

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7173320号
(P7173320)

(45)発行日 令和4年11月16日(2022.11.16)

(24)登録日 令和4年11月8日(2022.11.8)

(51)国際特許分類

F I

H 0 4 W	8/24 (2009.01)	H 0 4 W	8/24	
H 0 4 W	8/26 (2009.01)	H 0 4 W	8/26	1 1 0
H 0 4 W	12/02 (2009.01)	H 0 4 W	12/02	
H 0 4 W	76/10 (2018.01)	H 0 4 W	76/10	

請求項の数 9 (全31頁)

(21)出願番号	特願2021-521549(P2021-521549)	(73)特許権者	000004237
(86)(22)出願日	令和1年11月6日(2019.11.6)		日本電気株式会社
(65)公表番号	特表2022-505486(P2022-505486 A)	(74)代理人	東京都港区芝五丁目7番1号 100103894 弁理士 家入 健
(43)公表日	令和4年1月14日(2022.1.14)	(72)発明者	デ キーフィット サンダー
(86)国際出願番号	PCT/JP2019/043451		東京都港区芝五丁目7番1号 日本電気株式会社内
(87)国際公開番号	WO2020/095938	(72)発明者	ブラサド アナンド ラガワ
(87)国際公開日	令和2年5月14日(2020.5.14)		東京都港区芝五丁目7番1号 日本電気株式会社内
審査請求日	令和3年4月20日(2021.4.20)	(72)発明者	バスカラン シーバ バッキア メーリ
(31)優先権主張番号	201811041964		東京都港区芝五丁目7番1号 日本電気株式会社内
(32)優先日	平成30年11月6日(2018.11.6)	(72)発明者	バスカラン シーバ バッキア メーリ
(33)優先権主張国・地域又は機関	インド(IN)	審査官	松野 吉宏

最終頁に続く

(54)【発明の名称】 通信端末装置、コアネットワーク装置、及びそれらの方法

(57)【特許請求の範囲】

【請求項1】

更新されたRouting IDを、コアネットワーク装置から受信する受信部と、
前記更新されたRouting IDに関連するMAC-I (Message Authentication Code for Integrity)を確認し、
前記MAC-Iが有効な場合には、前記更新されたRouting IDをUSIM (Universal Subscriber Identity Module)に格納する制御部と、
暗号化されたSUPI (Subscription Permanent Identifier)と前記更新されたRouting IDとから少なくとも構成されるSUCI (Subscription Concealed Identifier)を、前記コアネットワーク装置へ送信する送信部と、
を備える通信端末装置。

【請求項2】

前記受信部は、確認メッセージを前記コアネットワーク装置から受信する請求項1に記載の通信端末装置。

【請求項3】

更新されたRouting IDを通信端末装置へ送信する送信部と、
暗号化されたSUPIと前記更新されたRouting IDとから少なくとも構成されるSUCIを、前記通信端末装置から受信する受信部と、

前記 S U P I が前記更新された R o u t i n g I D に対応しているかを検証する検証部と、

を備えるコアネットワーク装置。

【請求項 4】

前記暗号化された S U P I は、前記 S U C I に対して S I D F (S u b s c r i p t i o n I d e n t i f i e r D e - c o n c e a l i n g F u n c t i o n) を実行することによって取得される請求項 3 に記載のコアネットワーク装置。

【請求項 5】

前記検証部は、前記 S I D F から取得された前記 S U P I と、前記更新された R o u t i n g I D に関連付けて記憶された別の S U P I と比較することによって、前記 S U P I を検証する請求項 4 に記載のコアネットワーク装置。

【請求項 6】

前記送信部は、前記検証部による検証の結果に基づいて、前記通信端末装置に確認メッセージを送信する請求項 5 に記載のコアネットワーク装置。

【請求項 7】

前記コアネットワーク装置は、A M F (A c c e s s a n d M o b i l i t y M a n a g e m e n t F u n c t i o n) である、請求項 3 から 6 のいずれか一項に記載のコアネットワーク装置。

【請求項 8】

更新された R o u t i n g I D を、コアネットワーク装置から受信し、

前記更新された R o u t i n g I D に関連する M A C - I を確認し、

前記 M A C - I が有効な場合には、前記更新された R o u t i n g I D を U S I M に格納し、

暗号化された S U P I と前記更新された R o u t i n g I D とから少なくとも構成される S U C I を、前記コアネットワーク装置へ送信する、通信端末装置の方法。

【請求項 9】

更新された R o u t i n g I D を通信端末装置へ送信し、

暗号化された S U P I と前記更新された R o u t i n g I D とから少なくとも構成される S U C I を、前記通信端末装置から受信し、

前記 S U P I が前記更新された R o u t i n g I D に対応しているかを検証する、コアネットワーク装置の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、通信システムにおける装置及び方法に関する。

【背景技術】

【0002】

5 G モバイルネットワークでは、攻撃者がエアインターフェイス上の永続的な ID を盗聴することを防ぐ新しい保護メカニズムが導入されている。この機能を使用するモバイルデバイス (U E と呼ばれる) は、公開キーを使用して永続的な ID (S U P I として知られている) を暗号化し、暗号化された ID (S U C I として知られている) をネットワークに送信する。モバイルネットワークは一般に相互接続されており、モバイルデバイスが、サブスクリプションが保持されていない第 2 のモバイルネットワークに接続することはよくあることである。このような場合、モバイルデバイスは、訪問したネットワーク、訪問した P L M N 、 V P L M N をローミングしていると呼ばれる。したがって、S U C I を復号化するために、S U C I を、モバイルデバイスがサブスクリプションを保持するホームネットワーク、又はホーム P L M N 、 H P L M N に送信する必要がある。

【0003】

暗号化された ID を、正しいネットワーク、及び第 2 のネットワーク内の加入者データ

10

20

30

40

50

ベース（UDMと呼ばれる）にルーティングできるようにするために、モバイルデバイスは、MCC（mobile country code）、MNC（mobile network code）、ルーティングID（Routing ID）、及びホームネットワーク公開鍵識別子などのルーティングデータをSUCIに不可又は追加する。MCC及びMNCは、共に、SUCIを受信した訪問ネットワークがSUCIをホームネットワークにルーティングすることを可能にし、Routing IDは、ホームネットワークにより、ホームネットワーク内のUDMインスタンスを特定するために使用される。最後に、ホームネットワーク公開鍵識別子は、SUCIの復号化に使用される対応する秘密鍵を検索するために使用される。最後のアクションは、通常、SUCIの秘匿解除機能、又はSIDFによって実行される。

【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)

S3-183074 - Reply LS on RoutingID

S2-1810060, Update of Routing ID in the UE, 2018/10/15

S2-1811541, Update of Default Configured NSSAI and other UE parameters via a Control Plane Solution from UDM to AMF with Direct NAS Transport to UE, 2018/10/15

【発明の概要】

【発明が解決しようとする課題】

【0005】

MNC/MCC及びRouting IDが正しくないと、SUCIは、間違ったネットワーク、又はホームネットワーク内の間違ったエンティティにそれぞれルーティングされ、その後復号化されなくなる。ホームネットワーク公開鍵識別子にエラーがあると、SIDFが対応する秘密キーを見つけられないか、或いは、間違ったキーを見つけるため、SIDFがSUCIを復号できなくなる。同様に、ホームネットワーク公開鍵にエラーがあると、UEは、SUP Iを暗号化するために誤った公開鍵を使用し、保護スキームにエラーがあると、UEは、誤った保護スキームを使用する。どちらの場合も、受信SIDFは、復号できない。

【0006】

前の段落で説明したエラーケースは、ネットワークへのアクセスを取得するために必要なため、回復できない。これらのパラメータがない場合、又は破損したパラメータがある場合、SUCIを正しいエンティティにルーティングできないか、復号化できないため、ネットワークへのアクセスができない。これらのパラメータの破壊を防止するために、これらのパラメータは、一般に、UICC（Universal Integrated Circuit Card）又はeUICC（Embedded UICC）と呼ばれるセキュアな読取り専用記憶装置に格納され、上述のエラーを防止することができる。

【0007】

しかしながら、近年、3GPP SA 2ワーキンググループは、サブスクリプションデータがあるUDMインスタンスから別のUDMインスタンスに移行される場合（非特許文献4及び非特許文献5を参照）、Routing IDを更新する必要があると考えた。この新たに導入されたニーズは、Routing IDが読み取り／書き込みメモリに格納される必要があり、そのため攻撃者による攻撃に対して脆弱になることを意味する。さらに、将来的には、ホームネットワーク公開鍵、ホームネットワーク公開鍵識別子、保護スキーム、及びUSIM（universal subscriber identity module）に格納される他のアタッチリキティカルデータを更新する必要性が生じる可能性がある。これらパラメータは、ネットワークにアタッチするために重要であるため、堅牢なセキュリティメカニズムを導入

10

20

30

40

50

する必要がある。

【0008】

本開示は、上記課題に鑑み、様々な課題の少なくとも1つを解決する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】

【0009】

第1の態様において、本開示は、装置を提供する。装置は、1つ以上の命令を格納するメモリと、前記1つ以上の命令を実行することで、ネットワーク通信に対応する更新情報を外部機器から受信し、前記更新情報に基づいてSUCI (Subscription Concealed Identifier) を取得し、前記SUCIを前記外部装置に送信するように構成されるプロセッサを含む。

10

【0010】

第2の態様において、本開示は、装置を提供する。装置は、1つ以上の命令を格納するメモリと、前記1つ以上の命令を実行することで、ネットワーク通信に対応する更新情報を外部機器に送信し、前記更新情報に基づいて取得されるSUCI (Subscription Concealed Identifier) を前記外部装置から受信し、前記受信したSUCIに基づいてSUP I (Subscription Permanent Identifier) を取得し、前記SUP Iが前記更新情報に対応しているかを検証するように構成されるプロセッサを含む。

【0011】

第3の態様において、本開示は、方法を提供する。方法は、外部機器から、ネットワーク通信に対応する更新情報を受信し、前記更新情報に基づいてSUCI (Subscription Concealed Identifier) を取得し、前記SUCIを前記外部装置に送信することを含む。

20

【0012】

第4の態様において、本開示は、方法を提供する。方法は、ネットワーク通信に対応する更新情報を外部機器に送信し、前記更新情報に基づいて取得されるSUCI (Subscription Concealed Identifier) を前記外部装置から受信し、前記受信したSUCIに基づいてSUP I (Subscription Permanent Identifier) を取得し、前記SUP Iが前記更新情報に対応しているかを検証することを含む。

