを実現するために強化されたSLFが使用される場合、有益ではないことになる。

【0038】

第2の例示的な実施形態において、ネットワークがプライバシー保護されている識別子を取り扱うことができることを5G UEに指示するべく、例えば、ネットワークマスタ情報ブロック（MIB）/システム情報ブロック（SIB）ブロードキャストに追加することをオペレータが決めることが可能な別のプライバシーインジケータ、例えば、プライバシーが予期される、処理することが可能である、または所望されることを指示するフラグが、提供される。すると、このインジケータが送信されない場合、そもそも、ネットワークにアタッチすべきかが、5G UEによって実装される/構成されるポリシーに任せられる。4G/5Gネットワーク側のインジケータは、国/地域ごとの規制ニーズを指示するようになる、すなわち、プライバシーをオン/オフにすることになる。UEが移動先ネットワークにおいてローミングしている間、移動先ネットワークからのUE認証要求は、ホームネットワークに転送され、これに関する識別プライバシーインジケータ（上記の第1の例示的な実施形態）が説明されているが、一方で、サービングネットワークにも適合させる必要があることに留意されたい。MME/SEAF（SEAFは、セキュリティアンカ機能である）が、UEからの強化された最初のアタッチメッセージを取り扱い、UE認証要求メッセージを形成し、それを、AVを要求するためにホームネットワークにルーティングしなければならない。サブスクリプション識別子が暗号化されている場合、暗号化されたIMSIのためのメッセージフィールドのサイズは、今日の4G IMSIフィールドとは異なってよい（選ばれたソリューションクラスに依存して）。

【0039】

また、移動先ネットワークは、その利用可能性、および、該当する場合、それがプライバシーを使用しないことを指示することも可能であることに留意されたい。この情報は、例えば、SIBもしくは他の情報ブロックの一部としてブロードキャストされることが可能であり、または各UEへの明示的な要求メッセージとして送信されることが可能である。

【0040】

第3の例示的な実施形態において、UEは、5G UEがIMS I ページングに応答するのを禁止するように設定されることが可能なプライバシーインジケータを管理するように構成される。このため、UEがネットワークにアタッチすることを所望し、ネットワークがUEの真の識別を要求する場合、このプライバシーインジケータを有するように構成されたプライバシー構成された5G UEは、返答しないことになる。

10

【0041】

上で説明されたプライバシーインジケータが与えられると、多種多様なネットワーク構成が、プライバシーインジケータを実装するために採用されることが可能である。図1ー図7は、これらのネットワーク構成のうちのいくつかを描画する。しかし、実施形態は、ここで例示される、またはそうでなければ下で説明されるネットワーク構成に限定されないことを認識されたい。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、サービングゲートウェイ機能、その他を表すように意図されることを理解されたい。このため、図1に描画されるブロックは、主要な機能を提供するLTEおよび5Gネットワークにおける特定の要素を参照する。しかし、表される主要な機能のいくつか、またはすべ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よい。また、LTEまたは5Gネットワークのすべての機能が図1に示されるわけではないことも理解されたい。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。

20

【0042】

したがって、示されるとおり、通信システム100は、無線インターフェース103を介してアクセスポイント(eNB/gNB)104と通信するユーザ機器(UE)102を備える。UE102は、移動局であってよく、そのような移動局は、例として、モバイル電話、コンピュータ、または他の任意のタイプの通信デバイスを備えてよい。LTE-V2X実装において、1つ以上のUEが、所与の車両に配備されてよい。したがって、本明細書において使用されるとき、「ユーザ機器」という用語は、様々な異なるタイプの移動局、サブスクライバ局、または、より一般的に、ラップトップもしくは他の機器(例えば、車両)に挿入されたデータカードの組合せなどの例を含む、通信デバイスを包含するように広く解釈されるように意図される。また、そのような通信デバイスは、アクセス端末と普通、呼ばれるデバイスを包含するようにも意図される。

30

【0043】

一実施形態において、UE102は、汎用ICカード(UICC)と、モバイル機器(ME)とから成る。UICCは、UEのユーザ依存の部分であり、少なくとも1つのユニバーサルサブスクライバ識別モジュール(Universal Subscriber Identity Module)(USIM)と、適切なアプリケーションソフトウェアとを収容する。USIMは、ネットワークにアクセスするサブスクライバを識別し、認証するために使用される、国際移動体加入者識別番号(IMS I)番号、およびIMS Iに関連する鍵をセキュアに格納する。MEは、UEのユーザ独立の部分であり、端末機器(TE)機能および様々なモバイル終端(MT)機能を収容する。

40

【0044】

アクセスポイント104は、例示的に、通信システム100のアクセスネットワークの部分である。そのようなアクセスネットワークは、例えば、複数の基地局と、1つ以上の関連付けられた無線ネットワーク制御機能とを有するE-UTRANまたは5Gシステム(または混成)を備えてよい。基地局と無線ネットワーク制御機能は、論理的に分離したエンティティであってよいが、所与の実施形態において、例えば、基地局ルータまたはフェ

