(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119364345 A
(43)申请公布日 2025.01.24

(21)申请号 202411471578.5
(22)申请日 2019.09.24
(30)优先权数据
62/735,732 2018.09.24 US
(62)分案原申请数据
201980071244.X 2019.09.24
(71)申请人 诺基亚技术有限公司
地址 芬兰埃斯波
(72)发明人 J·刘
(74)专利代理机构 北京市金杜律师事务所 11256
专利代理师 姚宗妮
(51)Int.Cl.
H04W 12/03(2021.01)
H04W 12/08(2021.01)
H04L 9/40(2022.01)
H04W 60/00(2009.01)

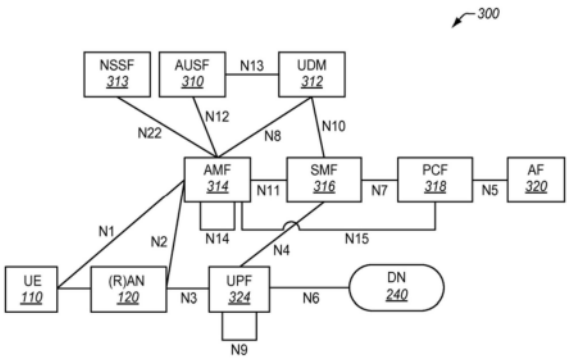
权利要求书2页 说明书22页 附图19页

(54)发明名称

用于NAS消息的安全保护的系统和方法

(57)摘要

为移动网络提供NAS安全保护的系统和方法。在一个实施方案中,当不存在NAS安全上下文时,移动网络的网络元件在多个阶段中执行NAS过程以与用户设备(UE)建立NAS通信会话。对于第一阶段,所述网络元件从所述UE接收用被指定用于安全相关处理的NAS协议信息元素(IE)的子集填充的初始NAS消息,选择用于所述NAS安全上下文的NAS安全算法,并向所述UE发送指示所述NAS安全算法的响应。对于第二阶段,所述网络元件从所述UE接收具有NAS消息容器的后续NAS消息,所述NAS消息容器包含用用于所述NAS过程的每个所述NAS协议IE填充的所述初始NAS消息,并使用所述NAS安全算法对所述后续NAS消息的所述NAS消息容器进行解密。



CN 119364345 A

1.一种移动网络的网络元件,所述网络元件包括:

至少一个处理器;以及

至少一个存储器,所述至少一个存储器包括可由所述处理器执行的计算机程序代码;

所述处理器被配置成使所述网络元件在多个阶段中执行非接入层(NAS)过程,以在所述网络元件与用户设备(UE)之间建立NAS通信会话;

对于所述NAS过程的第一阶段,所述处理器进一步被配置成使所述网络元件:

从所述UE接收初始NAS消息,其中所述初始NAS消息用来自用于所述NAS过程的NAS协议信息元素(IE)的被指定用于安全相关处理的所述NAS协议IE的子集填充;

处理所述NAS协议IE的所述子集以确定对于所述UE不存在NAS安全上下文;

选择用于所述NAS安全上下文的NAS安全算法;以及

向所述UE发送指示所述NAS安全上下文的所述NAS安全算法以及安全密钥集标识符的响应;

对于所述NAS过程的第二阶段,所述处理器进一步被配置成使所述网络元件:

从所述UE接收具有NAS消息容器的后续NAS消息,所述NAS消息容器包含基于所述NAS安全算法加密的所述初始NAS消息;以及

对所述后续NAS消息的所述NAS消息容器进行解密,其中包含在所述后续NAS消息的所述NAS消息容器中的所述初始NAS消息用用于所述NAS过程的每个所述NAS协议IE填充。

2.如权利要求1所述的网络元件,其中:

对于所述第一阶段,使用用于所述UE的归属公共陆地移动网络(HPLMN)的公钥来对所述初始NAS消息中的所述NAS协议IE的所述子集进行加密;并且

所述处理器进一步被配置成使所述网络元件发起对所述NAS协议IE的所述子集的解密。

3.如权利要求2所述的网络元件,其中:

所述网络元件包括所述移动网络的接入和移动性管理功能(AMF)元件。

4.如权利要求3所述的网络元件,其中:

所述处理器进一步被配置成使所述网络元件将已加密的NAS协议IE的所述子集发送至统一数据管理(UDM)元件,以基于所述HPLMN的私钥来对NAS协议IE的所述子集进行解密。

5.如权利要求1所述的网络元件,其中:

所述初始NAS消息包括注册请求消息;并且

被指定用于安全相关处理的所述NAS协议IE的所述子集由以下项组成:所述UE的移动身份、指示所述UE支持的一种或多种NAS安全算法的UE安全能力、注册类型,以及NAS安全上下文的安全密钥集标识符。

6.如权利要求1所述的网络元件,其中:

所述响应包括指示所述NAS安全算法和所述安全密钥集标识符的安全模式命令消息;并且

从所述UE接收的所述后续NAS消息包括安全模式完成消息,所述安全模式完成消息具有包含基于所述NAS安全算法加密的所述初始NAS消息的所述NAS消息容器。

7.如权利要求1所述的网络元件,其中:

所述移动网络包括第五代(5G)网络。

8.一种执行非接入层(NAS)过程以在用户设备(UE)与移动网络的网络元件之间建立NAS通信会话的方法,所述方法包括:

对于所述NAS过程的第一阶段:

在所述网络元件处从所述UE接收初始NAS消息,其中所述初始NAS消息用来自用于所述NAS过程的NAS协议信息元素(IE)的被指定用于安全相关处理的所述NAS协议IE的子集填充;

在所述网络元件处处理所述NAS协议IE的所述子集以确定对于所述UE不存在NAS安全上下文;

在所述网络元件处选择用于所述NAS安全上下文的NAS安全算法;以及

从所述网络元件向所述UE发送指示所述NAS安全上下文的所述NAS安全算法以及安全密钥集标识符的响应;

对于所述NAS过程的第二阶段:

在所述网络元件处从所述UE接收具有NAS消息容器的后续NAS消息,所述NAS消息容器包含基于所述NAS安全算法加密的所述初始NAS消息;以及

在所述网络元件处对所述后续NAS消息的所述NAS消息容器进行解密,其中包含在所述后续NAS消息的所述NAS消息容器中的所述初始NAS消息用用于所述NAS过程的每个所述NAS协议IE填充。

9.如权利要求8所述的方法,其中:

对于所述第一阶段,使用用于所述UE的归属公共陆地移动网络(HPLMN)的公钥来对所述初始NAS消息中的所述NAS协议IE的所述子集进行加密;并且

所述方法进一步包括:

发起对所述NAS协议IE的所述子集的解密。

10.如权利要求9所述的方法,其中:

所述网络元件包括所述移动网络的接入和移动性管理功能(AMF)元件;并且

发起对所述NAS协议IE的所述子集的解密包括将已加密的NAS协议IE的所述子集发送至统一数据管理(UDM)元件,以基于所述HPLMN的私钥来对NAS协议IE的所述子集进行解密。

用于NAS消息的安全保护的系统和方法

[0001] 本申请是国际申请号为PCT/FI2019/050685、国际申请日为2019年09月24日、于2021年04月27日进入中国国家阶段、中国国家申请号为201980071244X、发明名称为“用于NAS消息的安全保护的系统和方法”的发明专利申请的分案申请。

[0002] 相关申请

[0003] 本非临时专利申请要求2018年9月24日提交的第62/735,732号美国临时专利申请的优先权,所述美国临时专利申请如同完全提供一般以引用的方式并入本文。

技术领域

[0004] 本公开涉及通信系统领域,且具体地,涉及网络中的安全性。

背景技术

[0005] 服务提供商或运营商实施移动网络,以向通常被称为用户设备(UE)的移动电话或其他移动装置/终端的最终用户提供大量语音和数据服务。语音服务的一些示例是语音呼叫、呼叫转移、呼叫等待等。数据服务的一些示例是因特网访问、流媒体音频、流媒体视频、在线游戏、因特网协议电视(IP-TV)等。移动网络是到最终用户的最后链接为无线的一种网络类型。移动网络通常包括核心网络以及通过无线电接口与UE交换信令和数据的一个或多个无线电接入网(RAN)。典型的移动网络在逻辑上分为用户平面和控制平面。用户平面是负责承载通过网络发送的用户数据的逻辑平面,而控制平面是负责承载用于为UE建立通信的信令的逻辑平面。第三代合作伙伴计划(3GPP)规范将蜂窝协议分为两个层次:非接入层(NAS)和接入层(AS)。AS由UE与RAN(例如,eNodeB)之间经由射频(RF)信道发生的通信组成。NAS由UE与核心网络(例如,用于LTE的移动性管理实体(MME)或用于网络生成网络的接入和移动性管理功能(AMF))之间的非无线电信令流量组成。3GPP已经实施了安全过程来保护控制平面消息(例如,NAS消息)免受各种攻击。然而,有利的是识别为控制平面消息提供进一步保护的增强的安全过程。

发明内容

[0006] 本文描述的实施方案为NAS消息提供增强的保护。NAS过程(例如,UE的注册)包括携带信息的信息元素(IE)集。以下描述的实施方案阐述了保护在NAS消息中发送的IE或IE的子集的方式。因此,IE中携带的信息不太容易受到恶意攻击。

[0007] 一个实施方案包括移动网络的网络元件。所述网络元件包括处理器和存储器,所述存储器包括可由处理器执行的计算机程序代码。处理器被配置成使网络元件在多个阶段中执行NAS过程,以在网络元件与UE之间建立NAS通信会话。对于NAS过程的第一阶段,处理器进一步被配置成使网络元件从UE接收初始NAS消息,其中所述初始NAS消息用来自用于NAS过程的NAS协议IE的指定用于安全相关处理的NAS协议IE的子集填充。处理器进一步被配置成使网络元件处理NAS协议IE的子集以确定对于UE不存在NAS安全上下文,选择用于NAS安全上下文的NAS安全算法,并且向UE发送指示NAS安全上下文的NAS安全算法以及安全

密钥集标识符的响应。对于NAS过程的第二阶段,处理器进一步被配置成使网络元件从UE接收具有NAS消息容器的后续NAS消息,所述NAS消息容器包含基于NAS安全算法加密的初始NAS消息;并对后续NAS消息的NAS消息容器进行解密,其中包含在后续NAS消息的NAS消息容器中的初始NAS消息用用于NAS过程的每个NAS协议IE填充。

[0008] 在另一个实施方案中,对于第一阶段,使用用于UE的归属公共陆地移动网络(HPLMN)的公钥来对初始NAS消息中的NAS协议IE的子集进行加密。处理器进一步被配置成使网络元件发起对NAS协议IE的子集的解密。

[0009] 在另一个实施方案中,网络元件包括移动网络的接入和移动性管理功能(AMF)元件。

[0010] 在另一个实施方案中,处理器进一步被配置成使网络元件将已加密的NAS协议IE的子集发送至统一数据管理(UDM)元件,以基于HPLMN的私钥来对NAS协议IE的子集进行解密。

[0011] 在另一个实施方案中,初始NAS消息包括注册请求消息。被指定用于安全相关处理的NAS协议IE的子集由以下项组成:UE的移动身份、指示UE支持的一种或多种NAS安全算法的UE安全能力、注册类型,以及NAS安全上下文的安全密钥集标识符。

[0012] 在另一个实施方案中,响应包括指示NAS安全算法和安全密钥集标识符的安全模式命令消息,并且从UE接收的后续NAS消息包括安全模式完成消息,所述安全模式完成消息具有包含基于NAS安全算法加密的初始NAS消息的NAS消息容器。

[0013] 在另一个实施方案中,移动网络包括第五代(5G)网络。

[0014] 另一个实施方案包括一种执行NAS过程以在UE与移动网络的网络元件之间建立NAS通信会话的方法。对于NAS过程的第一阶段,所述方法包括在网络元件处从UE接收初始NAS消息,其中所述初始NAS消息用来自用于NAS过程的NAS协议IE的指定用于安全相关处理的NAS协议IE的子集填充。进一步对于第一阶段,所述方法包括:在网络元件处处理NAS协议IE的子集以确定对于UE不存在NAS安全上下文,在网络元件处选择用于NAS安全上下文的NAS安全算法,以及从网络元件向UE发送指示NAS安全上下文的NAS安全算法以及安全密钥集标识符的响应。对于NAS过程的第二阶段,所述方法包括在网络元件处从UE接收具有NAS消息容器的后续NAS消息,所述NAS消息容器包含基于NAS安全算法加密的初始NAS消息;并在网络元件处对后续NAS消息的NAS消息容器进行解密,其中包含在后续NAS消息的NAS消息容器中的初始NAS消息用用于NAS过程的每个NAS协议IE填充。

[0015] 在另一个实施方案中,对于第一阶段,使用用于UE的HPLMN的公钥来对初始NAS消息中的NAS协议IE的子集进行加密,并且所述方法进一步包括发起对NAS协议IE的子集的解密。

[0016] 在另一个实施方案中,网络元件包括移动网络的AMF元件,并且发起对NAS协议IE的子集的解密的步骤包括:将已加密的NAS协议IE的子集发送至UDM元件,以基于HPLMN的私钥来对NAS协议IE的子集进行解密。

[0017] 在另一个实施方案中,初始NAS消息包括注册请求消息,并且被指定用于安全相关处理的NAS协议IE的子集由以下项组成:UE的移动身份、指示UE支持的一种或多种NAS安全算法的UE安全能力、注册类型,以及NAS安全上下文的安全密钥集标识符。