【図面の簡単な説明】

【0013】

【図1】図1は、本開示の第1実施形態に従ってパラメータが更新された後に、パラメータの正確性を確認するための方法を示すシーケンス図である。

30

【図2A】図2Aは、SUCIが確認される第1のシナリオを示すシーケンス図である。

【図2B】図2Bは、SUCIが確認される第2のシナリオを示すシーケンス図である。

【図2C】図2Cは、SUCIが確認される第3のシナリオを示すシーケンス図である。

【図3】図3に障害発生時の対処方法を示すシーケンス図を示す。

【図4】図4は、別の障害処理を示すシーケンス図である。

【図5】図5は、他の障害の対処方法を示すシーケンス図である。

【図6】図6は、新しいアタッチを用いる回復手順を示すシーケンス図である。

【図7】図7は、本開示の第2実施形態に従ってパラメータが更新された後にパラメータの正当性を確認する方法を示すシーケンス図である。

40

【図8】図8は、パラメータの正当性を確認する方法の一部を示すシーケンス図である。

【図9】図9は、USIMの内容の一例を示す図である。

【図10】図10は、本開示の第3実施形態に従ってパラメータが更新された後に、パラメータの正確性を確認するための方法を示すシーケンス図である。

【図11】図11は、パラメータの優先度を変更するための手順を示すシーケンス図である。

【図12】図12は、優先度変更後のUSIMのテーブルを示す。

【図13】図13は、UEの主要な構成要素を示すブロック図である。

【図14】図14は、例示的な(R)ANノードの主要な構成要素を示すブロック図であ

50

る。

【図 1 5】図 1 5 は、例示的なコアネットワークノードの主要な構成要素を示すブロック図である。

【図 1 6 A】図 1 6 A は、第 1 の更新シナリオを示すシーケンス図である。

【図 1 6 B】図 1 6 B は、第 2 の更新シナリオを示すシーケンス図である。

【図 1 6 C】図 1 6 C は、第 3 の更新シナリオを示すシーケンス図である。

【図 1 7】図 1 7 は、パラメータを更新するためのメカニズムを示すシーケンス図である。

【図 1 8】図 1 8 は、本開示の第 2 実施形態によるパラメータの正確性を確認するための別の方法を示すフローチャートである。

【発明を実施するための形態】

【0014】

本文書の目的のために、非特許文献 1 及び以下に示す略語を適用する。この文書で定義された省略形は、もしあれば、非特許文献 1 の同じ省略形の定義より優先される。

5GC 5G Core Network

5GS 5G System

5G-AN 5G Access Network

5G-GUTI 5G Globally Unique Temporary Identifier

5G S-TMSI 5G S-Temporary Mobile Subscription Identifier

5G (Home)BSF 5G (Home) Boot Strapping Function

AMF Access and Mobility Management Function

AN Access Node

AKMA Authentication and Key Management for Applications

AS Access Stratum

AUSF Authentication Server Function

CP Control Plane

CM Connection Management

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)

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

ME Mobile Equipment

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

MME Mobility Management Entity

N3IWF Non-3GPP Inter Working Function

NAI Network Access Identifier

NAS Non-Access Stratum

10

20

30

40

50

NEF	Network Exposure Function	
NF	Network Function	
NG-RAN	Next Generation Radio Access Network	
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	10
PEI	Permanent Equipment Identifier	
PER	Packet Error Rate	
PFD	Packet Flow Description	
PLMN	Public land mobile network	
PPD	Paging Policy Differentiation	
PPI	Paging Policy Indicator	
PSA	PDU Session Anchor	
QFI	QoS Flow Identifier	
QoE	Quality of Experience	
(R)AN	(Radio) Access Network	20
RLC	Radio Link Control	
RM	Registration Management	
RQA	Reflective QoS Attribute	
RQI	Reflective QoS Indication	
RRC	Radio Resource Control	
SA NR	Standalone New Radio	
SBA	Service Based Architecture	
SBI	Service Based Interface	
SD	Slice Differentiator	
SDAP	Service Data Adaptation Protocol	30
SEAF	Security Anchor Functionality	
SEPP	Security Edge Protection Proxy	
SMF	Session Management Function	
S-NSSAI	Single Network Slice Selection Assistance Information	
SSC	Session and Service Continuity	
SST	Slice/Service Type	
SUCI	Subscription Concealed Identifier	
SUPI	Subscription Permanent Identifier	
UDSF	Unstructured Data Storage Function	
UL	Uplink	40
UL	CL Uplink Classifier	
UPF	User Plane Function	
UDR	Unified Data Repository	
URSP	UE Route Selection Policy	
USIM	Universal Subscriber Identity Module	
SMS	Short Message Service	
SMSF	SMS Function	
SQN	Sequence number	
MT	Mobile Terminated	
[0 0 1 5]		50

本開示の目的のために、非特許文献1及び以下に示す用語及び定義が適用される。本開示で定義されている用語は、もしあれば、非特許文献1の同じ用語の定義よりも優先される。

【0016】

上述のように、3GPP SA2は、移動通信事業者があるUDMから別のUDMにサブスクリプションを移動させることができるようにするために、USIM内のRouting IDを更新する必要性を議論した。本開示は、加えて、ホームネットワーク公開鍵などの他のパラメータの更新も考える。メカニズムは似ているように見えるかもしれないが、わずかな違いがある。

【0017】

図16A～16Cは、3つの更新シナリオを示す。図16Aに示すように、第1の更新シナリオは、サブスクリプションを移動するターゲットUDM (UDM2) が、新たなサブスクリプション情報を受信した後、UEにRouting IDを更新する指令を送信することにより、UEと更新手順を開始するシナリオである。図16Bに示すように、第2の更新シナリオは、サブスクリプションデータが削除されるソースUDM (UDM1) が、更新手順を開始するシナリオである。観察されたように、サブスクリプション情報を2つのUDM間で移動することは、Routing IDを更新する理由であり、したがって、更新手順を実行しなければならない。

【0018】

図16Cに示すように、最後のシナリオは、サブスクリプション情報が1つのUDMから別のUDMに移動されないという点でわずかに異なる。このようなシナリオは、ホームネットワーク公開鍵と、ホームネットワーク公開鍵識別子及び保護スキームのような他のパラメータを更新するために使用することができる。このような手順が実行される他のシナリオは、例えば、ローミングのステアリングが使用される場合である。ローミングのステアリングは、UEをある訪問ネットワークから別の訪問ネットワークに移動させるために、ホームオペレータによって適用される。このような場合、UDMは、UEを所望のネットワークに誘導する目的で、ローミングパートナーのリストを送信する。

【0019】

ローミングのステアリングのために、非特許文献2に記述されているようなセキュリティソリューションがある。このソリューションは、非特許文献3に記述され、図17に示されるように、Routing IDの更新、又はキー更新に適合され得る。このソリューションは、AUSF、ホームネットワーク内のエンティティ、及びモバイル機器 (ME: mobile equipment) の間で、AUSF及びMEに格納されている秘密鍵に基づいて、データを安全に送信するメカニズムを提供する。KAUSFに格納されている秘密鍵は、モバイルデバイスがネットワークへのアクセスを要求した後に、モバイルデバイスとホームネットワークとによって正常に実行される認証と鍵合意の成功の結果である。したがって、このキーは、UEが認証に成功した場合にのみ使用でき、UEがサービスネットワークから切断された後は使用できない。

【0020】

より詳細には、このようなソリューションは次のように機能する。UDMは、アタッチ関連パラメータ更新 (図17では、キー更新が例として示されている) のメッセージを準備し、AUSFに送信する。AUSFは、キー導出関数 (KDF: key derivation function) を使用してMACを作成し、MACを次のように計算する。 $MAC = KDF(K_{AUSF}, \text{「Attach Parameter Update」}, \text{カウンタ}, \text{メッセージ})$ KAUSFは、キー導出関数への入力キーであり、「Attach Parameter Update」は、このMACがアタッチパラメータ更新手順に対して計算されることを示すテキストフィールドである。テキストフィールドには異なる値を指定できるが、後続の手順に対しては常に固定される。テキストフィールドは、メソッドの固定値である。カウンタは、キーの繰り返しを避けるために使用され、全てのアタッチ関連パラメータ更新メッセージで拡張される。メッセージは、UDMからのプレーンテキストメッセージである。追加的に、他の値もKDFに追加でき

10

20

30

40

50

る。

【0021】

次のステップで、AUSFは、MACとカウンタを返す。UDMは、MAC、カウンタ、及びメッセージをAMFに送信し、AMFは、NAS DL転送メッセージを使用してメッセージをUEに転送する。UEがメッセージを受信すると、UEは、プレーンテキストメッセージ、カウンタ、テキストフィールド、及びKAUSF(XMAC=KDF(KAUSF,「Attach Parameter Update」、カウンタ、メッセージ))からMACを計算し、XMACがMACと一致する場合、キーを保存する。

【0022】

次に、ネットワークが確認を要求した場合、UEは、UEがキーを受信したことを示す確認メッセージを送信する。保護するために、UEは同様の計算、すなわちMAC=KDF(KAUSF,「Attach Parameter Update」、カウンタ、メッセージ)を使用する。カウンタは、UEが受信したカウンタと比較して1つ増加し、メッセージは、UEがネットワークに送信するプレーンテキストメッセージである。UEは、確認、MAC、及びカウンタをAMFに送信し、AMFは、これをUDMに転送する。受信すると、UDMはメッセージ、MAC、及びカウンタをAUSFに転送し、AUSFがMACを確認できるようにする。

【0023】

上記の変更が可能である。例えば、この方法のためにKAUSFから特定の鍵を導出し、異なる完全性保護メカニズムを使用することができる。しかしながら、このようなKAUSFベースのソリューションは、MEとAUSFと間のメッセージ交換を保護するだけであることに注意されたい。非特許文献3においてコメントされているように、このような、MEがファイルの更新を許可されるメカニズムを使用すると、ファイルは攻撃に対して脆弱になる。したがって、秘密鍵を使用してUDMとMEとの間を保護することに基づくメカニズムは、通信を保護するだけであり、正しいデータが安全な記憶装置に書き込まれ、正しいデータを取り出すことができるという確実性を提供しないため、この問題に対処するには不十分である。

【0024】

非特許文献3では、さらに2つのソリューションが記述されている。特に、USIMが、USIM内にあらかじめ記憶される複数の値の間で切り替えることができる解決策が記述される。このメカニズムは、次のアタッチのためにUSIMによって使用されるデータセットを切り替えるAUTHENTICATEコマンドに依存する。その代わり、USIMは、UDMがメッセージがUSIMによって受信されたことを知ることができるように、SUCIに暗号化された部分を追加することができる。しかしながら、このソリューションは、USIMからUDMへの確認が欠けているため、USIMに切り替えコマンドを発行する前に、UDMがアタッチクリティカルパラメータが正しく格納されているかどうかを知る方法がない。このように、UEは、アタッチクリティカルパラメータセットを切り替えた後でも、サービスなしのままでいることができた。

【0025】

以上を考慮すると、本発明者らは、パラメータを更新した後、セキュアストレージに正しいパラメータが格納されていること、及び、モバイルデバイスがネットワークから切り離された後、ネットワークにアタッチできることを確認する必要性を認識した。

【0026】

(第1実施形態)

図1は、本開示の第1実施形態に従ってRouting IDなどのアタッチ関連パラメータが更新された後、それらパラメータの正確性を確認するための方法を示す。図1は、例としてRouting IDを使用しているが、これらの方法は、ホームネットワーク公開鍵、ホームネットワーク公開鍵識別子、保護スキームなどの更新後に同様に適用することができる。以下の説明において、Routing IDは、それらパラメータの一例としてのみ理解される。

10

20

30

40

50

【0027】

図1に示すように、ステップ1において、UDMは、MEとUSIMを含むUEの新しいRouting IDをサービングネットワークのAMFに送信する。UDMが登録中にこの情報を送信する場合、UDMは、AMFのNudm__SDM__Get要求に応答してSDM__Get__ResponseメッセージでRouting IDを送信できる。UDMがUEが接続されている間にこの情報を送信したい場合、UDMは、SDM__UpdateNotificationを用いて、UEにデータを転送する必要があることをAMFに通知することができる。また、ローミングのステアリングのために、非特許文献2に記述されている方法、又は図17に説明されている方法に従って、このメッセージを完全に保護することも可能である。その方法が使われる場合、Routing IDは、関連したセキュリティパラメータ、とりわけMEがRouting IDの完全性を検証するために使うことができるMAC-Iを持つことができる。

