

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2025-519829
(P2025-519829A)

(43)公表日 令和7年6月26日(2025.6.26)

(51)国際特許分類	F I	テーマコード (参考)
H 0 4 W 12/069 (2021.01)	H 0 4 W 12/069	5 K 0 6 7
H 0 4 W 8/08 (2009.01)	H 0 4 W 8/08	
H 0 4 W 12/04 (2021.01)	H 0 4 W 12/04	

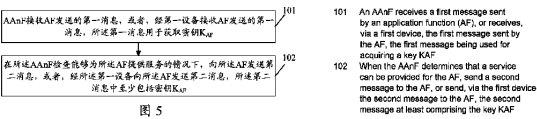
審査請求 有 予備審査請求 未請求 (全51頁)

(21)出願番号	特願2024-574772(P2024-574772)	(71)出願人	518389015
(86)(22)出願日	令和5年6月15日(2023.6.15)		中国移动通信有限公司研究院
(85)翻訳文提出日	令和7年1月22日(2025.1.22)		China Mobile Commu
(86)国際出願番号	PCT/CN2023/100416		ication Co., Ltd Re
(87)国際公開番号	WO2023/246614		search Institute
(87)国際公開日	令和5年12月28日(2023.12.28)		中華人民共和國100053北京市西城
(31)優先権主張番号	202210701088.4		区宣武門西大街32号
(32)優先日	令和4年6月20日(2022.6.20)		32 Xuanwumen West S
(33)優先権主張国・地域又は機関	中国(CN)		treet, Xicheng Dist
			riect, Beijing 10005
(81)指定国・地域	AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ	(71)出願人	507142144
	,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),		中国移动通信集团有限公司
	EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(		CHINA MOBILE COMMUN
	AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,		ICATIONS GROUP CO.,
	FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV		
	最終頁に続く		最終頁に続く

(54)【発明の名称】 通信方法、通信装置、通信機器及びコンピュータ記憶媒体

(57)【要約】

本願の実施例は、通信方法、通信装置、通信機器及びコンピュータ記憶媒体を提供する。前記方法は、アプリケーションの認証と鍵管理 (A K M A) アンカー機能 (A A n F) が、アプリケーション機能 (A F) から送信された第 1 メッセージを受信し、又は、第 1 機器を介して A F から送信された第 1 メッセージを受信するステップであって、前記第 1 メッセージは、鍵を取得するためのものである、ステップと、前記 A A n F が前記 A F にサービスを提供できることをチェックした場合、前記 A F に第 2 メッセージを送信し、又は、前記第 1 機器を介して前記 A F に第 2 メッセージを送信するステップであって、前記第 2 メッセージは、少なくとも鍵を含む、ステップと、を含む。



【特許請求の範囲】**【請求項 1】**

通信方法であって、

アプリケーションの認証と鍵管理 (AKMA) アンカー機能 (AAnF) が、アプリケーション機能 (AF) から送信された第 1 メッセージを受信し、又は、第 1 機器を介して AF から送信された第 1 メッセージを受信するステップであって、前記第 1 メッセージは鍵 K_{AF} を取得するためのものである、ステップと、

前記 AAnF が前記 AF にサービスを提供できることをチェックした場合、前記 AF に第 2 メッセージを送信し、又は、前記第 1 機器を介して前記 AF に第 2 メッセージを送信するステップであって、前記第 2 メッセージは少なくとも鍵 K_{AF} を含む、ステップと、
を含む、通信方法。

10

【請求項 2】

前記 AAnF はホームネットワーク (HPLMN) に位置し、及び / 又は、前記第 1 機器は訪問ネットワーク (VPLMN) に位置し、及び / 又は、前記 AF は訪問ネットワーク (VPLMN) に位置する、

請求項 1 に記載の通信方法。

【請求項 3】

前記第 1 メッセージは AKMA 鍵識別子 (A-KID) 及び / 又は前記 AF の識別子を含む、

請求項 1 に記載の通信方法。

20

【請求項 4】

前記通信方法は、

前記 AAnF が AKMA アンカー鍵 K_{AKMA} に基づいて前記鍵 K_{AF} を導出するステップをさらに含む、

請求項 1 に記載の通信方法。

【請求項 5】

前記第 2 メッセージは、

前記鍵 K_{AF} の有効時間情報、

購読永久識別子 (SUPI)、

一般公衆購読識別子 (GPSI) のうちの少なくとも 1 つをさらに含む、

請求項 1 に記載の通信方法。

30

【請求項 6】

前記通信方法は、

前記 AAnF が認証サーバ機能 (AUSF) から送信された第 3 メッセージを受信するステップをさらに含み、前記第 3 メッセージは鍵を登録するためのものであり、前記第 3 メッセージは、

A-KID、AKMA アンカー鍵 K_{AKMA} 、SUPI、端末のローミング情報のうちの少なくとも 1 つを含む、

請求項 1 ~ 5 のいずれか一項に記載の通信方法。

40

【請求項 7】

前記端末のローミング情報は、

端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む、

請求項 6 に記載の通信方法。

【請求項 8】

前記端末のローミング情報は前記 AUSF が統合データ管理 (UDM) から取得したものである、

請求項 6 に記載の通信方法。

【請求項 9】

50

前記 A U S F が U D M から取得した前記端末のローミング情報は、前記端末 S U P I に関連付けられた前記端末のローミング情報である、

請求項 8 に記載の通信方法。

【請求項 10】

前記第 1 メッセージを受信した後、前記通信方法は、

前記 A A n F が U D M から端末のローミング情報を取得するステップをさらに含み、前記端末のローミング情報は前記第 1 メッセージ内の A - K I D に対応する端末に関連する、

請求項 3 に記載の通信方法。

【請求項 11】

10

前記 A A n F が、前記 A F にサービスを提供できるか否かをチェックするステップは、前記 A A n F が前記端末のローミング情報に基づいて前記 A F にサービスを提供できるか否かをチェックするステップを含む、

請求項 6 ~ 10 のいずれか一項に記載の通信方法。

【請求項 12】

通信方法であって、

第 1 機器が、A F から送信された第 1 メッセージを受信し、前記第 1 メッセージを A A n F に送信するステップであって、前記第 1 メッセージは鍵 K A F を取得するためのものである、ステップと、

前記 A A n F が前記 A F にサービスを提供できる場合、前記第 1 機器が、前記 A A n F から送信された第 2 メッセージを受信し、前記第 2 メッセージを前記 A F に送信するステップであって、前記第 2 メッセージは少なくとも前記鍵 K A F を含む、ステップと、を含む、通信方法。

20

【請求項 13】

前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置し、及び / 又は、前記 A F は V P L M N に位置する、

請求項 12 に記載の通信方法。

【請求項 14】

前記第 1 メッセージは A K M A 鍵識別子 (A - K I D) 及び / 又は前記 A F の識別子を含む、

30

請求項 12 に記載の通信方法。

【請求項 15】

前記第 2 メッセージは、

前記鍵 K A F の有効時間情報、

購読永久識別子 (S U P I) 、

一般公衆購読識別子 (G P S I) のうちの少なくとも 1 つをさらに含む、

請求項 12 に記載の通信方法。

【請求項 16】

通信方法であって、

第 1 機器が A F から送信された第 1 メッセージを受信するステップであって、前記第 1 メッセージは鍵 K A F を取得するためのものである、ステップと、

40

前記第 1 機器が前記 A F にサービスを提供できることをチェックした場合、前記 A F に第 2 メッセージを送信するステップであって、前記第 2 メッセージは少なくとも前記鍵 K A F を含む、ステップと、を含む、通信方法。

【請求項 17】

前記第 1 メッセージは A - K I D 及び / 又は前記 A F の識別子を含む、

請求項 16 に記載の通信方法。

【請求項 18】

前記通信方法は、

前記第 1 機器が A A n F から送信された第 1 情報を受信するステップをさらに含み、前

50

記第 1 情報は A K M A コンテキスト情報を含む、
請求項 1 6 に記載の通信方法。

【請求項 1 9】

前記第 1 情報は、A - K I D、A K M A アンカー鍵 K_{AKMA} 、S U P I のうちの少なくとも 1 つを含む、
請求項 1 8 に記載の通信方法。

【請求項 2 0】

前記通信方法は、
前記第 1 機器が A K M A アンカー鍵 K_{AKMA} に基づいて前記鍵 K_{AF} を導出するステップをさらに含む、
請求項 1 9 に記載の通信方法。

10

【請求項 2 1】

前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置し、及び / 又は、前記 A F は V P L M N に位置する、
請求項 1 8 に記載の通信方法。

【請求項 2 2】

通信方法であって、
A A n F が、第 1 機器に第 1 情報を送信するステップをさらに含み、前記第 1 情報は、A K M A コンテキスト情報を含む、通信方法。

【請求項 2 3】

20

前記第 1 情報は、A - K I D、A K M A アンカー鍵 K_{AKMA} 、S U P I のうちの少なくとも 1 つを含む、
請求項 2 2 に記載の通信方法。

【請求項 2 4】

前記通信方法は、
前記 A A n F が A U S F から送信された第 3 メッセージを受信するステップをさらに含み、前記第 3 メッセージは鍵を登録するためのものであり、前記第 3 メッセージは、
A - K I D、A K M A アンカー鍵 K_{AKMA} 、S U P I、端末のローミング情報のうちの少なくとも 1 つを含む、
請求項 2 2 に記載の通信方法。

30

【請求項 2 5】

前記端末のローミング情報は、
端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む、
請求項 2 4 に記載の通信方法。

【請求項 2 6】

前記端末のローミング情報は前記 A U S F が U D M から取得したものである、
請求項 2 5 に記載の通信方法。

【請求項 2 7】

40

前記 A U S F が U D M から取得した前記端末のローミング情報は、前記端末 S U P I に関連付けられた前記端末のローミング情報である、
請求項 2 6 に記載の通信方法。

【請求項 2 8】

前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置する、
請求項 2 2 に記載の通信方法。

【請求項 2 9】

通信方法であって、
A F が第 1 機器又は A A n F に第 1 メッセージを送信するステップであって、前記第 1

50

メッセージは鍵 K_{AF} を取得するためのものである、ステップと、

前記第 1 機器又は前記 AA_nF が前記 AF にサービスを提供できることをチェックした場合、前記 AF が前記第 1 機器又は前記 AA_nF から送信された第 2 メッセージを受信するステップであって、前記第 2 メッセージは、少なくとも鍵 K_{AF} を含む、ステップと、を含む、通信方法。

【請求項 30】

前記 AA_nF は $HPLMN$ に位置し、及び / 又は、前記第 1 機器は $VPLMN$ に位置し、及び / 又は、前記 AF は $VPLMN$ に位置する、
請求項 29 に記載の通信方法。

【請求項 31】

前記第 1 メッセージは $AKMA$ 鍵識別子 ($A-KID$) 及び / 又は前記 AF の識別子を含む、

請求項 29 に記載の通信方法。

【請求項 32】

前記第 2 メッセージは、

前記鍵 K_{AF} の有効時間情報、

購読永久識別子 ($SUPI$)、

一般公衆購読識別子 ($GPSSI$) のうちの少なくとも 1 つをさらに含む、

請求項 29 に記載の通信方法。

【請求項 33】

通信方法であって、

$AUSF$ が統合データ管理 (UDM) から認証関連情報を取得するステップを含み、前記認証関連情報は、

端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第 3 指示情報、端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末のルーティング識別子 (RID) 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む、通信方法。

【請求項 34】

前記端末のローミング情報は、

端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む、

請求項 33 に記載の通信方法。

【請求項 35】

前記通信方法は、

前記 $AUSF$ が AA_nF に第 3 メッセージを送信するステップをさらに含み、前記第 3 メッセージは鍵を登録するためのものであり、前記第 3 メッセージは、

$A-KID$ 、 $AKMA$ アンカー鍵 K_{AKMA} 、 $SUPI$ 、前記端末のローミング情報のうちの少なくとも 1 つを含む、

請求項 33 に記載の通信方法。

【請求項 36】

通信方法であって、

UDM が $AUSF$ に認証関連情報を送信するステップを含み、前記認証関連情報は、

端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第 3 指示情報、前記端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末の RID 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む、通信方法。

【請求項 37】

前記端末のローミング情報は、

端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記

10

20

30

40

50

端末のローミング先でのポリシー情報のうちの少なくとも１つを含む、
請求項３６に記載の通信方法。

【請求項３８】

前記通信方法は、

前記ＵＤＭがＡＡｎＦから送信された第４メッセージを受信するステップであって、前記第４メッセージは端末のローミング情報を要求するためのものである、ステップと、

前記ＵＤＭが前記ＡＡｎＦに第５メッセージを送信するステップであって、前記第５メッセージは前記端末のローミング情報を含む、ステップと、をさらに含む、

請求項３６又は３７に記載の通信方法。

【請求項３９】

10

ＡＡｎＦに適用される通信装置であって、第１通信ユニットと、第１処理ユニットと、を備え、

前記第１通信ユニットは、アプリケーション機能（ＡＦ）から送信された第１メッセージを受信し、又は、第１機器を介してＡＦから送信された第１メッセージを受信するように構成され、前記第１メッセージは鍵Ｋ_{ＡＦ}を取得するためのものであり、

前記第１処理ユニットは、前記ＡＦにサービスを提供できるか否かをチェックするように構成され、

前記第１通信ユニットはさらに、前記第１処理ユニットが前記ＡＦにサービスを提供できることをチェックした場合、前記ＡＦに第２メッセージを送信し、又は、前記第１機器を介して前記ＡＦに第２メッセージを送信するように構成され、前記第２メッセージは少なくとも鍵Ｋ_{ＡＦ}を含む、通信装置。

20

【請求項４０】

第１機器に適用される通信装置であって、第１受信ユニットと、第１送信ユニットと、を備え、

前記第１受信ユニットは、ＡＦから送信された第１メッセージを受信し、前記第１メッセージをＡＡｎＦに送信するように構成され、前記第１メッセージは鍵Ｋ_{ＡＦ}を取得するためのものであり、

前記第１送信ユニットは、前記ＡＡｎＦが前記ＡＦにサービスを提供できる場合、前記ＡＡｎＦから送信された第２メッセージを受信し、前記第２メッセージを前記ＡＦに送信するように構成され、前記第２メッセージは少なくとも前記鍵Ｋ_{ＡＦ}を含む、通信装置。

30

【請求項４１】

第１機器に適用される通信装置であって、第２通信ユニットと、第２処理ユニットと、を備え、

前記第２通信ユニットはＡＦから送信された第１メッセージを受信するように構成され、前記第１メッセージは鍵Ｋ_{ＡＦ}を取得するためのものであり、

前記第２処理ユニットは、前記ＡＦにサービスを提供できるか否かをチェックするように構成され、

前記第２通信ユニットはさらに、前記第２処理ユニットが前記ＡＦにサービスを提供できることをチェックした場合、前記ＡＦに第２メッセージを送信するように構成され、前記第２メッセージは少なくとも前記鍵Ｋ_{ＡＦ}を含む、通信装置。

40

【請求項４２】

ＡＡｎＦに適用される通信装置であって、第２送信ユニットを備え、

前記第２送信ユニットは、第１機器に第１情報を送信するように構成され、前記第１情報はＡＫＭＡコンテキスト情報を含む、通信装置。

【請求項４３】

ＡＦに適用される通信装置であって、第３送信ユニットと、第３受信ユニットと、を備え、

前記第３送信ユニットは、第１機器又はＡＡｎＦに第１メッセージを送信するように構成され、前記第１メッセージは鍵Ｋ_{ＡＦ}を取得するためのものであり、

前記第３受信ユニットは、前記第１機器又は前記ＡＡｎＦが前記ＡＦにサービスを提供

50

できることをチェックした場合、前記第 1 機器又は前記 A A n F から送信された第 2 メッセージを受信するように構成され、前記第 2 メッセージは少なくとも鍵 K A F を含む、通信装置。

【請求項 4 4】

A U S F に適用される通信装置であって、第 4 受信ユニットを備え、

前記第 4 受信ユニットは U D M から認証関連情報を取得するように構成され、前記認証関連情報は、

端末に対して A K M A 鍵材料を生成する必要があることを表す第 3 指示情報、端末に対して A K M A 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末の R I D 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む、通信装置。

10

【請求項 4 5】

U D M に適用される通信装置であって、第 5 送信ユニットを備え、

前記第 5 送信ユニットは A U S F に認証関連情報を送信するように構成され、前記認証関連情報は、

端末に対して A K M A 鍵材料を生成する必要があることを表す第 3 指示情報、前記端末に対して A K M A 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末の R I D 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む、通信装置。

【請求項 4 6】

コンピュータプログラムが記憶されたコンピュータ可読記憶媒体であって、

前記プログラムはプロセッサによって実行されるときに、請求項 1 ~ 1 1 のいずれか一項に記載の方法のステップ、又は、

20

請求項 1 2 ~ 1 5 のいずれか一項に記載の方法のステップ、又は、

請求項 1 6 ~ 2 1 のいずれか一項に記載の方法のステップ、又は、

請求項 2 2 ~ 2 8 のいずれか一項に記載の方法のステップ、又は、

請求項 2 9 ~ 3 2 のいずれか一項に記載の方法のステップ、又は、

請求項 3 3 ~ 3 5 のいずれか一項に記載の方法のステップ、又は、

請求項 3 6 ~ 3 8 のいずれか一項に記載の方法のステップを実現する、コンピュータ可読記憶媒体。

【請求項 4 7】

通信機器であって、

30

メモリと、プロセッサと、メモリに記憶され、プロセッサで実行可能なコンピュータプログラムと、を備え

前記プロセッサは、前記プログラムを実行するときに、請求項 1 ~ 1 1 のいずれか一項に記載の方法のステップ、又は、

請求項 1 2 ~ 1 5 のいずれか一項に記載の方法のステップ、又は、

請求項 1 6 ~ 2 1 のいずれか一項に記載の方法のステップ、又は、

請求項 2 2 ~ 2 8 のいずれか一項に記載の方法のステップ、又は、

請求項 2 9 ~ 3 2 のいずれか一項に記載の方法のステップ、又は、

請求項 3 3 ~ 3 5 のいずれか一項に記載の方法のステップ、又は、

請求項 3 6 ~ 3 8 のいずれか一項に記載の方法のステップを実現する、通信機器。

40

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本願は、通信技術分野に関し、特に、通信方法、通信装置、通信機器及びコンピュータ記憶媒体に関するものである。