50

ムトセルラ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おいて実装されてよい。

【0045】

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。LTEネットワークにおいて、この機能は、モビリティ管理要素(MME)によって通常実装される一方で、5Gネットワークにおいて、この機能は、アクセスおよびモビリティ管理機能(AMF)によって実装される。明確に示されないものの、SEAFは、UEをモビリティ管理と接続するAMFを用いて実装されることが可能である。本明細書において使用されるとき、モビリティ管理機能は、ネットワーク動作のなかでもとりわけ、UEとのアクセスおよび認証動作(アクセスポイント104を通じた)を管理する通信システムのCN部分における要素または機能である。

10

【0046】

この例示的な実施形態におけるMME/AMF106は、SLF107に動作可能に結合される。例示的な実施形態において、SLF107は、SLF107が受信するメッセージにおいて設定された1つ以上のプライバシーシグネチャに応答するように、上で説明されたように構成される。上で説明されたように、SLF107は、1つ以上のプライバシーシグネチャに依存して、サブスクライバ識別を復号してよく、または暗号化された情報を、UE102の適切なホームネットワークに単に転送してよい。このため、示されるとおり、SLF107は、複数のHSS/UDM108-1、108-2、...、108-Nに動作可能に結合される。これらのHSS/UDMは、通信システム100にアタッチしてよいUEのホームネットワークを表す。SLF107は、適切なHSS/UDM108にUE情報を提供するように構成される。

20

【0047】

また、アクセスポイント104は、パケットデータネットワーク(PDN)ゲートウェイ(PGW)112に動作可能に結合される、サービングゲートウェイ機能110(例えば、LTEネットワークにおけるサービングゲートウェイ(SGW)、および5Gネットワークにおけるセッション管理機能(SMF))にも動作可能に結合される。PGW112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。MME/AMF106およびSLF107は、CNの一部であるとみなされてよい。また、MME/AMF106およびSLF107は、サービングネットワークの一部であることも可能である。そのようなネットワーク要素のさらなる通常の動作および機能については、それらが、例示的な実施形態の焦点ではなく、適切な3GPP LTE文献または5G文献において見出されてよいので、ここで説明されることはない。

30

【0048】

システム要素のこの特定の配置は例に過ぎず、他のタイプおよび配置のさらなる、または代替の要素が、他の実施形態において通信システムを実施するために使用されることが可能であることを認識されたい。例えば、他の実施形態において、システム100は、認証要素、および本明細書において明確に示されない他の要素を備えてよい。

【0049】

したがって、図1の配置は、無線セルラシステムの1つの例示的な配置に過ぎず、システム要素の多数の代替の構成が使用されてよい。例えば、単一のUE、eNB/gNB、MME/AMF、SLF、SGW/SMF、およびPGW要素だけが図1の実施形態に示されるものの、これは、説明の簡明のために過ぎない。所与の代替の実施形態が、無論、より多くの数のそのようなシステム要素、および従来のシステム実装に普通、関連付けられるタイプのさらなる要素または代替の要素を含んでよい。

40

【0050】

また、図1は、システム要素を単独の機能ブロックとして例示するが、5Gネットワークを作る様々なサブネットワークは、いわゆるネットワークスライスに分割されることに留意されたい。ネットワークスライス(ネットワークパーティション)は、共通の物理インフラストラクチャ上でネットワーク機能仮想化(NVF)を使用する対応するサービスタイプごとに一連の機能セット(すなわち、機能チェーン)を備える。ネットワークスライ

50

スは、所与のサービス、例えば、e M B B サービス、大規模な I o T サービス（例えば、V 2 X サービス）、およびミッションクリティカルな I o T サービスのために必要に応じてインスタンス化される。このため、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ネットワーク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において、このことは、ネットワークスライスまたは機能を、基礎をなす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にインストールすること、またはそうでなければ、そのようなホストデバイス上で走らせることを伴う。U E 1 0 2 は、e N B / g N B 1 0 4 を介してこ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。

【0051】

図2は、例示的な実施形態における S L F 1 0 7 および1つの H S S / U D M 1 0 8 のより詳細な図を示す。図1における各 H S S / U D M 1 0 8 (1 0 8 - 1、1 0 8 - 2、. . .、1 0 8 - N) は、図2に示されるとおり構成されることが可能である。S L F 1 0 7 は、メモリ202およびインターフェース回路204に結合されたプロセッサ200を備える。S L F 1 0 7 のプロセッサ200は、プロセッサ200によって実行されるソフトウェアの形態で少なくとも部分的に実装されてよい認証処理モジュール210を含む。認証処理モジュール210は、後続の図と併せて説明され、それ以外で本明細書において説明されるプロセスの認証動作をおこなう。S L F 1 0 7 のメモリ202は、認証動作中に生成される、またはそうでなければ使用される認証および関連するデータを記憶する認証ストレージモジュール212を含む。