10

【0028】

ステップ2で、AMFは、DL NASトランスポートメッセージを使用してUEに新しいRouting ID（及び、Routing IDが完全性保護されている場合はMAC-Iのような他の関連パラメータ）を転送する。UEは、DL NAS転送メッセージを受信した後、MAC-Iが正しいかどうかを確認する（存在する場合）。その場合、UEは、ステップ4において、USIMに新しいRouting IDを格納する。

【0029】

ステップ5において、USIMは、ホームネットワーク公開キー、MCC/MNC、及び新たに格納されたRouting IDを使用して、新しいSUCIを作成する。ステップ6において、USIMは、MEに新しいSUCIを送信し、ステップ7において、MEは、UL NASトランスポートメッセージで新しいSUCIをAMFに送信する。MEは、MEとAUSFとの間のこのメッセージを、図17に記載される方法を使用して、完全性保護することができる。その場合、UL NASトランスポートメッセージは、メッセージが変更されずにAUSFに到着したことをAUSFが確認することを可能にするセキュリティ関連パラメータも含む。

20

【0030】

UL NASトランスポートメッセージを受信した後、AMFは、ステップ8において、Nudm__SDM__Infoメッセージを使用して、SUCI、及び関連するセキュリティ・パラメータ（含まれる場合）をUDMに転送する。セキュリティパラメータが含まれている場合、UDMは、非特許文献1に従った検証のためにメッセージをAUSFに送信する。メッセージが正しく検証されると、UDMは、Routing IDの値が正しいか否かをチェックする。

30

【0031】

UDMが上記のチェックを実行する方法は、Routing IDの受信方法に依存して異なる。図2A～2Cは、SUCIが確認されるシナリオを示している。図2Aは、第1のシナリオを示す。最初のシナリオでは、Routing IDの更新手順はサブスクリプションの移動先であるUDM2によって実行され、そのため、UDM2は、Routing IDをローカルにチェックすることができる。図2Aに示すように、UDM2はSUCI（一例として、UDM2はRouting IDを受信することもできる）を受信し、SUCIはSIDF2に転送され、SUP IはUDM2に戻される。UDM2は、SUP IがSUCIを含む更新確認メッセージを受信したばかりのSUP Iに対応していることを確認できるようになった。

40

【0032】

図2Bは、第2のシナリオを示す。第2のシナリオの場合、アタッチアップデートパラメータ確認メッセージを受信するUDMは、新しいサブスクリプションの移動先のUDMと同じではない。このような場合、UDM1は、アタッチアップデートパラメータ確認メッセージでSUCIを受信した後、SUCIをUDM2に転送する。次いで、UDM2は、UDM2に属するSIDF2にSUCIを転送する。図2Bに示すように、SIDF2

50

は、S U P IをU D M 2に返す。U D M 2は、S U P Iを、U D M 1に転送し、第1のシナリオと同様の比較が実行される。

【0033】

図2Cは、第3のシナリオを示す。第3のシナリオでは、サブスクリプションが格納される場所に変更はなく、図2Cから分かるように、第3のシナリオは第1のシナリオに似ている。U D M 1は、U Eからアタッチ更新パラメータ確認メッセージを受信し、S U C Iを抽出し、S U C IをS I D F 1に転送する。S I D F 1は、S U C Iの秘匿を解除し、比較のためにS U P IをU D M 1に返す。

【0034】

何れの場合も、アタッチパラメータ更新確認メッセージを受信したU D Mでの比較結果が成功すると、U D Mは、R o u t i n g I DがU S I Mに正しく格納されていることを確認する。S I D FがS U C Iを秘匿解除できない、R o u t i n g I Dが誤ったU D M又は存在しないU D Mを指しているなどの理由でエラーが発生し、アタッチパラメータ更新確認メッセージを受信したU D Mは、更新が失敗したと判断できる。このような場合には、障害が発生したことがU Eに報告され、及び／又は、復旧手順が開始される必要がある。失敗した場合の対処については後述する。

【0035】

前述の例では、S U C Iは、S I D Fを使用して秘匿解除される。これは、R o u t i n g I Dに代えてホームネットワークの公開鍵が更新される場合に特に有効である。ホームネットワーク公開鍵が更新され、S I D Fが新しいホームネットワークの公開鍵で暗号化されたS U C IからS U P Iを秘匿解除できる場合、U D Mは、新しくプロビジョニングされたホームネットワークの公開鍵がU S I Mに正しく格納されていることを確認する。

【0036】

ステップ5において、U Eは、ホームネットワーク公開鍵でS U P Iを暗号化することにより非対称暗号化を実行する。S U P Iに代わり、U Eは、更新されたパラメータ（この場合はR o u t i n g I D）のみを暗号化し、或いは、同じメッセージ内でR o u t i n g I DとS U P Iとを連結することもできる。これは、特にS U C IがM EではなくU S I Mで計算される場合に、R o u t i n g I Dの正確性に対する追加の保証を提供する。そのような場合において、図2Aから2Cの場合、S U P Iの全てのインスタンスはR o u t i n g I Dに置き換えられ、S U C Iの全てのインスタンスは「暗号化されたR o u t i n g I D」に置き換えられる。

【0037】

図1のステップ11～13のメッセージは、U D Mが正しい情報を受信したことを確認するための、U D MからU Eへの確認メッセージのセットである。これらメッセージは、ステップ1～3のメッセージと同じ経路をたどる。U D Mは、S D M__U p d a t e N o t i f i c a t i o nを使用して確認メッセージをA M Fに送信し、ステップ11においてデータをU Eに転送する必要があることをA M Fに通知する。ステップ1のメッセージと同様に、ローミングのステアリングのために、非特許文献2に記述された方法に従って、確認メッセージを完全性保護することも可能である。その方法が使用される場合、追加のセキュリティパラメータが含まれる必要がある。A M Fは、ステップ12において、D L N A Sトランスポートメッセージを使用してU Eに確認メッセージを転送する。M Eは、D L N A S転送メッセージを受信した後、M A C - Iが正しいかどうかを確認する（存在する場合）。そうであれば、M Eは、ステップ13においてU S I Mに確認メッセージを転送する。

【0038】

確認自体には、状況が正しいことを示す、単純なバイナリ値「正しい」又は「1」を含めることができる。加えて、ホームネットワークは、U S I Mに格納されているホームネットワーク公開鍵に対応するホームネットワーク秘密鍵を使用してメッセージを完全性保護できる。このように、U S I Mは、ネットワークが確認を送信したことを検証できる。

【0039】

しかしながら、前段落で説明した確認メッセージは、他のUSIMに再生することができる。それを防止する場合、確認メッセージは、UDMによって受信されたSUCIをさらに含み、USIMによって作成されたSUCIとUDMによって返された確認とが結合される。ただし、ステップ5において、USIMは、USIMが確認メッセージを受信するまで、USIMが構築したSUCIを格納する必要がある。USIMが確認メッセージを受信した場合、USIMは、メッセージの完全性が保護されているか否かを確認し、また、確認メッセージに含まれるSUCIがUSIMが格納したものと同一であることを確認する。

【0040】

このような確認メッセージの利点は、USIMとUDMの双方が、双方が保存したアタッチリティカルパラメータが正しく、かつ検証済みであることを確認することである。USIMがメッセージを確認した後、USIMは、新しいアタッチパラメータを恒久的に格納し、これらのパラメータを後続のアタッチに使用することができる。

【0041】

図2A～2Cにおい説明されるように、障害が発生する可能性がある。例えば、UEが正しいホームネットワークキーを格納していない、或いは誤ったRoutingIDを格納することがある。そのような場合、図2Aから2Cに記載されるUDMによる検証は、エラーを示す。UDMからUEへの確認メッセージ（図1のステップ11～13）が失われると、別の障害が発生する可能性がある。このような場合、UEは、新しいアタッチリティカルパラメータが正しいかどうかを見つけるために、回復手順を実行する必要がある。

【0042】

図3に障害発生ケースの対処方法を示す。図3のステップ1及び2は、図1のステップ6～8に対応する。違いは、USIMとMEとを図3では1つのものとみなし、組み合わせて「UE」という用語を使用している点である。ステップ3において、図1の説明文に示すように、UDMにてアタッチパラメータ更新確認メッセージを処理し、その際にエラーとなる。例えば、RoutingIDが正しくない場合、SUCIを秘匿解除できないか、或いはSUCIの秘匿解除から誤った値が生じる。ステップ3の後、UDMは更新が失敗したことを認識し、正しい値を提供し、障害が発生したことを通知するために、ステップ4及び5において、メッセージを、AMFを介してUEに送信する。ステップ4及び5のメッセージは、図1のステップ1～3のメッセージに類似している。受信後、UEは、再びメッセージを検証し、ステップ6で新しい値を格納する。図3のステップ6は、図1のステップ4及び5に対応する。UEは、ステップ7及び8の検証のために、再び「アタッチパラメータ更新確認」メッセージを、AMFを介してUDMに送信することができる。UDMは、全てが正しいかどうかを再度検証する。検証に失敗した場合は、ステップ4から処理を繰り返す。

【0043】

図4に別の障害処理を示す。図4のステップ1～3は、図3のステップ1～3と同じである。ただし、ステップ4及び5において、UDMは、UEに障害を示し、AMFを介してUEにこの障害を送信する。UEは、受信すると、ステップ6において、新しいキーを削除して元の値に戻す。また、UDMは、ステップ6で古い値を復元する。UDMは、UDMとUDM2との間でサブスクリプションが転送される場合、ステップ7においてUE側の更新が失敗し、サブスクリプションが転送できないことを、第2のUDM（UDM2）に通知してもよい。この手順の結果、UE及びUDMは共に元の状態に戻り、UEは、次回、古い値を使用してアクセスできるようになる。

【0044】

図5に別の故障事例を示す。別の障害ケースは、UDMからUEへの確認メッセージ又は障害メッセージが転送中に失われるケースである。図5のステップ1～3は、図3のステップ1～3とほぼ同じである。相違点は、ステップ1aにおいて、UEは、「アタッチパラメータ更新確認メッセージ」を送信した後、UDMの確認メッセージ又は失敗メッセ

10

20

30

40

50

ージをどれだけ待機するかを示す待機タイマを設定することである。ステップ 4 において、UDM は UE に障害又は確認を通知し、UE にこのメッセージを送信しようとし得る。UDM から UE への途中に、エアインターフェイスなどでメッセージが消失することがある。ステップ 5 では、UE 側のタイマが期限切れになり、そのため、UE は、ステップ 6 及び 7 で、新しい「アタッチパラメータ更新確認」メッセージを AMF を介して UDM に送信する。この場合も、UDM は前述のように処理し、確認メッセージ又は失敗メッセージを送り返す。メッセージが UE によって正しく受信された場合、UE は、新しいアタッチパラメータを永続的に保存し、ステップ 11 で手順が完了したと考える。