[0018] 在另一个实施方案中,响应包括指示NAS安全算法和安全密钥集标识符的安全模

式命令消息,并且从UE接收的后续NAS消息包括安全模式完成消息,所述安全模式完成消息具有包含基于NAS安全算法加密的初始NAS消息的NAS消息容器。

[0019] 在另一个实施方案中,对于NAS过程的第一阶段,所述方法在UE处包括以下步骤:识别用于NAS过程的指定用于安全相关处理的NAS协议IE的子集,将NAS协议IE的子集插入初始NAS消息中,将初始NAS消息从UE发送至网络元件,以及从网络元件接收指示NAS安全上下文的NAS安全算法以及安全密钥集标识符的响应。对于NAS过程的第二阶段,所述方法在UE处包括以下步骤:将用于NAS过程的NAS协议IE插入初始NAS消息中,将初始NAS消息插入后续NAS消息的NAS消息容器中,使用NAS安全算法对后续NAS消息的NAS消息容器进行加密,以及将后续NAS消息从UE发送至网络元件。

[0020] 在另一个实施方案中,对于第一阶段,所述方法进一步包括在UE处使用用于UE的HPLMN的公钥来对初始NAS消息中的NAS协议IE的子集进行加密。

[0021] 另一个实施方案包括一种UE,所述UE包括处理器和存储器,所述存储器包括可由处理器执行的计算机程序代码。处理器被配置成使UE在多个阶段中发起NAS过程,以在UE与移动网络的网络元件之间建立NAS通信会话。对于NAS过程的第一阶段,处理器进一步被配置成使UE从用于NAS过程的NAS协议IE中识别指定用于安全相关处理的NAS协议IE的子集。处理器进一步被配置成使UE将NAS协议IE的子集插入初始NAS消息中,将初始NAS消息发送至网络元件,以及从网络元件接收指示NAS安全上下文的NAS安全算法以及安全密钥集标识符的响应。对于NAS过程的第二阶段,处理器进一步被配置成使UE将用于NAS过程的NAS协议IE插入初始NAS消息中,将初始NAS消息插入后续NAS消息的NAS消息容器中,使用NAS安全算法对后续NAS消息的NAS消息容器进行加密,以及将后续NAS消息发送至网络元件。

[0022] 在另一个实施方案中,对于第一阶段,处理器进一步被配置成使UE使用用于UE的HPLMN的公钥来对初始NAS消息中的NAS协议IE的子集进行加密。

[0023] 在另一个实施方案中,处理器进一步被配置成:当UE在UMTS订户标识模块(USIM)上编程了公钥时,使UE使用公钥对初始NAS消息中的NAS协议IE的子集进行加密;以及当UE未在USIM上编程公钥时,使UE将初始NAS消息发送至网络元件而不对初始NAS消息中的NAS协议IE的子集进行加密。

[0024] 在另一个实施方案中,初始NAS消息包括注册请求消息,并且被指定用于安全相关处理的NAS协议IE的子集由以下项组成:UE的移动身份、指示UE支持的一种或多种NAS安全算法的UE安全能力、注册类型,以及NAS安全上下文的安全密钥集标识符。

[0025] 在另一个实施方案中,处理器被配置成:当注册类型不指示紧急时,使UE使用用于UE的HPLMN的公钥来对初始NAS消息中的NAS协议IE的子集进行加密;以及当注册类型指示紧急时,使UE将初始NAS消息发送至网络元件而不对初始NAS消息中的NAS协议IE的子集进行加密。

[0026] 在另一个实施方案中,响应包括指示NAS安全算法和安全密钥集标识符的安全模式命令消息,并且后续NAS消息包括安全模式完成消息,所述安全模式完成消息具有包含基于NAS安全算法加密的初始NAS消息的NAS消息容器。

[0027] 另一个实施方案包括移动网络的网络元件。所述网络元件包括用于使网络元件在多个阶段中执行NAS过程以在网络元件与UE之间建立NAS通信会话的构件。对于NAS过程的第一阶段,网络元件包括用于从UE接收初始NAS消息的构件,其中所述初始NAS消息用来自

用于NAS过程的NAS协议IE的指定用于安全相关处理的NAS协议IE的子集填充。网络元件进一步包括用于处理NAS协议IE的子集以确定对于UE不存在NAS安全上下文的构件,用于选择用于NAS安全上下文的NAS安全算法的构件,以及用于向UE发送指示NAS安全上下文的NAS安全算法以及安全密钥集标识符的响应的构件。对于NAS过程的第二阶段,网络元件进一步包括用于从UE接收具有NAS消息容器的后续NAS消息的构件,所述NAS消息容器包含基于NAS安全算法加密的初始NAS消息;以及用于对后续NAS消息的NAS消息容器进行解密的构件,其中包含在后续NAS消息的NAS消息容器中的初始NAS消息用用于NAS过程的每个NAS协议IE填充。

[0028] 上面的概述提供了对说明书某些方面的基本理解。此概述不是对本说明书的详尽概述。它既不旨在识别本说明书的关键或重要元素,也不旨在描述本说明书的特定实施方案的任何范围或权利要求的任何范围。其唯一目的是以简化形式呈现本说明书的一些概念,以作为稍后所呈现的更详细描述的序言。

附图说明

[0029] 现将通过仅示例的方式并且参照附图来描述本发明的一些实施方案。在所有附图上,相同的附图标记表示相同的元件或相同类型的元件。

[0030] 图1示出了说明性实施方案中的移动网络。

[0031] 图2示出了演进分组核心(EPC)网络。

[0032] 图3示出了下一代网络的非漫游架构。

[0033] 图4示出了下一代网络的漫游架构。

[0034] 图5示出了无线电协议栈。

[0035] 图6是说明性实施方案中的UE的框图。

[0036] 图7是说明性实施方案中的网络元件的框图。

[0037] 图8是示出说明性实施方案中在UE中执行NAS过程的方法的流程图。

[0038] 图9是示出说明性实施方案中在网络元件中执行NAS过程的方法的流程图。

[0039] 图10是示出在说明性实施方案中当UE没有安全上下文时的NAS过程的消息图。

[0040] 图11是示出另一个说明性实施方案中在UE 110中执行NAS过程的方法的流程图。

[0041] 图12是示出另一个说明性实施方案中在网络元件中执行NAS过程的方法的流程图。

[0042] 图13是示出在说明性实施方案中当UE没有安全上下文时的NAS过程的消息图。

[0043] 图14是示出另一个说明性实施方案中在UE中执行NAS过程的方法的流程图。

[0044] 图15是示出另一个说明性实施方案中在网络元件中执行NAS过程的方法的流程图。

[0045] 图16是示出在说明性实施方案中当UE具有有效安全上下文时的NAS注册过程的消息图。

[0046] 图17是示出在说明性实施方案中当UE具有有效安全上下文时的NAS服务请求过程的消息图。

[0047] 图18是示出在说明性实施方案中当UE具有有效安全上下文时的NAS注销过程的消息图。

[0048] 图19A至图19B是示出说明性实施方案中在UE中执行NAS过程的方法的流程图。

[0049] 图20是示出说明性实施方案中在网络元件中执行NAS过程的方法的流程图。

[0050] 图21是示出在说明性实施方案中当UE具有NAS安全上下文,但NAS安全上下文无效或未找到时的NAS注册过程的消息图。

[0051] 图22是示出在说明性实施方案中当UE具有NAS安全上下文,但NAS安全上下文无效或未找到时的NAS服务请求过程的消息图。

具体实施方式

[0052] 附图和以下描述示出了具体的示例性实施方案。因此应了解,本领域的技术人员将能够设想各种布置,虽然这些布置未在本文中明确地描述或展示,但是它们体现了实施方案的原理并且包括在实施方案的范围内。此外,本文中描述的任何示例旨在帮助理解实施方案的原理,并且应解释为不限于这些具体列举的示例和条件。因此,一个或多个发明构思不限于以下描述的特定实施方案或示例,而是由权利要求书及其等同物来限定。

[0053] 图1示出了说明性实施方案中的移动网络100。移动网络100(也称为蜂窝网络)是最后一条链路为无线的一种网络类型,并且向多个装置提供语音和/或数据服务。移动网络100可以是第三代(3G)、第四代(4G)和/或下一代网络(例如,第五代(5G))。

[0054] 移动网络100被示为向UE 110(以及未示出的其他UE)提供通信服务。可以使UE 110获得语音服务、数据服务、机器对机器(M2M)或机器类型通信(MTC)服务和/或其他服务。UE 110可以是例如移动电话(例如,智能电话)、平板计算机或PDA、具有移动宽带适配器的计算机等最终用户装置。

[0055] 移动网络100包括通过无线电接口122与UE 110进行通信的一个或多个无线电接入网(RAN)120。RAN 120可以支持演进型UMTS陆地无线接入网(E-UTRAN)接入、无线局域网(WLAN)接入、固定接入、卫星无线电接入、新无线电接入技术(RAT)等。作为示例,RAN 120可以包括E-UTRAN或下一代RAN(NG-RAN),其包括分散在地理区域上的一个或多个基站124。基站124可以包括使用无线电通信技术在许可频谱上与UE进行通信并且使UE与核心网络介接的实体。E-UTRAN中的基站124被称为演进型NodeB(eNodeB)。NG-RAN中的基站124被称为gNodeB(NR基站)和/或ng-eNodeB(支持5G核心网的LTE基站)。作为另一示例,RAN 120可以包括WLAN,所述WLAN包括一个或多个无线接入点(WAP)125。WLAN是其中UE能够通过无线(无线电)连接而连接至局域网(LAN)的网络。WAP 125是使用无线电通信技术以通过非许可频谱与UE进行通信并提供对核心网络的UE访问的节点。WAP 125的一个示例是在2.4GHz或5GHz无线电频段上运行的WiFi接入点。如本文所使用的术语“基站”可以指eNodeB、gNodeB、ng-eNodeB、WAP等。

[0056] UE 110能够附接至RAN 120的小区126以访问核心网络130。因此,RAN 120代表UE 110与核心网络130之间的无线电接口。核心网络130是移动网络100的中心部分,其向通过RAN 120所连接的客户提供各种服务。核心网络130的一个示例是由3GPP针对LTE建议的演进分组核心(EPC)网络。核心网络130的另一个示例是3GPP建议的5G核心网络。核心网络130包括网络元件132,其可以包括为UE 110提供服务的服务器、装置、设备或装备(包括硬件)。EPC网络中的网络元件132可以包括移动性管理实体(MME)、服务网关(S-GW)、分组数据网络网关(P-GW)等。5G网络中的网络元件132可以包括访问和移动性管理功能(AMF)、会话管理

功能(SMF)、策略控制功能(PCF)、应用功能(AF)、用户平面功能(UPF)等。

[0057] 图2示出了演进分组核心(EPC)网络200,其是用于LTE的核心网络。EPC网络200包括移动性管理实体(MME)214、服务网关(S-GW)215、分组数据网络网关(P-GW)216、归属订户服务器(HSS)217以及策略和计费规则功能(PCRF)218,但也可以包括其他未显示的元件,例如IP多媒体子系统(IMS)应用服务器。在EPC网络200内,用户数据(也称为“用户平面”)和信令(也称为“控制平面”)是分开的。MME 214处理EPC网络200中的控制平面。例如,MME 214处理与用于E-UTRAN接入的移动性和安全性有关的信令。MME 214负责跟踪和寻呼空闲模式下的UE 110。S-GW 215和P-GW 216处理用户平面。S-GW 215和P-GW 216在UE 110与外部数据网络240(DN或分组数据网络(PDN))之间传输数据流量。S-GW 215是无线电侧与EPC网络200之间的互连点,并且通过路由传入和传出IP分组来为UE 110服务。S-GW 215也是LTE内移动性的锚点(即,在eNodeB之间进行切换的情况下),并且在LTE与其他3GPP接入之间。P-GW 216是EPC网络200与外部数据网络240之间的互连点(即,数据网络240的入口点或出口点),并将分组路由到数据网络240和从所述数据网络路由分组。HSS217是存储与用户有关和与订户有关的信息的数据库。PCRF 218在EPC网络200中提供策略和计费控制(PCC)解决方案,并且是EPC网络200的为最终用户请求的服务制定PCC规则的节点或实体。

[0058] MME 214通过S1-MME接口连接至RAN 120(即,eNodeB),并且S-GW 215通过S1-U接口连接至RAN 120。MME 214通过S11接口连接至S-GW 215,并且通过S6a接口连接至HSS217。PCRF 218通过Gx接口连接至P-GW 216,所述接口将策略和计费规则从PCRF 218传输到P-GW 216中的策略和计费执行功能(PCEF)。PCRF 218通过Gxx接口连接至S-GW 215,并且S-GW 215通过S5接口连接至P-GW 216。

[0059] 图3示出了下一代网络的非漫游架构300。图3中的架构是参考点表示,如在如同完全包含在本文中以引用方式并入的3GPP TS 23.501(v15.3.0)中进一步描述。架构300包括用于核心网络的网络功能(NF),并且用于控制平面的网络功能与用户平面分开。核心网络的控制平面包括认证服务器功能(AUSF)310、统一数据管理(UDM)312、网络片选择功能(NSSF)313、接入和移动性管理功能(AMF)314、会话管理功能(SMF)316、策略控制功能(PCF)318和应用功能(AF)320。核心网络的用户平面包括与数据网络240通信的一个或多个用户平面功能(UPF)324。UE 110能够通过(R)AN 120访问核心网络的控制平面和用户平面。