【0052】

H S S / U D M 1 0 8 は、メモリ222およびインターフェース回路224に結合されたプロセッサ220を備える。H S S / U D M 1 0 8 のプロセッサ220は、プロセッサ220によって実行されるソフトウェアの形態で少なくとも部分的に実装されてよい認証処理モジュール230を含む。認証処理モジュール230は、後続の図と併せて説明され、それ以外で本明細書において説明されるプロセスの認証動作をおこなう。H S S / U D M 1 0 8 のメモリ222は、認証動作中に生成される、またはそうでなければ使用される認証データおよび関連するデータを記憶する認証ストレージモジュール232を含む。

【0053】

S L F 1 0 7 および H S S / U D M 1 0 8 それぞれのプロセッサ200および220は、例えば、マイクロプロセッサ、特定用途向け集積回路 (A S I C)、デジタルシグナルプロセッサ (D S P)、または他のタイプの処理デバイス、およびそのような要素の部分もしくはは組合せを備えてよい。

【0054】

S L F 1 0 7 および H S S / U D M 1 0 8 それぞれのメモリ202および222は、本明細書において説明される機能の少なくとも一部分を実装すべくプロセッサ200および220それぞれ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よい。例えば、後続の図と併せて説明され、それ以外で本明細書において説明される認証動作および他の機能は、プロセッサ200および220によって実行されるソフトウェアコードを使用して単純明快な状態で実装されてよい。

【0055】

したがって、メモリ202または222のうちの所与の1つが、より一般的にはコンピュータプログラム製品と、あるいは、さらにより一般的には、その中に実行可能プログラムコードを具現化しているプロセッサ可読記憶媒体と、本明細書によって呼ばれるものの例と考えられてよい。プロセッサ可読記憶媒体の他の例は、任意の組合せで、ディスク、または他のタイプの磁気媒体もしくはは光媒体を含んでよい。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備える製造品を含むことが可能である。

【0056】

メモリ202または222は、より詳細には、例えば、スタティック R A M (S R A M)

10

20

30

40

50

、ダイナミックRAM（DRAM）などの電子ランダムアクセスメモリ（RAM）、または他のタイプの揮発性電子メモリもしくは不揮発性電子メモリを備えてよい。後者は、例えば、フラッシュメモリ、磁気RAM（MRAM）、相変化RAM（PC-RAM）、または強誘電体RAM（FRAM）などの不揮発性メモリを含んでよい。本明細書において使用されるとき、「メモリ」という用語は、広く解釈されるように意図され、さらに、または代替として、例えば、読取り専用メモリ（ROM）、ディスクベースのメモリ、もしくは他のタイプのストレージデバイス、およびそのようなデバイスの部分もしくは組合せを包含してよい。

【0057】

S L F 1 0 7 および H S S / U D M 1 0 8 それぞれのインターフェース回路 2 0 4 および 2 2 4 は、例示的に、関連付けられたシステム要素が、本明細書において説明される状態で互いに通信することを可能にするトランシーバ、または他の通信ハードウェアもしくは通信ファームウェアを備える。

【0058】

S L F 1 0 7 は、H S S / U D M 1 0 8 との、あるいはその逆での、それぞれインターフェース回路 2 0 4 および 2 2 4 を介しての、通信のために構成されることが図 2 から明白である。この通信は、S L F 1 0 7 が H S S / U D M 1 0 8 にデータを送信すること、および H S S / U D M 1 0 8 が S L F 1 0 7 にデータを送信することを伴う。しかし、代替の実施形態において、他のネットワーク要素が、S L F と H S S / U D M との間に動作可能に結合されてよい。本明細書において使用されるとき、「データ」という用語は、基地局要素を介してユーザ機器とコアネットワークとの間で送信されてよい任意のタイプの情報を包含するように、広く解釈されるように意図され、識別データ、認証データ、制御データ、オーディオ、ビデオ、マルチメディア、その他を含むが、これらには限定されない。

【0059】

図 2 に示される構成要素の特定の配置は、例に過ぎず、多数の代替の構成が他の実施形態において使用されてよいことを認識されたい。例えば、ユーザ機器およびモビリティ管理機能は、さらなる、または代替の構成要素を組み込むように、および他の通信プロトコルをサポートするように構成されることが可能である。

【0060】

また、U E 1 0 2、e N B / g N B 1 0 4、M M E / A M F 1 0 6、S G W / S M F 1 1 0、および P G W 1 1 2 などの他のシステム要素は、プロセッサ、メモリ、およびネットワークインターフェースなどの構成要素を含むように各々構成されてもよい。これらの要素は、別々のスタンドアロンの処理プラットフォーム上に実装される必要はなく、代わりに、例えば、単一の共通の処理プラットフォームの異なる機能部分を表すことが可能である。そのような処理プラットフォームは、e N B / g N B の少なくとも部分と、関連付けられた無線ネットワーク制御機能とをさらに備えてよい。