【0 0 0 2】

(関連出願への相互参照)

本願は、2 0 2 2 年 0 6 月 2 0 日に中国特許庁に提出された、出願番号が第 2 0 2 2 1 0 7 0 1 0 8 8 . 4 号である中国特許出願の優先権を主張し、その内容の全てが引用により本願に組み込まれる。

50

【背景技術】

【0003】

現在、アプリケーションの認証と鍵管理（AKMA：Authentication and Key Management for Applications）の処理プロセスは、ユーザ機器（UE：User Equipment）が帰属先にある場合に対してのみであり、UEが訪問ネットワークにローミングした場合（即ち、ローミングセッション）に対しては、現在効果的な解決策がない。

【発明の概要】

【発明が解決しようとする課題】

【0004】

本願の実施例は、通信方法、通信装置、通信機器及びコンピュータ記憶媒体を提供する。

【課題を解決するための手段】

【0005】

本願の実施例の技術的解決策は、次のように実現される。

【0006】

第1態様では、本願の実施例は通信方法を提供し、前記方法は、

AKMAアンカー機能（AAnF：AKMA Anchor Function）が、アプリケーション機能（AF：Application Function）から送信された第1メッセージを受信し、又は、第1機器を介してAFから送信された第1メッセージを受信するステップであって、前記第1メッセージは鍵 K_{AF} を取得するためのものである、ステップと、

前記AAnFが前記AFにサービスを提供できることをチェックした場合、前記AFに第2メッセージを送信し、又は、前記第1機器を介して前記AFに第2メッセージを送信するステップであって、前記第2メッセージは少なくとも鍵 K_{AF} を含む、ステップと、を含む。

【0007】

本願のいくつかの代替実施例では、前記AAnFは、ホーム・パブリック・ランド・モバイル・ネットワーク（HPLMN：Home Public Land Mobile Network、ホームネットワークと略称する）に位置し、及び／又は、前記第1機器は、ビジット・パブリック・ランド・モバイル・ネットワーク（VPLMN：Visit Public Land Mobile Network、訪問ネットワークと略称する）に位置し、及び／又は、前記AFは、VPLMNに位置する。

【0008】

本願のいくつかの代替実施例では、前記第1メッセージは、AKMA鍵識別子（A-KID：AKMA-Key Identifier）及び／又は前記AFの識別子を含む。

【0009】

本願のいくつかの代替実施例では、前記通信方法は、前記AAnFが、AKMAアンカー鍵（ K_{AKMA} ）に基づいて前記鍵 K_{AF} を導出するステップをさらに含む。

【0010】

本願のいくつかの代替実施例では、前記第2メッセージは、

前記鍵 K_{AF} の有効時間情報、

購読永久識別子（SUPI：Subscription Permanent Identifier）、

一般公衆購読識別子（GPSI：Generic Public Subscription Identifier）のうちの少なくとも1つをさらに含む。

【0011】

本願のいくつかの代替実施例では、前記通信方法は、前記AAnFが、認証サーバ機能（AUSF：Authentication Server Function）から送信された第3メッセージを受信するステップをさらに含み、前記第3メッセージは鍵を登

10

20

30

40

50

録するためのものであり、前記第 3 メッセージは、A - K I D、K A K M A、S U P I、端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 0 1 2 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む。

【 0 0 1 3 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、前記 A U S F が統合データ管理 (U D M : U n i f i e d D a t a M a n a g e m e n t) から取得したものである。 10

【 0 0 1 4 】

本願のいくつかの代替実施例では、前記 A U S F が U D M から取得した前記端末のローミング情報は、前記端末 S U P I に関連付けられた前記端末のローミング情報である。

【 0 0 1 5 】

本願のいくつかの代替実施例では、前記第 1 メッセージを受信した後、前記通信方法は、前記 A A n F が、U D M から端末のローミング情報を取得するステップをさらに含み、前記端末のローミング情報は、前記第 1 メッセージ内の A - K I D に対応する端末に関連する。

【 0 0 1 6 】

本願のいくつかの代替実施例では、前記 A A n F が、前記 A F にサービスを提供できるか否かをチェックするステップは、前記 A A n F が、前記端末のローミング情報に基づいて、前記 A F にサービスを提供できるか否かをチェックするステップを含む。 20

【 0 0 1 7 】

第 2 態様では、本願の実施例は通信方法をさらに提供し、前記方法は、

第 1 機器が、A F から送信された第 1 メッセージを受信し、前記第 1 メッセージを A A n F に送信するステップであって、前記第 1 メッセージは鍵 K A F を取得するためのものである、ステップと、

前記 A A n F が前記 A F にサービスを提供できる場合、前記第 1 機器が、前記 A A n F から送信された第 2 メッセージを受信し、前記第 2 メッセージを前記 A F に送信するステップであって、前記第 2 メッセージは少なくとも前記鍵 K A F を含む、ステップと、を含む。 30

【 0 0 1 8 】

本願のいくつかの代替実施例では、前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置し、及び / 又は、前記 A F は V P L M N に位置する。

【 0 0 1 9 】

本願のいくつかの代替実施例では、前記第 1 メッセージは、A - K I D 及び / 又は前記 A F の識別子を含む。

【 0 0 2 0 】

本願のいくつかの代替実施例では、前記第 2 メッセージは、前記鍵 K A F の有効時間情報、S U P I、G P S I のうちの少なくとも 1 つをさらに含む。 40

【 0 0 2 1 】

第 3 態様では、本願の実施例は通信方法をさらに提供し、前記方法は、

第 1 機器が、A F から送信された第 1 メッセージを受信するステップであって、前記第 1 メッセージは鍵 K A F を取得するためのものである、ステップと、

前記第 1 機器が前記 A F にサービスを提供できることをチェックした場合、前記 A F に第 2 メッセージを送信するステップであって、前記第 2 メッセージは少なくとも前記鍵 K A F を含む、ステップと、を含む。

【 0 0 2 2 】

本願のいくつかの代替実施例では、前記第 1 メッセージは、A - K I D 及び / 又は前記 A F の識別子を含む。

【 0 0 2 3 】

本願のいくつかの代替実施例では、前記通信方法は、前記第 1 機器が、A A n F から送信された第 1 情報を受信するステップをさらに含み、前記第 1 情報は、A K M A コンテキスト情報を含む。

【 0 0 2 4 】

本願のいくつかの代替実施例では、前記第 1 情報は、A - K I D、A K M A アンカー鍵 (K A K M A)、S U P I のうちの少なくとも 1 つを含む。

【 0 0 2 5 】

本願のいくつかの代替実施例では、前記通信方法は、前記第 1 機器が、K A K M A に基づいて前記鍵 K A F を導出するステップをさらに含む。

【 0 0 2 6 】

本願のいくつかの代替実施例では、前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置し、及び / 又は、前記 A F は V P L M N に位置する。

【 0 0 2 7 】

第 4 態様では、本願の実施例は、通信方法をさらに提供し、前記方法は、A A n F が、第 1 機器に第 1 情報を送信するステップをさらに含み、前記第 1 情報は A K M A コンテキスト情報を含む。

【 0 0 2 8 】

本願のいくつかの代替実施例では、前記第 1 情報は、A - K I D、A K M A アンカー鍵 (K A K M A)、S U P I のうちの少なくとも 1 つを含む。

【 0 0 2 9 】

本願のいくつかの代替実施例では、前記通信方法は、前記 A A n F が、A U S F から送信された第 3 メッセージを受信するステップをさらに含み、前記第 3 メッセージは鍵を登録するためのものであり、前記第 3 メッセージは、A - K I D、K A K M A、S U P I、端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 0 3 0 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む。

【 0 0 3 1 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、前記 A U S F が U D M から取得したものである。

【 0 0 3 2 】

本願のいくつかの代替実施例では、前記 A U S F が U D M から取得した前記端末のローミング情報は、前記端末 S U P I に関連付けられた前記端末のローミング情報である。

【 0 0 3 3 】

本願のいくつかの代替実施例では、前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置する。

【 0 0 3 4 】

第 5 態様では、本願の実施例は通信方法をさらに提供し、前記方法は、

A F が第 1 機器又は A A n F に第 1 メッセージを送信するステップであって、前記第 1 メッセージは鍵 K A F を取得するためのものである、ステップと、

前記第 1 機器又は前記 A A n F が前記 A F にサービスを提供できることをチェックした場合、前記 A F が前記第 1 機器又は前記 A A n F から送信された第 2 メッセージを受信するステップであって、前記第 2 メッセージは少なくとも鍵 K A F を含む、ステップと、を含む。

【 0 0 3 5 】

10

20

30

40

50

本願のいくつかの代替実施例では、前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置し、及び / 又は、前記 A F は V P L M N に位置する。

【 0 0 3 6 】

本願のいくつかの代替実施例では、前記第 1 メッセージは、A K M A 鍵識別子 (A - K I D) 及び / 又は前記 A F の識別子を含む。

【 0 0 3 7 】

本願のいくつかの代替実施例では、前記第 2 メッセージは、前記鍵 K A F の有効時間情報、S U P I、G P S I のうちの少なくとも 1 つをさらに含む。

【 0 0 3 8 】

10

第 6 態様では、本願の実施例は通信方法をさらに提供し、前記方法は、A U S F が、U D M から認証関連情報を取得するステップを含み、前記認証関連情報は

、端末に対して A K M A 鍵材料を生成する必要があることを表す第 3 指示情報、端末に対して A K M A 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末のルーティング識別子 (R I D) 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 0 3 9 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む。

20

【 0 0 4 0 】

本願のいくつかの代替実施例では、前記通信方法は、前記 A U S F が A A n F に第 3 メッセージを送信するステップをさらに含み、前記第 3 メッセージは鍵を登録するためのものであり、前記第 3 メッセージは、A - K I D、K A K M A、S U P I、前記端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 0 4 1 】

第 7 態様では、本願の実施例は通信方法をさらに提供し、前記方法は、

U D M が A U S F に認証関連情報を送信するステップを含み、前記認証関連情報は、端末に対して A K M A 鍵材料を生成する必要があることを表す第 3 指示情報、前記端末に対して A K M A 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末の R I D 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む。

30

【 0 0 4 2 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む。

【 0 0 4 3 】

本願のいくつかの代替実施例では、前記通信方法は、前記 U D M が、A A n F から送信された第 4 メッセージを受信するステップであって、前記第 4 メッセージは、端末のローミング情報を要求するためのものである、ステップと、前記 U D M が、前記 A A n F に第 5 メッセージを送信するステップであって、前記第 5 メッセージは、前記端末のローミング情報を含む、ステップと、をさらに含む。

40

【 0 0 4 4 】

第 8 態様では、本願の実施例は A A n F に適用される通信装置をさらに提供し、前記装置は、第 1 通信ユニットと、第 1 処理ユニットと、を備え、

前記第 1 通信ユニットは、A F から送信された第 1 メッセージを受信し、又は、第 1 機器を介して A F から送信された第 1 メッセージを受信するように構成され、前記第 1 メッセージは鍵 K A F を取得するためのものであり、

前記第 1 処理ユニットは、前記 A F にサービスを提供できるか否かをチェックするよう

50

に構成され、

前記第1通信ユニットはさらに、前記第1処理ユニットが前記AFにサービスを提供できることをチェックした場合、前記AFに第2メッセージを送信し、又は、前記第1機器を介して前記AFに第2メッセージを送信するように構成され、前記第2メッセージは少なくとも鍵 K_{AF} を含む。

【0045】

第9態様では、本願の実施例は、第1機器に適用される通信装置をさらに提供し、前記装置は、第1受信ユニットと、第1送信ユニットと、を備え、

前記第1受信ユニットは、AFから送信された第1メッセージを受信し、前記第1メッセージをAAnFに送信するように構成され、前記第1メッセージは鍵 K_{AF} を取得するためのものであり、

前記第1送信ユニットは、前記AAnFが前記AFにサービスを提供できる場合、前記AAnFから送信された第2メッセージを受信し、前記第2メッセージを前記AFに送信するように構成され、前記第2メッセージは少なくとも前記鍵 K_{AF} を含む。

【0046】

第10態様では、本願の実施例は第1機器に適用される通信装置をさらに提供し、前記装置は、第2通信ユニットと、第2処理ユニットと、を備え、

前記第2通信ユニットは、AFから送信された第1メッセージを受信するように構成され、前記第1メッセージは、鍵 K_{AF} を取得するためのものであり、

前記第2処理ユニットは、前記AFにサービスを提供できるか否かをチェックするように構成され、

前記第2通信ユニットはさらに、前記第2処理ユニットが前記AFにサービスを提供できることをチェックした場合、前記AFに第2メッセージを送信するように構成され、前記第2メッセージは少なくとも前記鍵 K_{AF} を含む。

【0047】

第11態様では、本願の実施例はAAnFに適用される通信装置をさらに提供し、前記装置は、第2送信ユニットを備え、前記第2送信ユニットは、第1機器に第1情報を送信するように構成され、前記第1情報はAKMAコンテキスト情報を含む。

【0048】

第12態様では、本願の実施例はAFに適用される通信装置をさらに提供し、前記装置は、第3送信ユニットと、第3受信ユニットと、を備え、

前記第3送信ユニットは、第1機器又はAAnFに第1メッセージを送信するように構成され、前記第1メッセージは鍵 K_{AF} を取得するためのものであり、

前記第3受信ユニットは、前記第1機器又は前記AAnFが前記AFにサービスを提供できることをチェックした場合、前記第1機器又は前記AAnFから送信された第2メッセージを受信するように構成され、前記第2メッセージは少なくとも鍵 K_{AF} を含む。

【0049】

第13態様では、本願の実施例はAUSFに適用される通信装置をさらに提供し、前記装置は、第4受信ユニットを備え、前記第4受信ユニットは、UDMから認証関連情報を取得するように構成され、前記認証関連情報は、端末に対してAKMA鍵材料を生成する必要があることを表す第3指示情報、端末に対してAKMA鍵材料を生成する必要があることを表す第4指示情報、前記端末のRID情報、前記端末のローミング情報のうちの少なくとも1つを含む。

【0050】

第14態様では、本願の実施例はUDMに適用される通信装置をさらに提供し、前記装置は、第5送信ユニットを備え、前記第5送信ユニットは、AUSFに認証関連情報を送信するように構成され、前記認証関連情報は、端末に対してAKMA鍵材料を生成する必要があることを表す第3指示情報、前記端末に対してAKMA鍵材料を生成する必要があることを表す第4指示情報、前記端末のRID情報、前記端末のローミング情報のうちの少なくとも1つを含む。

【 0 0 5 1 】

第 1 5 態様では、本願の実施例は、コンピュータプログラムが記憶されたコンピュータ可読記憶媒体をさらに提供し、前記プログラムはプロセッサによって実行されるときに、本願の実施例の上記第 1 態様～第 7 態様のいずれかに記載の通信方法のステップを実現する。

【 0 0 5 2 】

第 1 6 態様では、本願の実施例は通信機器をさらに提供し、前記通信機器は、メモリと、プロセッサと、メモリに記憶され、プロセッサで実行可能なコンピュータプログラムと、を備え、前記プロセッサは、前記プログラムを実行するときに、本願の実施例の上記第 1 態様～第 7 態様のいずれかに記載の通信方法のステップを実行する。

10

【 発明の効果 】

【 0 0 5 3 】

本願の実施例によって提供される通信方法、通信装置、通信機器及びコンピュータ記憶媒体によれば、一方、前記方法は、A A n F が、A F から送信された第 1 メッセージを受信し、又は、第 1 機器を介して A F から送信された第 1 メッセージを受信するステップであって、前記第 1 メッセージは鍵 K_{A F} を取得するためのものである、ステップと、前記 A A n F が前記 A F にサービスを提供できることをチェックした場合、前記 A F に第 2 メッセージを送信し、又は、前記第 1 機器を介して前記 A F に第 2 メッセージを送信するステップであって、前記第 2 メッセージは少なくとも鍵 K_{A F} を含む、ステップと、を含む。上記のインタラクションプロセスにより、端末が訪問ネットワークにローミングする A K M A サービスを実現する。

20

【 0 0 5 4 】

他方では、第 1 機器により、A F から送信された第 1 メッセージを受信し、前記第 1 メッセージは鍵 K_{A F} を取得するためのものであり、前記第 1 機器が前記 A F にサービスを提供できることをチェックした場合、前記 A F に第 2 メッセージを送信し、前記第 2 メッセージは少なくとも前記鍵 K_{A F} を含む。この実施形態では、ネットワークアーキテクチャに、ホームネットワークから得られる A K M A 鍵材料を管理・記憶するための第 1 機器を導入して、この訪問先の端末及び A F に A K M A 鍵サービスを提供することで、A F と各ホームネットワークとのインタラクション及び管理コストを削減する。

【 図面の簡単な説明 】

30

【 0 0 5 5 】

【 図 1 】 A K M A ネットワークアーキテクチャの模式図である。

【 図 2 】 ネットワークアーキテクチャの別の模式図である。

【 図 3 】 本願の実施例の通信方法が適用されるシステムアーキテクチャの模式図である。

【 図 4 a 】 本願の実施例の通信方法が適用されるシステムアーキテクチャのモデルの模式図である。

【 図 4 b 】 本願の実施例の通信方法が適用されるシステムアーキテクチャのモデルの模式図である。

【 図 5 】 本願の実施例の通信方法のフローチャート 1 である。

【 図 6 】 本願の実施例の通信方法のフローチャート 2 である。

40

【 図 7 】 本願の実施例の通信方法のフローチャート 3 である。

【 図 8 】 本願の実施例の通信方法のフローチャート 4 である。

【 図 9 】 本願の実施例の通信方法のフローチャート 5 である。

【 図 1 0 】 本願の実施例の通信方法のフローチャート 6 である。

【 図 1 1 】 本願の実施例の通信方法のフローチャート 7 である。

【 図 1 2 】 本願の実施例の通信方法のインタラクションフローチャート 1 である。

【 図 1 3 】 本願の実施例の通信方法のインタラクションフローチャート 2 である。

【 図 1 4 】 本願の実施例の通信方法のインタラクションフローチャート 3 である。

【 図 1 5 】 本願の実施例の通信装置の構成を示す模式図 1 である。

【 図 1 6 】 本願の実施例の通信装置の構成を示す模式図 2 である。

50

【図 17】本願の実施例の通信装置の構成を示す模式図 3 である。

【図 18】本願の実施例の通信装置の構成を示す模式図 4 である。

【図 19】本願の実施例の通信装置の構成を示す模式図 5 である。

【図 20】本願の実施例の通信装置の構成を示す模式図 6 である。

【図 21】本願の実施例の通信装置の構成を示す模式図 7 である。

【図 22】本願の実施例の通信機器のハードウェアの構成を示す模式図である。

【発明を実施するための形態】

【0056】

以下では、図面及び具体的な実施例を参照して、本願をさらに詳細に説明する。

【0057】

本願実施例における技術的解決策は、様々な通信システム、例えば、グローバル移動通信 (GSM: Global System of Mobile communication) システム、ロングエボリューション (LTE: Long Term Evolution) システム又は 5G システムなどに適用され得る。任意選択的に、5G システム又は 5G ネットワークは、ニューラジオ (NR: New Radio) システム又は NR ネットワークとも呼ばれ得る。