[0060] AUSF 310被配置成支持UE 110的认证。UDM 312被配置成存储UE 110的订阅数据/信息。UDM 312可以存储三种类型的用户数据:订阅、策略和与会话有关的上下文(例如,UE位置)。AMF 314被配置成提供基于UE的认证、授权、移动性管理等。SMF 316被配置成提供以下功能性:会话管理(SM)、UE因特网协议(IP)地址分配和管理、UPF的选择和控制、朝向PCF 318的接口的终止、策略执行和服务质量(QoS)的控制部分、合法拦截、NAS消息的SM部分的终止、下行链路数据通知(DNN)、漫游功能性、处理本地执行以对服务水平协议(SLA)应用QoS、计费数据收集和计费接口等。如果UE 110具有多个会话,则可以将不同的SMF分配给每个会话以分别管理它们,并可能在每个会话提供不同的功能性。PCF 318被配置成支持统一策略框架以管理网络行为,并提供策略规则来控制平面功能以用于QoS执行、计费、接入控制、流量路由等。AF 320将有关分组流的信息提供给PCF 318。基于所述信息,PCF 318被配置成确定关于移动性和会话管理的策略规则,以使AMF 314和SMF 316正常运行。

[0061] UPF 324支持各种用户平面操作和功能性,例如分组路由和转发、流量处理(例如

QoS执行)、RAT内/RAT间移动性的锚点(适用时)、分组检查和策略规则执行、合法拦截(UP收集)、流量统计和报告等。数据网络240不是核心网络的一部分,并且提供因特网访问、运营商服务、第三方服务等。例如,国际电信联盟(ITU)将5G移动网络服务分为三类:增强型移动宽带(eMBB)、超可靠和低延迟通信(uRLLC),以及大规模机器类型通信(mMTC)或大规模物联网(MIoT)。eMBB专注于具有高带宽要求的服务,例如HD视频、虚拟现实(VR)和增强现实(AR)。uRLLC专注于对延迟敏感的服务,例如自动驾驶和远程管理。mMTC和MIoT专注于对连接密度要求很高的服务,例如智慧城市和智慧农业。数据网络240可以被配置成提供这些和其他服务。

[0062] 架构300包括以下参考点。N1参考点在UE 110与AMF 314之间实现。N2参考点在(R)AN 120与AMF 314之间实现。N3参考点在(R)AN 120与UPF 324之间实现。N4参考点在SMF 316与UPF 324之间实现。N5参考点在PCF 318与AF 320之间实现。N6参考点在UPF 324与数据网络240之间实现。N7参考点在SMF 316与PCF 318之间实现。N8参考点在UDM 312与AMF 314之间实现。N9参考点在两个UPF 324之间实现。N10参考点在UDM 312与SMF 316之间实现。N11参考点在AMF 314与SMF 316之间实现。N12参考点在AMF 314与AUSF 310之间实现。N13参考点在UDM 312与AUSF 310之间实现。N14参考点在两个AMF之间实现。N15参考点在非漫游场景下在PCF 318与AMF 314之间实现。N22参考点在NSSF 313与AMF 314之间实现。

[0063] 图4示出了下一代网络的漫游架构400。图4中的架构是参考点表示中的本地疏导场景,如在3GPP TS23.501(v15.3.0)中进一步描述的。在漫游场景中,示出了拜访公共陆地移动网络(VPLMN)402和归属PLMN(HPLMN)404。HPLMN 404识别其中保存了移动订户的简档的PLMN。VPLMN是移动订户在离开其HPLMN时漫游的PLMN。漫游到其他网络的用户将从HPLMN 404接收订阅信息。在本地疏导场景中,PCF 318(hPCF)、UDM 312和AUSF 310位于UE 110的HPLMN 404中。包括访问的PCF(vPCF)418在内的其他网络功能位于VPLMN 402中。

[0064] 图5示出了例如用于无线电接口122的无线电协议栈500。如本文描述的,用户平面512包括用于通过网络传输实际用户数据的一组协议,并且控制平面514包括用于控制和建立网络内的用户连接和承载的协议。对于用户平面512和控制平面514,无线电协议栈500包括物理(PHY)层501,媒体接入控制(MAC)层502、无线电链路控制(RLC)层503和分组数据汇聚协议(PDCP)层504。控制平面514另外包括无线电资源控制(RRC)层505和非接入层(NAS)层506。

[0065] 物理层501在无线电接口上承载来自MAC传输信道的所有信息。数据和信令消息承载于物理层501的不同层级之间的物理信道上。物理信道分为物理数据信道和物理控制信道。物理数据信道可以包括物理下行链路共享信道(PDSCH)、物理广播信道(PBCH)、物理组播信道(PMCH)、物理上行链路共享信道(PUSCH)和物理随机接入信道(PRACH)。物理控制信道可以包括物理控制格式指示符信道(PCFICH)、物理混合ARQ指示符信道(PHICH)、物理下行链路控制信道(PDCCH)和物理上行链路控制信道(PUCCH)。

[0066] MAC层502负责逻辑信道与传输信道之间的映射;将来自一个或不同逻辑信道的MAC服务数据单元(SDU)多路复用到要在传输信道上传递到物理层的传输块(TB)上;从在传输信道上从物理层传递的传输块解复用来自一个或不同逻辑信道的MAC SDU;调度信息报告;通过混合自动重传请求(HARQ)进行纠错;借助于动态调度在UE之间进行优先级处理;在一个UE的逻辑信道之间进行优先级处理;以及逻辑信道优先化。RLC层503负责上层协议数

据单元(PDU)的传输,通过ARQ进行纠错,以及RLC SDU的级联、分段和重组。RLC层503还负责RLC数据PDU的重新分段、RLC数据PDU的重新排序、复制检测、RLC SDU丢弃、RLC重建以及协议错误检测。PDCP层504负责IP数据的报头压缩和解压缩;数据(用户平面或控制平面)的传输;PDCP序列号(SN)的维护;在重建下层时上层PDU的按顺序传递;在重建下层用于RLC确认模式(AM)上映射的无线电承载时下层SDU的复制删除;用户平面数据和控制平面数据的加密和解密;控制平面数据的完整性保护和完整性验证;基于计时器的丢弃;重复丢弃等。RRC层505负责与NAS有关的系统信息的广播;与接入层(AS)有关的系统信息的广播;UE与RAN之间的RRC连接的寻呼、建立、维护和释放;包括点对点无线电承载(RB)的密钥管理、建立、配置、维护和释放在内的安全功能。NAS层506表示UE与核心网络之间的控制平面514的最高层(例如MME/AMF),并且支持UE的移动性和会话管理程序以建立和维持UE与核心网络之间的IP连接。

[0067] 网络的目标之一是提高整体系统安全性。一个特别关注的领域是NAS消息的安全保护。在本文描述的实施方案中,UE 110和网络元件132被增强以提供对NAS消息的附加安全保护。

[0068] 图6是说明性实施方案中的UE 110的框图。UE 110包括无线电接口组件602、一个或多个处理器604、存储器606、用户接口组件608和电池610。无线电接口组件602是表示UE 110的本地无线电资源的硬件组件,例如RF单元620(例如,收发器)和一个或多个天线622,其用于经由无线电或“空中”信号与基站(例如,基站124)进行无线通信。处理器604表示提供UE 110的功能的内部电路系统、逻辑、硬件、软件等。处理器604可以被配置成对加载到存储器606中的软件执行指令640。取决于特定的实现方式,处理器604可以包括一个或多个处理器的集合,或者可以包括多处理器核心。存储器606是用于数据、指令640、应用程序等的计算机可读存储介质,并且可由处理器604访问。存储器606是能够临时和/或永久地存储信息的硬件存储装置。存储器606可以包括随机存取存储器或任何其他易失性或非易失性存储装置。用户接口组件608是用于与最终用户进行交互的硬件组件。例如,用户接口组件608可以包括显示器650、屏幕、触摸屏等(例如,液晶显示器(LCD)、发光二极管(LED)显示器等)。用户接口组件608可以包括键盘或小键盘652、跟踪装置(例如,轨迹球或触控板)、扬声器、麦克风等。UE 110还包括通用集成电路卡(UICC)660,其是为UE 110提供安全和完整性功能的硬件装置。UICC 660可以托管通用订户标识模块(USIM)662,所述USIM存储或指示用于UE 110的HPLMN的一个或多个公钥以及其他凭证。UE 110可以包括图6中未具体示出的各种其他组件。

[0069] 处理器604可以实现一个或多个应用程序630。这些应用程序630可以通过RAN 120和核心网络130访问下行链路(DL)数据,并且还可以生成用于通过RAN 120和核心网络130传输到目的地的上行链路(UL)数据。处理器604还实现被配置成控制NAS过程的NAS控制器634,如下面更详细地描述。

[0070] 图7是说明性实施方案中的网络元件132的框图。网络元件132是处理UE的安全和注册的服务器、装置、设备、装备(包括硬件)、系统、构件等。例如,网络元件132可以包括LTE网络中的MME214、下一代网络的AMF元件314等。在此实施方案中,网络元件132包括在一个或多个平台上运行的以下子系统:网络接口组件702、安全管理器704和注册管理器706。网络接口组件702可以包括被配置成与其他网络元件和/或UE(例如,通过RAN 120)交换控制

平面消息或信令的电路系统、逻辑、硬件、构件等。网络接口组件702可以使用多种协议(包括NAS协议)或参考点进行操作。安全管理器704可以包括电路系统、逻辑、硬件、构件等,其被配置成处理UE的认证和/或安全过程,例如创建NAS安全上下文,选择用于NAS安全上下文的NAS安全算法等。注册管理器706可以包括被配置成处理UE的注册的电路系统、逻辑、硬件、构件等。

[0071] 网络元件132的一个或多个子系统可以在由模拟和/或数字电路系统组成的硬件平台上实现。网络元件132的一个或多个子系统可以在执行存储器732中存储的指令的处理器730上实现。处理器730包括被配置成执行指令的集成硬件电路,并且存储器732是用于数据、指令、应用程序等的非暂时性计算机可读存储介质,且可由处理器730访问。

[0072] 网络元件132可以包括图7中未具体示出的各种其他组件。

[0073] 当UE与接入安全管理实体(例如AMF、MME等)之间已经存在NAS安全上下文时,可以执行或调用NAS过程。NAS安全的目的是使用NAS安全密钥在控制平面中在UE与接入安全管理实体之间安全地传递NAS消息。每次对UE执行认证时,都会生成NAS安全密钥。在完成NAS安全设置之后,UE和接入安全管理实体将共享NAS加密密钥和NAS完整性密钥,这两个密钥分别用于NAS消息传输之前的加密和完整性保护。当不存在NAS安全上下文时,也可以执行或调用NAS过程。首先描述这种场景。

[0074] 示例1:无安全上下文

[0075] 图8是示出说明性实施方案中在UE 110中执行NAS过程的方法800的流程图。将参考图6中的UE 110来描述方法800的步骤,但是本领域技术人员将理解,方法800可以在其他网络或架构中执行。而且,本文描述的流程图的步骤也不是全部包括在内,且可以包括未示出的其他步骤,并且这些步骤可以按可替代的顺序执行。

[0076] 对于此实施方案,可以假设在UE 110与网络元件132之间不存在NAS通信会话。可以进一步假设UE 110处于非连接模式(例如,空闲模式),并且正在转变为连接模式。UE 110中的NAS控制器634发起NAS过程以在UE 110与网络元件132之间建立NAS通信会话(步骤802)。例如,NAS过程可以包括注册过程。每个NAS过程包括强制性NAS协议IE集,并且还可以包括用于传输信息的可选NAS协议IE集。因此,NAS控制器634可以识别用于NAS过程的NAS协议IE(强制性和可选的)。

[0077] 在此实施方案中,NAS过程在多个阶段831至832中执行。对于NAS过程的第一阶段831,NAS控制器634识别指定用于安全相关处理的NAS协议IE的子集(步骤804)。指定用于安全相关处理的NAS协议IE的子集是指用于为UE创建或建立NAS安全上下文的IE。可能期望在第一阶段831中提供最少的信息,因此NAS协议IE的子集可以包括用于NAS过程的用于建立NAS安全上下文的最小数量的IE。对于注册过程,在一个示例中,NAS协议IE的子集可以由以下项组成:UE的移动身份(例如5G-GUTI或订阅隐藏标识符(SUCI))、指示UE支持的一种或多种安全算法的UE安全能力、注册类型(例如,初始、移动性、周期性、紧急情况等),以及UE的NAS安全上下文的安全密钥集标识符(例如,ngKSI、eKSI等)。

[0078] NAS控制器634可以格式化或生成用于NAS过程的初始NAS消息,例如类型为“初始”的注册请求。初始NAS消息是指在UE从非连接模式(例如,空闲模式)转变为连接模式之后发送的第一NAS消息。NAS控制器634将NAS协议IE的子集包括在或插入初始NAS消息中(步骤806)。在第一阶段831中,用NAS协议IE的子集填充初始NAS消息,并且在初始NAS消息中填充