【0061】

図 3 - 図 7 は、上で説明されたプライバシーインジケータのうちの 1 つ以上が実装されることが可能なメッセージフローおよびネットワーク構成を例示する。これらのメッセージフローおよびネットワーク構成は、例示的な実施形態であるものと理解される。

【0062】

図 3 は、1 つの例示的な実施形態による、暗号化されていない I M S I、S L F、および複数の H S S を使用する L T E における高レベル U E 認証手続き 3 0 0 を例示する。

【0063】

より詳細には、図 3 は、U E 3 0 2、R A N 3 0 4、M M E 3 0 6、S L F 3 0 8、H S S 1 3 1 0 - 1、および H S S 2 3 1 0 - 2 を示す。2 つだけの H S S が描画されるものの、本明細書において説明される実施形態によれば、任意の数の H S S が実装されてよい。図 3 の U E 認証手続きフローのステップ 1 において、U E 3 0 2 は、R A N 3 0 4 を通じて M M E 3 0 6 にアタッチ要求（I M S I）を送信する。ステップ 2 において、次に、M M E 3 0 6 が、認証要求（I M S I）を S L F 3 0 8 に送信する。ステップ 3 におい

10

20

30

40

50

て、S L F 3 0 8 が、H S S への I M S I マッピングに基づいて H S S を選択する。ステップ 4 において、S L F 3 0 8 が、図 3 に指示されたとおり、H S S 1 3 1 0 - 1 である、選択された H S S に認証要求 (I M S I) を送信する。ステップ 5 において、H S S 1 3 1 0 - 1 が、ルート鍵に基づいて認証ベクトル (A V) を生成する。ステップ 6 において、H S S 1 3 1 0 - 1 が、認証応答 (A V) を S L F 3 0 8 に送信し、ステップ 7 において、S L F 3 0 8 が、認証応答 (A V) を M M E 3 0 6 に送信する。認証応答は、ランダムチャレンジ (R A N D) と、認証トークン (A U T N) と、キーセット識別子 (K S I) とを備えることが可能である。ステップ 9 において、M M E 3 0 6 が、R A N 3 0 4 を通じてアタッチ応答を U E 3 0 2 に送信する。

【 0 0 6 4 】

図 4 は、暗号化された I M S I 、S L F 、および複数の U D M を使用する 5 G における高レベル U E 認証手続き 4 0 0 を例示する。U D M の代わりに S L F において I M S I 復号をおこなうことは、1 つの例示的な実施形態によれば、コア認証機能を変更なしに保持するために役立つ。本明細書において使用されるとき、E A P という頭字語は、拡張可能認証プロトコルを指し、A K A という頭字語は、認証および鍵合意を指す。

【 0 0 6 5 】

より詳細には、図 4 は、U E 4 0 2 、(R) A N 4 0 4 、A M F 4 0 6 、S L F 4 0 8 、A U S F / U D M 4 1 0 - 1 、および A U S F / U D M 4 1 0 - 2 を示す。2 つだけの A U S F / U D M が描画されるものの、本明細書において説明される実施形態によれば、任意の数の A U S F / U D M が実装されてよい。図 4 の U E 認証手続きフローのステップ 1 において、U E 4 0 2 が、(R) A N 4 0 4 を通じて A M F 4 0 6 に登録要求 (暗号化された I M S I) を送信する。暗号化された I M S I を指すことによって、これは通常、暗号化される I M S I の部分、例えば、M S I N 、または I M S I のすべての部分、もしくは他の部分を指すことになり得ることに留意されたい。ステップ 2 において、A M F 4 0 6 が、認証要求 (暗号化された I M S I) を S L F 4 0 8 に送信する。ステップ 3 は、サブステップ 3 a および 3 b を含む。ステップ 3 a において、S L F 4 0 8 が、暗号化された I M S I を復号する。一実施形態において、S L F 4 0 8 は、プロビジョニングされた証明書を使用して、暗号化された I M S I を復号する。ステップ 3 b において、S L F 4 0 8 は、U D M への I M S I マッピングに基づいて H S S を選択する。ステップ 4 において、S L F 4 0 8 が、図 4 に指示されたとおり、A U S F / U D M 4 1 0 - 1 である、選択された U D M に認証要求 (I M S I) を送信する。ステップ 5 において、A U S F / U D M 4 1 0 - 1 が、ルート鍵に基づいて認証ベクトル (A V) を生成する。ステップ 6 において、A U S F / U D M 4 1 0 - 1 が、E A P A K A ' 認証または E A P A K A * 認証 (A K A * は、より大きいホーム制御を伴う A K A を指す) を開始する。ステップ 7 において、A U S F / U D M 4 1 0 - 1 が、認証応答 (A V) を S L F 4 0 8 に送信し、ステップ 8 において、S L F 4 0 8 が、認証応答 (A V) を A M F 4 0 6 に送信する。ステップ 9 において、A M F 4 0 6 が、(R) A N 4 0 4 を通じて認証要求を U E 4 0 2 に送信する。