【0045】

図 6 は、新たなアタッチを用いた回復手順を示す。図 6 のステップ 1-3 は、図 5 のステップ 1-3 に対応する。ステップ 4 において、確認メッセージ又は失敗メッセージは失われ、UE タイマはステップ 5 において期限切れになる。図 6 の場合、UE は、アタッチ手順を用いて新たな SUCI を確認する。これを行うために、UE は、ステップ 6 で新しいアタッチ手順を開始する。例えば、UE は、同じネットワークに再びアタッチし、或いは別のネットワークにアタッチできる（UE がローミング中の場合）。ステップ 7 において、通常のアタッチ手順が実行され、このアタッチ手順の一部として、UE は、UDM に SUCI を送信する。成功すると、ステップ 8 において、アタッチは、AMF 2 から UE に返される「アタッチ完了」メッセージをという結果になる。UE がこのアタッチ完了を受信しない場合、又はエラーメッセージを受信する場合、UE は、新しいアタッチ関連パラメータが不完全であると仮定し、元のパラメータに戻る。

【0046】

ホームネットワーク側では、UDM 2 は、SUCI の秘匿を解除した後、ステップ 9 において、特定の加入者（SUP I によって示される）に対して正しい SUCI を受信したことを UDM 1 に通知できる。これは、サブスクリプションの転送が成功したことを UDM 1 に示し、UDM 1 は、ステップ 11 において、対応するサブスクリプションをメモリから削除することができる。

【0047】

ステップ 10 において、UE は、アタッチされていたネットワークからデタッチする。ステップ 10 は、ネットワークへの二重登録を回避するために、ステップ 6 の前に実行することもできる。ステップ 10 を先に行うことの欠点は、UE がユーザエクスペリエンスを妨げるダウンタイムを経験する可能性があることである。ステップ 12 において、UE は、新しいマテリアルを使用に移し、それを永久的に保存する。UE は、古いアタッチクリティカルパラメータを削除することもできる。

【0048】

（第 2 実施形態）

図 7 は、本開示の第 2 実施形態に従って、ホームネットワーク公開鍵などのアタッチ関連パラメータが更新された後に、これらのパラメータの正当性を確認するための方法を示す。図 7 は、一例としてホームネットワーク公開鍵を用いているが、方法は、Routing ID、保護スキームなどの更新後に同様に適用することができる。以下の説明において、ホームネットワーク公開鍵は、それらパラメータの一例としてのみ理解される。他のパラメータとの違いが発生する場合、違いは本文に示される。

【0049】

図 7 に示す方法では、UDM は、ネットワーク内の鍵サーバ（KS）から新しいホームネットワーク公開鍵を取得する。ステップ 1 において、UDM は、KS に新しい鍵マテリアルを要求する。ステップ 2 において、KS は、UDM に新しい鍵マテリアルを提供する。オプションとして、ステップ 1 をスキップすることができ、UDM は、KS から新しい鍵マテリアルのメッセージを受信することによってトリガされ、UE に新しい鍵マテリアルを送信できる。あるいは、新しい鍵マテリアルは UDM に直接提供されず、UDM に、新しい鍵マテリアルをダウンロードするための URL（Uniform Resource Locator）のみが KS により提供される。説明の残りの部分では、KS が UE に新しい鍵マテリアルを

ダウンロードするためのURLを提供したと仮定する。

【0050】

KSから新しい鍵マテリアル又は新しい鍵マテリアルのURLを受信した後、UDMは、サービングネットワーク内のAMFを介して、ME及びUSIMを含むメッセージをUEに送信する。UDMがUEの登録中にこのメッセージを送信する場合、UDMは、ステップ3において、AMFのNudm__SDM__Get要求に応答して、SDM__Get__Responseメッセージを使用してこのメッセージをAMFに送信できる。ステップ3において、UDMがUEの手順の登録が完了した後にこのメッセージを送信する必要がある場合、UDMは、SDM__UpdateNotificationを使用してこのメッセージをAMFに送信できる。UDMが送信するメッセージは、鍵マテリアルを直接含んでいてもよいし、ダウンロード用のURLを含む、鍵マテリアルのダウンロードをUEに開始させる指示が含まれていてもよい。非特許文献2及び図17に記述された方法を使用して、このメッセージは、AUSFとMEの間で保護することができ、それによってMEはメッセージが正当な発信元（図示されない）から来たことを検証することができる。

【0051】

AMFがメッセージを受信すると、AMFは、ステップ4でUEにメッセージを配信するために、DL NASトランスポートメッセージを使用して、受信したメッセージをUEに転送する。このメッセージを受信すると、MEは、非特許文献2または図17の説明に従って、メッセージの完全性を検証する。完全性が正しい場合、UEは、ステップ5において、示されたURLから新しい鍵マテリアルのダウンロードを続行する。当業者が知るように、URLは、非セキュアなプロトコルとして、HTTP (hypertext transfer protocol)、又はFTP (file transfer protocol) など、セキュアなプロトコルとしてHTTPS (hypertext transfer protocol secure) 又はSFTP (SSH (secure shell) file transfer protocol) などの使用されるプロトコルを含み得る。非セキュアなWebアドレスの例は、http://key-server.operator.3gpp/key_download/new_keyである。セキュアなWebアドレスの例は、https://key-server.operator.3gpp.org/key_download/new_keyである。

【0052】

鍵マテリアルのダウンロードは、ME又はUSIMのいずれかによって実行できる。MEがステップ5でダウンロードを実行すると、MEはサーバに接続して新しい鍵をダウンロードし、メモリに一時的に保存する。以降、ステップ6において、MEは、新しい鍵をUSIMに送信し、保管する。

【0053】

図8は、アタッチ関連パラメータの正当性確認方法の一部を示す。図8のステップ1～4は、図7のステップ1～4と同じでよい。USIMがダウンロードを実行する場合、MEは、USIMに、ステップ5においてAMFから受信したメッセージに含まれるURLを送信する。USIMは、MEからダウンロードトリガーを受信し、ステップ6においてダウンロードを開始する。図7と図8の違いは、ステップ5および6のみであり、したがって、図8のさらなる説明は省略される。ダウンロード後、USIMは、ステップ7において、例えば、新しい鍵ファイルに、又はキーを含むテーブルの新しいエントリとして、キーを直接格納する。

【0054】

図9は、USIMの内容の一例を示す。USIMは、複数の鍵を、テーブルとして表される登録に格納する。USIMは、ホームネットワーク公開鍵（HNキー）、HN公開キーID（HN KID）、Routing ID、保護スキーム、及び優先度又は優先順位フィールドを格納する。これは、MEがSUCIを計算する場合に有利である。なぜならば、MEはUSIM内で見つけた鍵マテリアルに基づいてSUCIを計算するからである。そのためには、MEは、図8に示す登録を、優先度フィールドなしで取得するし、MEがサポートする保護スキームを見つけるまで、それらが格納されているリストを順番に調べる。MEが保護スキーム2をサポートし、リストが保護スキーム1、3、2、4、1、

2のキーを（その順に）含む場合、MEは、常にテーブルの3番目のエントリを選択し、テーブルの6番目のエントリに到達することはない。6番目のエントリに更新されたキーが含まれている場合、MEは、そのキーを選択しない。同様に、3番目のエントリに障害のあるキー又は障害のあるRouting IDが含まれている場合、MEは、別のエントリを選択することではなく、ロックアウトされたままになる。

【0055】

したがって、更新の場合、通常、古いキーの代わりにキーが上書きされる。しかしながら、新しいキーに何らかの障害があるか、或いは、Routing ID、HN KID、若しくは保護スキームなどの関連パラメータに障害がある場合、UEはサービスを取得できない。この問題を解決するために、USIMにエントリを追加することができるが、これはMEがこのキーを使用しないことを意味する。優先度パラメータを追加することで、この問題を次のように解決できる。

【0056】

図7を再び参照すると、ステップ5及び7に従ってキーがダウンロードされ、格納されると、ステップ6において、同じ保護スキームを有する既存のキーの優先度パラメータよりも低い優先度パラメータがUSIMによって割り当てられる。

【0057】

ステップ8において、キー検証、又はアタッチパラメータ確認プロセスが開始される。そのために、MEは、ステップ8において、USIMに公開鍵のリストを要求する。USIMは、ステップ9において、修正されたリストを提示し、リストにおいて、最近更新された鍵がリストの先頭に来るように、ホームネットワーク公開鍵の高優先度エントリは、公開鍵の、新しい、低い優先度エントリで置き換えられる。あるいは、USIMは、MEがSUCI計算のために新しいキーを選択することを強制するために、MEに新たに更新されたキーを提示するだけでよい。MEは、ステップ10においてSUCIを計算し、ステップ11において、アタッチパラメータ確認メッセージを使用して、SUCIをネットワーク（AMF）に送信する。図7において、このメッセージは、例えば、MEが新たに計算されたSUCIを含めるNAS UL転送メッセージである。ステップ11で送信されるメッセージは、Nudm__SDM__Infoメッセージ内で搬送され得る。ステップ12において、AMFは、SUCIをUDMに転送する。SUCIを受信したUDMは、ステップ13において、図1において説明したようにSUCIの検証を行い、ステップ14～16に従って、UEにSUCIが正しいかどうかを通知する。ステップ17において、USIMは、鍵マテリアルを確認する。

【0058】

図18に示される別の例において、鍵検証手順は、別の方法で起動される。図18において、UEは、アタッチパラメータの更新を行い、その後ネットワークからデタッチしている。このデタッチは、これらのパラメータの更新後に常にデタッチが必要なUEの設定の結果であるか、或いは、ネットワークからのデタッチメッセージの結果である可能性がある。しばらくして、UEは、ステップ1でネットワークへのアタッチを試行し、AMFにアタッチメッセージを送信する。AMFは、ステップ2において、ID要求で応答する。MEがSUCIを計算する場合、MEは、ステップ3において、鍵マテリアルをUSIMに要求する。USIMは、ステップ4において、修正されたリストを提示し、リストにおいて、最近更新された鍵がリストの先頭に来るように、ホームネットワーク公開鍵の高優先度エントリが、公開鍵の新しい低優先度のエントリに置き換えられる。あるいは、USIMは、MEがSUCI計算のために新しいキーを選択することを強制するために、MEに新たに更新されたキーを提示するだけでよい。MEは、ステップ5においてSUCIを計算し、ステップ6においてSUCIをネットワークに送信する。

【0059】

サービングネットワークのAMFは、ステップ7において、SUCIのMCC/MNC部分に基づいて、認証要求メッセージ内のSUCIを正しいホームネットワークに送信し、その後、ホームネットワークはRouting IDに基づいてUDMを選択する。UD

10

20

30

40

50

Mは、ステップ8において、S I D FにS U C Iを転送し、S I D Fは、S U C Iを復号化し、UDMにS U P Iを返送する。

【0060】

このS U P Iに基づいて、UDMは認証ベクトルを生成し、UDMは、ステップ9において、認証応答で認証ベクトルをAMFに送り返す。AMFは、ステップ10において、認証要求メッセージを用いてR A N D及びA U T NをUEに転送する。UE内部において、ME部は、ステップ11においてR A N D及びA U T Nを受信し、それらをU S I Mに転送する。