的IE被限制为选择用于安全相关处理的NAS协议IE的子集(即,仅由其组成或唯一地由其组成)。因为初始NAS消息不包括用于NAS过程的所有强制性NAS协议IE,所以在第一阶段831中,初始NAS消息被视为“部分”消息。从子集中排除的其他强制性NAS协议IE将包括在另一个NAS消息中(作为第二阶段832的一部分)。然后,NAS控制器634将初始NAS消息发送至网络元件132(步骤810)。

[0079] 在发送初始NAS消息之前,NAS控制器634可以可选地使用用于UE 110的HPLMN的公钥来对初始NAS消息中的NAS协议IE的子集进行加密(可选步骤808)。每个HPLMN可以根据椭圆曲线整体加密方案(ECIES)分配公钥。根据保护方案,可能会有多个公钥。HPLMN的公钥通常在UE 110的USIM 662上提供。因此,NAS控制器634能够对在初始NAS消息中为第一阶段831识别的NAS协议IE的子集进行加密。关于是否使用公钥对NAS协议IE的子集进行加密的决定可以基于策略或标准。例如,当注册类型不指示紧急时(例如,注册类型=初始),NAS控制器634可以对NAS协议IE的子集进行加密,而当注册类型指示紧急时,所述NAS控制器可以发送未加密的初始NAS消息。在另一示例中,当UE 110在其USIM 662上编程了公钥时,NAS控制器634可以对NAS协议IE的子集进行加密,而当UE 110未在USIM 662上编程公钥时,所述NAS控制器可以发送未加密的初始NAS消息。

[0080] 图9是示出说明性实施方案中在网络元件132中执行NAS过程的方法900的流程图。将参考图7中的网络元件132来描述方法900的步骤,但是本领域技术人员将理解,方法900可以在其他网络或架构中执行。

[0081] 对于第一阶段831,网络元件132的网络接口组件702从UE 110接收初始NAS消息(步骤902)。在接收到初始NAS消息之后,安全管理器704可以可选地处理初始NAS消息,以确定是否使用HPLMN的公钥来对信息进行加密。当初始NAS消息被加密时,安全管理器704可以发起对初始NAS消息中的NAS协议IE的子集的解密(可选步骤904)。在一个示例中,安全管理器704可以被配置成在内部对NAS协议IE的子集进行解密。在另一个示例中,安全管理器704可以将NAS协议IE的子集发送至另一个网络元件(例如,UDM元件312)以对NAS协议IE的子集进行解密。

[0082] 安全管理器704处理NAS协议IE的子集,并确定对于UE 110不存在NAS安全上下文(步骤906)。因为不存在NAS安全上下文,所以安全管理器704可以发起认证过程以认证UE 110(步骤908)。认证过程(例如,认证和密钥协商(AKA))用于在UE 110与移动网络100之间执行相互认证。尽管认证过程可能不同,但是通常,安全管理器704可以通过网络接口组件702将认证请求连同认证令牌一起发送至UE 110(可选步骤910)。响应于认证请求,UE 110在其终端处理认证步骤,并尝试验证认证令牌(参见图8的步骤812)。如果成功,则UE 110将移动网络100视为已认证。UE 110计算响应令牌,并发送带有响应令牌的认证响应,安全管理器704通过网络接口组件702接收所述响应令牌(可选步骤912)。然后,安全管理器704(或另一个网络元件)可以确定响应令牌是否有效(例如,将响应令牌与预期响应令牌进行比较)。如果响应令牌有效,则安全管理器704将UE 110视为已认证。

[0083] 在UE 110已验证的情况下,安全管理器704发起NAS安全过程以建立NAS安全上下文(步骤914)。对于NAS安全过程,安全管理器704为NAS安全上下文选择一种或多种NAS安全算法(步骤916),并导出一个或多个NAS安全密钥(例如,K_{AMF}、K_{ASME}等)。NAS安全算法可以包括NAS加密算法和完整性保护算法。然后,安全管理器704通过网络接口组件702向UE发送响

应,所述响应指示或包括为NAS安全上下文选择的NAS安全算法和安全密钥集标识符(步骤918)。响应可以包括安全模式命令,所述安全模式命令包括NAS安全算法、安全密钥集标识符(例如,ngKSI、eKSI等)以及其他信息。

[0084] 在图8中,UE 110的NAS控制器634从网络元件132接收指示NAS安全算法和安全密钥集标识符的响应(步骤814)。利用在来自网络元件132的响应中提供的信息,在UE 110与网络元件132之间建立NAS安全上下文。因此,可以使用NAS安全上下文来保护UE 110与网络元件132之间的后续NAS消息。

[0085] 对于NAS过程的第二阶段832,NAS控制器634将用于NAS过程的NAS协议IE包括在或插入初始NAS消息中(步骤816)。初始NAS消息是先前在第一阶段831中发送至网络元件132的初始NAS消息的副本、复制或相同类型。在此步骤中,初始NAS消息包括用于NAS过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为初始NAS消息包括用于NAS过程的每个强制性NAS协议IE,所以在第二阶段832中,将初始NAS消息视为“完成的”NAS消息。

[0086] UE 110的NAS控制器634可以格式化或生成用于NAS过程的后续NAS消息。例如,后续NAS消息可以包括安全模式完成消息。NAS控制器634将初始NAS消息包括在或插入后续NAS消息的NAS消息容器中(步骤818)。NAS消息容器是一种用于封装普通NAS消息的IE。NAS控制器634使用NAS安全算法对后续NAS消息的NAS消息容器进行加密(步骤820)。因此,在后续NAS消息的NAS消息容器中对完成的初始NAS消息进行加密。然后,NAS控制器634将后续NAS消息发送至网络元件132(步骤822)。

[0087] 在图9中,对于第二阶段832,网络接口组件702从UE 110接收后续NAS消息(步骤920)。安全管理器704使用NAS安全算法对后续NAS消息的NAS消息容器进行解密(步骤922),以访问完成的初始NAS消息。然后,安全管理器704或网络元件132的其他子系统可以处理来自完成的初始NAS消息的NAS协议IE,以进一步执行NAS过程。例如,注册管理器706可以将注册接受消息发送至UE 110,并且从UE 110接收注册完成消息(可选步骤924)。此过程的一个技术益处是,仅建立NAS安全上下文所需的NAS协议IE根据部分初始NAS消息中的HPLMN公钥以未加密或加密的形式发送,而完成的初始NAS消息在后续NAS消息中加密,这提供进一步的安全保护。

[0088] 图10是示出在说明性实施方案中当UE没有安全上下文时的NAS过程的消息图。图10所示的NAS过程是注册过程,但是类似的概念可以应用于其他NAS过程。此示例以5G网络示出,其中网络元件132包括AMF元件314。

[0089] 此NAS过程再次以多个阶段执行。对于第一阶段,UE 110生成或格式化针对NAS注册过程的初始注册请求。NAS注册过程具有用于传输信息的NAS协议IE集(强制性和可选的)。在此实施方案中,UE 110在第一阶段中不使用完整NAS协议IE集填充初始注册请求。而是,UE 110识别对于建立NAS安全上下文必不可少的NAS协议IE。因此,UE 110识别指定用于安全相关处理的NAS协议IE的子集。在此示例中,NAS协议IE的子集可以由5G全球唯一临时身份(5G-GUTI)、UE安全能力、注册类型和ngKSI组成。UE 110将NAS协议IE的子集插入初始注册请求中。因为初始注册请求不包括用于NAS注册过程的所有强制性NAS协议IE,所以初始注册请求在第一阶段是“部分”请求。UE 110还可以将其他信息插入初始注册请求中,例如由UE 110生成的SUCI。在此示例中,UE 110使用HPLMN公钥对NAS协议IE的子集进行加密,并且将初始注册请求发送至AMF元件314(S1)。用于加密的保护方案和公钥标识符与SUCI中

指示的保护方案和公钥标识符相同。然而,如上所述,使用HPLMN公钥对NAS协议IE的子集进行加密是可选的。如果SUCI的保护方案为NULL,则不对NAS协议IE的子集进行加密。

[0090] 响应于接收到初始注册请求,AMF元件314基于UE的PLMN ID和路由ID将信息路由到UE的归属UDM以进行解密。因此,A MF元件314格式化或生成认证请求(即,Nausf_UEAuthentication_A uthenticate请求),并将加密的NAS协议IE的子集与其他信息(例如,SUCI和服务网络名称)一起插入认证请求中。然后,AMF元件314将认证请求发送至AUSF元件310(S2)。响应于接收到认证请求,AU SF元件310格式化或生成认证请求(即,Nudm_UEAuthentication_Ge t请求),并将NAS协议IE的加密子集连同其他信息一起插入认证请求中。然后,AUSF元件310将认证请求发送至UDM元件312(S3)。

[0091] 响应于认证请求,UDM元件312使用HPLMN私钥(即,使用根据为SUCI选择的保护方案的信息)对NAS协议IE的子集进行解密,使得NAS协议IE的子集是可读的。UDM元件312还托管与认证凭证存储库和处理功能(ARPF)有关的功能,所述功能选择认证方法并为AUSF元件310计算认证数据和密钥材料(例如,令牌)(如果需要)。UDM元件312格式化或生成针对AUSF元件310的认证响应(即,Nudm_UEAuthentication_Get响应),并将解密的NAS协议IE的子集、认证矢量(AV)和其他信息插入认证响应中。然后,UDM元件312将认证响应发送至AUSF元件310(S4)。响应于接收到认证响应,AUSF元件310格式化或生成针对AMF元件314的认证响应(即,Nuasf-_UEAuthentication_Authenticate响应),并将解密的NAS协议IE的子集、AV和其他信息插入认证响应中。然后,AUSF元件310将认证响应发送至AMF元件314(S5)。

[0092] AMF元件314被配置成使用由UDM/AUSF提供的信息来执行对UE 110的认证过程。例如,AMF元件314将认证请求连同来自AV的认证令牌(S6)一起发送至UE 110,并且UE 110尝试验证认证令牌。如果成功,则UE 110计算响应令牌,并发送带有所述响应令牌的认证响应,所述响应令牌由AMF元件314接收(S7)。AMF元件314格式化或生成另一个认证请求(即,Nausf_UEAuthentication_Auth enticate请求),并将来自UE 110的响应令牌连同其他信息一起插入认证请求中。然后,AMF元件314将认证请求发送至AUSF元件310(S8)。AUSF元件310验证来自UE 110的响应令牌是否与期望的响应令牌匹配,并且向AMF元件314发送指示认证成功/失败的认证响应(即,Nausf_UEAuthentication_Authenticate响应)。

[0093] 当UE 110被认证到网络时,AMF元件314发起NAS安全过程以建立NAS安全上下文。AMF元件314选择用于加密和完整性保护的NAS安全算法(或多种算法)。AMF元件314格式化或生成安全模式命令消息,并且将NAS安全算法的指示符、ngKSI和其他信息插入安全模式命令消息中。然后,AMF元件314将安全模式命令消息发送至UE 110(S10)。

[0094] 对于NAS过程的第二阶段,UE 110使用ngKSI和NAS安全算法来导出用于保护后续NAS消息的对应密钥。因此,在UE 110与AMF元件314之间建立了NAS安全上下文。UE 110将用于NAS注册过程的NAS协议IE包括在或插入初始注册请求中,所述初始注册请求是先前在第一阶段中发送的初始注册请求的消息的副本、复制或相同类型。初始注册请求包括所有强制性NAS协议IE,以及用于传输信息的任何可选的NAS协议IE。附加的NAS协议IE可以包括:非当前本机NAS密钥集标识符、5G移动管理(MM)能力、请求的网络片选择辅助信息(NSSAI)、上次访问的注册跟踪区域标识符(TAI)、S1 UE网络能力、上行链路数据状态、PDU会话状态、仅移动发起连接(MICO)指示、UE状态、附加GUTI、允许的PDU会话状态、UE的使用设置、请求的不连续接收(DRX)参数、EPS NAS消息容器,以及有效载荷容器。因此,初始注册请求在第

二阶段是“完成的”请求,因为它包括所有强制性NAS协议IE。UE 110格式化或生成安全模式完成消息,并将完成的初始注册请求插入安全模式完成消息的NAS消息容器中。UE 110使用NAS安全上下文的NAS安全算法来对安全模式完成消息的NAS消息容器进行加密。因此,在安全模式完成消息的NAS消息容器中对完成的初始注册请求进行加密。然后,UE 110将安全模式完成消息发送至AMF元件314(S11)。

[0095] AMF元件314从UE 110接收安全模式完成消息,并对安全模式完成消息的NAS消息容器进行解密以根据完成的初始注册请求访问NAS协议IE。然后,AMF元件314例如通过将注册接受消息发送至UE 110来继续注册过程(S12)。UE 110以注册完成消息来回复AMF元件314(S13),这时UE 110向网络注册以访问服务。

[0096] 示例2:无安全上下文

[0097] 在不存在安全上下文时的NAS过程的另一示例中,图11是示出说明性实施方案中在UE 110中执行NAS过程的方法1100的流程图。UE 110中的NAS控制器634发起NAS过程以在UE 110与网络元件132之间建立NAS通信会话(步骤1102)。NAS控制器634识别用于NAS过程的NAS协议IE(强制性和可选的)(步骤1104)。NAS控制器634可以格式化或生成用于NAS过程的第一初始NAS消息,并将NAS协议IE包括在或插入第一初始NAS消息中(步骤1106)。在此步骤中,第一初始NAS消息包括用于NAS过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第一初始NAS消息包括用于NAS过程的每个强制性NAS协议IE,所以将第一初始NAS消息视为“完成的”NAS消息。