【 0 0 6 6 】

図 5 は、1 つの例示的な実施形態による、4 G L T E ネットワークおよび 5 G ネットワークをサポートする U D M および H S S の混成コアアーキテクチャに関する手続き 5 0 0 を例示する。S L F における I M S I 復号が、両方のコアを管理するために役立つ。

【 0 0 6 7 】

より詳細には、図 5 は、U E 5 0 2 、g N B 5 0 4 、A M F / M M E 5 0 6 、S L F 5 0 8 、A U S F / U D M 5 1 0 - 1 および 5 1 0 - 2 、ならびに H S S 5 1 2 を示す。2 つだけの A U S F / U D M が描画されるものの、本明細書において説明される実施形態によれば、任意の数の A U S F / U D M が実装されてよい。

【 0 0 6 8 】

図 5 の手続きのステップ 1 において、U E 5 0 2 が、g N B 5 0 4 を通じてアタッチ要求 (暗号化された I M S I) を A M F / M M E 5 0 6 に送信する。暗号化された I M S I を

10

20

30

40

50

指すことによって、これは通常、暗号化されるIMSIの部分、例えば、MSIN、またはIMSIのすべての部分、もしくは他の部分を指すことになり得ることに留意されたい。次に、ステップ2において、AMF/MME 506が、認証要求（暗号化されたIMSI）をSLF 508に送信する。ステップ3は、サブステップ3aおよび3bを含む。ステップ3aにおいて、SLF 508が、暗号化されたIMSIを復号する。一実施形態において、SLF 508が、プロビジョニングされた証明書を使用して、暗号化されたIMSIを復号する。ステップ3bにおいて、SLF 508が、HSSへのIMSIマッピングに基づいてHSSを選択する。ステップ4において、SLF 508が、AUSF/UDM 510-1および510-2を通じて認証要求（IMSI）を、選択されたHSS、HSS 512に送信する。ステップ5において、HSS 512が、ルート鍵に基づいて認証ベクトル（AV）を生成する。ステップ6において、HSS 512が、AUSF/UDM 510-1および510-2を通じて認証応答（AV）をSLF 508に送信し、ステップ7において、SLF 508が、認証応答（AV）をAMF/MME 506に送信する。ステップ8において、AMF/MME 506が、gNB 504を通じてアタッチ応答をUE 502に送信する。

【0069】

図6は、例示的な実施形態による、暗号化されたIMSI、SLF、および複数のUDMを使用する5Gにおける高レベルUE認証手続き600を例示する。UDMの代わりにSLFにおいてIMSI復号をおこなうことは、コア認証機能を変更なしに保持するために役立つ。

【0070】

より詳細には、図6は、UE 602、(R)AN 604、AMF 606、AUSF 608、SLF 610、およびUDM 612-1および612-2を示す。2つだけのUDMが描画されるものの、本明細書において説明される実施形態によれば、任意の数のUDMが実装されてよい。図6の高レベルUE認証手続きフローのステップ1において、UE 602が、(R)AN 604を通じてAMF 606に登録要求（暗号化されたIMSI）を送信する。暗号化されたIMSIを指すことによって、これは通常、暗号化されるIMSIの部分、例えば、MSIN、またはIMSIのすべての部分、もしくは他の部分を指すことになり得ることに留意されたい。次に、ステップ2において、AMF 606が、認証要求（暗号化されたIMSI）をAUSF 608に送信する。ステップ3において、AUSF 608が、認証要求（暗号化されたIMSI）をSLF 610に送信する。ステップ3aにおいて、SLF 610が、暗号化されたIMSIを復号する。一実施形態において、SLF 610は、プロビジョニングされた証明書を使用して、暗号化されたIMSIを復号する。ステップ3bにおいて、SLF 610が、UDMへのIMSIマッピングに基づいてHSSを選択する。ステップ4において、SLF 610が、図6に示されるとおり、UDM 612-1である、選択されたUDMに認証要求（IMSI）を送信する。ステップ5において、UDM 612-1が、ルート鍵に基づいて認証ベクトル（AV）を生成する。ステップ6において、UDM 612-1が、認証応答（AV）をSLF 610に送信し、ステップ7において、SLF 610が、認証応答（AV）をAUSF 608に送信する。ステップ8において、AUSF 608が、EAP AKA'認証またはEAP AK^{AK}認証を開始する。ステップ9において、AUSF 608が、認証応答をAMF 606に送信する。ステップ10において、AMF 606が、(R)AN 604を通じて認証要求をUE 602に送信する。

【0071】

図7は、例示的な実施形態による、非3GPPアクセス（WLAN）および認証を介して5GネットワークにアクセスするUEに関する手続き700を例示する。本明細書において使用されるとき、ANという頭字語は、アクセスネットワークを指し、NAIという頭字語は、ネットワークアクセス識別子を指し、SUP Iという頭字語は、UEのシリアル化された一意製品識別子を指す。