【0058】

例示的に、本願の実施例が適用される通信システムは、ネットワーク機器及び端末機器 (端末、通信端末などとも呼ばれ得る) を含んでもよく、ネットワーク機器は、端末機器と通信する機器であってもよい。ここで、ネットワーク機器は、一定のエリア内で通信能力を提供することができ、このエリア内に位置する端末と通信することができる。任意選択的に、ネットワーク機器は、各通信システムにおける基地局、例えば、LTE システムにおける進化型基地局 (eNB: Evolutional Node B)、又は、5G システム又は NR システムにおける基地局 (gNB) であってもよい。

【0059】

なお、本願の実施例では、ネットワーク / システムにおける通信機能を備えた機器は、通信機器と呼ばれ得る。通信機器は、通信機能を備えたネットワーク機器及び端末を含んでもよく、ネットワーク機器及び端末は、上記の特定の機器であってもよく、ここでは繰り返して説明しない。通信機器は、通信システムにおける他の機器、例えば、ネットワークコントローラー、モバイル管理エンティティなどの他のネットワークエンティティをさらに含んでもよいが、本願の実施例はこれらを限定しない。

【0060】

なお、本明細書における「システム」及び「ネットワーク」という用語は、本明細書で常に互換可能に使用される。本明細書における「及び / 又は」という用語は、関連付け対象の関連付け関係についてのみ説明し、3つの関係が存在し得ることを表す。例えば、A 及び / 又は B は、A が独立で存在する場合、A と B の両方が存在する場合、B が独立で存在する場合の 3つの場合を表すことができる。また、本明細書における記号「/」は、通常、前後の関連付け対象間の関係が、「又は」という関係にあることを表す。

【0061】

本願の明細書、特許請求の範囲における「第 1」、「第 2」などの用語は、特定の順番又は前後順番を限定するものではなく、類似する対象を区別するものである。なお、このように使用されるデータは、適切な場合に交換できるため、本明細書で説明される本願の実施例は、本明細書で図示又は説明されるもの以外の順序で実施できる。さらに、「含む」、「有する」という用語、及びその変形は、非排他的な包含を意図している。例えば、一連のステップ又はユニットを組み込んだプロセス、方法、システム、製品、又は機器は、明確に列挙されているものに限定される必要はないが、明確に列挙されていない、又はそれらのプロセス、方法、製品、又は機器に固有の他のものを含んでもよい。

【0062】

本願の実施例を詳細に説明する前に、まず、AKMA の関連技術について簡単に説明する。

10

20

30

40

50

【 0 0 6 3 】

図 1 は、A K M A ネットワークアーキテクチャの模式図であり、図 1 に示すように、A K M A ネットワークアーキテクチャのコアネットワーク要素は、主に A A n F、A F、A U S F などを含み、ここで、

A A n F は、ホームオペレータ（又はホームネットワーク）内に配置されたアンカー機能であり、A A n F は、A K M A サービスのために A K M A アンカー鍵（K A K M A）を記憶し、U E と A U S F との間で 5 G マスター認証が正常に完了した後、A U S F によってこの鍵を A A n F に送信する。A A n F は同時に、U E と A F との間で使用するための鍵 K A F も生成し、U E の A K M A コンテキストを維持する。

【 0 0 6 4 】

A K M A サービスを備えた A F は、A K M A 鍵識別子（A - K I D）を介して A A n F に A K M A アプリケーション鍵 K A F を要求することができる。A F は、オペレータのネットワークの認証及び認可を得てから鍵 K A F を取得することができる。

【 0 0 6 5 】

A U S F は、U E の識別子及び A K M A 鍵材料、例えば、A - K I D 及び K A K M A などを A A n F に提供する。

【 0 0 6 6 】

現在、A K M A ローミングシーンにおけるネットワークアーキテクチャ及び応答の処理プロセスは提案されていないが、図 1 に示す A K M A ネットワークアーキテクチャに基づいて、U E が訪問ネットワークにローミングするたびに、A F も当該訪問ネットワークと契約するアプリケーション機能である場合、A K M A サービスのアーキテクチャは図 2 に示すようになることが想定される。このようなネットワークアーキテクチャにおいて、一方、同じ A F の場合、複数の公共陸上モバイルネットワーク（P L M N：P u b l i c L a n d M o b i l e N e t w o r k）に属する U E にアプリケーションサービスを提供し、これは、これらの U E が、当該 A F が位置している訪問 P L M N（V P L M N）にローミングし、U E が A K M A サービスを使用する場合、当該 A F は、A K M A 鍵材料（K A F など）を取得するために、これらの U E のホーム P L M N（H P L M N）とインタラクションを行う必要があることを意味する。ここで、H P L M N は、ホームネットワーク又は帰属先ネットワークとも呼ばれ得、V P L M N は、訪問ネットワーク又は訪問先ネットワークとも呼ばれ得る。

【 0 0 6 7 】

他方では、同じ U E の場合、それ自体が位置する訪問先の複数の A F と A K M A サービスを契約する場合があります、これは、U E が A K M A サービスを使用する場合、A K M A 鍵材料を取得するために、これらの A F が、当該 U E が位置する H P L M N とインタラクションを行うことを意味する。

【 0 0 6 8 】

このようにして直面する問題は以下の通りである。1）A F は、A K M A 鍵材料を取得するために、複数の H P L M N とインタラクションを行う必要がある。即ち、A F は、複数の H P L M N と、対応する A K M A ローミングプロトコルを契約する必要があり、A F の管理コストが増加する。2）U E が A F とインタラクションを行い、A K M A サービスを使用する場合、A F は、鍵材料を取得するために、H P L M N とインタラクションを行う必要があり、A K M A サービスの遅延が増加する。

【 0 0 6 9 】

図 3 は、本願の実施例の通信方法が適用されるシステムアーキテクチャの模式図であり、図 4 a 及び図 4 b は、それぞれ本願の実施例の通信方法が適用されるシステムアーキテクチャのモデルの模式図である。図 3、図 4 a 及び図 4 b を参照すると、本願の実施例では、V P L M N に配置された第 1 機器が追加され、その機能は、少なくとも以下を含む。1）訪問先の A F（v A F）と帰属先の A A n F（H A A n F）との間のプロキシとして機能する。2）U E に対応するホームネットワーク及び H A A n F をアドレッシングし、当該 H A A n F と安全通信を確立する。3）v A F の正当性を検証し、v A F が要求する

10

20

30

40

50

A K M A 鍵材料を認可する。

【 0 0 7 0 】

本願の各実施例では、前記第 1 機器は、複数の実現可能な実施形態を有し、前記第 1 機器は、例えば、プロキシ、プロキシ機能、プロキシネットワーク要素、ネットワーク要素、proxy、proxy function、proxy NF、ネットワーク機能 (NF: Network Function) などと呼ばれてもよく、プロキシ機能、管理機能、伝送機能、鍵管理機能、鍵記憶機能、鍵配布機能のうちの少なくとも 1 つの機能を備える機器であってもよい。当該第 1 機器は、上記のネットワーク機能のみを備えてもよく、他のネットワーク機能を備えてもよく、即ち、上記のネットワーク機能と他のネットワーク機能とが併設されてもよい。

10

【 0 0 7 1 】

実際に配置又は実現するとき、第 1 機器は V P L M N 内の他のネットワーク要素と併設されてもよく、又は他のネットワーク要素によってこの論理機能を実現してもよい。例示的に、V P L M N に A K M A サービスが配置された場合、当該プロキシ機能は、当該 V P L M N の A A n F であり、当該 V P L M N に A K M A サービスが配置されていない場合、プロキシ機能は、独立したネットワーク要素であってもよく、又は当該 V P L M N の N E F、U P F 又は他のネットワーク要素と併設されてもよく、又は他のネットワーク要素によってプロキシ機能の論理機能を実現してもよい。

【 0 0 7 2 】

また、第 1 機器は、オプション機能であってもよく、V P L M N は、必要に応じて第 1 機器を配置してもよい。例えば、V P L M N には、H P L M N によって提供される A K M A サービスを使用する、ローカルに配置された複数の A F があり、管理と契約を容易にするために、V P L M N は、ローカルに第 1 機器を配置することを選択することで、これらの A F が A K M A 鍵を取得するために H P L M N の A A n F とインタラクションを行うことをプロキシしてもよく、又は、V P L M N に配置された A F が、複数の H P L M N の U E にサービスを提供し、A K M A サービスを使用する場合、V P L M N は、ローカルに第 1 機器を配置することを選択することで、この A F が A K M A 鍵を取得するためにこれらの U E の H P L M N の A A n F とインタラクションを行うことをプロキシしてもよい。

20

【 0 0 7 3 】

A F が第 3 者の A F である場合、A F は、図 4 b に示すように、ネットワークエクスポージャー機能 (N E F: Network Exposure Function) を介して第 1 機器又は A A n F とインタラクションを行う。

30

【 0 0 7 4 】

少なくとも上記のネットワークアーキテクチャに基づいて、本願の以下の各実施例を提案する。

【 0 0 7 5 】

本願の実施例は通信方法を提供する。図 5 は、本願の実施例の通信方法のフローチャート 1 であり、図 5 に示すように、前記方法は、以下のステップを含む。

【 0 0 7 6 】

ステップ 1 0 1 において、A A n F は、A F から送信された第 1 メッセージを受信し、又は、第 1 機器を介して A F から送信された第 1 メッセージを受信し、前記第 1 メッセージは鍵 K A F を取得するためのものである。

40

【 0 0 7 7 】

ステップ 1 0 2 において、前記 A A n F が前記 A F にサービスを提供できることをチェックした場合、前記 A F に第 2 メッセージを送信し、又は、前記第 1 機器を介して前記 A F に第 2 メッセージを送信し、前記第 2 メッセージは少なくとも鍵 K A F を含む。

【 0 0 7 8 】

いくつかの代替実施例では、前記 A A n F は、ホームネットワーク (H P L M N) に位置し、及び / 又は、前記第 1 機器は、訪問ネットワーク (V P L M N) に位置し、及び / 又は、前記 A F は、V P L M N に位置する。

50

【 0 0 7 9 】

例示的に、この実施例は、A K M A ローミングシーンに適用可能である。例えば、U E が訪問ネットワークにローミングし、A F も当該訪問ネットワークと契約されたアプリケーション機能であり、U E が A K M A サービスを使用する場合、A F は、鍵 K_{A F} などの A K M A 鍵材料を取得する必要がある。ホームネットワークの A A n F は、A F からの、鍵 K_{A F} を取得するための第 1 メッセージを受信し、前記 A F にサービスを提供できることをチェックした場合、少なくとも鍵 K_{A F} を含む第 2 メッセージを A F に送信する。

【 0 0 8 0 】

一実施形態では、第 1 機器が配置されている場合、第 1 機器が U E に対応するホームネットワーク及び A A n F をアドレッシングし、A A n F と安全通信を確立することにより、第 1 メッセージは、第 1 機器を介して A A n F に伝送され、これに対応して、第 2 メッセージは、第 1 機器を介して A F に送信される。別の実施形態では、第 1 機器が配置されていない場合、A F は、U E に対応するホームネットワークの A A n F を検索し、A A n F と安全通信を確立することができ、A F は、第 1 メッセージを A A n F に直接送信することができ、これに対応して、A A n F は、第 2 メッセージを A F に直接送信する。任意選択的に、A F は、ネットワークリポジトリ機能 (N R F : Network Repository Function) に照会メッセージを送信して、A A n F の関連情報 (A A n F のアドレスなど) を取得し、さらに、取得した A A n F の関連情報に基づいて第 1 メッセージを送信することができる。

【 0 0 8 1 】

いくつかの代替実施例では、前記第 1 メッセージは、A - K I D 及び / 又は前記 A F の識別子を含む。

【 0 0 8 2 】

いくつかの代替実施例では、前記通信方法は、前記 A A n F が、K_{A K M A} に基づいて前記鍵 K_{A F} を導出するステップをさらに含む。

【 0 0 8 3 】

本実施例では、端末 (又は U E) と A U S F との間の認証プロセス中又は認証完了後、A U S F は、A K M A アンカー鍵 (K_{A K M A}) を A A n F に送信する。A A n F は、ホームオペレータ (又はホームネットワーク) 内の機能であり、A K M A サービスのために K_{A K M A} を記憶する。A A n F は、第 1 メッセージを受信した後、K_{A K M A} に基づいて鍵 K_{A F} を導出することができ、鍵 K_{A F} は、アプリケーション鍵とも呼ばれ得る。

【 0 0 8 4 】

いくつかの代替実施例では、前記第 2 メッセージは、前記鍵 K_{A F} の有効時間情報、S U P I、G P S I のうちの少なくとも 1 つをさらに含む。

【 0 0 8 5 】

本実施例では、前記鍵 K_{A F} の有効時間情報は、鍵 K_{A F} の有効期間、又は鍵 K_{A F} の失効時間を表し、又は鍵 K_{A F} expiration time と表示してもよい。

【 0 0 8 6 】

本願のいくつかの代替実施例では、前記通信方法は、前記 A A n F が、A U S F から送信された第 3 メッセージを受信するステップをさらに含み、前記第 3 メッセージは、鍵を登録するためのものであり、前記第 3 メッセージは、A - K I D、K_{A K M A}、S U P I、端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 0 8 7 】

本実施例では、A A n F は、第 3 メッセージを受信した後、鍵を登録する。任意選択的に、前記通信方法は、前記 A A n F が、A U S F に前記第 3 メッセージの応答メッセージを送信するステップをさらに含む。

【 0 0 8 8 】

いくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ロー

10

20

30

40

50

ミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも1つを含む。

【0089】

本実施例では、端末がローミング状態にない場合、即ち、端末がホームネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にないことを表す第2指示情報を含んでもよい。端末がローミング状態にある場合、即ち、端末が訪問ネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にあることを表す第1指示情報、ローミング先情報、前記端末のローミング先での契約情報、及び前記端末のローミング先でのポリシー情報のうちの少なくとも1つの情報を含んでもよい。

【0090】

ここで、前記ローミング先情報は、ローミング先ネットワーク（又は訪問ネットワーク）を指示する情報であってもよく、例えば、ローミング先ネットワーク名/識別子など、例えば、サービスネットワーク名（SN name: Service Network name）であってもよい。

【0091】

上記の端末のローミング先での契約情報は、具体的には、端末とローミング先とのサービス契約リスト、端末とローミング先との契約ポリシーなどを含んでもよい。

【0092】

上記の端末のローミング先でのポリシー情報は、具体的には、ホームネットワークが当該端末の訪問先でのAKMAサービス使用を許可するか否か、訪問ネットワークが当該端末のAKMAサービス使用を許可するか否か、ホームネットワークと訪問ネットワーク間のサービスプロトコル、ホームネットワークの正当な監視ポリシー、訪問ネットワークの正当な監視ポリシーなどを含んでもよい。

【0093】

いくつかの代替実施例では、前記端末のローミング情報は、前記AUSFがUDMから取得したものである。

【0094】

任意選択的に、前記AUSFがUDMから取得した前記端末のローミング情報は、前記端末SUP Iに関連付けられた前記端末のローミング情報である。

【0095】

本願のいくつかの代替実施例では、前記第1メッセージを受信した後、前記通信方法は、前記AAnFが、UDMから端末のローミング情報を取得するステップをさらに含み、前記端末のローミング情報は、前記第1メッセージ内のA-KIDに対応する端末に関連する。

【0096】

本実施例では、AAnFは、第1メッセージを受信した後、第1メッセージ内のA-KIDに基づいて対応する端末のSUP Iを検索し、当該SUP Iを利用してUDMから対応する端末のローミング情報を取得することができる。

【0097】

いくつかの代替実施例では、前記AAnFが、前記AFにサービスを提供できるか否かをチェックするステップは、前記AAnFが、前記AFの識別子に基づいて、前記AFにサービスを提供できるか否かをチェックするステップを含む。

【0098】

別のいくつかの代替実施例では、前記AAnFが、前記AFにサービスを提供できるか否かをチェックするステップは、前記AAnFが、前記端末のローミング情報に基づいて、前記AFにサービスを提供できるか否かをチェックするステップを含む。

【0099】

本実施例では、前記AAnFは、前記AFの識別子に基づいて、さらに、前記端末のローミング情報（例えば、端末のローミング先での契約情報及び/又は端末のローミング先でのポリシー情報）と結合して、前記AFにサービスを提供できるか否かをチェックする

10

20

30

40

50

ことができる。

【0100】

上記の実施例に基づき、本願の実施例は、通信方法をさらに提供する。図6は、本願の実施例の通信方法のフローチャート2であり、図6に示すように、前記方法は、以下のステップを含む。

【0101】

ステップ201において、第1機器は、AFから送信された第1メッセージを受信し、前記第1メッセージをAAnFに送信し、前記第1メッセージは鍵K_{AF}を取得するためのものである。