[0098] NAS控制器634还格式化或生成作为第一初始NAS消息的复制的第二初始NAS消息(步骤1108)。复制消息是指用于NAS过程的相同类型的消息。例如,如果第一初始NAS消息是注册请求,则第二初始NAS消息也是注册请求。然而,复制消息中填充的IE可能与原始消息不同。NAS控制器634将第一初始NAS消息包括在或插入第二初始NAS消息的NAS消息容器中(步骤1110)。NAS控制器634使用用于UE 110的HPLMN的公钥对第二初始NAS消息的NAS消息容器进行加密(步骤1112)。因此,在第二初始NAS消息的NAS消息容器中对完成的第一初始NAS消息进行加密。然后,NAS控制器634将第二初始NAS消息发送至网络元件132(步骤1114)。

[0099] 图12是示出说明性实施方案中在网络元件132中执行NAS过程的方法1200的流程图。网络元件132的网络接口组件702从UE 110接收第二初始NAS消息(步骤1202)。当如此示例中那样对NAS消息容器进行加密时,安全管理器704发起对NAS消息容器的解密(步骤1204)以访问第一初始NAS消息。在一个示例中,安全管理器704可以被配置成对NAS消息容器进行解密。在另一个示例中,安全管理器704可以将NAS消息容器发送至另一个网络元件(例如,UDM元件312)以对NAS消息容器进行解密。

[0100] 在NAS消息容器被解密的情况下,安全管理器704可以访问第一初始NAS消息。用用于NAS过程的NAS协议IE填充第一初始NAS消息。安全管理器704可以处理NAS协议IE,并确定对于UE 110不存在NAS安全上下文(步骤1206)。因为不存在NAS安全上下文,所以安全管理器704可以发起认证过程以认证UE 110(步骤1208)。对于认证过程,安全管理器704可以通过网络接口组件702将认证请求连同认证令牌一起发送至UE 110(可选步骤1210)。响应于认证请求,UE 110在其终端处理认证步骤,并尝试验证认证令牌(参见图11的步骤1116)。如果成功,则UE 110将移动网络100视为已认证。UE 110计算响应令牌,并发送带有响应令牌

的认证响应,安全管理器704通过网络接口组件702接收所述响应令牌(可选步骤1212)。然后,安全管理器704(或另一个网络元件)可以确定响应令牌是否有效(例如,将响应令牌与预期响应令牌进行比较)。如果响应令牌有效,则安全管理器704将UE 110视为已认证。

[0101] 在UE 110已验证的情况下,安全管理器704发起NAS安全过程以建立NAS安全上下文(步骤1214)。对于NAS安全过程,安全管理器704为NAS安全上下文选择一种或多种NAS安全算法(步骤1216),并导出一个或多个NAS安全密钥(例如,K_{AMF}、K_{ASME}等)。然后,安全管理器704格式化或生成安全模式命令,并通过网络接口组件702将安全模式命令发送至UE 110,所述安全模式命令指示或包括为NAS安全上下文选择的NAS安全算法和安全密钥集标识符(步骤1218)。

[0102] 在图11中,UE 110的NAS控制器634从网络元件132接收指示NAS安全算法的安全模式命令(步骤1118)。利用在安全模式命令中提供的信息,在UE 110与网络元件132之间建立NAS安全上下文。因此,可以使用NAS安全上下文来保护UE 110与网络元件132之间的后续NAS消息。然后,UE 110的NAS控制器634可以格式化或生成安全模式完成消息,并将安全模式完成消息发送至网络元件132(步骤1120)。在图12中,网络接口组件702从UE 110接收安全模式完成(步骤1220)。安全管理器704可以使用NAS安全算法对任何后续NAS消息进行解密。此过程的一个技术益处是,仅建立NAS安全上下文所需的NAS协议IE在部分初始NAS消息中以未加密的形式插入,而完成的初始NAS消息在部分初始NAS消息中加密,这提供进一步的安全保护。

[0103] 图13是示出在说明性实施方案中当UE没有安全上下文时的NAS过程的消息图。图13所示的NAS过程是注册过程,但是类似的概念可以应用于其他NAS过程。UE 110生成或格式化针对NAS注册过程的注册请求。在此实施方案中,UE 110用整个NAS协议IE集填充注册请求。因此,注册请求是完成的注册请求。

[0104] UE 110还生成或格式化另一个注册请求,所述另一个注册请求是完成的注册请求的复制。另一个注册请求的类型为“初始”,因此是初始注册请求。代替对完成的注册请求中的每个强制性NAS协议IE进行填充,UE 110将完成的注册请求插入初始注册请求的NAS消息容器中。UE 110还可以将其他信息插入初始注册请求中,例如由UE 110生成的SUCI。在此示例中,UE 110使用HPLMN公钥对初始注册请求的NAS消息容器进行加密,并将初始注册请求发送至AMF元件314(S1)。

[0105] 响应于接收到初始注册请求,AMF元件314基于UE的PLMN ID和路由ID将信息路由到UE的归属UDM以进行解密。因此,A MF元件314格式化或生成认证请求(即,Nausf_UEAuthentication_A uthenticate请求),并将初始注册请求的加密的NAS消息容器连同其他信息一起插入认证请求中。然后,AMF元件314将认证请求发送至AUSF元件310(S2)。响应于接收到认证请求,AUSF元件310格式化或生成认证请求(即,Nudm_UEAuthentication_Get请求),并将加密的NAS消息容器连同其他信息一起插入认证请求中。然后,AUS F元件310将认证请求发送至UDM元件312(S3)。

[0106] 响应于认证请求,UDM元件312使用HPLMN私钥对加密的NAS消息容器进行解密,使得完成的注册请求是可读的。UDM元件312还选择认证方法,并为AUSF元件310计算认证数据和密钥材料(例如,令牌)(如果需要)。UDM元件312格式化或生成针对AUSF元件310的认证响应(即,Nudm_UEAuthentication_Get响应),并将解密的NAS消息容器、认证矢量(AV)和其他

信息插入认证响应中。然后,UDM元件312将认证响应发送至AUSF元件310(S4)。响应于接收到认证响应,AUSF元件310格式化或生成针对AMF元件314的认证响应(即,Nuasf-_UEAuthentication_Authenticate响应),并将解密的NAS消息容器、AV和其他信息插入认证响应中。然后,AUSF元件310将认证响应发送至AMF元件314(S5)。

[0107] AMF元件314被配置成使用由UDM/AUSF提供的信息来执行对UE 110的认证过程。例如,AMF元件314将认证请求连同来自AV的认证令牌(S6)一起发送至UE 110,并且UE 110尝试验证认证令牌。如果成功,则UE 110计算响应令牌,并发送带有所述响应令牌的认证响应,所述响应令牌由AMF元件314接收(S7)。AMF元件314格式化或生成另一个认证请求(即,Nausf_UEAuthentication_Auth enticate请求),并将来自UE 110的响应令牌连同其他信息一起插入认证请求中。然后,AMF元件314将认证请求发送至AUSF元件310(S8)。AUSF元件310验证来自UE 110的响应令牌是否与期望的响应令牌匹配,并且向AMF元件314发送指示认证成功/失败的认证响应(即,Nausf_UEAuthentication_Authenticate响应)。

[0108] 当UE 110被认证到网络时,AMF元件314发起NAS安全过程以建立NAS安全上下文。AMF元件314选择用于加密和完整性保护的NAS安全算法(或多种算法)。AMF元件314格式化或生成安全模式命令消息,并且将NAS安全算法的指示符、ngKSI和其他信息插入安全模式命令消息中。然后,AMF元件314将安全模式命令消息发送至UE 110(S10)。UE 110使用ngKSI和NAS安全算法来导出用于保护后续NAS消息的相应密钥。因此,在UE 110与AMF元件314之间建立了安全上下文。UE 110格式化或生成安全模式完成消息,并将安全模式完成消息发送至AMF元件314(S11)。

[0109] AMF元件314例如通过将注册接受消息发送至UE 110来继续注册过程(S12)。UE 110以注册完成消息来回复AMF元件314(S13),这时UE 110向网络注册以访问服务。

[0110] 示例3:存在安全上下文-安全上下文有效

[0111] 在另外的示例中,当UE与接入安全管理实体(例如AMF、MME等)之间已经存在NAS安全上下文时,可以执行或调用NAS过程。以下提供存在NAS安全上下文时NAS过程的示例。

[0112] 图14是示出说明性实施方案中在UE 110中执行NAS过程的方法1400的流程图。UE 110中的NAS控制器634发起NAS过程以在UE 110与网络元件132之间建立(或重新建立)NAS通信会话(步骤1402)。NAS控制器634识别指定用于安全相关处理的NAS协议IE的子集(步骤1404)。NAS控制器634格式化或生成用于NAS过程的第一NAS消息,例如类型为“移动性”、“周期性”等的注册请求。NAS控制器634将NAS协议IE的子集包括在或插入第一NAS消息中(步骤1406)。

[0113] NAS控制器634还格式化或生成作为第一NAS消息的复制的第二NAS消息。NAS控制器634将用于NAS过程的NAS协议IE包括在或插入第二NAS消息中(步骤1408)。在此步骤中,第二NAS消息包括用于NAS过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第二NAS消息包括用于NAS过程的每个强制性NAS协议IE,所以将第二NAS消息视为“完成的”NAS消息。

[0114] NAS控制器634将第二NAS消息包括在或插入第一NAS消息的NAS消息容器中(步骤1410)。NAS控制器634使用NAS安全上下文的NAS安全算法对第一NAS消息的NAS消息容器进行加密(步骤1412)。因此,在第一NAS消息的NAS消息容器中对完成的第二NAS消息进行加密。然后,NAS控制器634将第一NAS消息发送至网络元件132(步骤1414)。

[0115] 图15是示出说明性实施方案中在网络元件132中执行NAS过程的方法1500的流程图。网络元件132的网络接口组件702从UE 110接收第一NAS消息(步骤1502)。安全管理器704处理第一NAS消息中的NAS协议IE的子集,以识别用于UE 110的NAS安全上下文(步骤1504)。然后,安全管理器704使用NAS安全上下文对第一NAS消息的NAS消息容器进行解密,以访问包含在NAS消息容器中的第二NAS消息(步骤1506)。在第一NAS消息中的NAS消息容器被解密的情况下,安全管理器704可以访问已解密的第二NAS消息。用用于NAS过程的NAS协议IE填充第二NAS消息。因此,安全管理器704可以处理第二NAS消息中的NAS协议IE,以继续对NAS过程的进一步处理(步骤1508)。此过程的一个技术益处是,仅识别NAS安全上下文所需的NAS协议IE在第一NAS消息中以未加密的形式发送,而完成的第二NAS消息在第一NAS消息中加密,这提供进一步的安全保护。

[0116] 图16是示出在说明性实施方案中当UE具有有效安全上下文时的NAS注册过程的消息图。UE 110生成或格式化针对NAS注册过程的第一注册请求。在此实施方案中,UE 110用指定用于安全相关处理的NAS协议IE的子集填充第一注册请求。此信息用于向AMF元件314指示NAS安全上下文。例如,NAS协议IE的子集可以包括5G-GUTI、注册类型和ngKSI。UE 110还格式化或生成第二注册请求,所述第二注册请求是第一注册请求的复制。UE 110将用于NAS注册过程的NAS协议IE包括在或插入第二注册请求中。在此步骤中,第二注册请求包括用于NAS注册过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第二注册请求包括用于NAS注册过程的每个强制性NAS协议IE,所以将第二注册请求视为“完成的”注册请求。

[0117] UE 110将第二注册请求包括在或插入第一注册请求的NAS消息容器中,并且使用NAS安全上下文的NAS安全算法对第一注册请求的NAS消息容器进行加密。因此,在第一注册请求的NAS消息容器中对完成的第二注册请求进行加密。然后,UE 110将第一注册请求发送至AMF元件314(S1)。

[0118] 响应于接收到第一注册请求,AMF元件314基于包括在第一注册请求中的NAS协议IE的子集来识别或检索NAS安全上下文。然后,AMF元件314使用NAS安全上下文对第一注册请求的加密的NAS消息容器进行解密,使得第二注册请求是可读的。因此,AMF元件314能够处理用于NAS注册过程的整个NAS协议IE集,并且继续对NAS注册过程的处理。例如,AMF元件314将注册接受消息发送至UE 110(S2)。UE 110以注册完成消息来回复AMF元件314(S3),这时UE 110向网络注册以访问服务。

[0119] 图17是示出在说明性实施方案中当UE具有有效安全上下文时的NAS服务请求过程的消息图。UE 110生成或格式化针对NAS服务请求过程的第一服务请求。在此实施方案中,UE 110用指定用于安全相关处理的NAS协议IE的子集填充第一服务请求,所述NAS协议IE的子集用于向AMF元件314指示NAS安全上下文。在此示例中,NAS协议IE的子集可以包括5G-S-TMSI和ngKSI。UE 110还格式化或生成第二服务请求,所述第二服务请求是第一服务请求的复制。UE 110将用于NAS服务请求过程的NAS协议IE包括在或插入第二服务请求中。在此步骤中,第二服务请求包括用于NAS服务请求过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第二服务请求包括用于NAS服务请求过程的每个强制性NAS协议IE,所以将第二服务请求视为“完成的”服务请求。