【0072】

10

20

30

40

50

より詳細には、図7は、UE702、非3GPP AN704、AMF706、AUSF708、およびUDM710を示す。図7の手続きのステップ1において、UE702が、非3GPP AN704を通じて登録要求をAMF706に送信する。ステップ2において、AMF706が、認証要求（NAI，[EAP]）をAUSF708に送信する。AUSF708が、認証タイプ（例えば、EAP AKA'認証またはEAP AKAA'認証）を決定し、EAPサーバの役割をして、EAP AKA'認証またはEAP AKAA'認証をおこなう。ステップ3において、セキュリティ材料が、NAIに基づいてUDM710から取り出される。ステップ4において、AUSF708が認証応答（[EAP]）をAMF706に送信し、AMF706が、ステップ5においてUE認証を開始する。示されるとおり、UE認証中、AMF706が、認証要求（SUP I，[EAP]）をAUSF708に送信する。選ばれたEAP認証方法に依存して、いくつかの認証要求メッセージが、UE702とAUSF708との間で（AMF706を介して）要求される可能性がある。UE認証が成功すると、AUSF708が、認証応答（[EAP]，Key）をAMF706に送信する。Keyは、非アクセス層（NAS）、制御プレーン（CP）、およびユーザプレーン（UP）特有のセキュリティ鍵を生成するためにAMF706によって使用されてよいセキュリティ鍵である。

【0073】

本明細書において説明される技法は、通信システムにおける認証要求のための1つ以上のプライバシーシールドを提供する。例えば、そのようなプライバシーシールドは、通信システムの要素に伝送される情報要素またはフラグにおける1つ以上のビットを使用することによって制御される（例えば、設定される）ことが可能である。さらに、ユーザ機器のホームネットワーク、およびコアネットワークにおける他の要素／機能（例えば、サーバ位置特定機能）がどのように、1つ以上のプライバシーシールドを効率的に処理することができるかに対処する方法および機構が提供される。有利には、1つ以上のプライバシーシールドは、プライバシーシールドが実装される1つ以上のネットワーク構成において浪費されるコンピューティングリソースを節約する。

【0074】

本明細書において言及される識別子の命名、例えば、IMSI、その他は、例示を目的としているに過ぎないことを認識されたい。すなわち、UEに関する識別子は、異なる通信ネットワーク技術に関する異なるプロトコルおよび標準において異なる名前または頭字語を有してよい。このため、本明細書においてこれらの識別子に与えられる特定の名前または頭字語のいずれも、いずれの様態においても実施形態を限定するようには意図されない。

【0075】

前に指示されたとおり、実施形態は、LTEまたは5Gコンテキストに限定されず、開示される技法は、識別要求プロセスにおいて識別（例えば、IMSIまたは均等物）を採用する他の3GPPシステムおよび非3GPPシステムを含むが、これらには限定されない多種多様な他の通信システムコンテキストに単純明快な様態で適合されることが可能である。

【0076】

本明細書において開示される通信システムのユーザ機器または基地局要素のプロセッサ、メモリ、コントローラ、およびその他の構成要素は、上で説明された識別要求機能の少なくとも一部分を実装するように適切に変更された、よく知られた回路を含んでよい。

【0077】

上で説明されたように、実施形態は、ユーザ機器、基地局、または通信システムの他の要素の処理回路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各々が備える製造品の形態で実装されてよい。そのような回路の従来の態様は、当業者にはよく知られており、したがって、本明細書において詳細に説明されることはない。また、実施形態は、任意の組合せにおける、1つ以上のASIC、FPGA、または他のタイプの集積回路デバイスにおいて実装されてもよい。そのような集積回路デバイス、および集積回路デバイスの部分または組合せは、本明細書において「回路」の用語が使用されるとき、「回路」の

10

20

30

40

50

例である。ハードウェア、および関連付けられたソフトウェアもしくはファームウェアの多種多様な他の配置が、例示的な実施形態を実装するために使用されてよい。

【0078】

したがって、本明細書において説明される様々な実施形態は、例示的な例として提示されるに過ぎず、特許請求の範囲を限定するものと解釈されるべきではないことが、再び強調されなければならない。例えば、代替の実施形態は、例示的な実施形態のコンテキストにおいて上記で説明される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、識別要求プロセス、メッセージングプロトコル、およびメッセージフォーマットを利用することが可能である。添付の特許請求の範囲に含まれるこれら、および他の多数の代替の実施形態が、当業者には直ちに明白となろう。