【0061】

U S I MがR A N D及びA U T Nを受信すると、U S I Mは、まずA U T Nが正しいか否かを確認する。A U T Nが正しい場合、U S I Mは、A U T Nを受信されたという事実から、新しい鍵材料が正しいこと、及びそれがサブスクリプションを保持するUDMにつながることを控除することができる。その後、U S I Mは、新しい鍵材料をより高い優先度の場所に移動させ、古い鍵材料を除去するか、又は潜在的なフォールバック位置のために古い鍵材料を保持し、より低い優先度を割り当てるかを決定することができる。後者は、MEが古い鍵材料で暗号化されたS U C Iをネットワークに送信した場合に、U S I Mが脅威を軽減することを可能にし、その後、ネットワークがR A N D及びA U T NをMEに返すようにすることができる。U S I Mが古い鍵を保持するが、低い優先度で保持する場合、U S I Mは、新しい鍵材料が使用されており、古い鍵材料を除去することができることを示すUDMからの明示的な信号を待機してもよい。

【0062】

U S I MがR A N D及びA U T Nを受信しなかった場合、或いは正しいA U T Nを受信しなかった場合、U S I Mは、新しい鍵材料が不正である可能性がある結論づけることができる。このように、U S I Mは、UEが古い正しい鍵材料に基づいて再びアクセスできることを確実にするために、古い鍵材料をより高い優先度で保持する。アクセスが取得されると、UDMは、古い鍵材料が使用されていることを監視し、UEと共にリカバリ手順を開始できる。

【0063】

加えて、シーケンス番号、AMFビット、及びMAC (A U T N = S Q N * A K | | A M F | | M A C) を含むA U T Nが、新しい鍵で暗号化されたS U C I、又は新しいR o u t i n g I Dを持つS U C Iが正しく受信されたことを信号で伝えるため、UDMにより使用され得る。UDMは、サブスクリプションが2つのUDM間で移動された場合、AMFビットを設定するか、又はS Q Nを0に設定することによって、これを行うことができる。これは、U S I Mにとって、新しいアタッチクリティカルパラメータが正しいことの確認となる。そのため、U S I Mはメッセージを削除できる。

【0064】

(第3実施形態)

図10は、本開示の第3実施形態に従って、ホームネットワーク公開鍵などのアタッチ関連パラメータが更新された後に、これらのパラメータの正当性を確認するための方法を示す。図10は、一例としてホームネットワーク公開鍵を使用するが、方法は、R o u t i n g I D、保護スキーム等の更新後に等しく適用することができる。以下の説明において、ホームネットワーク公開鍵は、それらパラメータの一例としてのみ理解される。他のパラメータとの違いが発生した場合、本文に示されている。

【0065】

図10の方法は、重要なアタッチ関連パラメータが過去に更新されたと仮定している。UDMは、U S I M内の特定のパラメータ(パラメータ1)が正しいか否かを確認したい。そのために、UDMは、ステップ1において、チェックするパラメータを含む「チェックアタッチパラメータ」メッセージをAMFに送信する。チェックアタッチパラメータのメッセージは、図17に従ってオプションで保護される。ステップ2において、AMFは、チェックアタッチパラメータメッセージを、例えばN A S D Lトランスポートを使用

してMEに転送する。MEは、ステップ3において、チェックアタッチパラメータメッセージをUSIMに転送する。USIMは、受信すると、ステップ4において応答を計算し、ステップ5においてMEに応答を返す。MEは、ステップ6において応答をAMFに転送する。AMFは、ステップ7においてUDMに応答を返し、UDMは検証を行うことができる。

【0066】

USIMの応答は、複数の方法で計算できる。1. USIMがSUCIを計算するMEの一部である場合、応答は要求されたパラメータの暗号化された表現にすることができる。その後、HN公開鍵を使用して暗号化を行うことができる。UDMは、SIDFに送信して値を復号化することにより値を検証し、プレーンテキスト値を比較する。2. 応答は、パラメータ自体にすることもできる。この場合、MEは、HN公開鍵でパラメータを暗号化し、ステップ6でパラメータの暗号化表現を含めることができる。UDMによる検証方法は同じである。3. UDMからのチェックパラメータメッセージは、認証ベクトルのRAND及びAUTNを含むことができる。USIMは、RESを計算し、AUTNを検証し、全てが正しければ、RESとパラメータとの間、又はAK (Anonymity key) と要求されたパラメータとの間にXOR演算を適用することにより、パラメータの暗号化表現を返すことができる。UDM側では、同じXORが実行され、比較のためにプレーンテキストパラメータが再度取得される。

【0067】

上記は、USIMが、図9に示されるように、異なる優先度を有するアタッチクリティカルパラメータの複数のセットを記憶するように構成される場合に特に有用である。そのような場合、UDMは、最初にパラメータを検証することができ、正しい場合、USIMに、以下に説明するように、新しいアタッチクリティカルパラメータが最初のパラメータになるように、パラメータの優先度を変更するように指示することができる。

【0068】

図11は、アタッチクリティカルパラメータの優先度を変更するための手順を示す。ステップ1において、UDMは、変更する優先度を含む「アタッチパラメータの優先度変更」メッセージをAMFに送信する。例えば、アタッチパラメータの優先度変更メッセージは、優先度を変更するキーIDの優先度付きリストを含んでもよく、或いは、USIMにおいて最も高い優先度を取得するキーIDを含んでもよい。ステップ2において、AMFは、例えばNAS-DLトランスポートを使用して、アタッチパラメータの優先度変更メッセージをMEに転送する。MEは、ステップ3において、アタッチパラメータの優先度変更メッセージをUSIMに転送する。USIMは受信すると、ステップ4において優先度を再編成する。USIMは、ステップ5においてMEに確認を返す。MEは、ステップ6において確認をAMFに転送する。AMFは、ステップ7においてUDMに確認を返す。

【0069】

図12に優先度変更後のUSIMのテーブルを示す。ステップ3及びステップ4のメッセージの効果は、次のように説明できる。ここで、UE (MEとUSIMを組み合わせたもの) は、図11のステップ2に従って、優先度変更メッセージを受信する。MEは、優先度変更メッセージを、図12のテーブルに従ってキーを再編成するUSIMに転送する。前述したように、この再編成は永久的なものであっても一時的なものであってもよい。一時的な場合には、図12のテーブルは、USIMが鍵マテリアルの次の要求時にMEに提示するであろうテーブルを表す。永久的な場合には、図12のテーブルは、MEの内部ストレージを表す。

【0070】

優先度ベースのアプローチの利点は、UDMが最初にパラメータの正確性を検証し、次いで、計算のためにMEに提示される順序、又は計算のためにUSIMによって使用される順序を効果的に変更できることである。最初に検証することで、フォールバックが必要になる可能性は大幅に低くなる。

【0071】

(他の実施形態)

本開示におけるユーザ機器（「UE」、「移動局」、「モバイルデバイス」、又は「ワイヤレスデバイス」）は、無線インタフェースを介してネットワークに接続されたエンティティである。

【0072】

なお、本開示におけるUEは、専用の通信装置に限定されるものではなく、後述するように、本開示で説明するUEとしての通信機能を有する任意の装置に適用することができる。

【0073】

「ユーザ機器」又は「UE」（この用語は3GPPで使用されている）、「移動局」、「モバイルデバイス」、及び「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を意図しており、端末、携帯電話、スマートフォン、タブレット、携帯IoTデバイス、IoTデバイス、及び機械などのスタンドアロンの移動局を含む。

【0074】

用語「UE」及び「ワイヤレスデバイス」は、長期間静止したままである装置も含むことが理解される。

【0075】

UEは、例えば、生産又は製造用の機器のアイテム、及び／又はエネルギー関連機械のアイテムであり得る（例えば、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、及び／又は関連機器、重電機器、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、油圧機器、空気圧機器、金属加工機械、マニピュレータ、ロボットやその応用システム、ツール、金型、ロール、搬送装置、昇降装置、運搬設備、繊維機械、ミシン、印刷及び／又は関連機械、紙加工機械、化学機械、鉱山機械及び／又は建設機械、及び／又は関連設備、農林水産用機械器具、安全及び／又は環境保全設備、トラクタ、精密軸受、チェーン、歯車、動力伝達装置、潤滑装置、バルブ、配管継手、及び／又は、上記の装置又は機械などの何れかのためのアプリケーションシステムなどの設備又は機械）。

【0076】

UEは、例えば、搬送機器（例えば、車両、自動車、オートバイ、自転車、列車、バス、カート、人力車、船やその他の船舶、航空機、ロケット、衛星、ドローン、バルーンなどの運輸機器）のアイテムであってもよい。

【0077】

UEは、例えば、情報通信機器（例えば、電子計算機及び関連機器、通信及び関連機器、電子部品などの情報通信機器）のアイテムであってもよい。

【0078】

UEは、例えば、冷凍機、冷凍機応用製品、取引及び／又はサービス産業機器のアイテム、自動販売機、自動サービス機械、事務用機械や機器、消費者電子機器や家電製品（例えば、オーディオ機器、ビデオ機器、スピーカー、ラジオ、テレビ、電子レンジ、炊飯器、コーヒーメーカー、食器洗い機、洗濯機、乾燥機、電子扇風機又は関連する器具、掃除機などの電子製品）であってもよい。

【0079】

UEは、例えば、電気アプリケーションシステム又は機器（例えば、X線システム、粒子加速器、ラジオアイソトープ装置、音響装置、電磁応用装置、電力応用機器などの電気アプリケーションシステム又は機器）であってもよい。

【0080】

UEは、例えば、電子ランプ、照明器具、測定器具、分析器、テスト、又は測量又はセンシング器具（例えば、煙警報器、人間の警報センサ、モーションセンサー、無線タグなどの測量又はセンシング機器）、時計又は置き時計、実験器具、光学装置、医療機器及び／又はシステム、武器、刃物のアイテム、ハンドツールなどであり得る。

【0081】

10

20

30

40

50

UEは、例えば、無線を備えた携帯情報端末又は関連機器（他の電子機器（例えばパソコン、電気測定機）に取り付けたり、挿入したりするように設計されたワイヤレスカードやモジュールなど）であってもよい。

【0082】

UEは、様々な有線及び／又は無線通信技術を使用して、IoT（internet of things）に関して以下に記載されるアプリケーション、サービス、及び解決策を提供する装置又はシステムの一部であり得る。

【0083】

IoTデバイス（又はthings）は、これらの装置が互いに、及び他の通信装置とデータを収集及び交換することを可能にする、適切な電子機器、ソフトウェア、センサ、ネットワーク接続などを備えることができる。IoTデバイスは、内部メモリに記憶されたソフトウェア命令に従う自動化された機器を含むことができる。IoTデバイスは、人間の監視や対話を必要とせずに動作することができる。IoTデバイスはまた、長期間にわたって静止及び／又は非アクティブのままであり得る。IoTデバイスは、（一般的に）固定装置の一部として実装されてもよい。IoTデバイスはまた、非固定装置（例えば車両）に組み込まれてもよく、又は監視／追跡される動物若しくは人に取り付けられてもよい。

【0084】

IoT技術は、通信デバイスが人間の入力によって制御されているか、又はメモリに記憶されたソフトウェア命令によって制御されているかどうかにかかわらず、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上に実装することができることが理解される。

【0085】

IoTデバイスは、MTC（Machine-Type Communication）デバイス、M2M（Machine-to-Machine）通信デバイス、或いはNB-IoT UE（Narrow Band-IoT UE）と呼ばれることもあることが理解される。UEは、1つ又は複数のIoT又はMTCアプリケーションをサポートすることができ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が下記表（供給源：3GPP TS 22.368 V13.1.0、附則B、その内容は参照によりここに組み込まれる）にリストされる。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している。

10

20

30

40

50

【表 1】

Table 1: Some examples of machine-type communication applications.