[0120] UE 110将第二服务请求包括在或插入第一服务请求的NAS消息容器中,并且使用

NAS安全上下文的NAS安全算法对第一服务请求的NAS消息容器进行加密。因此,在第一服务请求的NAS消息容器中对完成的第二服务请求进行加密。然后,UE 110将第一服务请求发送至AMF元件314(S1)。

[0121] 响应于接收到第一服务请求,AMF元件314基于包括在第一服务请求中的NAS协议IE的子集来识别或检索NAS安全上下文。然后,AMF元件314使用NAS安全上下文对第一服务请求的加密的NAS消息容器进行解密,使得第二服务请求是可读的。因此,AMF元件314能够处理用于NAS服务请求过程的整个NAS协议IE集,并且继续对NAS服务请求过程的处理。例如,AMF元件314将服务接受消息发送至UE 110(S2)。

[0122] 图18是示出在说明性实施方案中当UE具有有效安全上下文时的NAS注销过程的消息图。UE 110生成或格式化针对NAS注销过程的第一注销请求。在此实施方案中,UE 110用指定用于安全相关处理的NAS协议IE的子集填充第一注销请求,所述NAS协议IE的子集用于向AMF元件314指示NAS安全上下文。在此示例中,NAS协议IE的子集可以包括5G-S-TMSI和ngKSI。UE 110还格式化或生成第二注销请求,所述第二注销请求是第一注销请求的复制。UE 110将用于NAS注销过程的NAS协议IE包括在或插入第二注销请求中。在此步骤中,第二注销请求包括用于NAS注销过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第二注销请求包括用于NAS注销过程的每个强制性NAS协议IE,所以将第二注销请求视为“完成的”注销请求。

[0123] UE 110将第二注销请求包括在或插入第一注销请求的NAS消息容器中,并且使用NAS安全上下文的NAS安全算法对第一注销请求的NAS消息容器进行加密。因此,在第一注销请求的NAS消息容器中对完成的第二注销请求进行加密。然后,UE 110将第一注销请求发送至AMF元件314(S1)。

[0124] 响应于接收到第一注销请求,AMF元件314基于包括在第一注销请求中的NAS协议IE的子集来识别或检索NAS安全上下文。然后,AMF元件314使用NAS安全上下文对第一注销请求的加密的NAS消息容器进行解密,使得第二注销请求是可读的。因此,AMF元件314能够处理用于NAS注销过程的整个NAS协议IE集,并且继续对NAS注销过程的处理。例如,AMF元件314将注销接受消息发送至UE 110(S2)。

[0125] 示例4:存在安全上下文-安全上下文无效或找不到

[0126] 图19A至图19B是示出说明性实施方案中在UE 110中执行NAS过程的方法1900的流程图。UE 110中的NAS控制器634发起NAS过程以在UE 110与网络元件132之间建立(或重新建立)NAS通信会话(步骤1902)。对于NAS过程的第一阶段1931,NAS控制器634识别指定用于安全相关处理的NAS协议IE的子集(步骤1904)。NAS控制器634格式化或生成用于NAS过程的第一NAS消息,并将NAS协议IE的子集包括在或插入第一NAS消息中(步骤1906)。

[0127] NAS控制器634还格式化或生成作为第一NAS消息的复制的第二NAS消息。NAS控制器634将用于NAS过程的NAS协议IE包括在或插入第二NAS消息中(步骤1908)。在此步骤中,第二NAS消息包括用于NAS过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第二NAS消息包括用于NAS过程的每个强制性NAS协议IE,所以将第二NAS消息视为“完成的”NAS消息。

[0128] NAS控制器634将第二NAS消息包括在或插入第一NAS消息的NAS消息容器中(步骤1910)。NAS控制器634使用NAS安全上下文的NAS安全算法对第一NAS消息的NAS消息容器进

行加密(步骤1912)。因此,在第一NAS消息的NAS消息容器中对完成的第二NAS消息进行加密。然后,NAS控制器634将第一NAS消息发送至网络元件132(步骤1914)。

[0129] 图20是示出说明性实施方案中在网络元件132中执行NAS过程的方法2000的流程图。对于NAS过程的第一阶段1931,网络元件132的网络接口组件702从UE 110接收第一NAS消息(步骤2002)。安全管理器704处理第一NAS消息中的NAS协议IE的子集,并且未能识别用于UE 110的有效NAS安全上下文(步骤2004)。例如,即使存在NAS安全上下文,安全管理器704也可能无法基于第一NAS消息中提供的NAS协议IE的子集来识别NAS安全上下文,基于NAS协议IE的子集识别的NAS安全上下文无效等。因为没有找到有效NAS安全上下文,所以安全管理器704发起认证过程以认证UE 110(步骤2006)。即使可能先前已经执行认证过程,但是当没有找到有效NAS安全上下文时,安全管理器704会再次执行认证过程。作为认证过程的一部分,安全管理器704可以通过网络接口组件702将认证请求连同认证令牌一起发送至UE 110(可选步骤2008)。响应于认证请求,UE 110尝试验证认证令牌(参见图19A的步骤1916)。如果成功,则UE 110将移动网络100视为已认证。UE 110计算响应令牌,并发送带有响应令牌的认证响应,安全管理器704通过网络接口组件702接收所述响应令牌(可选步骤2010)。然后,安全管理器704(或另一个网络元件)可以确定响应令牌是否有效(例如,将响应令牌与预期响应令牌进行比较)。如果响应令牌有效,则安全管理器704将UE 110视为已认证。

[0130] 在UE 110已验证的情况下,安全管理器704发起NAS安全过程以建立新的NAS安全上下文(步骤2012)。对于NAS安全过程,安全管理器704为新的NAS安全过程选择一种或多种NAS安全算法(步骤2014),并导出一个或多个NAS安全密钥。然后,安全管理器704通过网络接口组件702向UE 110发送响应(步骤2016),所述响应指示或包括为新的NAS安全上下文选择的NAS安全算法和安全密钥集标识符。响应可以包括安全模式命令,所述安全模式命令包括NAS安全算法、安全密钥集标识符(例如,ngKSI、eKSI等)以及其他信息。

[0131] 在图19A中,NAS控制器634从网络元件132接收指示NAS安全算法和安全密钥集标识符的响应(步骤1918)。利用在来自网络元件132的响应中提供的信息,在UE 110与网络元件132之间建立新的NAS安全上下文。因此,可以使用新的NAS安全上下文来保护UE 110与网络元件132之间的后续NAS消息。

[0132] 对于图19B中的NAS过程的第二阶段1932,UE 110的NAS控制器634然后可以格式化或生成用于NAS过程的后续NAS消息。例如,后续NAS消息可以包括安全模式完成消息。NAS控制器634将用于NAS过程的第二NAS消息包括或插入后续NAS消息的NAS消息容器中(步骤1920)。如上所述,第二NAS消息包括用于NAS过程的整个NAS协议IE集(强制性和可选的(如果需要)),并且被视为“完成的”NAS消息。NAS控制器634使用新的NAS安全上下文的NAS安全算法对后续NAS消息的NAS消息容器进行加密(步骤1922)。然后,NAS控制器634将后续NAS消息发送至网络元件132(步骤1924)。

[0133] 在图20中,对于第二阶段1932,网络接口组件702从UE 110接收后续NAS消息(步骤2018)。安全管理器704使用新NAS安全上下文的NAS安全算法对后续NAS消息的NAS消息容器进行解密(步骤2020),以访问完成的第二NAS消息。然后,安全管理器704或网络元件132的其他子系统可以处理来自完成的第二NAS消息的NAS协议IE,以提供对NAS过程的进一步处理。此过程的一个技术益处是,仅识别NAS安全上下文所需的NAS协议IE在第一NAS消息中以

未加密的形式发送。当找不到有效的NAS安全上下文时,建立新的NAS安全上下文,并根据新的NAS安全上下文在后续NAS消息中对完成的NAS消息进行加密,从而提供进一步的安全保护。

[0134] 图21是示出在说明性实施方案中当UE具有NAS安全上下文,但NAS安全上下文无效或未找到时的NAS注册过程的消息图。对于NAS过程的第一阶段,UE 110生成或格式化针对NAS注册过程的第一注册请求。在此实施方案中,UE 110用指定用于安全相关处理的NAS协议IE的子集填充第一注册请求。此信息用于向AMF元件314指示NAS安全上下文。例如,NAS协议IE的子集可以包括5G-GUTI、注册类型和ngKSI。UE 110还格式化或生成第二注册请求,所述第二注册请求是第一注册请求的复制。UE 110将用于NAS注册过程的NAS协议IE包括在或插入第二注册请求中。在此步骤中,第二注册请求包括用于NAS注册过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第二注册请求包括用于NAS注册过程的每个强制性NAS协议IE,所以将第二注册请求视为"完成的"注册请求。

[0135] UE 110将第二注册请求包括在或插入第一注册请求的NAS消息容器中,并且使用NAS安全上下文的NAS安全算法对第一注册请求的NAS消息容器进行加密。因此,在第一注册请求的NAS消息容器中对完成的第二注册请求进行加密。然后,UE 110将第一注册请求发送至AMF元件314(S1)。

[0136] 响应于接收到第一注册请求,AMF元件314基于包括在第一注册请求中的NAS协议IE的子集来尝试识别或检索NAS安全上下文。在此示例中,AMF元件314无法识别用于UE 110的有效NAS安全上下文。因此,AMF元件314无法对第一注册请求的NAS消息容器进行解密。为了允许安全通信,AMF元件314发起新的认证过程以创建新的NAS安全上下文。AMF元件314格式化或生成认证请求(即,Nausf_UEAuthentication_Authenticate请求),并将认证请求发送至AUSF元件310(S2)。响应于接收到认证请求,AUSF元件310格式化或生成认证请求(即,Nudm-_UEAuthentication_Get请求),并将认证请求发送至UDM元件312(S3)。

[0137] 响应于认证请求,UDM元件312使SUCI去隐藏,并将认证响应(即,Nudm_UEAuthentication_Get响应)发送至AUSF元件310(S4)。响应于接收到认证响应,AUSF元件310格式化或生成用于AMF元件314的认证响应(即,Nuasf-_UEAuthentication_Authenticate响应),并将认证响应发送至AMF元件314(S5)。

[0138] AMF元件314被配置成使用由UDM/AUSF提供的信息来执行对UE 110的认证过程。例如,AMF元件314将认证请求连同认证令牌一起发送至UE 110(S6),并且UE 110尝试验证认证令牌。如果成功,则UE 110计算响应令牌,并发送带有所述响应令牌的认证响应,所述响应令牌由AMF元件314接收(S7)。AMF元件314格式化或生成另一个认证请求(即,Nausf_UEAuthentication_Authenticate请求),并将来自UE 110的响应令牌连同其他信息一起插入认证请求中。然后,AMF元件314将认证请求发送至AUSF元件310(S8)。AUSF元件310验证来自UE 110的响应令牌是否与期望的响应令牌匹配,并且向AMF元件314发送指示认证成功/失败的认证响应(即,Nausf_UEAuthentication_Authenticate响应)。

[0139] 当UE 110被认证到网络时,AMF元件314发起NAS安全过程以建立新的NAS安全上下文。AMF元件314选择用于加密和完整性保护的NAS安全算法(或多种算法)。AMF元件314格式化或生成安全模式命令消息,并且将NAS安全算法的指示符、ngKSI和其他信息插入安全模式命令消息中。然后,AMF元件314将安全模式命令消息发送至UE 110(S10)。

[0140] 对于NAS过程的第二阶段,UE 110使用ngKSI和NAS安全算法来导出用于保护后续NAS消息的对应密钥。因此,在UE 110与AMF元件314之间建立了新的NAS安全上下文。UE 110格式化或生成安全模式完成消息,并将第二注册请求插入安全模式完成消息的NAS消息容器中。如上所述,第二注册请求包括用于NAS注册过程的整个NAS协议IE集(强制性和可选的(如果需要)),并且被视为"完成的"NAS消息。UE 110使用新的NAS安全上下文的NAS安全算法来对安全模式完成消息的NAS消息容器进行加密。因此,在安全模式完成消息的NAS消息容器中对第二注册请求进行加密。然后,UE 110将安全模式完成消息发送至AMF元件314(S11)。

[0141] AMF元件314从UE 110接收安全模式完成消息,并对安全模式完成消息的NAS消息容器进行解密以根据第二注册请求访问NAS协议IE。然后,AMF元件314例如通过将注册接受消息发送至UE 110来继续NAS注册过程(S12)。UE 110以注册完成消息来回复AMF元件314(S13),这时UE 110向网络注册以访问服务。

[0142] 图22是示出在说明性实施方案中当UE具有NAS安全上下文,但NAS安全上下文无效或未找到时的NAS服务请求过程的消息图。对于NAS过程的第一阶段,UE 110生成或格式化用于NAS服务请求过程的第一服务请求。在此实施方案中,UE 110用指定用于安全相关处理的NAS协议IE的子集填充第一服务请求。此信息用于向AMF元件314指示NAS安全上下文。例如,NAS协议IE的子集可以包括5G-S-TMSI和ngKSI。UE 110还格式化或生成第二服务请求,所述第二服务请求是第一服务请求的复制。UE 110将用于NAS服务请求过程的NAS协议IE包括在或插入第二服务请求中。在此步骤中,第二服务请求包括用于NAS服务请求过程的整个NAS协议IE集(强制性和可选的(如果需要))。因为第二服务请求包括用于NAS服务请求过程的每个强制性NAS协议IE,所以将第二服务请求视为"完成的"服务请求。