10

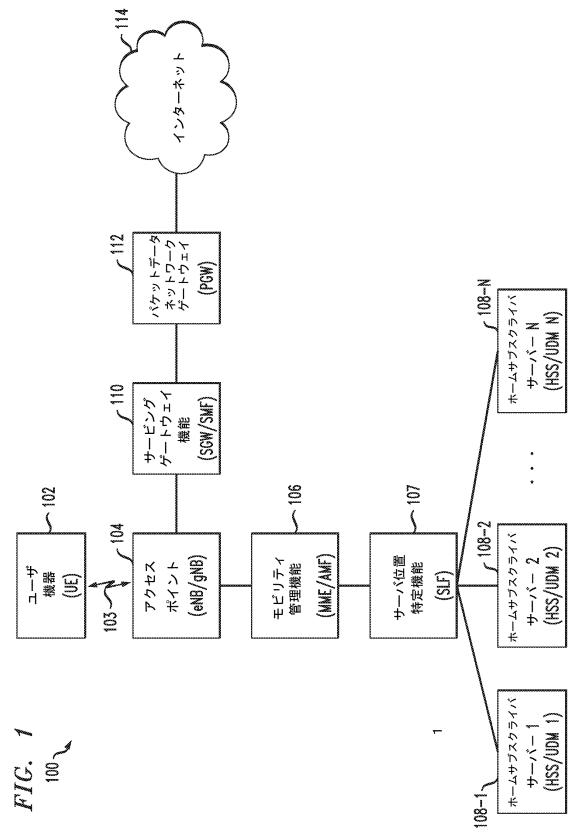
20

30

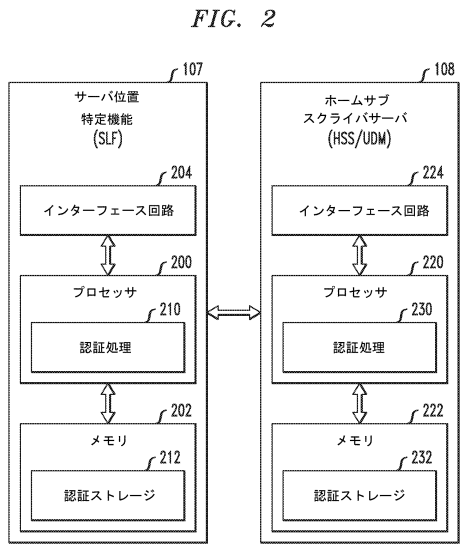
40

50

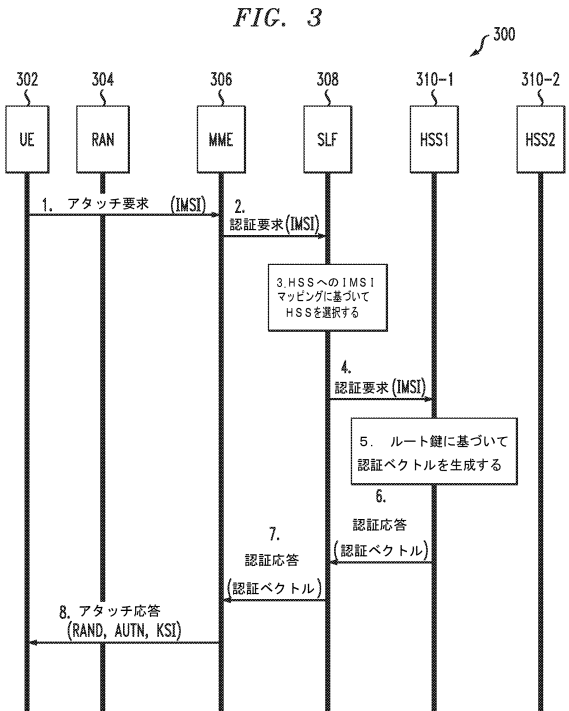
【図面】
【図 1】



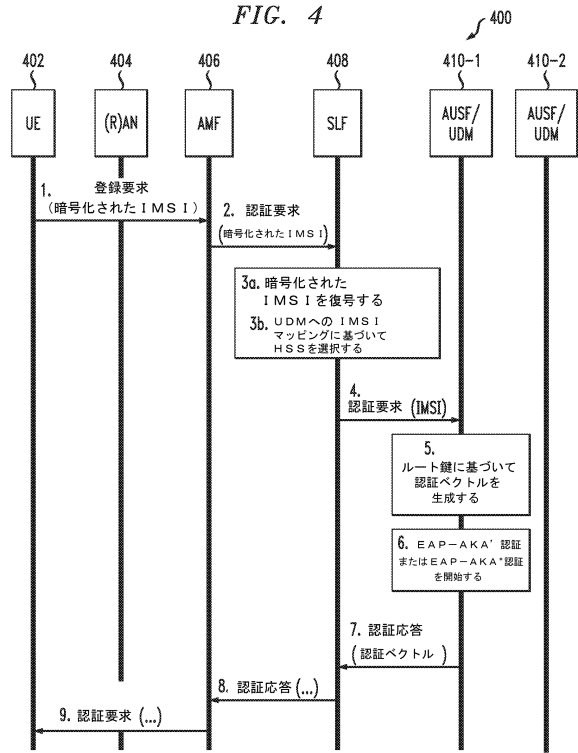
【図 2】



【図 3】



【図 4】



10

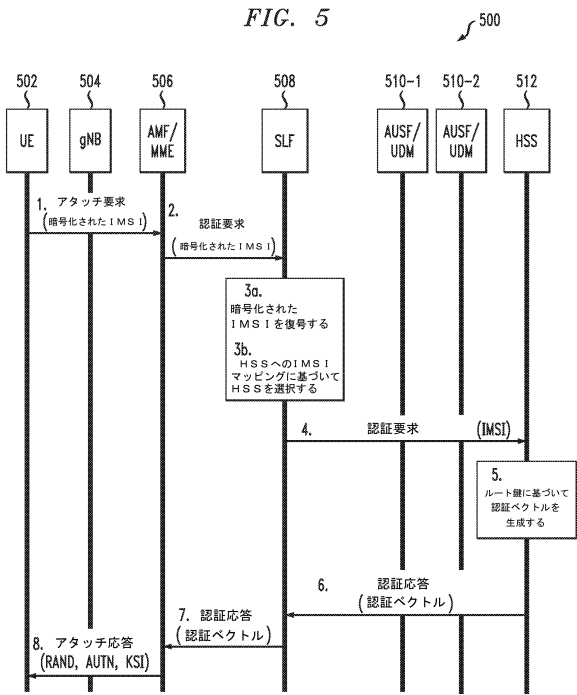
20

30

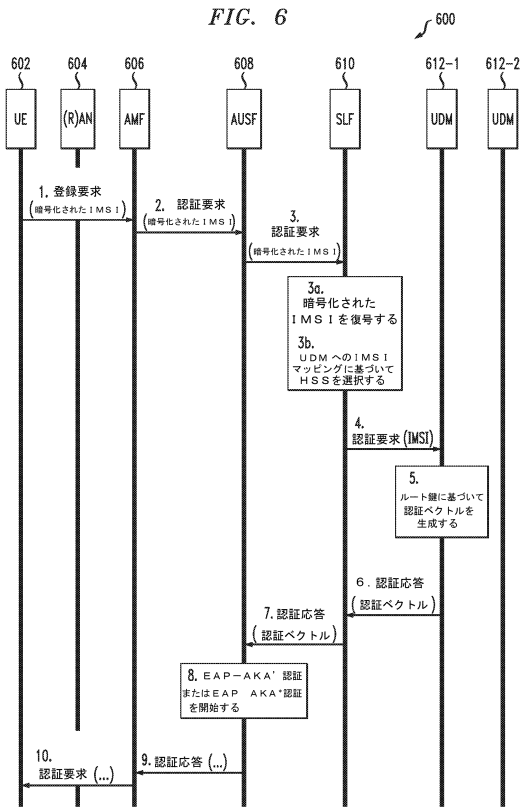
40

50

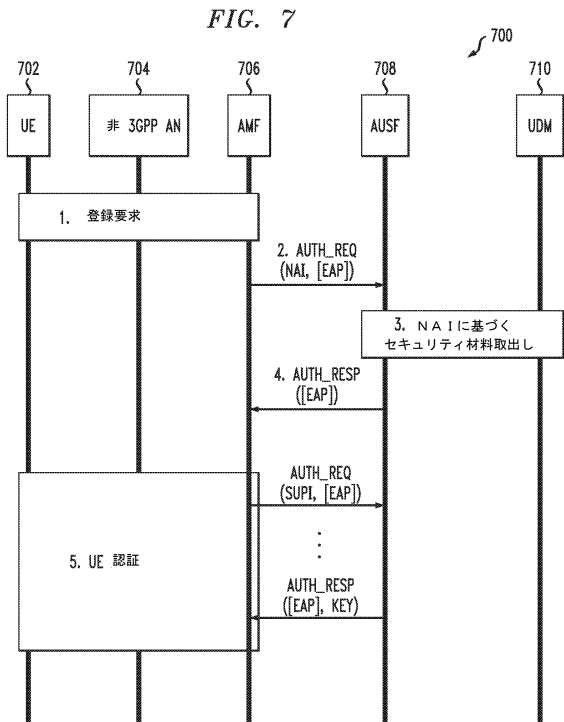
【図 5】



【図 6】



【図 7】



10

20

30

40

50

フロントページの続き

(33)優先権主張国・地域又は機関

米国(US)

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

(72)発明者 ネアー, スレッシュ

アメリカ合衆国、ニュー・ジャージー・07974-0636、マレイ・ヒル、マウンテン・アベ
ニュー・600-700

(72)発明者 イェリホー, アンヤ

ドイツ国、81541・ミュンヘン、ベリンハシュトラッセ・91、ビルディング・41

(72)発明者 ゼーフェルト, アネット

ドイツ国、10587・ベルリン、ザルツウーファー・11

審査官 米倉 明日香

(56)参考文献 特開2000-031980(JP, A)

米国特許出願公開第2015/0148020(US, A1)

3GPP TR 33.899 V1.1.0(2017-03), 2017年04月13日

(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