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

10

20

30

40

【 0 0 8 6 】

アプリケーション、サービス、及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 (Personal Handy-phone System) / デジタルコードレス通信システム、POS (Point of sale) システム、広告呼出システム、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、課金サービス、無線オンデマンドサービス、ロー

50

ミングサービス、活動監視サービス、電気通信キャリア／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）サービスなどであり得る。

【0087】

また、上述したUEカテゴリは、本開示に記載された技術的思想及び例示的实施形態の適用例に過ぎない。いうまでもなく、これらの技術思想及び実施形態は、上記UEに限定されるものではなく、種々の変形が可能である。

【0088】

ユーザ機器（UE）

図13は、本開示の実施形態に係るUEの主要な構成要素を示すブロック図である。図示のように、UE10は、一つ以上のアンテナ11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送受信回路12を含む。図13に必ずしも示されているわけではないが、UEは、当然ながら、通常のモバイルデバイスの通常の機能の全て（ユーザインタフェース13など）を有し、これは、必要に応じて、任意のハードウェア、ソフトウェア、及びファームウェアの任意の組み合わせによって提供され得る。ソフトウェアは、メモリ15にあらかじめインストールされてもよく、及び／又は、例えば、電気通信ネットワークを介して、又は取り外し可能なデータ記憶装置（RMD：removable data storage device）からダウンロードされてもよい。

【0089】

コントローラ14は、メモリ15に記憶されたソフトウェアに従って、UE10の動作を制御する。例えば、コントローラ14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16、及び少なくともトランシーバ制御モジュール18を有する通信制御モジュール17を含む。通信制御モジュール18（そのトランシーバ制御サブモジュールを使用する）は、UE10と、基地局／（R）ANノード、MME、AMF（及び他のコアネットワークノード）などの他のノードとの間のシグナリング及びアップリンク／ダウンリンクのデータパケットの処理を担当（生成／送信／受信）する。そのようなシグナリングは、例えば、接続の確立及び維持に関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）、周期的な位置更新に関連するメッセージ（例えば、トラッキングエリアの更新、ページングエリアの更新、ロケーションエリアの更新）などのNASメッセージなどが含まれる。

【0090】

（R）ANノード

図14aは、本開示の実施の形態に係る例示的な（R）ANノード、例えば基地局（LTEでは「eNB」、5Gでは「gNB」）の主要な構成要素を示すブロック図である。図示のように、（R）ANノード30は、1以上のアンテナ31を介して、接続されたUEとの間で信号を送受信し、他のネットワークノードとの間で、ネットワークインタフェース33を介して信号を（直接的又は間接的に）送受信するように動作可能な送受信回路32を含む。コントローラ34は、メモリ35に記憶されたソフトウェアに従って、ANノード30の動作を制御する。例えば、コントローラ34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35にあらかじめインストールされてもよく、及び／又は、例えば、電気通信ネットワークを介して、又は取り外し可能なデータ記憶装置（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36、及び少なくともトランシーバ制御モジュール38を有する通信制御モジュール37を含む。

【0091】

通信制御モジュール37（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30と他のノード、例えばUE、MME、AMFとの間のシグナリング（例えば直接的又は間接的に）の処理を担当（生成／送信／受信）する。シグナリングは、例えば、無線接続及びロケーション手順（特定のUEに対して）に関連する適切にフォーマ

10

20

30

40

50

ットされたシグナリングメッセージを含むことができ、特に、接続の確立及び保守（例えば R R C 接続の確立及び他の R R C メッセージ）、定期的なロケーション更新（例えば、トラッキングエリアの更新、ページングエリアの更新、ロケーションエリアの更新）、S 1 A P メッセージ、及び N G A P メッセージ（すなわち N 2 基準点によるメッセージ）など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を含むことができる。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（マスタ情報やシステム情報など）も含み得る。

【0092】

コントローラ 34 は、また、実行時に U E 移動度推定及び／又は移動軌跡推定などの関連タスクを担当するように（ソフトウェア又はハードウェアによって）構成される。

【0093】

コアネットワークノード

図 15 a は、本開示の実施形態に係る例示的なコアネットワークノード、例えば、A M F、S E A F、A U S F、K S、U D M、又は他の任意のコアネットワークノードの主要構成要素を示す。A M F は、S E A F の代替となり得る。A U S F は、U D M の代替となり得る。コアネットワークノード 50 は、5 G C に含まれる。図に示すように、コアネットワークノード 50 は、ネットワークインタフェース 52 を介して他のノード（U E を含む）と信号を送受信するように動作可能な送受信回路 51 を含む。コントローラ 53 は、メモリ 54 に記憶されたソフトウェアに従ってコアネットワークノード 50 の動作を制御する。例えば、コントローラ 53 は、C P U（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 54 にあらかじめインストールされてもよく、及び／又は、例えば、電気通信ネットワークを介して、又は取り外し可能なデータ記憶装置（R M D）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 55、及び少なくともトランシーバ制御モジュール 57 を有する通信制御モジュール 56 を含む。

【0094】

通信制御モジュール 56（そのトランシーバ制御サブモジュールを使用）は、コアネットワークノード 50 と U E、基地局／（R）A N ノードなどの他のノード（例えば「g N B」又は「e N B」）との間のシグナリングの処理を担当（生成／送信／受信）する（直接的又は間接的に）。そのようなシグナリングは、例えば、本明細書に記載する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、U E との間で N A S メッセージを伝達するための N G A P メッセージ（すなわち N 2 基準点によるメッセージ）などが含まれる。

【0095】

開示された例の前述の説明は、当業者が本開示を作成又は使用することを可能にするために提供される。これらの実施例に対する種々の修正は、当業者には容易に明らかであり、本明細書に定義される一般原理は、本開示の精神又は範囲から逸脱することなく、他の実施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及び新規の特徴と一致する最も広い範囲を与えるものである。

【0096】

例えば、上記の実施形態の全部又はいくつかは、以下の付記のようにも記載され得るが、以下には限られない。

【0097】

〔付記 1〕

1 つ以上の命令を格納するメモリと、

前記 1 つ以上の命令を実行することで、

ネットワーク通信に対応する更新情報を外部装置から受信し、

前記更新情報に基づいて S U C I（Subscription Concealed Identifier）を取得し、

前記 S U C I を前記外部装置に送信する

ように構成されるプロセッサとを備える装置。

【0098】

[付記2]

前記プロセッサは、S U P I (Subscription Permanent Identifier) を前記更新情報に基づいて暗号化することにより前記S U C Iを取得するように更に構成される付記1に記載の装置。

【0099】

[付記3]

前記プロセッサは、S U P I (Subscription Permanent Identifier) と前記更新情報とを連結することによって前記S U C Iを取得するように更に構成される付記1に記載の装置。

10

【0100】

[付記4]

前記プロセッサは、前記S U C Iに対応する前記S U P Iと、前記更新情報に対応付けて格納される他のS U P Iとの一致に基づく確認メッセージを前記外部装置から受信するように更に構成される付記2又は3に記載の装置。

【0101】

[付記5]

前記更新情報は、ホームネットワーク公開鍵、ルーティングID、ホームネットワーク公開鍵識別子と、及び前記装置における保護スキームの少なくとも1つを含む付記1から4の何れか1項に記載の装置。

20

【0102】

[付記6]

1つ以上の命令を格納するメモリと、
前記1つ以上の命令を実行することで、
ネットワーク通信に対応する更新情報を外部装置に送信し、
前記更新情報に基づいて取得されるS U C I (Subscription Concealed Identifier) を前記外部装置から受信し、
前記受信したS U C Iに基づいてS U P I (Subscription Permanent Identifier) を取得し、

30

前記S U P Iが前記更新情報に対応しているかを検証するように構成されるプロセッサとを備える装置。

【0103】

[付記7]

前記S U P Iは、前記S U C Iに対してS I D F (Subscription Identifier De-concealing function) を実行することによって取得される付記6に記載の装置。

【0104】

[付記8]

前記プロセッサは、前記S I D Fから取得された前記S U P Iと、前記更新情報に関連付けて記憶された別のS U P Iと比較することによって、前記S U P Iを検証するように更に構成される付記7に記載の装置。

40

【0105】

[付記9]

前記プロセッサは、前記S I D Fから取得されたS U P Iと、前記更新情報に対応付けて記憶されている他のS U P Iとの一致に基づいて、前記外部装置に確認を送信するように更に構成される付記8に記載の装置。

【0106】

[付記10]

前記更新情報は、ホームネットワーク公開鍵、ルーティングID、ホームネットワーク公開鍵識別子、及び前記装置内の保護スキームの少なくとも1つを含む付記6から9の何

50

れか 1 項に記載の装置。

【0107】

〔付記 11〕

外部装置から、ネットワーク通信に対応する更新情報を受信し、
前記更新情報に基づいて S U C I (Subscription Concealed Identifier) を取得し、
前記 S U C I を前記外部装置に送信する方法。

【0108】

〔付記 12〕

前記 S U C I は、前記更新情報に基づいて S U P I (Subscription Permanent Identifier) を暗号化することによって取得される付記 11 に記載の方法。

10

【0109】

〔付記 13〕

前記 S U C I は、S U P I (Subscription Permanent Identifier) サブスクリプションと前記更新情報とを連結することによって取得される付記 11 に記載の方法。

【0110】

〔付記 14〕

更に、前記 S U C I に対応する前記 S U P I と、前記更新情報に関連付けて記憶される他の S U P I との一致に基づく確認メッセージを前記外部装置から受信する付記 12 又は 13 に記載の方法。

【0111】

20

〔付記 15〕

前記更新情報は、ホームネットワーク公開鍵、ルーティング ID、ホームネットワーク公開鍵識別子、及び装置における保護スキームのうちの少なくとも一つを含む付記 11 から 14 の何れか 1 項に記載の方法。

【0112】

〔付記 16〕

ネットワーク通信に対応する更新情報を外部装置に送信し、
前記更新情報に基づいて取得される S U C I (Subscription Concealed Identifier) を前記外部装置から受信し、

前記受信した S U C I に基づいて S U P I (Subscription Permanent Identifier) を取得し、

30

前記 S U P I が前記更新情報に対応しているかを検証する方法。

【0113】

〔付記 17〕

前記 S U P I は、前記 S U C I に対して S I D F (Subscription Identifier De-concealing function) を実行することによって取得される付記 16 に記載の方法。

【0114】

〔付記 18〕

前記 S I D F から取得された前記 S U P I と、前記更新情報に関連付けて記憶される他の S U P I とを比較することにより、前記 S U P I を検証する付記 17 に記載の方法。

40

【0115】

〔付記 19〕

更に、前記 S I D F から取得された前記 S U P I と、前記更新情報に関連付けて記憶される S U P I との一致に基づいて、前記外部装置に確認を送信する付記 18 に記載の方法。

【0116】

〔付記 20〕

前記更新情報は、ホームネットワーク公開鍵、ルーティング ID、ホームネットワーク公開鍵識別子、及び装置における保護スキームの少なくとも一つを含む付記 16 から 19 の何れか 1 項に記載の方法。