【0102】

ステップ202において、前記AAnFが前記AFにサービスを提供できる場合、前記第1機器は、前記AAnFから送信された第2メッセージを受信し、前記第2メッセージを前記AFに送信し、前記第2メッセージは少なくとも前記鍵K_{AF}を含む。

【0103】

いくつかの代替実施例では、前記AAnFはHPLMNに位置し、及び/又は、前記第1機器はVPLMNに位置し、及び/又は、前記AFはVPLMNに位置する。

【0104】

本実施例では、第1機器は、訪問ネットワークに位置するプロキシ機能又はプロキシ機器として、訪問先のAFと帰属先のAAnFとの間のプロキシ機能を備え、AFから送信された第1メッセージを受信した後、対応する帰属先のAAnFをアドレッシングすることにより、AAnFに前記第1メッセージを送信し、前記AAnFが前記AFにサービスを提供できる場合、AAnFから送信された第2メッセージを受信し、第2メッセージを前記AFに送信する。

【0105】

いくつかの代替実施例では、前記第1メッセージは、A-KID及び/又は前記AFの識別子を含む。

【0106】

本実施例では、A-KIDはAKMA鍵識別子として使用され、第1機器は、第1メッセージを受信した後、第1メッセージ内のA-KIDに基づいて対応する端末の識別子、例えばSUPIを検索することができ、さらに、端末の識別子に基づいて対応する帰属先のAAnFの情報(AAnFの識別子及び/又はアドレス)を検索して決定することができる。

【0107】

いくつかの代替実施例では、前記第2メッセージは、前記鍵K_{AF}の有効時間情報、SUPI、GPSIのうちの少なくとも1つをさらに含む。

【0108】

本実施例では、前記鍵K_{AF}の有効時間情報は、鍵K_{AF}の有効期間、又は鍵K_{AF}の失効時間を表し、又は鍵K_{AF} expiration timeと表示してもよい。

【0109】

本願の実施例は、通信方法をさらに提供する。図7は、本願の実施例の通信方法のフローチャート3であり、図7に示すように、前記方法は、以下のステップを含む。

【0110】

ステップ301において、第1機器はAFから送信された第1メッセージを受信し、前記第1メッセージは鍵K_{AF}を取得するためのものである。

【0111】

ステップ302において、前記第1機器が前記AFにサービスを提供できることをチェックした場合、前記AFに第2メッセージを送信し、前記第2メッセージは少なくとも前記鍵K_{AF}を含む。

【0112】

いくつかの代替実施例では、前記第1機器はVPLMNに位置し、及び/又は、前記A

10

20

30

40

50

FはV P L M Nに位置する。

【0113】

例示的に、この実施例は、A K M Aローミングシーンに適用可能である。例えば、U Eが訪問ネットワークにローミングし、A Fも当該訪問ネットワーク契約のアプリケーション機能であり、U EがA K M Aサービスを使用する場合、A Fは、鍵 K_{AF} などのA K M A鍵材料を取得する必要がある。第1機器は、訪問ネットワークに配置されたプロキシ機能又はプロキシ機器として、A Fの正当性を検証し、A Fが要求するA K M A鍵材料を認可する機能を有する。

【0114】

いくつかの代替実施例では、前記第1メッセージは、A - K I D及び/又は前記A Fの識別子を含む。 10

【0115】

本実施例では、第1機器は、前記A Fの識別子に基づいて、前記A Fにサービスを提供できるか否かをチェックすることができ、前記A Fにサービスを提供できると決定した場合、鍵 K_{AF} をA Fに送信することを許可する。

【0116】

任意選択的に、第1機器が鍵 K_{AF} がないと決定した場合、前記通信方法は、前記第1機器が、 K_{AKMA} に基づいて前記鍵 K_{AF} を導出するステップをさらに含む。

【0117】

本実施例では、前記第1機器は、訪問先A Fと帰属先A A n Fとの間のプロキシとして、A A n Fから K_{AKMA} を事前に取得して記憶し、前記A Fにサービスを提供できることをチェックした場合、事前に取得した K_{AKMA} に基づいて前記鍵 K_{AF} を導出する。 20

【0118】

いくつかの代替実施例では、前記通信方法は、前記第1機器が、A A n Fから送信された第1情報を受信するステップをさらに含み、前記第1情報は、A K M Aコンテキスト情報を含む。

【0119】

本実施例では、第1機器が、A A n Fから送信された第1情報を受信するステップは、いくつかの実現可能な実施形態を含む。一実施形態として、第1機器は、A A n Fに要求メッセージを送信し、当該要求メッセージは、A K M Aコンテキスト情報を要求するためのものであり、第1機器は、A A n Fから送信された第1情報を受信する。別の実施形態として、第1機器は、A A n Fによって能動的にプッシュされる第1情報を受信する。上記の第2の実施形態において、本願の実施例では、第1機器がA A n Fによって能動的にプッシュされる第1情報を受信し、A Fから送信された第1メッセージを受信する時間的順番を限定しない。 30

【0120】

いくつかの代替実施例では、前記第1情報は、A - K I D、 K_{AKMA} 、S U P Iのうちの少なくとも1つを含む。

【0121】

任意選択的に、前記A A n Fは、H P L M Nに位置する。 40

【0122】

上記の実施例に基づき、本願の実施例は、通信方法をさらに提供する。図8は、本願の実施例の通信方法のフローチャート4であり、図8に示すように、前記方法は、以下のステップを含む。

【0123】

ステップ401において、A A n Fは第1機器に第1情報を送信し、前記第1情報はA K M Aコンテキスト情報を含む。

【0124】

いくつかの代替実施例では、前記第1情報は、A - K I D、 K_{AKMA} 、S U P Iのうちの少なくとも1つを含む。 50

【 0 1 2 5 】

本実施例では、A A n F が第 1 機器に第 1 情報を送信するステップは、いくつかの実現可能な実施形態を含む。別の実施形態として、A A n F は、第 1 機器が送信した要求メッセージを受信し、当該要求メッセージは、A K M A コンテキスト情報を要求するためのものであり、A A n F は、前記要求メッセージに基づいて、第 1 機器に第 1 情報を送信する。別の実施形態として、A A n F は、第 1 機器に前記第 1 情報を能動的にプッシュする。

【 0 1 2 6 】

本実施例では、A A n F は、鍵登録が完了した後、上記のいずれかの実施形態を採用して、第 1 機器に A K M A コンテキスト情報を送信する。

【 0 1 2 7 】

いくつかの代替実施例では、前記通信方法は、前記 A A n F が、A U S F から送信された第 3 メッセージを受信するステップをさらに含み、前記第 3 メッセージは、鍵を登録するためのものであり、前記第 3 メッセージは、A - K I D、K A K M A、S U P I、端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 1 2 8 】

本実施例では、上記の鍵登録プロセスは、A U S F が A A n F に対して開始する鍵登録プロセスであり、A U S F は、鍵登録のために、端末の識別子情報 (S U P I など) 及び A K M A 鍵材料 (A - K I D、K A K M A など) などの情報を A A n F に送信し、任意選択的に、A U S F は、A A n F に端末のローミング情報を提供することもできる。

【 0 1 2 9 】

任意選択的に、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む。

【 0 1 3 0 】

本実施例では、端末がローミング状態にない場合、即ち、端末がホームネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にないことを表す第 2 指示情報を含んでもよい。端末がローミング状態にある場合、即ち、端末が訪問ネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、ローミング先情報、前記端末のローミング先での契約情報、及び前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つの情報を含んでもよい。

【 0 1 3 1 】

ここで、前記ローミング先情報は、ローミング先ネットワーク (又は訪問ネットワーク) を指示する情報であってもよく、例えば、ローミング先ネットワーク名 / 識別子、例えば、S N n a m e であってもよい。

【 0 1 3 2 】

上記の端末のローミング先での契約情報は、具体的には、端末とローミング先とのサービス契約リスト、端末とローミング先との契約ポリシーなどを含んでもよい。

【 0 1 3 3 】

上記の端末のローミング先でのポリシー情報は、具体的には、ホームネットワークが当該端末の訪問先での A K M A サービス使用を許可するか否か、訪問ネットワークが当該端末の A K M A サービス使用を許可するか否か、ホームネットワークと訪問ネットワーク間のサービスプロトコル、ホームネットワークの正当な監視ポリシー、訪問ネットワークの正当な監視ポリシーなどを含んでもよい。

【 0 1 3 4 】

いくつかの代替実施例では、前記端末のローミング情報は、前記 A U S F が U D M から取得したものである。

【 0 1 3 5 】

任意選択的に、前記 A U S F が U D M から取得した前記端末のローミング情報は、前記端末 S U P I に関連付けられた前記端末のローミング情報である。

10

20

30

40

50

【 0 1 3 6 】

いくつかの代替実施例では、前記 A A n F は H P L M N に位置し、及び / 又は、前記第 1 機器は V P L M N に位置する。

【 0 1 3 7 】

上記の実施例に基づき、本願の実施例は、通信方法をさらに提供する。図 9 は、本願の実施例の通信方法のフローチャート 5 であり、図 9 に示すように、前記方法は、以下のステップを含む。

【 0 1 3 8 】

ステップ 5 0 1 において、A F は第 1 機器又は A A n F に第 1 メッセージを送信し、前記第 1 メッセージは鍵 K_{A F} を取得するためのものである。

10

【 0 1 3 9 】

ステップ 5 0 2 において、前記第 1 機器又は前記 A A n F が前記 A F にサービスを提供できることをチェックした場合、前記 A F は、前記第 1 機器又は前記 A A n F から送信された第 2 メッセージを受信し、前記第 2 メッセージは少なくとも鍵 K_{A F} を含む。

【 0 1 4 0 】

いくつかの代替実施例では、前記 A A n F は、H P L M N に位置し、及び / 又は、前記第 1 機器は、V P L M N に位置し、及び / 又は、前記 A F は、V P L M N に位置する。

【 0 1 4 1 】

いくつかの代替実施例では、前記第 1 メッセージは、A - K I D 及び / 又は前記 A F の識別子を含む。

20

【 0 1 4 2 】

いくつかの代替実施例では、前記第 2 メッセージは、前記鍵 K_{A F} の有効時間情報、S U P I、G P S I のうちの少なくとも 1 つをさらに含む。

【 0 1 4 3 】

本実施例では、前記鍵 K_{A F} の有効時間情報は、鍵 K_{A F} の有効期間、又は鍵 K_{A F} の失効時間を表し、又は鍵 K_{A F} e x p i r a t i o n t i m e と表示してもよい。

【 0 1 4 4 】

本願の実施例は、通信方法をさらに提供する。図 1 0 は、本願の実施例の通信方法のフローチャート 6 であり、図 1 0 に示すように、前記方法は、以下のステップを含む。

【 0 1 4 5 】

ステップ 6 0 1 において、A U S F は U D M から認証関連情報を取得し、前記認証関連情報は、

30

端末に対して A K M A 鍵材料を生成する必要があることを表す第 3 指示情報、端末に対して A K M A 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末のルーティング識別子 (R I D : R o u t e r I D) 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 1 4 6 】

本実施例では、A U S F 及び U D M は、いずれもホームネットワーク (H P L M N) に位置する。端末と A U S F との間の認証プロセスにおいて、A U S F は、当該端末に関連付けられた認証要求を U D M に送信し、前記認証要求は端末識別子を含み得、U D M は、当該認証要求内の端末識別子に基づいてチェックを行い、前記端末の認証関連情報 (又は認証情報) を決定し、認証応答を介して A U S F に当該認証関連情報を送信することができる。

40

【 0 1 4 7 】

本実施例では、A U S F は、上記の第 3 指示情報に基づいて、端末に対して A K M A 鍵材料を生成する必要があると決定することができ、例えば、K_{A U S F} から K_{A K M A} 及び A - K I D を導出する。又は、A U S F は、第 4 指示情報に基づいて、端末に対して A K M A 鍵材料を生成する必要があると決定することができる。

【 0 1 4 8 】

ここで、任意選択的に、前記端末識別子は、S U P I 及び / 又は購読秘匿化識別子 (S

50

UCI: Subscription Concealed Identifier)であってもよい。

【0149】

いくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第1指示情報、端末がローミング状態にないことを表す第2指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも1つを含む。

【0150】

本実施例では、端末がローミング状態にない場合、即ち、端末がホームネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にないことを表す第2指示情報を含んでもよい。端末がローミング状態にある場合、即ち、端末が訪問ネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にあることを表す第1指示情報、ローミング先情報、前記端末のローミング先での契約情報、及び前記端末のローミング先でのポリシー情報のうちの少なくとも1つの情報を含んでもよい。

10

【0151】

ここで、前記ローミング先情報は、ローミング先ネットワーク（又は訪問ネットワーク）を指示する情報であってもよく、例えば、ローミング先ネットワーク名/識別子など、例えば、SN nameであってもよい。

【0152】

上記の端末のローミング先での契約情報は、具体的には、端末とローミング先とのサービス契約リスト、端末とローミング先との契約ポリシーなどを含んでもよい。

20

【0153】

上記の端末のローミング先でのポリシー情報は、具体的には、ホームネットワークが当該端末の訪問先でのAKMAサービス使用を許可するか否か、訪問ネットワークが当該端末のAKMAサービス使用を許可するか否か、ホームネットワークと訪問ネットワーク間のサービスプロトコル、ホームネットワークの正当な監視ポリシー、訪問ネットワークの正当な監視ポリシーなどを含んでもよい。

【0154】

いくつかの代替実施例では、前記通信方法は、前記AUSFが、AAnFに第3メッセージを送信するステップをさらに含み、前記第3メッセージは、鍵を登録するためのものであり、前記第3メッセージは、

30

A-KID、KAKMA、SUP I、前記端末のローミング情報のうちの少なくとも1つを含む。

【0155】

上記の実施例に基づき、本願の実施例は、通信方法をさらに提供する。図11は、本願の実施例の通信方法のフローチャート7であり、図11に示すように、前記方法は、以下のステップを含む。

【0156】

ステップ701において、UDMはAUSFに認証関連情報を送信し、前記認証関連情報は、

40

端末に対してAKMA鍵材料を生成する必要があることを表す第3指示情報、前記端末に対してAKMA鍵材料を生成する必要があることを表す第4指示情報、前記端末のRID情報、前記端末のローミング情報のうちの少なくとも1つを含む。

【0157】

本実施例では、AUSF及びUDMは、いずれもホームネットワーク（HPLMN）に位置する。端末とAUSFとの間の認証プロセスにおいて、AUSFは、当該端末に関連付けられた認証要求をUDMに送信し、前記認証要求は端末識別子を含み得、UDMは、当該認証要求内の端末識別子に基づいてチェックを行い、前記端末の認証関連情報（又は認証情報）を決定し、認証応答を介してAUSFに当該認証関連情報を送信することができる。

50

【 0 1 5 8 】

ここで、任意選択的に、前記端末識別子は、S U P I 及び / 又は S U C I であってもよい。

【 0 1 5 9 】

いくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む。

【 0 1 6 0 】

本実施例では、端末がローミング状態にない場合、即ち、端末がホームネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にないことを表す第 2 指示情報を含んでもよい。端末がローミング状態にある場合、即ち、端末が訪問ネットワーク内にある場合、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、ローミング先情報、前記端末のローミング先での契約情報、及び前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つの情報を含んでもよい。

【 0 1 6 1 】

ここで、前記ローミング先情報は、ローミング先ネットワーク（又は訪問ネットワーク）を指示する情報であってもよく、例えば、ローミング先ネットワーク名 / 識別子など、例えば、S N n a m e であってもよい。

【 0 1 6 2 】

上記の端末のローミング先での契約情報は、具体的には、端末とローミング先とのサービス契約リスト、端末とローミング先との契約ポリシーなどを含んでもよい。

【 0 1 6 3 】

上記の端末のローミング先でのポリシー情報は、具体的には、ホームネットワークが当該端末の訪問先での A K M A サービス使用を許可するか否か、訪問ネットワークが当該端末の A K M A サービス使用を許可するか否か、ホームネットワークと訪問ネットワーク間のサービスプロトコル、ホームネットワークの正当な監視ポリシー、訪問ネットワークの正当な監視ポリシーなどを含んでもよい。

【 0 1 6 4 】

いくつかの代替実施例では、前記通信方法は、前記 U D M が A A n F から送信された第 4 メッセージを受信するステップであって、前記第 4 メッセージは、端末のローミング情報を要求するためのものである、ステップと、前記 U D M が前記 A A n F に第 5 メッセージを送信するステップであって、前記第 5 メッセージは前記端末のローミング情報を含む、ステップと、をさらに含む。

【 0 1 6 5 】

以下では、具体的な例を参照して、本願の実施例の通信方法について詳細に説明する。

【 0 1 6 6 】

例 1 について

図 1 2 は、本願の実施例の通信方法のインタラクションフローチャート 1 であり、図 1 2 に示すように、前記方法は、以下のステップを含む。

【 0 1 6 7 】

ステップ 8 0 1 において、U E と A U S F との間のマスター認証プロセスにおいて、A U S F は U D M に U E 認証要求を送信し、前記 U E 認証要求は U E 識別子を含んでもよい。

【 0 1 6 8 】

ここで、U E 識別子は、S U P I 及び / 又は S U C I を含んでもよい。

【 0 1 6 9 】

ステップ 8 0 2 において、U D M は A U S F に U E 認証応答を送信し、前記 U E 認証応答は、購読（subscription）証明書（例えば、A K A 認証ベクトル）及び認証方法を含んでもよい。

10

20

30

40

50

【 0 1 7 0 】

ここで、UDMは、AUSFにAKMA指示(AKMA Ind)(即ち、AUSFがUEに対してAKMA鍵材料を生成する必要があるか否かを指示し、例えば、A-KID及びKAKMAを含む)及びUEのRID情報を返すことに加えて、UEのローミング情報(即ち、端末のローミング情報)、例えば、UEがローミング状態にあることを表す第1指示情報、UEがローミング状態にないことを表す第2指示情報、ローミング先情報(ローミング先の識別子又は名称など)、前記UEのローミング先での契約情報、前記UEのローミング先でのポリシー情報などを搬送することもできる。

【 0 1 7 1 】

ステップ803において、AUSFは、UDMから受信したAKMA指示に基づいて、AUSFは、マスター認証プロセスが正常に完了した後、鍵KAUSFからKAKMA及びA-KIDを導出する。これに対応して、UEは、鍵KAUSFからKAKMA及びA-KIDを導出する。