[0143] UE 110将第二服务请求包括在或插入第一服务请求的NAS消息容器中,并且使用NAS安全上下文的NAS安全算法对第一服务请求的NAS消息容器进行加密。因此,在第一服务请求的NAS消息容器中对完成的第二服务请求进行加密。然后,UE 110将第一服务请求发送至AMF元件314(S1)。

[0144] 响应于接收到第一服务请求,AMF元件314基于包括在第一服务请求中的NAS协议IE的子集来尝试识别或检索NAS安全上下文。在此示例中,AMF元件314无法识别用于UE 110的有效NAS安全上下文。因此,AMF元件314无法对第一服务请求的NAS消息容器进行解密。为了允许安全通信,AMF元件314发起新的认证过程以创建新的NAS安全上下文。AMF元件314格式化或生成认证请求(即,Nausf_UEAuthentication_Authenticate请求),并将认证请求发送至AUSF元件310(S2)。响应于接收到认证请求,AUSF元件310格式化或生成认证请求(即,Nudm-_UEAuthentication_Get请求),并将认证请求发送至UDM元件312(S3)。

[0145] 响应于认证请求,UDM元件312使SUCI去隐藏,并将认证响应(即,Nudm_UEAuthentication_Get响应)发送至AUSF元件310(S4)。响应于接收到认证响应,AUSF元件310格式化或生成用于AMF元件314的认证响应(即,Nuasf-_UEAuthentication_Authenticate响应),并将认证响应发送至AMF元件314(S5)。

[0146] AMF元件314被配置成使用由UDM/AUSF提供的信息来执行对UE 110的认证过程。例如,AMF元件314将认证请求连同认证令牌一起发送至UE 110(S6),并且UE 110尝试验证认证令牌。如果成功,则UE 110计算响应令牌,并发送带有所述响应令牌的认证响应,所述响

应令牌由AMF元件314接收(S7)。AMF元件314格式化或生成另一个认证请求(即,Nausf_UEAuthentication_Authenticate请求),并将来自UE 110的响应令牌连同其他信息一起插入认证请求中。然后,AMF元件314将认证请求发送至AUSF元件310(S8)。AUSF元件310验证来自UE 110的响应令牌是否与期望的响应令牌匹配,并且向AMF元件314发送指示认证成功/失败的认证响应(即,Nausf_UEAuthentication_Authenticate响应)。

[0147] 当UE 110被认证到网络时,AMF元件314发起NAS安全过程以建立新的NAS安全上下文。AMF元件314选择用于加密和完整性保护的NAS安全算法(或多种算法)。AMF元件314格式化或生成安全模式命令消息,并且将NAS安全算法的指示符、ngKSI和其他信息插入安全模式命令消息中。然后,AMF元件314将安全模式命令消息发送至UE 110(S10)。

[0148] 对于NAS过程的第二阶段,UE 110使用ngKSI和NAS安全算法来导出用于保护后续NAS消息的对应密钥。因此,在UE 110与AMF元件314之间建立了新的NAS安全上下文。UE 110格式化或生成安全模式完成消息,并将第二服务请求插入安全模式完成消息的NAS消息容器中。如上所述,第二服务请求包括用于NAS服务请求过程的整个NAS协议IE集(强制性和可选的(如果需要)),并且被视为"完成的"NAS消息。UE 110使用新的NAS安全上下文的NAS安全算法来对安全模式完成消息的NAS消息容器进行加密。因此,在安全模式完成消息的NAS消息容器中对第二服务请求进行加密。然后,UE 110将安全模式完成消息发送至AMF元件314(S11)。

[0149] AMF元件314从UE 110接收安全模式完成消息,并对安全模式完成消息的NAS消息容器进行解密以根据第二服务请求访问NAS协议IE。然后,AMF元件314例如通过将注册接受消息发送至UE 110来继续NAS服务请求过程(S12)。UE 110用注册完成消息来答复AMF元件314(S13)。

[0150] 附图中所示或本文描述的各种元件或模块中的任何一个可以被实现为硬件、软件、固件或这些的某种组合。例如,元件可以被实现为专用硬件。专用硬件元件可以被称为"处理器"、"控制器"或一些类似的术语。当由处理器提供时,功能可以由单个专用处理器、单个共享处理器或多个单独的处理器提供,其中一些可以共享。此外,对术语"处理器"或"控制器"的明确使用不应解释为专门指代能够执行软件的硬件,并且可以隐含包括但不限于数字信号处理器(DSP)硬件、网络处理器、专用集成电路(ASIC)或其他电路系统、现场可编程门阵列(FPGA)、用于存储软件的只读存储器(ROM)、随机存取存储器(RAM)、非易失性存储装置、逻辑或某些其他物理硬件组件或模块。

[0151] 而且,元件可以被实现为可由处理器或计算机执行以执行所述元件的功能的指令。指令的一些示例是软件、程序代码和固件。指令在由处理器执行时是可操作的,以指导处理器执行元件的功能。指令可以存储在处理器可读的存储装置上。存储装置的一些示例是数字或固态存储器,例如磁盘和磁带的磁存储介质、硬盘驱动器或光学可读数字数据存储介质。

[0152] 如本申请中使用,术语"电路系统"可以指以下各项中的一者或多者或全部:

[0153] (a)纯硬件电路实现方式(例如仅模拟电路和/或数字电路系统中的实现方式);

[0154] (b)硬件电路和软件的组合,例如(如适用):

[0155] (i)模拟硬件电路和/或数字硬件电路与软件/固件的组合;和

[0156] (ii)具有软件的硬件处理器的任何部分(包括一起工作以使例如移动电话或服务

器的设备执行各种功能的数字信号处理器、软件和存储器);以及

[0157] (c)硬件电路和或处理器,例如微处理器或微处理器的一部分,其需要软件(例如,固件)进行操作,但在操作不需要所述软件时可不存在所述软件。

[0158] "电路系统"的这个定义适用于此术语在本申请、包括在任何权利要求中的所有用途。作为另一示例,如在本申请中所使用,术语"电路系统"还涵盖仅硬件电路或处理器(或多个处理器)的实现方式或硬件电路或处理器和其(或它们的)相伴软件和/或固件的部分的实现方式。术语"电路系统"还涵盖(例如并且在适用于特定权利要求要素的情况下)移动装置的基带集成电路或处理器集成电路或服务器、蜂窝网络装置或其他计算或网络装置中的类似集成电路。

[0159] 尽管本文描述了特定实施方案,但是本公开的范围不限于那些特定实施方案。本公开的范围由所附权利要求及其任何等同形式限定。

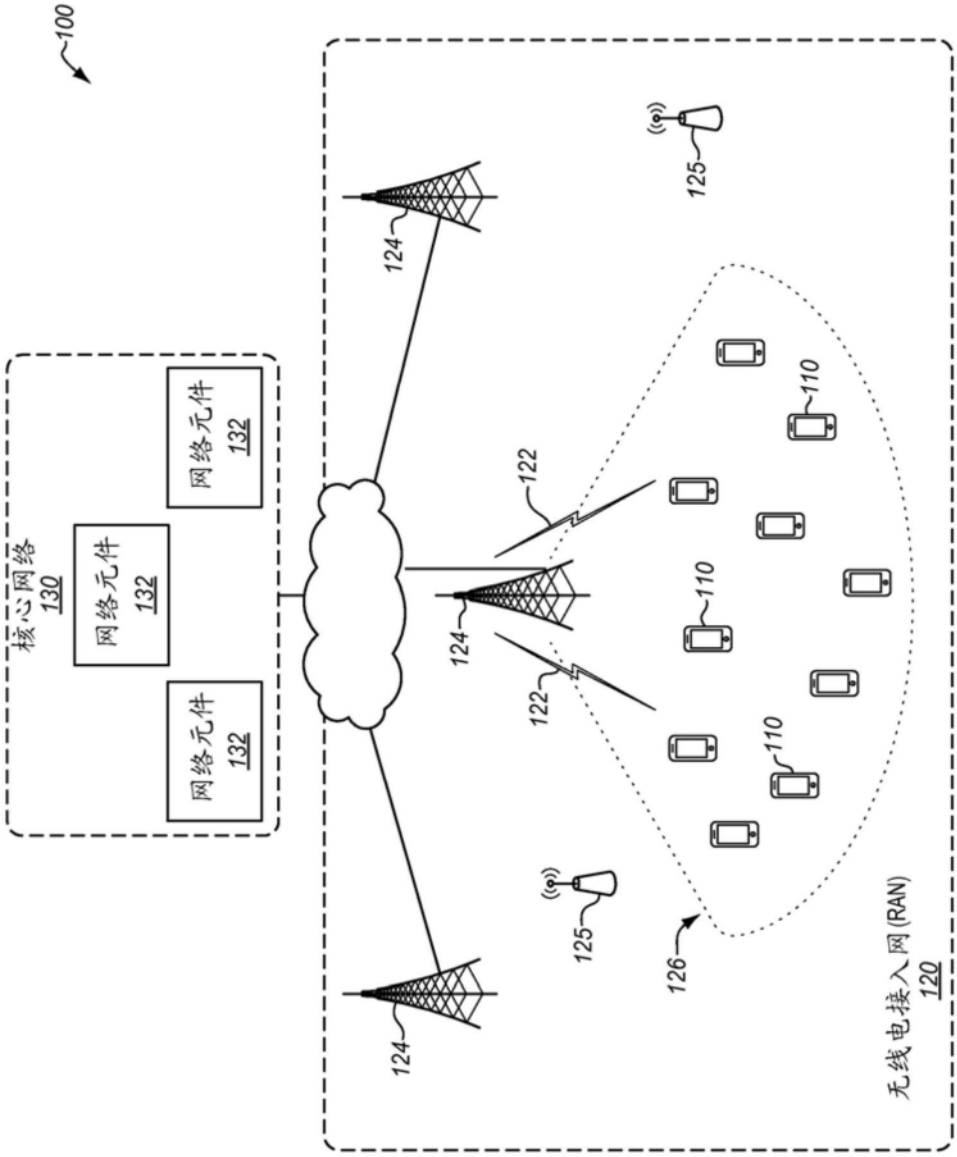

100
核心网络
130
网络元件
132
网络元件
132
网络元件
132
124
124
124
125
125
122
122
110
110
110
126
无线电接入网(RAN)
120

图1

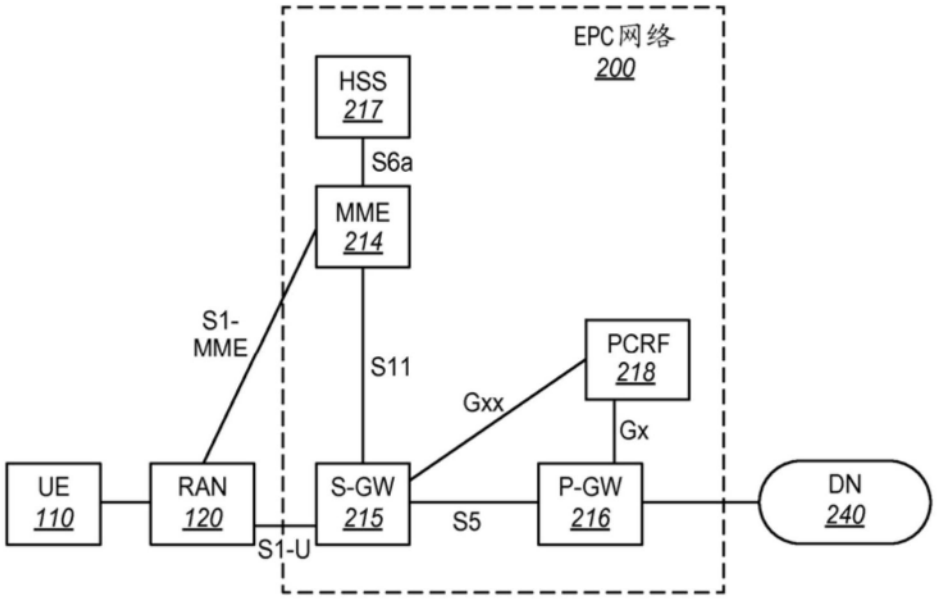

EPC网络
200
HSS
217
S6a
MME
214
S1-
MME
S11
PCRF
218
Gxx
Gx
UE
110
RAN
120
S-GW
215
S5
P-GW
216
DN
240
S1-U

图2

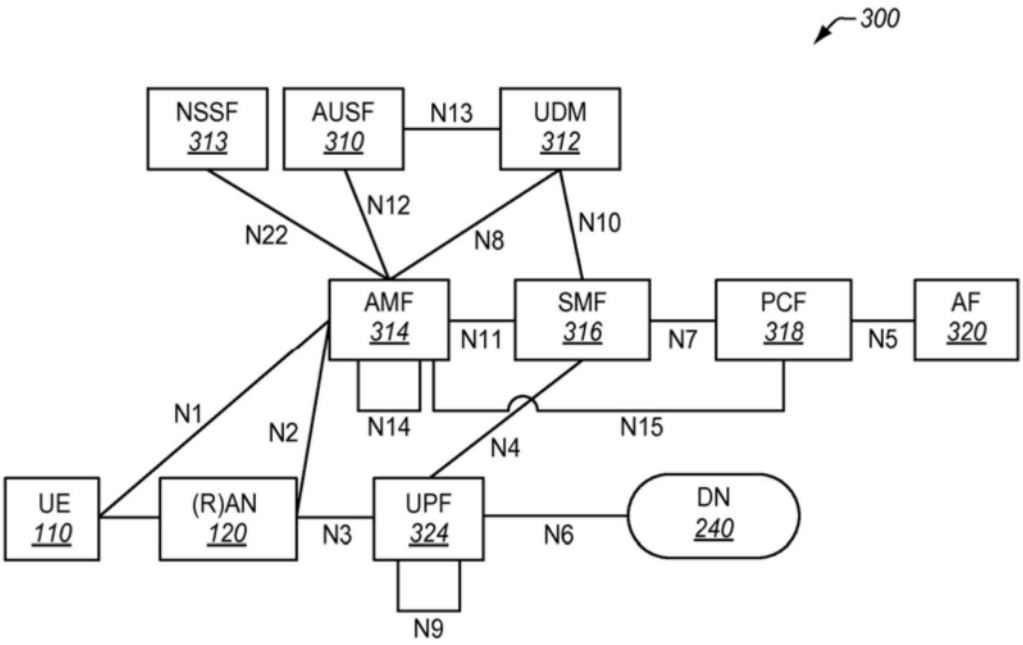

300
NSSF
313
AUSF
310
N13
UDM
312
N12
N22
N8
N10
AMF
314
N11
SMF
316
N7
PCF
318
N5
AF
320
N1
N2
N14
N15
N4
UE
110
(R)AN
120
N3
UPF
324
N6
DN
240
N9