【0117】

50

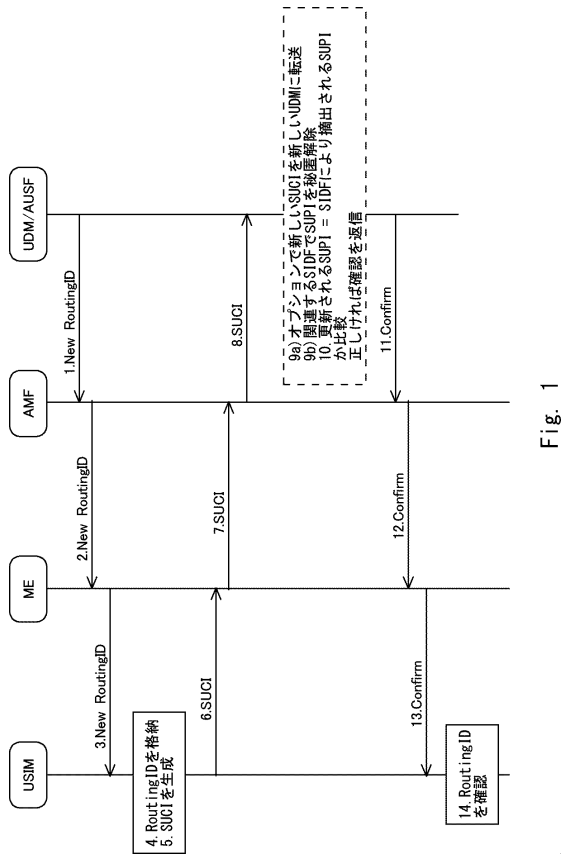
本出願は、2018年11月6日に出願されたインド特許出願第201811041964号に基づく優先権の利益を主張するものであり、その開示は、その全体が参照により本明細書に組み込まれる。

【符号の説明】

【0118】

10	UE	
11	アンテナ	
12	送受信回路	
13	ユーザインタフェース	
14	コントローラ	10
15	メモリ	
16	オペレーティングシステム	
17	通信制御モジュール	
18	トランシーバ制御モジュール	
30	(R)ANノード	
31	アンテナ	
32	送受信回路	
33	ネットワークインタフェース	
34	コントローラ	
35	メモリ	20
36	オペレーティングシステム	
37	通信制御モジュール	
38	トランシーバ制御モジュール	
50	コアネットワークノード	
51	送受信回路	
52	ネットワークインタフェース	
53	コントローラ	
54	メモリ	
55	オペレーティングシステム	
56	通信制御モジュール	30
57	トランシーバ制御モジュール	