10

【 0 1 7 2 】

ステップ804において、AUSFは、ホームネットワークのAAnFをアドレッシングし、当該AAnFに鍵登録要求を送信し、当該要求メッセージは、A-KID、KAKMA、及びUEのSUPIを搬送することができ、当該UEのローミング情報(即ち、端末のローミング情報)、例えば、UEがローミング状態にあることを表す第1指示情報、UEがローミング状態にないことを表す第2指示情報、ローミング先情報(ローミング先の識別子又は名称など)、前記UEのローミング先での契約情報、前記UEのローミング先でのポリシー情報などを搬送することもできる。

20

【 0 1 7 3 】

ステップ805において、AAnFは、AUSFに鍵登録応答を送信する。

【 0 1 7 4 】

ステップ806において、UEは、AFと通信を確立し、UEは、AFにアプリケーションセッション確立要求(Application Session Establishment Request)を送信し、当該要求メッセージは、A-KIDを含んでもよい。

【 0 1 7 5 】

ステップ807aにおいて、訪問ネットワーク内に第1機器が配置された場合において、AF内にA-KIDに関連付けられたAKMAコンテキストがない場合、AFは、ローカル構成又はポリシーに従って、又は他のネットワーク要素(NRFなど)から取得したポリシーに従って、ローカルに配置された第1機器をアドレッシングし、第1機器に鍵取得要求を送信し、第1機器は、当該鍵取得要求を受信した後、AAnFに当該鍵取得要求を送信し、当該要求メッセージは、A-KID及びAFの識別子(AF ID)を搬送することができる。

30

【 0 1 7 6 】

ステップ807bにおいて、訪問ネットワーク内に第1機器が配置されていない場合において、AF内にA-KIDに関連付けられたAKMAコンテキストがない場合、AFは、ローカル構成又はポリシーに従って、又は他のネットワーク要素(NRFなど)から取得したポリシーに従って、ホームネットワークのAAnFをアドレッシングすることを選択し、AAnFに鍵取得要求を送信し、当該要求メッセージは、A-KID及びAFの識別子(AF ID)を搬送することができる。

40

【 0 1 7 7 】

ステップ808において、AAnFに鍵KAFがない場合、KAKMAに基づいてAKMAアプリケーション鍵(KAF)を導出する。

【 0 1 7 8 】

ステップ809aにおいて、訪問ネットワーク内に第1機器が配置された場合、AAnFは、第1機器に鍵取得応答を送信し、第1機器は、当該鍵取得応答を受信した後、AFに当該鍵取得応答を送信し、当該応答メッセージは、鍵KAF、鍵KAFの有効時間情報

50

(ライフサイクルなど)、及びS U P Iを搬送することができる。

【0179】

ステップ809bにおいて、訪問ネットワーク内に第1機器が配置されていない場合、A A n Fは、A Fに鍵取得応答を送信し、当該応答メッセージは、鍵K_{A F}、鍵K_{A F}の有効時間情報(ライフサイクルなど)、及びS U P Iを搬送することができる。

【0180】

本例では、A A n Fは、構成されたローカルポリシーに従って、又はN R Fによって提供される認可情報又はポリシーに従って、A F I Dを使用して、A A n FがA Fにサービスを提供できるか否かをチェックし、又はA F I Dを使用し、U Eのローミング情報(例えば、U Eのローミング先での契約情報及び/又はU Eのローミング先でのポリシー情報)と結合して、A A n FがA Fにサービスを提供できるか否かをチェックする。A Fにサービスを提供できると決定した場合、ステップ808及び以降のプロセスを実行する。そうでなければ、A A n Fは、ステップ808及び以降のプロセスの実行を拒否する。

10

【0181】

ステップ810において、A Fは、U Eにアプリケーションセッション確立応答(Application Session Establishment Response)を送信する。

【0182】

例2について

図13は、本願の実施例の通信方法のインタラクションフローチャート2であり、図13に示すように、前記方法は、以下のステップを含む。

20

【0183】

ステップ901において、U EとA U S Fとの間のマスター認証プロセスにおいて、A U S Fは、U D MにU E認証要求を送信し、前記U E認証要求はU E識別子を含んでもよい。

【0184】

ここで、U E識別子は、S U P I及び/又はS U C Iを含んでもよい。

【0185】

ステップ902において、U D Mは、A U S FにU E認証応答を送信し、前記U E認証応答は、購読証明書(例えば、A K A認証ベクトル)及び認証方法を含んでもよい。

30

【0186】

ここで、U D Mは、A U S FにA K M A指示(A K M A I n d)(即ち、A U S FがU Eに対してA K M A鍵材料を生成する必要があるか否かを指示し、例えば、A - K I D及びK_{A K M A}などを含む)及びU EのR I D情報を返すことに加えて、U Eのローミング情報(即ち、端末のローミング情報)、例えば、U Eがローミング状態にあることを表す第1指示情報、U Eがローミング状態にないことを表す第2指示情報、ローミング先情報(ローミング先の識別子又は名称など)、前記U Eのローミング先での契約情報、前記U Eのローミング先でのポリシー情報などを搬送することもできる。

【0187】

ステップ903において、A U S Fは、U D Mから受信したA K M A指示に基づいて、A U S Fは、マスター認証プロセスが正常に完了した後、鍵K_{A U S F}からK_{A K M A}及びA - K I Dを導出する。これに対応して、U Eは、鍵K_{A U S F}からK_{A K M A}及びA - K I Dを導出する。

40

【0188】

ステップ904において、A U S Fは、ホームネットワークのA A n Fをアドレッシングし、当該A A n Fに鍵登録要求を送信し、当該要求メッセージは、A - K I D、K_{A K M A}、及びU EのS U P Iを搬送することができ、当該U Eのローミング情報(即ち、端末のローミング情報)、例えば、U Eがローミング状態にあることを表す第1指示情報、U Eがローミング状態にないことを表す第2指示情報、ローミング先情報(ローミング先の識別子又は名称など)、前記U Eのローミング先での契約情報、前記U Eのローミング

50

先でのポリシー情報などを搬送することもできる。

【0189】

ステップ905において、AAnFは、AUSFに鍵登録応答を送信する。

【0190】

ステップ906において、AAnFは、ローカルポリシーに従って、第1機器に当該UEのAKMAコンテキスト情報を送信し、前記AKMAコンテキスト情報は、A-KID、KAKMAなどを含む。

【0191】

ここで、ステップ906は、ステップ905の前に完了してもよく、又はステップ905と同時に実行してもよい。

【0192】

ステップ907において、UEは、AFと通信を確立し、UEは、AFにアプリケーションセッション確立要求(Application Session Establishment Request)を送信し、当該要求メッセージは、A-KIDを含んでもよい。

【0193】

ステップ908において、AKMA AF内にA-KIDに関連付けられたAKMAコンテキストがない場合、AFは、ローカル構成又はポリシーに従って、又は他のネットワーク要素(NRFなど)から取得したポリシーに従って、ローカルに配置された第1機器をアドレッシングし、第1機器に鍵取得要求を送信し、当該要求メッセージは、A-KID及びAFの識別子(AF ID)を搬送することができる。

【0194】

ステップ909において、第1機器は、構成されたローカルポリシーに従って、又はNRFによって提供される認可情報又はポリシーに従って、AF IDを使用して、第1機器がAFにサービスを提供できるか否かをチェックする。AFにサービスを提供できると決定した場合、後続のプロセスを実行し、そうでなければ、第1機器は、後続のプロセスの実行を拒否する。第1機器に鍵KAFがない場合、KAKMAに基づいてAKMAアプリケーション鍵(KAF)を導出する。

【0195】

ステップ910において、第1機器は、AFに鍵取得応答を送信し、当該応答メッセージは、鍵KAF、鍵KAFの有効時間情報(ライフサイクルなど)、及びSUP Iを搬送することができる。

【0196】

ステップ911において、AFは、UEにアプリケーションセッション確立応答(Application Session Establishment Response)を送信する。

【0197】

例3について

図14は、本願の実施例の通信方法のインタラクションフローチャート3であり、図14に示すように、前記方法は、以下のステップを含む。

【0198】

ステップ1001において、UEとAUSFとの間のマスター認証プロセスにおいて、AUSFは、UDMにUE認証要求を送信し、前記UE認証要求はUE識別子を含んでもよい。

【0199】

ここで、UE識別子は、SUP I及び/又はSUC Iを含んでもよい。

【0200】

ステップ1002において、UDMは、AUSFにUE認証応答を送信し、前記UE認証応答は、購読証明書(例えば、AKA認証ベクトル)及び認証方法を含んでもよい。

【0201】

10

20

30

40

50

ここで、UDMは、AUSFにAKMA指示(AKMA Ind)(即ち、AUSFがUEに対してAKMA鍵材料を生成する必要があるか否かを指示し、例えば、A-KID及びKAKMAなどを含む)及びUEのRID情報を返すことに加えて、UEのローミング情報(即ち、端末のローミング情報)、例えば、UEがローミング状態にあることを表す第1指示情報、UEがローミング状態にないことを表す第2指示情報、ローミング先情報(ローミング先の識別子又は名称など)、前記UEのローミング先での契約情報、前記UEのローミング先でのポリシー情報などを搬送することもできる。

【0202】

ステップ1003において、AUSFは、UDMから受信したAKMA指示に基づいて、AUSFは、マスター認証プロセスが正常に完了した後、鍵KAUSFからKAKMA及びA-KIDを導出する。これに対応して、UEは、鍵KAUSFからKAKMA及びA-KIDを導出する。

10

【0203】

ステップ1004において、AUSFは、ホームネットワークのAAnFをアドレッシングし、当該AAnFに鍵登録要求を送信し、当該要求メッセージは、A-KID、KAKMA、及びUEのSUP Iを搬送することができ、当該UEのローミング情報(即ち、端末のローミング情報)、例えば、UEがローミング状態にあることを表す第1指示情報、UEがローミング状態にないことを表す第2指示情報、ローミング先情報(ローミング先の識別子又は名称など)、前記UEのローミング先での契約情報、前記UEのローミング先でのポリシー情報などを搬送することもできる。

20

【0204】

ステップ1005において、AAnFは、AUSFに鍵登録応答を送信する。

【0205】

ステップ1006において、UEは、AFと通信を確立し、UEは、AFにアプリケーションセッション確立要求(Application Session Establishment Request)を送信し、当該要求メッセージは、A-KIDを含んでもよい。

【0206】

ステップ1007aにおいて、訪問ネットワーク内に第1機器が配置された場合において、AF内にA-KIDに関連付けられたAKMAコンテキストがない場合、AFは、ローカル構成又はポリシーに従って、又は他のネットワーク要素(NRFなど)から取得したポリシーに従って、ローカルに配置された第1機器をアドレッシングし、第1機器に鍵取得要求を送信し、第1機器は、当該鍵取得要求を受信した後、AAnFに当該鍵取得要求を送信し、当該要求メッセージは、A-KID及びAFの識別子(AF ID)を搬送することができる。

30

【0207】

ステップ1007bにおいて、訪問ネットワーク内に第1機器が配置されていない場合において、AF内にA-KIDに関連付けられたAKMAコンテキストがない場合、AFは、ローカル構成又はポリシーに従って、又は他のネットワーク要素(NRFなど)から取得したポリシーに従って、ホームネットワークのAAnFをアドレッシングすることを選択し、AAnFに鍵取得要求を送信し、当該要求メッセージは、A-KID及びAFの識別子(AF ID)を搬送することができる。

40

【0208】

ステップ1008～ステップ1009において、AAnFは、鍵取得要求を受信した後、UDMにローミング情報取得要求を送信し、要求メッセージはSUP Iが含まれ得、UDMは、SUP Iに基づいて対応するUEのローミング情報(即ち、端末のローミング情報)を照会して取得し、AAnFにローミング情報取得応答を送信し、当該応答メッセージは、UEのローミング情報(即ち、端末のローミング情報)を含む。

【0209】

ここで、UEのローミング情報(即ち、端末のローミング情報)は、UEがローミング

50

状態にあることを表す第 1 指示情報、UE がローミング状態にないことを表す第 2 指示情報、ローミング先情報（ローミング先の識別子又は名称など）、前記 UE のローミング先での契約情報、前記 UE のローミング先でのポリシー情報などを含んでもよい。

【0210】

ステップ 1010 において、AAnF に鍵 K_{AF} がない場合、 K_{AKMA} に基づいて A KMA アプリケーション鍵（ K_{AF} ）を導出する。

【0211】

ステップ 1011a において、訪問ネットワーク内に第 1 機器が配置された場合、AAnF は、第 1 機器に鍵取得応答を送信し、第 1 機器は、当該鍵取得応答を受信した後、AF に当該鍵取得応答を送信し、当該応答メッセージは、鍵 K_{AF} 、鍵 K_{AF} の有効時間情報（ライフサイクルなど）、及び SUP I を搬送することができる。 10

【0212】

ステップ 1011b において、訪問ネットワーク内に第 1 機器が配置されていない場合、AAnF は、AF に鍵取得応答を送信し、当該応答メッセージは、鍵 K_{AF} 、鍵 K_{AF} の有効時間情報（ライフサイクルなど）、及び SUP I を搬送することができる。

【0213】

本例では、AAnF は、構成されたローカルポリシーに従って、又は NRF によって提供される認可情報又はポリシーに従って、AF ID を使用して、AAnF が AF にサービスを提供できるか否かをチェックし、又は AF ID を使用し、UE のローミング情報（例えば、UE のローミング先での契約情報及び / 又は UE のローミング先でのポリシー情報）と結合して、AAnF が AF にサービスを提供できるか否かをチェックする。AF にサービスを提供できると決定した場合、ステップ 1010 及び以降のプロセスを実行する。そうでなければ、AAnF は、ステップ 1010 及び以降のプロセスの実行を拒否する。 20

【0214】

ステップ 1012 において、AF は、UE にアプリケーションセッション確立応答（Application Session Establishment Response）を送信する。

【0215】

上記の実施例に基づき、本願の実施例は、AAnF に適用される通信装置をさらに提供する。図 15 は、本願の実施例の通信装置の構成を示す模式図 1 であり、図 15 に示すように、前記装置は、第 1 通信ユニット 11 と、第 1 処理ユニット 12 と、を備え、 30

前記第 1 通信ユニット 11 は、アプリケーション機能（AF）から送信された第 1 メッセージを受信し、又は、第 1 機器を介して AF から送信された第 1 メッセージを受信するように構成され、前記第 1 メッセージは、鍵 K_{AF} を取得するためのものであり、

前記第 1 処理ユニット 12 は、前記 AF にサービスを提供できるか否かをチェックするように構成され、

前記第 1 通信ユニット 11 はさらに、前記第 1 処理ユニット 12 が前記 AF にサービスを提供できることをチェックした場合、前記 AF に第 2 メッセージを送信し、又は、前記第 1 機器を介して前記 AF に第 2 メッセージを送信するように構成され、前記第 2 メッセージは、少なくとも鍵 K_{AF} を含む。 40

【0216】

本願のいくつかの代替実施例では、前記 AAnF は、HPLMN に位置し、及び / 又は、前記第 1 機器は、VPLMN に位置し、及び / 又は、前記 AF は、VPLMN に位置する。

【0217】

本願のいくつかの代替実施例では、前記第 1 メッセージは、A-KID 及び / 又は前記 AF の識別子を含む。

【0218】

本願のいくつかの代替実施例では、前記第 1 処理ユニット 12 はさらに、 K_{AKMA} に 50

基づいて前記鍵 K_{AF} を導出するように構成される。

【0219】

本願のいくつかの代替実施例では、前記第2メッセージは、

前記鍵 K_{AF} の有効時間情報、 $SUPI$ 、 $GPSSI$ のうちの少なくとも1つをさらに含む。

【0220】

本願のいくつかの代替実施例では、前記第1通信ユニット11はさらに、 $AUSF$ から送信された第3メッセージを受信するように構成され、前記第3メッセージは、鍵を登録するためのものであり、前記第3メッセージは、 $A-KID$ 、 K_{AKMA} 、 $SUPI$ 、端末のローミング情報のうちの少なくとも1つを含む。

10

【0221】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第1指示情報、端末がローミング状態にないことを表す第2指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも1つを含む。

【0222】

本願のいくつかの代替実施例では、前記端末のローミング情報は、前記 $AUSF$ が UDM から取得したものである。

【0223】

本願のいくつかの代替実施例では、前記 $AUSF$ が UDM から取得した前記端末のローミング情報は、前記端末 $SUPI$ に関連付けられた前記端末のローミング情報である。

20

【0224】

本願のいくつかの代替実施例では、前記第1通信ユニット11はさらに、前記第1メッセージを受信した後、 UDM から端末のローミング情報を取得するように構成され、前記端末のローミング情報は、前記第1メッセージ内の $A-KID$ に対応する端末に関連する。

【0225】

本願のいくつかの代替実施例では、前記第1処理ユニット12は、前記端末のローミング情報に基づいて、前記 AF にサービスを提供できるか否かをチェックするように構成される。

30

【0226】

本願の実施例では、前記通信装置内の第1処理ユニット12は、実際の適用では、中央処理装置 (CPU : $Central\ Processing\ Unit$)、デジタル信号プロセッサ (DSP : $Digital\ Signal\ Processor$)、マイクロコントローラ (MCU : $Microcontroller\ Unit$) 又はフィールドプログラマブルゲートアレイ ($FPGA$: $Field-Programmable\ Gate\ Array$) によって実現でき、前記通信装置内の第1通信ユニット11は、実際の適用では、通信アセンブリ (基礎通信キット、オペレーティングシステム、通信モジュール、標準化インタフェース及びプロトコルを含む) 及びトランシーバアンテナと結合して実現できる。

40

【0227】

本願の実施例は、第1機器に適用される通信装置をさらに提供する。図16は、本願の実施例の通信装置の構成を示す模式図2であり、図16に示すように、前記装置は、第1受信ユニット21と、第1送信ユニット22と、を備え、

前記第1受信ユニット21は、 AF から送信された第1メッセージを受信し、前記第1メッセージを $AAnF$ に送信するように構成され、前記第1メッセージは、鍵 K_{AF} を取得するためのものであり、

前記第1送信ユニット22は、前記 $AAnF$ が前記 AF にサービスを提供できる場合、前記 $AAnF$ から送信された第2メッセージを受信し、前記第2メッセージを前記 AF に送信するように構成され、前記第2メッセージは、少なくとも前記鍵 K_{AF} を含む。

50

【 0 2 2 8 】

本願のいくつかの代替実施例では、前記 A A n F は、H P L M N に位置し、及び / 又は、前記第 1 機器は、V P L M N に位置し、及び / 又は、前記 A F は、V P L M N に位置する。

【 0 2 2 9 】

本願のいくつかの代替実施例では、前記第 1 メッセージは、A - K I D 及び / 又は前記 A F の識別子を含む。

【 0 2 3 0 】

本願のいくつかの代替実施例では、前記第 2 メッセージは、
前記鍵 K A F の有効時間情報、S U P I、G P S I のうちの少なくとも 1 つをさらに含む。 10

【 0 2 3 1 】

本願の実施例では、前記通信装置内の第 1 受信ユニット 2 1 及び第 1 送信ユニット 2 2 は、実際の適用では、通信アセンブリ（基礎通信キット、オペレーティングシステム、通信モジュール、標準化インタフェース及びプロトコルなどを含む）及びトランシーバアンテナと結合して実現できる。

【 0 2 3 2 】

本願の実施例は、第 1 機器に適用される通信装置をさらに提供する。図 1 7 は、本願の実施例の通信装置の構成を示す模式図 3 であり、図 1 7 に示すように、前記装置は、第 2 通信ユニット 3 1 と、第 2 処理ユニット 3 2 と、を備え、 20

前記第 2 通信ユニット 3 1 は、A F から送信された第 1 メッセージを受信するように構成され、前記第 1 メッセージは、鍵 K A F を取得するためのものであり、

前記第 2 処理ユニット 3 2 は、前記 A F にサービスを提供できるか否かをチェックするように構成され、

前記第 2 通信ユニット 3 1 はさらに、前記第 2 処理ユニット 3 2 が前記 A F にサービスを提供できることをチェックした場合、前記 A F に第 2 メッセージを送信するように構成され、前記第 2 メッセージは、少なくとも前記鍵 K A F を含む。

【 0 2 3 3 】

本願のいくつかの代替実施例では、前記第 1 メッセージは、A - K I D 及び / 又は前記 A F の識別子を含む。 30

【 0 2 3 4 】

本願のいくつかの代替実施例では、前記第 2 通信ユニット 3 1 はさらに、A A n F から送信された第 1 情報を受信するように構成され、前記第 1 情報は、A K M A コンテキスト情報を含む。

【 0 2 3 5 】

本願のいくつかの代替実施例では、前記第 1 情報は、A - K I D、K A K M A、S U P I のうちの少なくとも 1 つを含む。

【 0 2 3 6 】

本願のいくつかの代替実施例では、前記第 2 処理ユニット 3 2 はさらに、K A K M A に基づいて前記鍵 K A F を導出するように構成される。 40

【 0 2 3 7 】

本願のいくつかの代替実施例では、前記 A A n F は、H P L M N に位置し、及び / 又は、前記第 1 機器は、V P L M N に位置し、及び / 又は、前記 A F は、V P L M N に位置する。

【 0 2 3 8 】

本願の実施例では、前記通信装置内の第 2 処理ユニット 3 2 は、実際の適用では、C P U、D S P、M C U 又は F P G A によって実現でき、前記通信装置内の第 2 通信ユニット 3 1 は、実際の適用では、通信アセンブリ（基礎通信キット、オペレーティングシステム、通信モジュール、標準化インタフェース及びプロトコルなどを含む）及びトランシーバアンテナと結合して実現できる。 50

【 0 2 3 9 】

本願の実施例は、A A n F に適用される通信装置をさらに提供する。図 1 8 は、本願の実施例の通信装置の構成を示す模式図 4 であり、図 1 8 に示すように、前記装置は、第 2 送信ユニット 4 1 を備え、前記第 2 送信ユニット 4 1 は、第 1 機器に第 1 情報を送信するように構成され、前記第 1 情報は、A K M A コンテキスト情報を含む。

【 0 2 4 0 】

本願のいくつかの代替実施例では、前記第 1 情報は、A - K I D、K A K M A、S U P I のうちの少なくとも 1 つを含む。

【 0 2 4 1 】

本願のいくつかの代替実施例では、前記通信装置は、第 2 受信ユニット 4 2 をさらに備え、前記第 2 受信ユニット 4 2 は、A U S F から送信された第 3 メッセージを受信するように構成され、前記第 3 メッセージは、鍵を登録するためのものであり、前記第 3 メッセージは、A - K I D、K A K M A、S U P I、端末のローミング情報のうちの少なくとも 1 つを含む。

【 0 2 4 2 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含む。

【 0 2 4 3 】

本願のいくつかの代替実施例では、前記端末のローミング情報は、前記 A U S F が U D M から取得したものである。

【 0 2 4 4 】

本願のいくつかの代替実施例では、前記 A U S F が U D M から取得した前記端末のローミング情報は、前記端末 S U P I に関連付けられた前記端末のローミング情報である。

【 0 2 4 5 】

本願のいくつかの代替実施例では、前記 A A n F は、H P L M N に位置し、及び / 又は、前記第 1 機器は、V P L M N に位置する。

【 0 2 4 6 】

本願の実施例では、前記通信装置内の第 2 受信ユニット 4 2 及び第 2 送信ユニット 4 1 は、実際の適用では、通信アセンブリ（基礎通信キット、オペレーティングシステム、通信モジュール、標準化インタフェース及びプロトコルなどを含む）及びトランシーバアンテナと結合して実現できる。

【 0 2 4 7 】

本願の実施例は、A F に適用される通信装置をさらに提供する。図 1 9 は、本願の実施例の通信装置の構成を示す模式図 5 であり、図 1 9 に示すように、前記装置は、第 3 送信ユニット 5 1 と、第 3 受信ユニット 5 2 と、を備え、

前記第 3 送信ユニット 5 1 は、第 1 機器又は A A n F に第 1 メッセージを送信するように構成され、前記第 1 メッセージは、鍵 K A F を取得するためのものであり、

前記第 3 受信ユニット 5 2 は、前記第 1 機器又は前記 A A n F が前記 A F にサービスを提供できることをチェックした場合、前記第 1 機器又は前記 A A n F から送信された第 2 メッセージを受信するように構成され、前記第 2 メッセージは、少なくとも鍵 K A F を含む。

【 0 2 4 8 】

本願のいくつかの代替実施例では、前記 A A n F は、H P L M N に位置し、及び / 又は、前記第 1 機器は、V P L M N に位置し、及び / 又は、前記 A F は、V P L M N に位置する。

【 0 2 4 9 】

本願のいくつかの代替実施例では、前記第 1 メッセージは、A - K I D 及び / 又は前記 A F の識別子を含む。

【0250】

本願のいくつかの代替実施例では、前記第2メッセージは、
前記鍵 K_{AF} の有効時間情報、 $SUPI$ 、 $GPSI$ のうちの少なくとも1つをさらに含む。

【0251】

本願の実施例では、前記通信装置内の第3受信ユニット52及び第3送信ユニット51は、実際の適用では、通信アセンブリ（基礎通信キット、オペレーティングシステム、通信モジュール、標準化インタフェース及びプロトコルなどを含む）及びトランシーバアンテナと結合して実現できる。

【0252】

本願の実施例は、 $AUSF$ に適用される通信装置をさらに提供する。図20は、本願の実施例の通信装置の構成を示す模式図6であり、図20に示すように、前記装置は、第4受信ユニット61を備え、前記第4受信ユニット61は、 UDM から認証関連情報を取得するように構成され、前記認証関連情報は、端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第3指示情報、端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第4指示情報、前記端末の RID 情報、前記端末のローミング情報のうちの少なくとも1つを含む。

10

【0253】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第1指示情報、端末がローミング状態にないことを表す第2指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも1つを含む。

20

【0254】

本願のいくつかの代替実施例では、前記通信装置は、第4送信ユニット62をさらに備え、前記第4送信ユニット62は、 $AAnF$ に第3メッセージを送信するように構成され、前記第3メッセージは、鍵を登録するためのものであり、前記第3メッセージは、 $AKID$ 、 K_{AKMA} 、 $SUPI$ 、前記端末のローミング情報のうちの少なくとも1つを含む。

【0255】

本願の実施例では、前記通信装置内の第4受信ユニット61及び第4送信ユニット62は、実際の適用では、通信アセンブリ（基礎通信キット、オペレーティングシステム、通信モジュール、標準化インタフェース及びプロトコルなどを含む）及びトランシーバアンテナと結合して実現できる。

30

【0256】

本願の実施例は、 UDM に適用される通信装置をさらに提供する。図21は、本願の実施例の通信装置の構成を示す模式図7であり、図21に示すように、前記装置は、第5送信ユニット71を備え、前記第5送信ユニット71は、 $AUSF$ に認証関連情報を送信するように構成され、前記認証関連情報は、端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第3指示情報、前記端末に対して $AKMA$ 鍵材料を生成する必要があることを表す第4指示情報、前記端末の RID 情報、前記端末のローミング情報のうちの少なくとも1つを含む。

40

【0257】

本願のいくつかの代替実施例では、前記端末のローミング情報は、端末がローミング状態にあることを表す第1指示情報、端末がローミング状態にないことを表す第2指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも1つを含む。

【0258】

本願のいくつかの代替実施例では、前記通信装置は、第5受信ユニット72をさらに備え、前記第5受信ユニット72は、 $AAnF$ から送信された第4メッセージを受信するステップであって、前記第4メッセージは、端末のローミング情報を要求するためのもので

50

ある、ステップと、

前記 U D M が、前記 A A n F に第 5 メッセージを送信するステップであって、前記第 5 メッセージは、前記端末のローミング情報を含む、ステップと、を実行するように構成される。

【 0 2 5 9 】

本願の実施例では、前記通信装置内の第 5 受信ユニット 7 2 及び第 5 送信ユニット 7 1 は、実際の適用では、通信アセンブリ（基礎通信キット、オペレーティングシステム、通信モジュール、標準化インタフェース及びプロトコルなどを含む）及びトランシーバアンテナと結合して実現できる。

【 0 2 6 0 】

説明すべきこととして、上記の実施例によって提供される通信装置が通信を行うとき、上記の各プログラムモジュールの分割のみを例に挙げて説明したが、実際の適用では、必要に応じて上記の処理を異なるプログラムモジュールに割り当てて完了してもよく、即ち、装置の内部構造を異なるプログラムモジュールに分割して、上記の処理のすべて又は一部を完了することができる。また、上記の実施例によって提供される通信装置は、通信方法の実施例と同じ構想に属し、この具体的な実現プロセスについては方法の実施例を参照することができ、ここでは繰り返して説明しない。

【 0 2 6 1 】

本願の実施例は、通信機器をさらに提供し、前記通信機器は、例えば、A A n F、第 1 機器、A F、A U S F 又は U D M であってもよい。図 2 2 は、本願の実施例の通信機器のハードウェア構成を示す模式図であり、図 2 2 に示すように、前記通信機器は、メモリ 8 2 と、プロセッサ 8 1 と、メモリ 8 2 に記憶され、プロセッサ 8 1 で実行可能なコンピュータプログラムと、を備え、前記プロセッサ 8 1 は、前記プログラムを実行するときに、本願の実施例に係る A A n F に適用される通信方法のステップ、又は、本願の実施例に係る第 1 機器に適用される通信方法のステップ、又は、本願の実施例に係る A F に適用される通信方法のステップ、又は、本願の実施例に係る A U S F に適用される通信方法のステップ、又は、本願の実施例に係る U D M に適用される通信方法のステップを実現する。

【 0 2 6 2 】

任意選択的に、通信機器は、1 つ又は複数のネットワークインタフェース 8 3 をさらに含んでもよい。ここで、通信機器内の各コンポーネントは、バスシステム 8 4 を介して結合される。理解可能なこととして、バスシステム 8 4 は、これらの構成要素間の接続通信を実現する。バスシステム 8 4 は、データバスに加えて、電力バス、制御バス及び状態信号バスを含む。しかしながら、説明を明確にするために、図 2 2 では、各種バスをすべてバスシステム 8 4 として表記している。

【 0 2 6 3 】

理解可能なこととして、メモリ 8 2 は、揮発性メモリ又は不揮発性メモリであってもよく、揮発性及び不揮発性メモリの両方を含んでもよい。ここで、不揮発性メモリは、読み取り専用メモリ（ROM：Read Only Memory）、プログラマブル読み取り専用メモリ（PROM：Programmable Read-Only Memory）、消去可能なプログラマブル読み取り専用メモリ（EPROM：Erasable Programmable Read-Only Memory）、電氣的に消去可能なプログラマブル読み取り専用メモリ（EEPROM：Electrically Erasable Programmable Read-Only Memory）、磁気ランダムアクセスメモリ（FRAM（登録商標）：Ferromagnetic Random Access Memory）、フラッシュメモリ（Flash Memory）、磁気メモリ、コンパクトディスク、又は読み取り専用コンパクトディスク（CD-ROM：Compact Disc Read-Only Memory）であってもよく、磁気メモリは、磁気ディスクメモリ又は磁気テープメモリであってもよい。揮発性メモリは、外部キャッシュとして使用されるランダムアクセスメモリ（RAM：Random Access Memory）であってもよい。例示的であるが限定的ではない例示によ

10

20

30

40

50

れば、多くの形のRAM、例えば、静的ランダムアクセスメモリ（SRAM：Static Random Access Memory）、同期静的ランダムアクセスメモリ（SSRAM：Synchronous Static Random Access Memory）、ダイナミックランダムアクセスメモリ（DRAM：Dynamic Random Access Memory）、同期ダイナミックランダムアクセスメモリ（SDRAM：Synchronous Dynamic Random Access Memory）、ダブルデータレートの同期ダイナミックランダムアクセスメモリ（DDRSDRAM：Double Data Rate Synchronous Dynamic Random Access Memory）、拡張された同期ダイナミックランダムアクセスメモリ（ESDRAM：Enhanced Synchronous Dynamic Random Access Memory）、同期接続ダイナミックランダムアクセスメモリ（SLDRAM：SyncLink Dynamic Random Access Memory）、ダイレクトメモリバスランダムアクセスメモリ（DRRAM：Direct Rambus Random Access Memory）などが利用可能である。本願の実施例で説明されるメモリ82は、これら及び任意の他の適切なタイプのメモリを含むが、これらに限定されないことを意図している。

【0264】

本願の実施例で開示された上記の方法は、プロセッサ81に適用されてもよく、又はプロセッサ81によって実現されてもよい。プロセッサ81は、信号処理機能を備えた集積回路チップであってもよい。実現プロセスにおいて、上記の方法の各ステップは、プロセッサ81内のハードウェアの集積論理回路又はソフトウェアの形の命令によって完了されてもよい。上記のプロセッサ81は、汎用プロセッサ、DSP、又は他のプログラマブルロジックデバイス、ディスクリートゲート又はトランジスタロジックデバイス、ディスクリートハードウェアコンポーネントなどであってもよい。プロセッサ81は、本願の実施例で開示された各方法、ステップ及び論理ブロック図を実現又は実行することができる。汎用プロセッサは、マイクロプロセッサ、又は任意の従来のプロセッサなどであってもよい。本願の実施例で開示される方法のステップは、ハードウェア復号化プロセッサによって直接実行されてもよく、復号化プロセッサ内のハードウェアとソフトウェアモジュールの組み合わせによって実行されてもよい。ソフトウェアモジュールは記憶媒体に配置されてもよく、当該記憶媒体は、メモリ82に配置され、プロセッサ81は、メモリ82に記憶された情報を読み取って、そのハードウェアと組み合わせて上記の方法のステップを完了する。

【0265】

例示的な実施例では、通信機器は、上記の方法を実行するために、1つ又は複数の特定用途向け集積回路（ASIC：Application Specific Integrated Circuit）、DSP、プログラマブルロジックデバイス（PLD：Programmable Logic Device）、複合プログラマブルロジックデバイス（CPLD：Complex Programmable Logic Device）、FPGA、汎用プロセッサ、コントローラ、MCU、マイクロプロセッサ（Microprocessor）、又は他の電子素子によって実現されてもよい。

【0266】

例示的な実施例において、本願の実施例は、コンピュータプログラムを含むメモリ82などのコンピュータ可読記憶媒体をさらに提供し、前記コンピュータプログラムは、通信機器のプロセッサ81によって実行されることにより、上記の方法のステップを完了することができる。コンピュータ可読記憶媒体は、FRAM、ROM、PROM、EPROM、EEPROM、Flash Memory、磁気メモリ、光ディスク、又はCD-ROMなどのメモリであってもよいし、上記のメモリの1つ又は任意の組み合わせを含む様々な機器であってもよい。

【0267】

本願の実施例は、コンピュータプログラムが記憶されたコンピュータ可読記憶媒体をさ

らに提供し、前記プログラムはプロセッサによって実行されるときに、本願の実施例に係る A A n F に適用される通信方法のステップ、又は、本願の実施例に係る第 1 機器に適用される通信方法のステップ、又は、本願の実施例に係る A F に適用される通信方法のステップ、又は、本願の実施例に係る A U S F に適用される通信方法のステップ、又は、本願の実施例に係る U D M に適用される通信方法のステップを実現する。

【 0 2 6 8 】

本願で提供されるいくつかの方法の実施例で開示される方法は、矛盾することなく任意に組み合わせて、新しい方法の実施例を取得することができる。

【 0 2 6 9 】

本願で提供されるいくつかの製品の実施例で開示される特徴は、矛盾することなく任意に組み合わせて、新しい製品の実施例を取得することができる。

【 0 2 7 0 】

本願で提供されるいくつかの方法又は機器の実施例で開示される特徴は、矛盾することなく任意に組み合わせて、新しい方法の実施例又は機器の実施例を取得することができる。

【 0 2 7 1 】

本願で提供されるいくつかの実施例では、開示されたデバイス及び方法は、他の方式で実現できる。以上で説明された装置の実施例は、例示的なものに過ぎず、例えば、前記ユニットの分割は、論理機能の分割に過ぎず、実際の実現では、別の分割方法があってもよく、例えば、複数のユニット又はコンポーネントを組み合わせてもよく、別のシステムに統合してもよく、一部の特徴を無視してもよく、実行しなくてもよい。さらに、図示又は説明された各構成要素間の相互結合又は直接結合又は通信接続は、いくつかのインターフェース、デバイス又はユニットを介した間接結合又は通信接続であり得、電氣的、機械的又は他の形態であってもよい。