【図面】
【図 1】



【図 2 A】

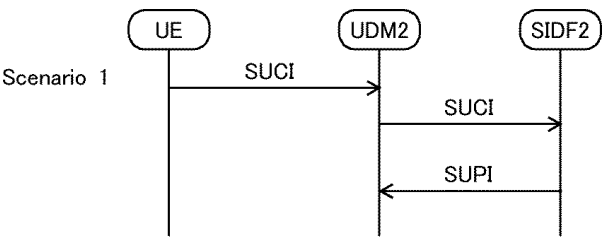


Fig. 2A

10

20

【図 2 B】

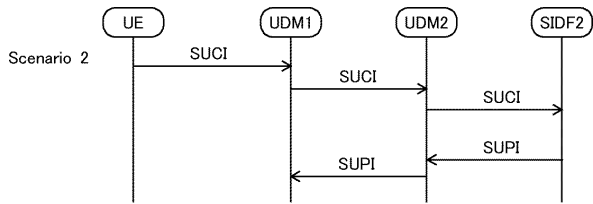


Fig. 2B

【図 2 C】

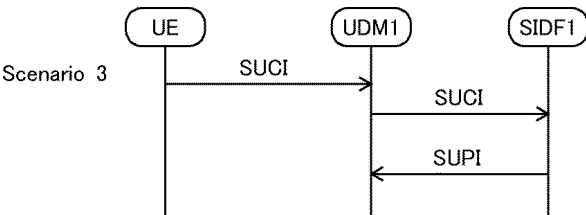


Fig. 2C

30

40

50

【図 3】

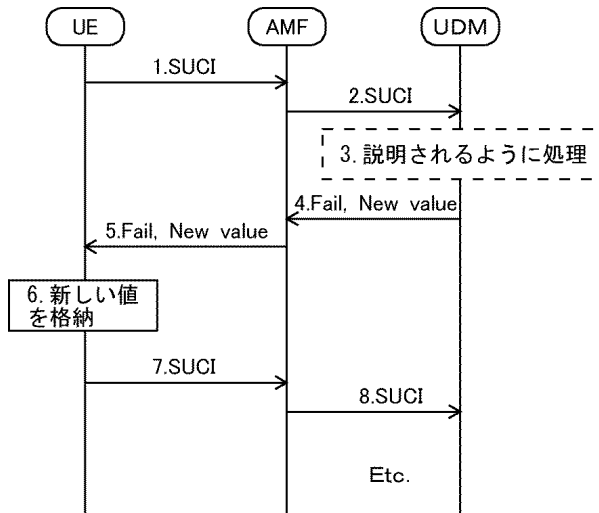


Fig. 3

【図 4】

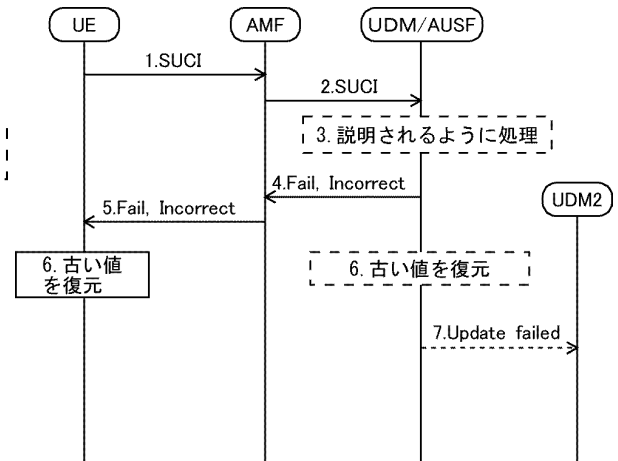


Fig. 4

【図 5】

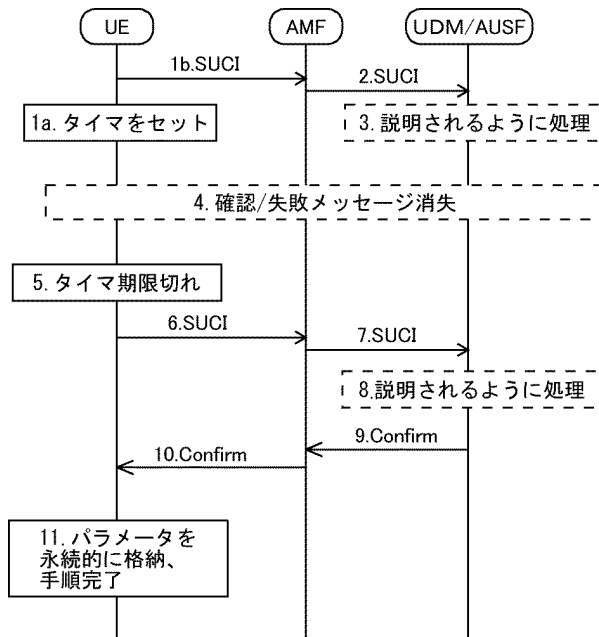


Fig. 5

【図 6】

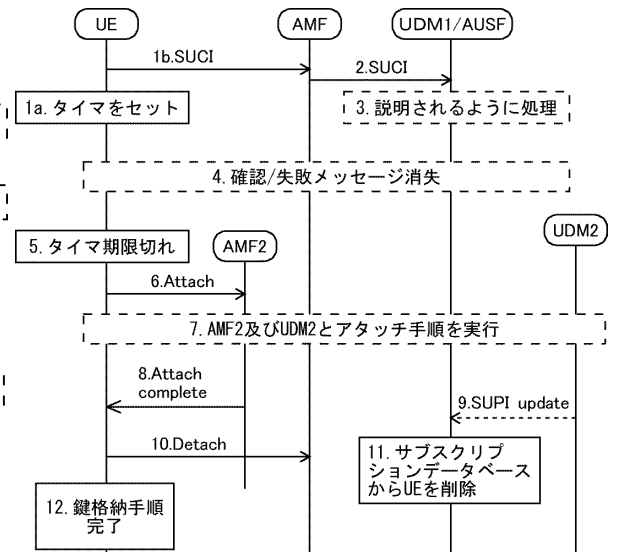


Fig. 6

10

20

30

40

50

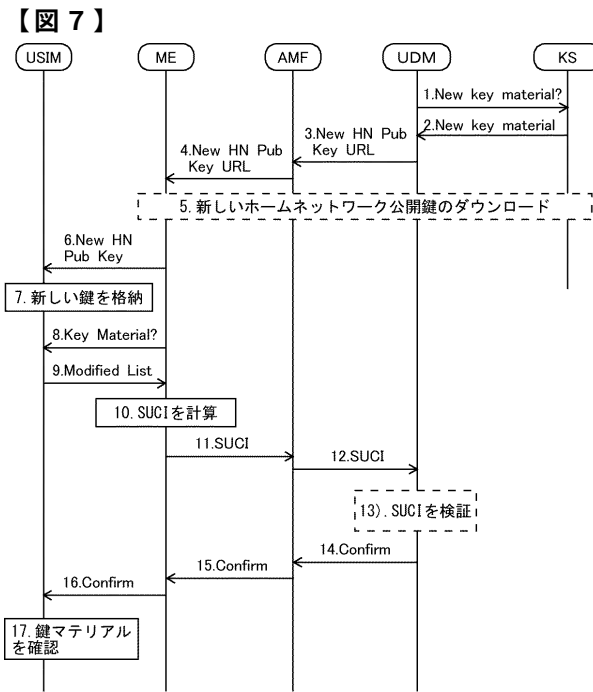


Fig. 7

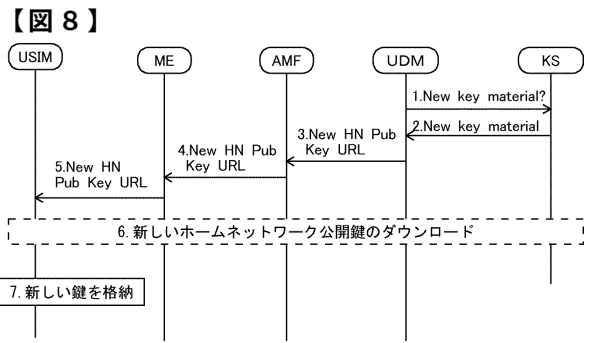


Fig. 8

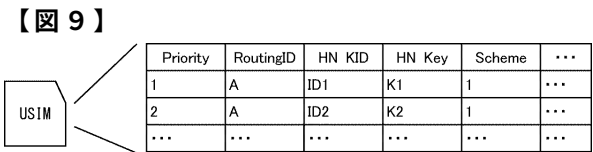


Fig. 9

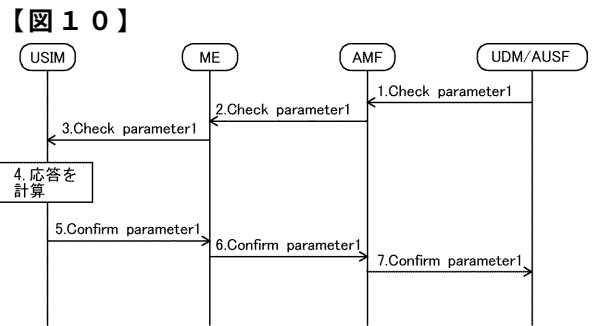


Fig. 10

【図 1 1】

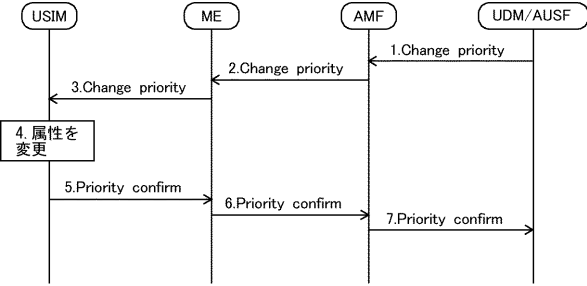


Fig. 11

【図 1 2】

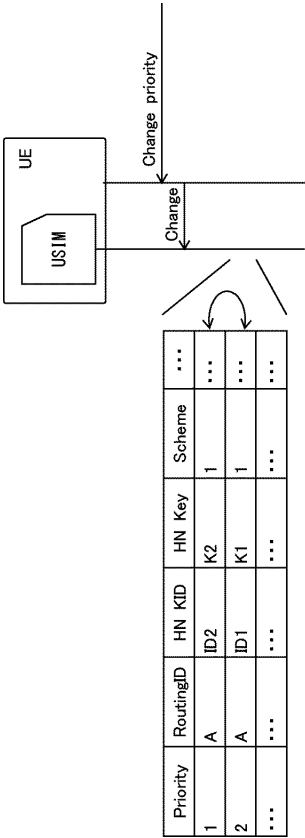


Fig. 12

【図 1 3】

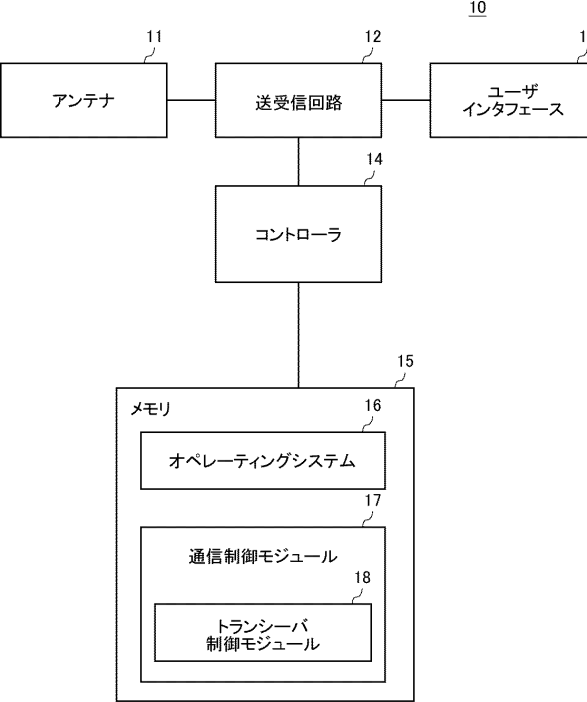


Fig. 13

【図 1 4】

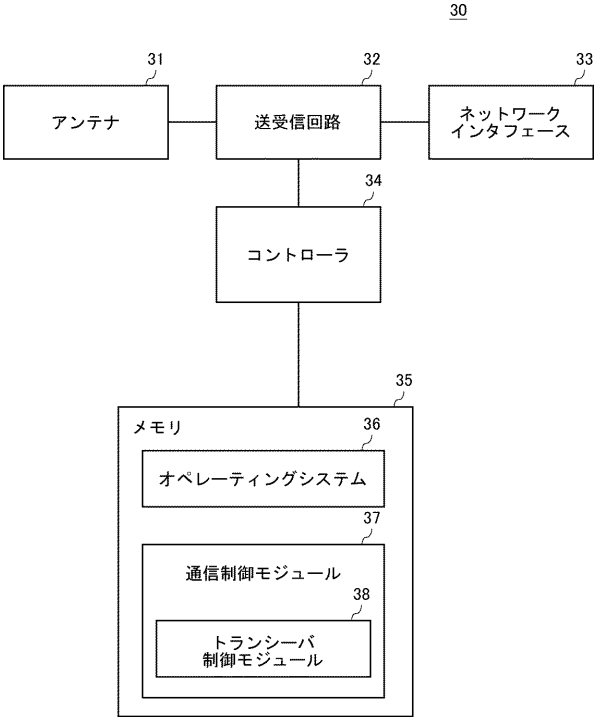


Fig. 14

【図 1 5】

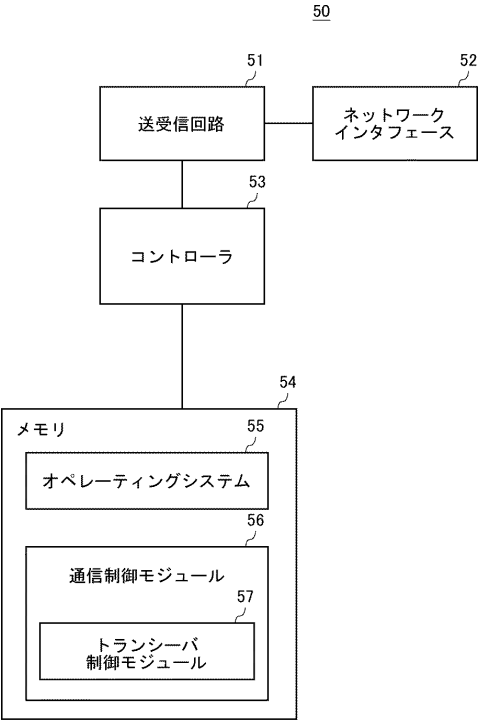


Fig. 15

【図 1 6 A】

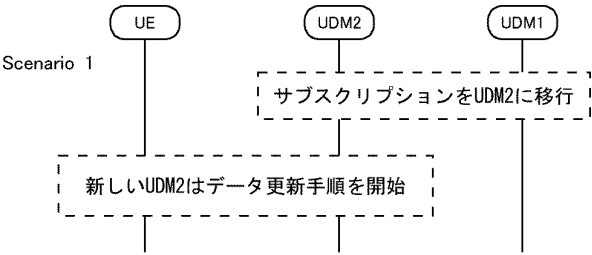


Fig. 16A

10

20

【図 1 6 B】

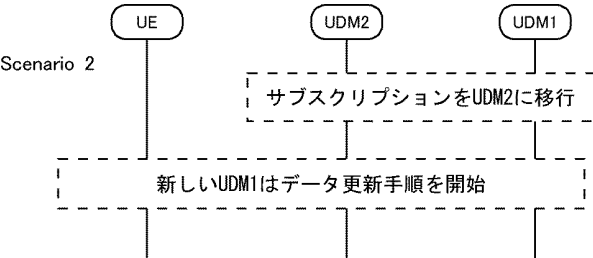


Fig. 16B

【図 1 6 C】

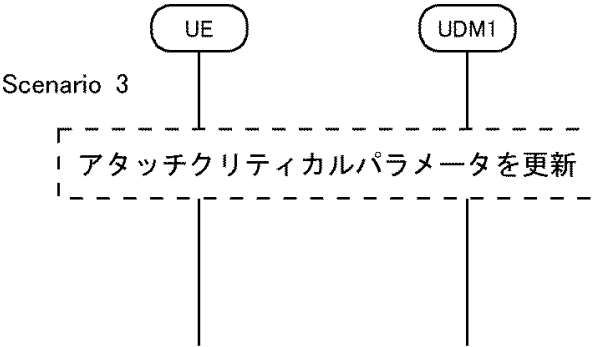


Fig. 16C

30

40

50

【図 17】

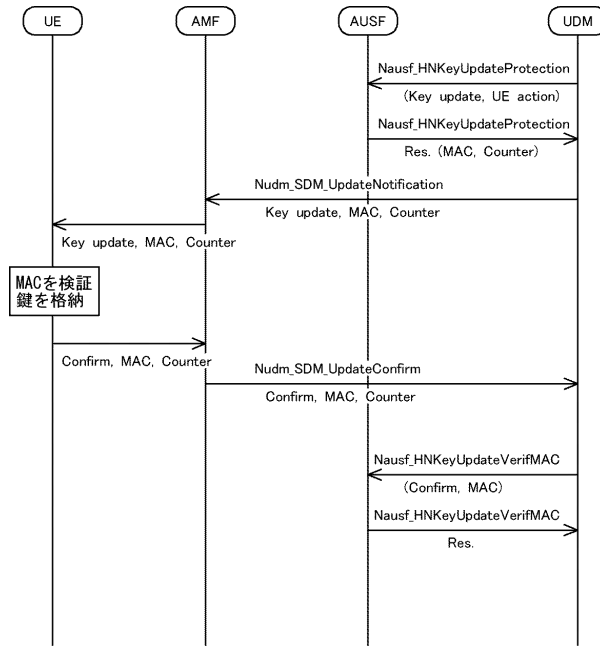


Fig. 17

【図 18】

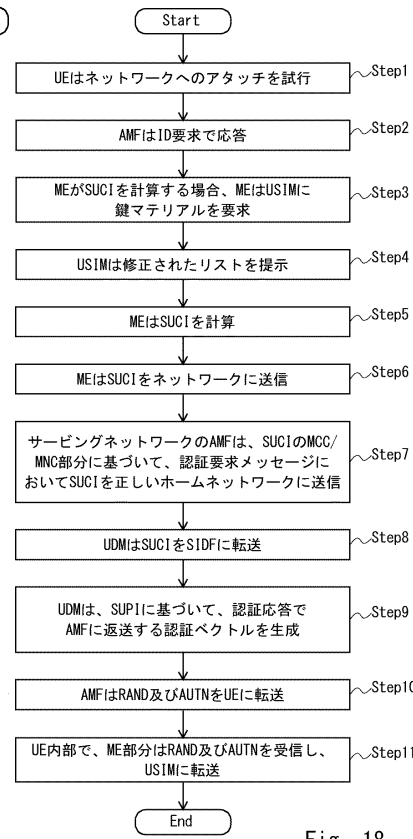


Fig. 18

10

20

30

40

50

フロントページの続き

- (56)参考文献 Nokia, Orange, T-Mobile USA, LI compliance when applying subscriber identifier privacy, 3GPP TSG SA WG3 #90 S3-180083, フランス, 3GPP, 2018年01月15日
Nokia, Nokia Shanghai Bell, Comments to LS on Routing ID CP-182238, 3GPP TSG SA WG3 #92Bis S3-183050, フランス, 3GPP, 2018年09月19日
Nokia, SIDF purpose in initiation of authentication, 3GPP TSG SA WG3 #88Bis S3-172355, フランス, 3GPP, 2017年10月02日
Nokia, Discussion on LI conformity by verification hash method, 3GPP TSG SA WG3 #90 Bis S3-180768, フランス, 3GPP, 2018年02月19日
- (58)調査した分野 (Int.Cl., DB名)
H 0 4 B 7 / 2 4 - 7 / 2 6
H 0 4 W 4 / 0 0 - 9 9 / 0 0
3 G P P T S G R A N W G 1 - 4
S A W G 1 - 4
C T W G 1、4