【 0 2 7 2 】

前記分離部材として説明されたユニットは、物理的に分離されてもされていなくてもよく、ユニットとして表示された部材は、物理ユニットである場合もそうでない場合もあり、1箇所に配置される場合もあれば、複数のネットワークユニットに分散される場合もあり、実際の必要に応じて、その一部又はすべてのユニットを選択して、本実施例の技術案の目的を実現することができる。

【 0 2 7 3 】

また、本発明の各実施例における各機能ユニットは、すべて1つの第2処理ユニットに統合されてもよく、各ユニットが個別に1つのユニットとして使用されてもよく、2つ以上のユニットが1つのユニットに統合されてもよい。前記統合されたユニットは、ハードウェアの形で、又はハードウェアとソフトウェア機能ユニットの組み合わせの形で具現することができる。

【 0 2 7 4 】

当業者は、上記した方法の実施例の全て又は一部のステップは、プログラム命令に関連するハードウェアによって完了することができ、前記プログラムは、コンピュータ可読記憶媒体に記憶されることができ、前記プログラムが実行されるとき、上記の方法の実施例のステップを実行し、前記記憶媒体は、リムーバブルストレージ、R O M、R A M、磁気メモリ又は光ディスクなどのプログラムコードを記憶することができる様々な媒体を含む。

【 0 2 7 5 】

又は、本願の上記の統合されたユニットは、ソフトウェア機能モジュールの形で実現され且つ独立した製品として販売又は使用される場合、コンピュータ可読記憶媒体に記憶されてもよい。このような理解に基づいて、本願の実施例の技術的解決策の本質的な部分、即ち先行技術に貢献のある部分は、ソフトウェア製品の形で具現されることができ、前記コンピュータソフトウェア製品は、1つの記憶媒体に記憶され、一台のコンピュータ機器（パーソナルコンピュータ、サーバ、又はネットワーク機器などであり得る）に本願の各

実施例に記載の方法の全部又は一部を実行させるためのいくつかの命令を含む。上記の記憶媒体は、リムーバブルストレージ、ROM、RAM、磁気メモリ又は光ディスクなどのプログラムコードを記憶することができる様々な媒体を含む。

【 0 2 7 6 】

上記の内容は、本願の実施形態に過ぎず、本願の保護範囲はこれに限定されない。本願で開示された技術的範囲内で、当業者が容易に想到し得る変形又は置換はすべて、本願の保護範囲内に含まれるべきである。したがって、本願の保護範囲は、特許請求の保護範囲に従うものとする。

【 図 面 】

【 図 1 】

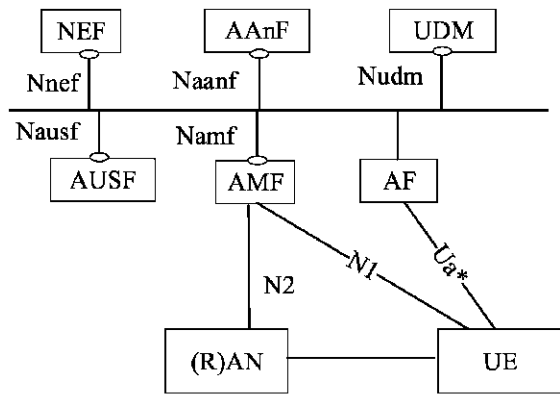
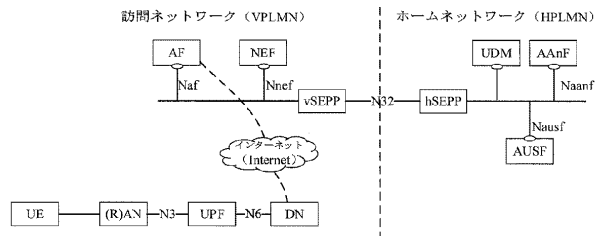


図 1

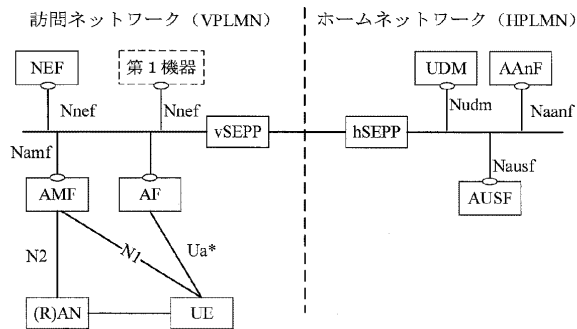
【 図 2 】



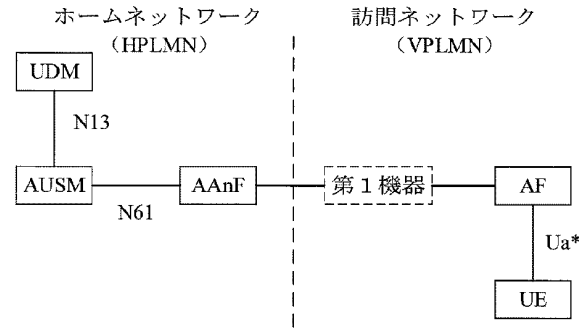
10

20

【 図 3 】



【 図 4 a 】

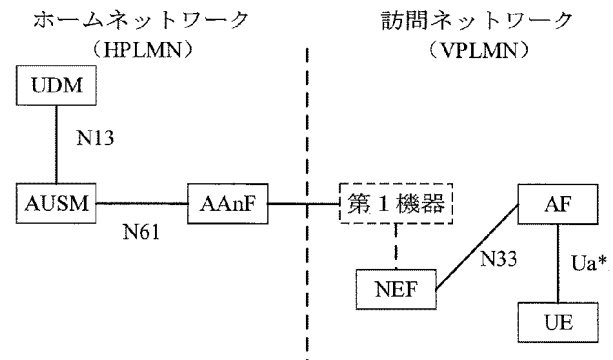


30

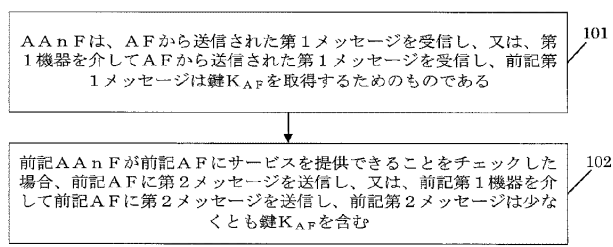
40

50

【図 4 b】

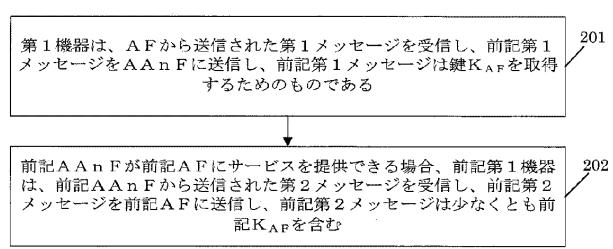


【図 5】

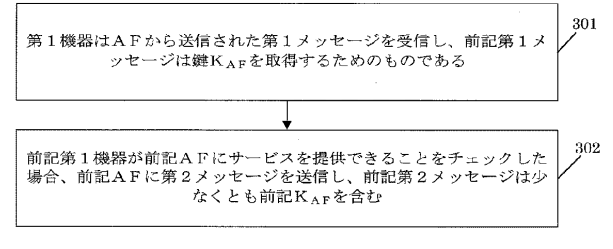


10

【図 6】

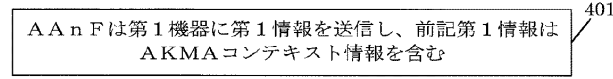


【図 7】

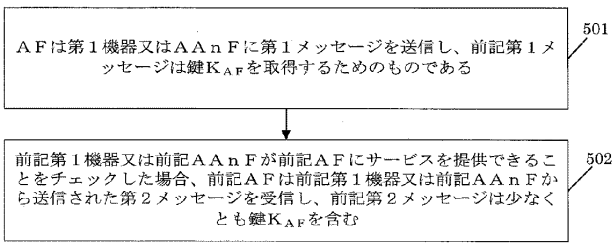


20

【図 8】



【図 9】



30

40

50

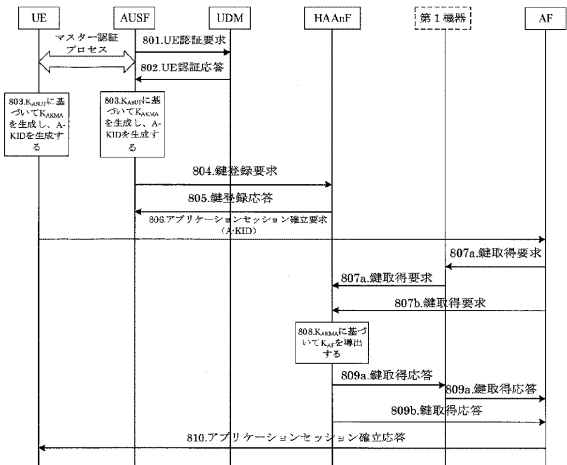
【図 10】

AUSFは、UDMから認証関連情報を取得し、前記認証関連情報は、端末に対してAKMA鍵材料を生成する必要があることを表す第3指示情報、端末に対してAKMA鍵材料を生成する必要があることを表す第4指示情報、前記端末のRID情報、前記端末のローミング情報のうちの少なくとも1つを含む

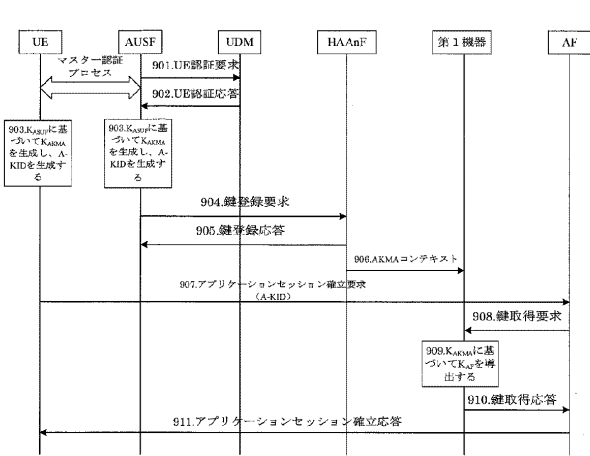
【図 11】

UDMは、AUSFに認証関連情報を送信し、前記認証関連情報は、端末に対してAKMA鍵材料を生成する必要があることを表す第3指示情報、前記端末に対してAKMA鍵材料を生成する必要があることを表す第4指示情報、前記端末のRID情報、前記端末のローミング情報のうちの少なくとも1つを含む

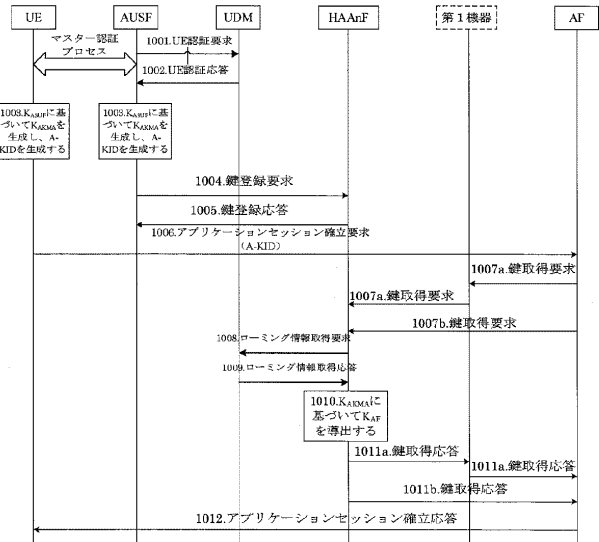
【図 12】



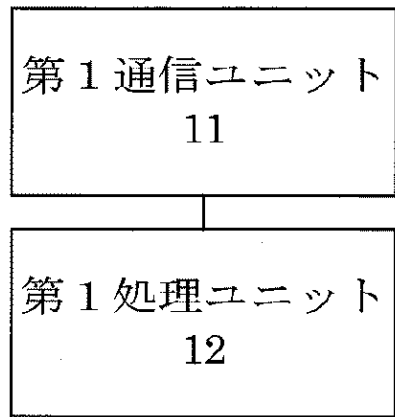
【図 13】



【図 14】



【図 15】



10

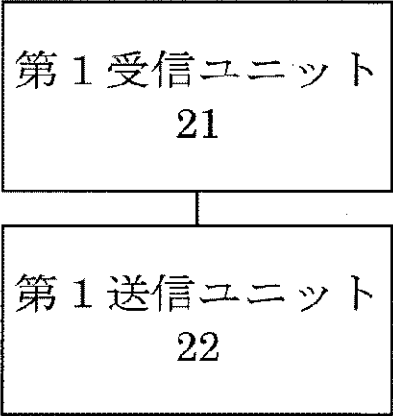
20

30

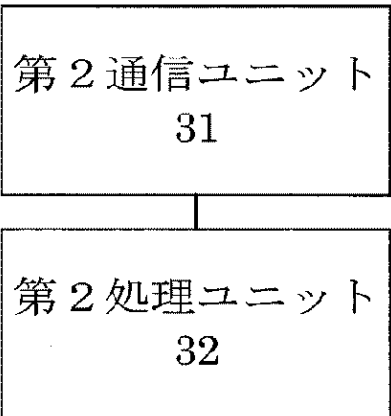
40

50

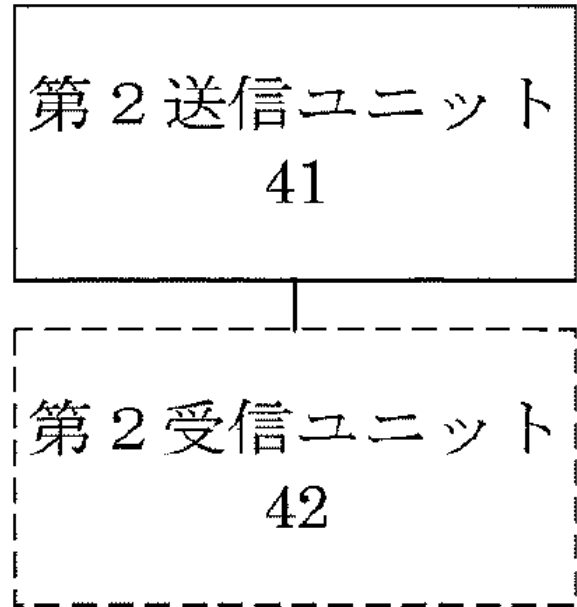
【図 16】



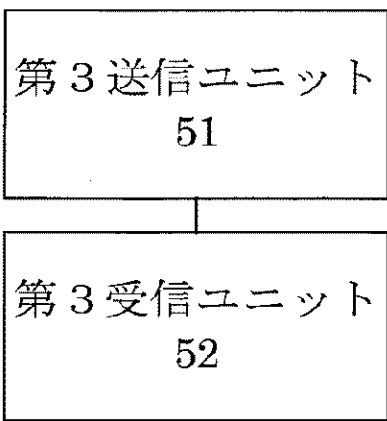
【図 17】



【図 18】



【図 19】



10

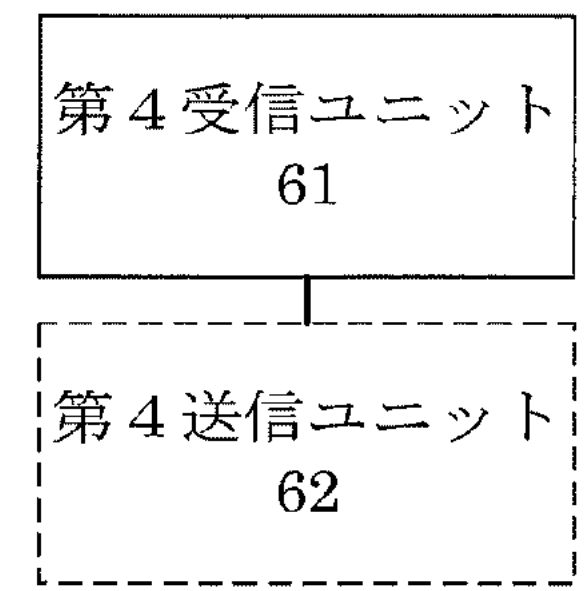
20

30

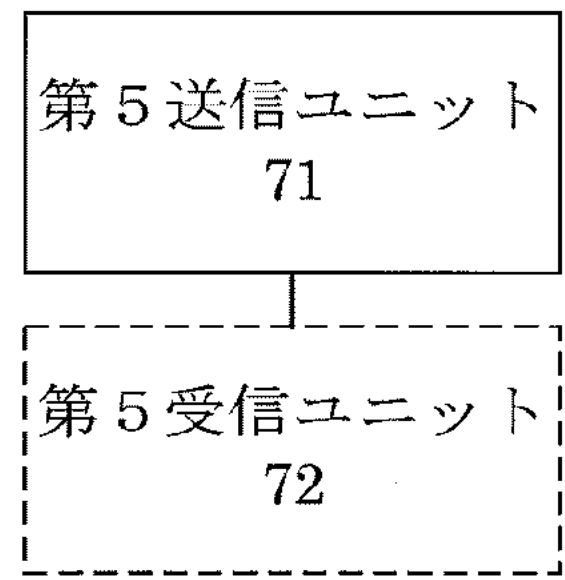
40

50

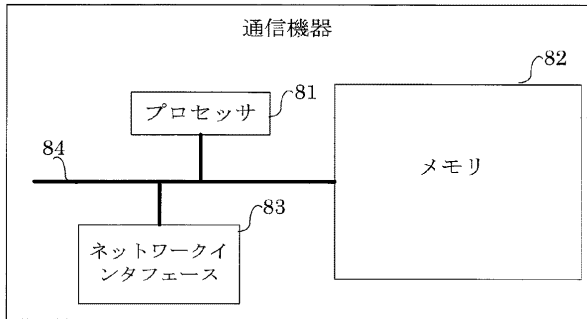
【図 2 0】



【図 2 1】



【図 2 2】



10

20

30

40

50

【手続補正書】

【提出日】令和7年1月22日(2025.1.22)

【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】

通信方法であって、

アプリケーションの認証と鍵管理(AKMA)アンカー機能(AAnF)が、アプリケーション機能(AF)から送信された第1メッセージを受信し、又は、第1機器を介してAFから送信された第1メッセージを受信するステップであって、前記第1メッセージは鍵K_{AF}を取得するためのものである、ステップと、

前記AAnFが前記AFにサービスを提供できることをチェックした場合、前記AFに第2メッセージを送信し、又は、前記第1機器を介して前記AFに第2メッセージを送信するステップであって、前記第2メッセージは少なくとも鍵K_{AF}を含む、ステップと、を含む、通信方法。

【請求項2】

前記AAnFはホームネットワーク(HPLMN)に位置し、及び/又は、前記第1機器は訪問ネットワーク(VPLMN)に位置し、及び/又は、前記AFは訪問ネットワーク(VPLMN)に位置し、

前記第1メッセージはAKMA鍵識別子(A-KID)及び/又は前記AFの識別子を含み、

前記第2メッセージは、

前記鍵K_{AF}の有効時間情報、

購読永久識別子(SUPI)、

一般公衆購読識別子(GPSI)のうちの少なくとも1つをさらに含む、

請求項1に記載の通信方法。

【請求項3】

前記通信方法は、

前記AAnFがAKMAアンカー鍵K_{AKMA}に基づいて前記鍵K_{AF}を導出するステップをさらに含む、

請求項1に記載の通信方法。

【請求項4】

前記通信方法は、

前記AAnFが認証サーバ機能(AUSF)から送信された第3メッセージを受信するステップをさらに含む、前記第3メッセージは鍵を登録するためのものであり、前記第3メッセージは、

A-KID、AKMAアンカー鍵K_{AKMA}、SUPI、端末のローミング情報のうちの少なくとも1つを含み、

前記端末のローミング情報は、

端末がローミング状態にあることを表す第1指示情報、端末がローミング状態にないことを表す第2指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも1つを含み、

前記端末のローミング情報は前記AUSFが統合データ管理(UDM)から取得したものであり、

前記AUSFがUDMから取得した前記端末のローミング情報は、前記端末SUPIに関連付けられた前記端末のローミング情報である、

請求項1に記載の通信方法。

10

20

30

40

50

【請求項 5】

前記第 1 メッセージを受信した後、前記通信方法は、

前記 A A n F が U D M から端末のローミング情報を取得するステップをさらに含み、前記端末のローミング情報は前記第 1 メッセージ内の A - K I D に対応する端末に関連する、

請求項 2 に記載の通信方法。

【請求項 6】

前記 A A n F が、前記 A F にサービスを提供できるか否かをチェックするステップは、

前記 A A n F が前記端末のローミング情報に基づいて前記 A F にサービスを提供できるか否かをチェックするステップを含む、

請求項 4 または 5 に記載の通信方法。

【請求項 7】

通信方法であって、

第 1 機器が、A F から送信された第 1 メッセージを受信するステップであって、前記第 1 メッセージは鍵 K_{A F} を取得するためのものである、ステップと、

前記第 1 機器が前記 A F にサービスを提供できることをチェックするステップ、または、前記第 1 機器が前記第 1 メッセージを A A n F に送信し、前記 A A n F が前記 A F にサービスを提供できる場合、前記第 1 機器が、前記 A A n F から送信された第 2 メッセージを受信するステップと、

前記第 1 機器が前記第 2 メッセージを前記 A F に送信するステップであって、前記第 2 メッセージは少なくとも前記鍵 K_{A F} を含む、ステップと、を含む、通信方法。

【請求項 8】

前記第 1 メッセージは A K M A 鍵識別子 (A - K I D) 及び / 又は前記 A F の識別子を含み、

前記第 2 メッセージは、

前記鍵 K_{A F} の有効時間情報、

購読永久識別子 (S U P I) 、

一般公衆購読識別子 (G P S I) のうちの少なくとも 1 つをさらに含む、

請求項 7 に記載の通信方法。

【請求項 9】

前記 A A n F に第 1 メッセージを送信する場合において、前記通信方法は、

前記第 1 機器が A A n F から送信された第 1 情報を受信するステップであって、前記第 1 情報は A K M A コンテキスト情報を含み、前記第 1 情報は、A - K I D 、 A K M A アンカー鍵 K_{A K M A}、S U P I のうちの少なくとも 1 つをさらに含む、ステップと、

前記第 1 機器が A K M A アンカー鍵 K_{A K M A} に基づいて前記鍵 K_{A F} を導出するステップと、をさらに含む、

請求項 7 に記載の通信方法。

【請求項 10】

通信方法であって、

A A n F が、第 1 機器に第 1 情報を送信するステップをさらに含み、前記第 1 情報は、A K M A コンテキスト情報を含む、通信方法。

【請求項 11】

前記第 1 情報は、A - K I D 、 A K M A アンカー鍵 K_{A K M A}、S U P I のうちの少なくとも 1 つを含み、

前記通信方法は、

前記 A A n F が A U S F から送信された第 3 メッセージを受信するステップをさらに含み、前記第 3 メッセージは鍵を登録するためのものであり、前記第 3 メッセージは、

A - K I D 、 A K M A アンカー鍵 K_{A K M A}、S U P I 、端末のローミング情報のうちの少なくとも 1 つを含み、

前記端末のローミング情報は、

10

20

30

40

50

端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含み、

前記端末のローミング情報は前記 A U S F が U D M から取得したものであり、

前記 A U S F が U D M から取得した前記端末のローミング情報は、前記端末 S U P I に関連付けられた前記端末のローミング情報である、

請求項 1 0 に記載の通信方法。

【請求項 1 2】

通信方法であって、

A F が第 1 機器又は A A n F に第 1 メッセージを送信するステップであって、前記第 1 メッセージは鍵 K_{A F} を取得するためのものである、ステップと、

前記第 1 機器又は前記 A A n F が前記 A F にサービスを提供できることをチェックした場合、前記 A F が前記第 1 機器又は前記 A A n F から送信された第 2 メッセージを受信するステップであって、前記第 2 メッセージは、少なくとも鍵 K_{A F} を含む、ステップと、を含む、通信方法。

【請求項 1 3】

前記第 1 メッセージは A K M A 鍵識別子 (A - K I D) 及び / 又は前記 A F の識別子を含み、

前記第 2 メッセージは、

前記鍵 K_{A F} の有効時間情報、

購読永久識別子 (S U P I) 、

一般公衆購読識別子 (G P S I) のうちの少なくとも 1 つをさらに含む、

請求項 1 2 に記載の通信方法。

【請求項 1 4】

通信方法であって、

U D M が A U S F に認証関連情報を送信するステップを含み、前記認証関連情報は、

端末に対して A K M A 鍵材料を生成する必要があることを表す第 3 指示情報、前記端末に対して A K M A 鍵材料を生成する必要があることを表す第 4 指示情報、前記端末の R I D 情報、前記端末のローミング情報のうちの少なくとも 1 つを含む、通信方法。

【請求項 1 5】

前記端末のローミング情報は、

端末がローミング状態にあることを表す第 1 指示情報、端末がローミング状態にないことを表す第 2 指示情報、ローミング先情報、前記端末のローミング先での契約情報、前記端末のローミング先でのポリシー情報のうちの少なくとも 1 つを含み、

前記通信方法は、

前記 U D M が A A n F から送信された第 4 メッセージを受信するステップであって、前記第 4 メッセージは端末のローミング情報を要求するためのものである、ステップと、

前記 U D M が前記 A A n F に第 5 メッセージを送信するステップであって、前記第 5 メッセージは前記端末のローミング情報を含む、ステップと、をさらに含む、

請求項 1 4 に記載の通信方法。

10

20

30

40

50

【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/CN2023/100416															
A. CLASSIFICATION OF SUBJECT MATTER H04W 12/069(2021.01)i According to International Patent Classification (IPC) or to both national classification and IPC																	
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC: H04W H04L Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) CNTXT, ENTXT, WPABS, 3GPP: 漫游, 拜访, 归属, 认证, 密钥, 锚点, 应用功能, 获取, 发送, 代理, roam, visit+, VPLMN, home, HPLMN, authenticat+, key, AKMA, AANF, AF, anchor, send, transmit, proxy																	
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>SAMSUNG. "AKMA Service Support for Roaming UE" 3GPP TSG-SA3 Meeting #105-e S3-214236, 19 November 2021 (2021-11-19), sections 4.2.x and 6.1-6.3</td> <td>1-21, 29-32, 39-41, 43, 46-47</td> </tr> <tr> <td>X</td> <td>CN 113543126 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 October 2021 (2021-10-22) description, paragraphs 87-123</td> <td>1-21, 29-32, 39-41, 43, 46-47</td> </tr> <tr> <td>A</td> <td>WO 2021201558 A1 (SAMSUNG ELECTRONICS CO., LTD.) 07 October 2021 (2021-10-07) entire document</td> <td>1-21, 29-32, 39-41, 43, 46-47</td> </tr> <tr> <td>A</td> <td>CN 113225176 A (HUAWEI TECHNOLOGIES CO., LTD.) 06 August 2021 (2021-08-06) entire document</td> <td>1-21, 29-32, 39-41, 43, 46-47</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	SAMSUNG. "AKMA Service Support for Roaming UE" 3GPP TSG-SA3 Meeting #105-e S3-214236, 19 November 2021 (2021-11-19), sections 4.2.x and 6.1-6.3	1-21, 29-32, 39-41, 43, 46-47	X	CN 113543126 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 October 2021 (2021-10-22) description, paragraphs 87-123	1-21, 29-32, 39-41, 43, 46-47	A	WO 2021201558 A1 (SAMSUNG ELECTRONICS CO., LTD.) 07 October 2021 (2021-10-07) entire document	1-21, 29-32, 39-41, 43, 46-47	A	CN 113225176 A (HUAWEI TECHNOLOGIES CO., LTD.) 06 August 2021 (2021-08-06) entire document	1-21, 29-32, 39-41, 43, 46-47
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.															
X	SAMSUNG. "AKMA Service Support for Roaming UE" 3GPP TSG-SA3 Meeting #105-e S3-214236, 19 November 2021 (2021-11-19), sections 4.2.x and 6.1-6.3	1-21, 29-32, 39-41, 43, 46-47															
X	CN 113543126 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 October 2021 (2021-10-22) description, paragraphs 87-123	1-21, 29-32, 39-41, 43, 46-47															
A	WO 2021201558 A1 (SAMSUNG ELECTRONICS CO., LTD.) 07 October 2021 (2021-10-07) entire document	1-21, 29-32, 39-41, 43, 46-47															
A	CN 113225176 A (HUAWEI TECHNOLOGIES CO., LTD.) 06 August 2021 (2021-08-06) entire document	1-21, 29-32, 39-41, 43, 46-47															
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.																	
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "D" document cited by the applicant in the international application "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family																	
Date of the actual completion of the international search 17 August 2023		Date of mailing of the international search report 23 August 2023															
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/CN) China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088		Authorized officer Telephone No.															

Form PCT/ISA/210 (second sheet) (July 2022)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/100416

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Invention I: Claims (1, 12, 16, 29, 39, 40, 41, 43, and the technical solutions of claims 46-47, when refer to any one of claims 1-11, 12-15, 16-21 and 29-32)

10

Invention II: Claims (22, 42, and the technical solutions of claims 46-47, when refer to any one of claims 22-28)

Invention III: Claims (33, 36, 44, 45, and the technical solutions of claims 46-47, when refer to any one of claims 33-35 and 36-38)

The same or corresponding technical features between the first group of claims and the second group of claims are: a communication method, an AAnF, a first device, and first information.

The same or corresponding technical feature between the first group of claims and the third group of claims as well as between the second group of claims and the third group of claims is: a communication method.

However, the above-mentioned features are all customary means in the art. Therefore, the three groups of claims do not have a same or corresponding special technical feature therebetween, and thus do not meet the requirement of unity of invention and do not comply with PCT Rule 13.1.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

20

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: **1-21, 29-32, 39-41, 43, 46-47 (when referring to any one of claims 1-11, 12-15, 16-21 and 29-32)**

30

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

40

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/100416

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	113543126	A	22 October 2021	None			
WO	2021201558	A1	07 October 2021	US	2023232221	A1	20 July 2023
				EP	4111722	A1	04 January 2023
				KR	20220159991	A	05 December 2022
				CN	115413414	A	29 November 2022
				IN	202041014023	A	08 October 2021
CN	113225176	A	06 August 2021	WO	2021155758	A1	12 August 2021
				VN	90618	A	25 October 2022
				EP	4089977	A1	16 November 2022
				US	2022377540	A1	24 November 2022
				IN	202237045195	A	27 January 2023
				JP	2023513501	A	31 March 2023

Form PCT/ISA/210 (patent family annex) (July 2022)

10

20

30

40

50

国际检索报告		国际申请号 PCT/CN2023/100416
A. 主题的分类 H04W 12/069(2021.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类		
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) IPC: H04W H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CNTXT, ENTXTC, WPABS, 3GPP: 漫游, 拜访, 归属, 认证, 密钥, 锚点, 应用功能, 获取, 发送, 代理, roam, visit+, VPLMN, home, HPLMN, authenticat+, key, AKMA, AAnF, AF, anchor, send, transmit, proxy		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	SAMSUNG. "AKMA service support for roaming UE" 3GPP TSG-SA3 Meeting #105-e S3-214236, 2021年11月19日 (2021 - 11 - 19), 第4.2.x, 6.1-6.3节	1-21, 29-32, 39-41, 43, 46-47
X	CN 113543126 A (华为技术有限公司) 2021年10月22日 (2021 - 10 - 22) 说明书第87-123段	1-21, 29-32, 39-41, 43, 46-47
A	WO 2021201558 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2021年10月7日 (2021 - 10 - 07) 全文	1-21, 29-32, 39-41, 43, 46-47
A	CN 113225176 A (华为技术有限公司) 2021年8月6日 (2021 - 08 - 06) 全文	1-21, 29-32, 39-41, 43, 46-47
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: "A" 认为不特别相关的表示了现有技术一般状态的文件 "D" 申请人在国际申请中引证的文件 "E" 在国际申请日的当天或之后公布的在先申请或专利 "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其特殊理由而引用的文件(如具体说明的) "O" 涉及口头公开、使用、展览或其他方式公开的文件 "P" 公布日先于国际申请日但迟于所要求的优先权日的文件 "T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 "&" 同族专利的文件		
国际检索实际完成的日期 2023年8月17日		国际检索报告邮寄日期 2023年8月23日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088		受权官员 王健 电话号码 (+86) 010-53961733

10

20

30

40

50

国际检索报告		国际申请号 PCT/CN2023/100416
第III栏 缺乏发明单一性的意见(续第I页第3项)		
本国际检索单位在该国际申请中发现多项发明，即： 第一组发明：权利要求（1，12，16，29，39，40，41，43，权利要求46-47引用权利要求1-11，12-15，16-21，29-32中任一项时的技术方案）。 第二组发明：权利要求（22，42，权利要求46-47引用权利要求22-28中任一项时的技术方案）。 第三组发明：权利要求（33，36，44，45，权利要求46-47引用权利要求33-35，36-38中任一项时的技术方案）。 第一组和第二组之间相同或相应的技术特征为：一种通信方法，AAnF，第一设备，第一信息。 第一组和第三组之间以及第二组和第三组之间相同或相应的技术特征为：一种通信方法。 但是上述特征均为本领域的惯用手段，因此，上述三组权利要求彼此之间不具有相同或者相应的特定技术特征，因而不满足单一性的要求，不符合PCT实施细则13.1的规定。 1. ☐ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告涉及全部可作检索的权利要求。 2. ☐ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本单位未通知缴纳任何加费。 3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求，具体地说，是权利要求： 4. ☒ 申请人未按时缴纳被要求缴纳的附加检索费。因此，本国际检索报告仅涉及权利要求书中首先提及的发明；包含该发明的权利要求是： 1-21，29-32，39-41，43，46-47（引用权利要求1-11，12-15，16-21，29-32任一项） 对异议的意见 ☐ 申请人缴纳了附加检索费，同时提交了异议书，适用时，缴纳了异议费。 ☐ 申请人缴纳了附加检索费，同时提交了异议书，但未在通知书规定的时间期限内缴纳异议费。 ☐ 缴纳附加检索费时未提交异议书。		

国际检索报告 关于同族专利的信息					国际申请号 PCT/CN2023/100416		
检索报告引用的专利文件			公布日 (年/月/日)	同族专利		公布日 (年/月/日)	
CN	113543126	A	2021年10月22日	无			
WO	2021201558	A1	2021年10月7日	US	2023232221	A1	2023年7月20日
				EP	4111722	A1	2023年1月4日
				KR	20220159991	A	2022年12月5日
				CN	115413414	A	2022年11月29日
				IN	202041014023	A	2021年10月8日
CN	113225176	A	2021年8月6日	WO	2021155758	A1	2021年8月12日
				VN	90618	A	2022年10月25日
				EP	4089977	A1	2022年11月16日
				US	2022377540	A1	2022年11月24日
				IN	202237045195	A	2023年1月27日
				JP	2023513501	A	2023年3月31日

PCT/ISA/210 表(同族专利附件) (2022年7月)

10

20

30

40

50

フロントページの続き

,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,
ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,C
O,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,I
R,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MU,MW
,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL
,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW
L T D .

中華人民共和国北京市西城区金融大街 2 9 号

(74)代理人 100145403
弁理士 山尾 憲人

(74)代理人 100135703
弁理士 岡部 英隆

(72)発明者 黄 晓 ▲ティン ▼
中華人民共和国 1 0 0 0 5 3 北京市西城区宣武門西大街 3 2 号

(72)発明者 庄 小君
中華人民共和国 1 0 0 0 5 3 北京市西城区宣武門西大街 3 2 号

F ターム (参考) 5K067 AA35 DD11 EE16 HH22