图3

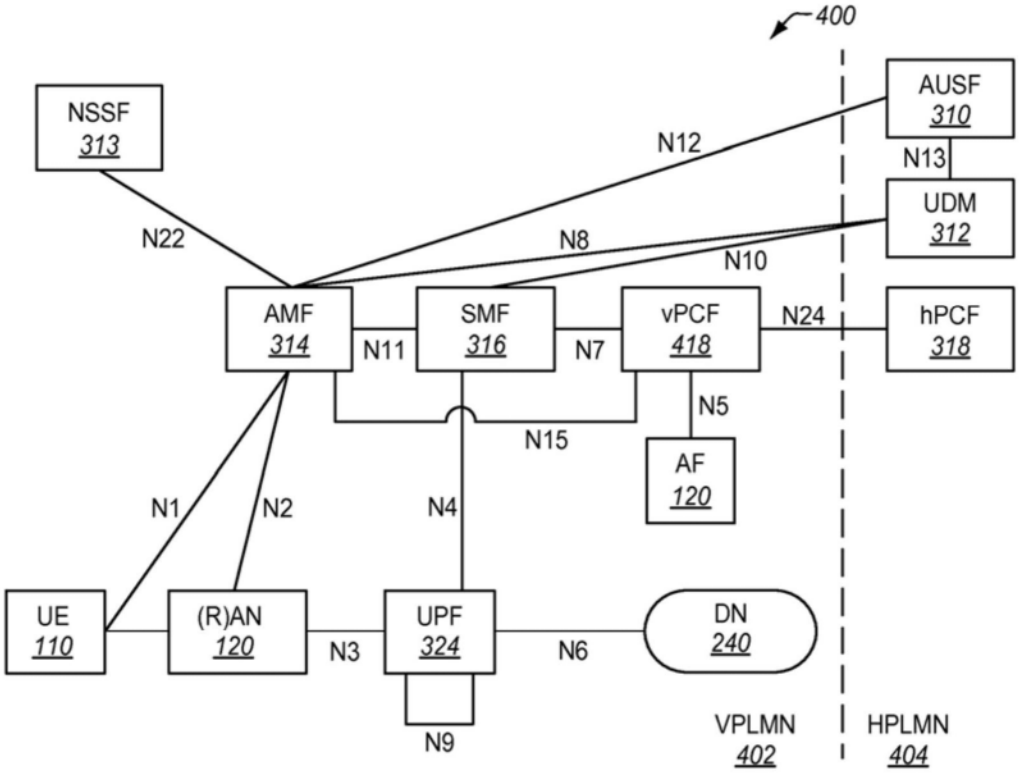

400
NSSF
313
AUSF
310
N12
N13
UDM
312
N22
N8
N10
AMF
314
N11
SMF
316
N7
vPCF
418
N24
hPCF
318
N5
N15
AF
120
N1
N2
N4
UE
110
(R)AN
120
N3
UPF
324
N6
DN
240
N9
VPLMN
402
HPLMN
404

图4

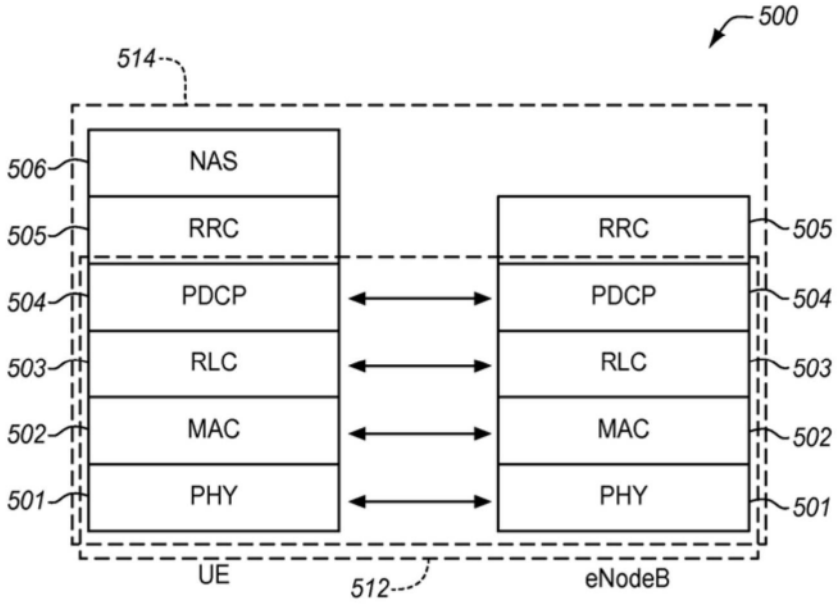

500
514
506
NAS
505
RRC
RRC
505
504
PDCP
PDCP
504
503
RLC
RLC
503
502
MAC
MAC
502
501
PHY
PHY
501
UE
512
eNodeB

图5

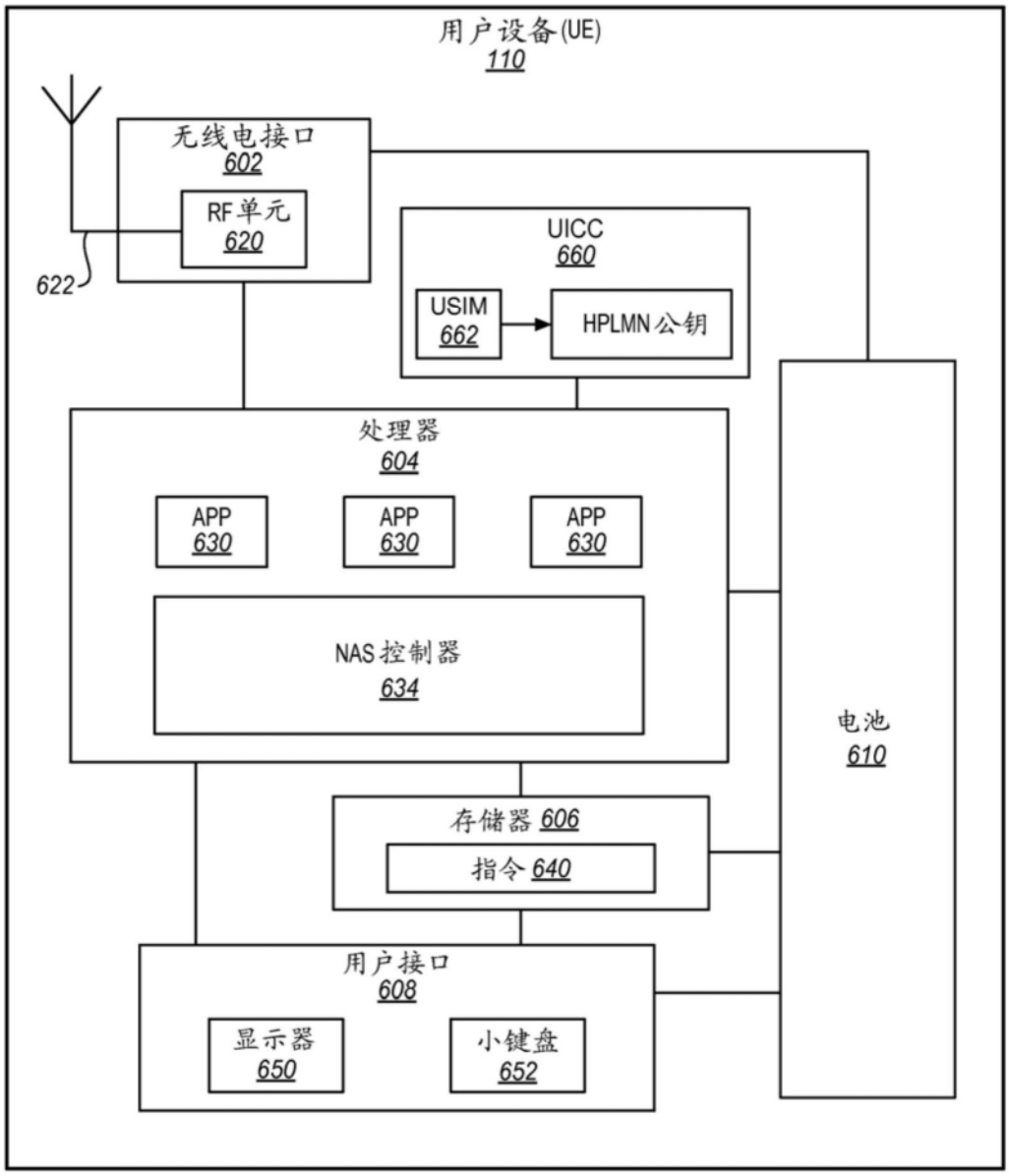

用户设备(UE)
110
无线电接口
602
RF单元
620
622
UICC
660
USIM
662
HPLMN公钥
处理器
604
APP
630
APP
630
APP
630
NAS控制器
634
电池
610
存储器 606
指令 640
用户接口
608
显示器
650
小键盘
652

图6

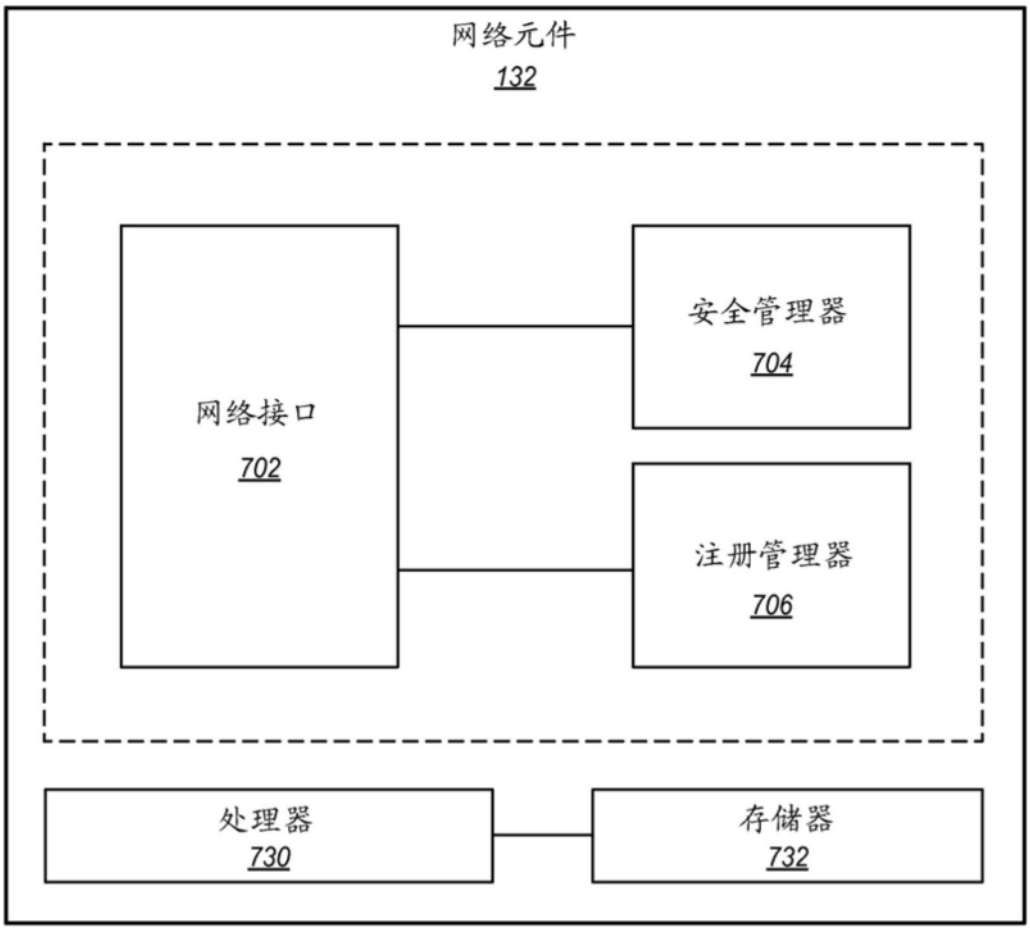


图7

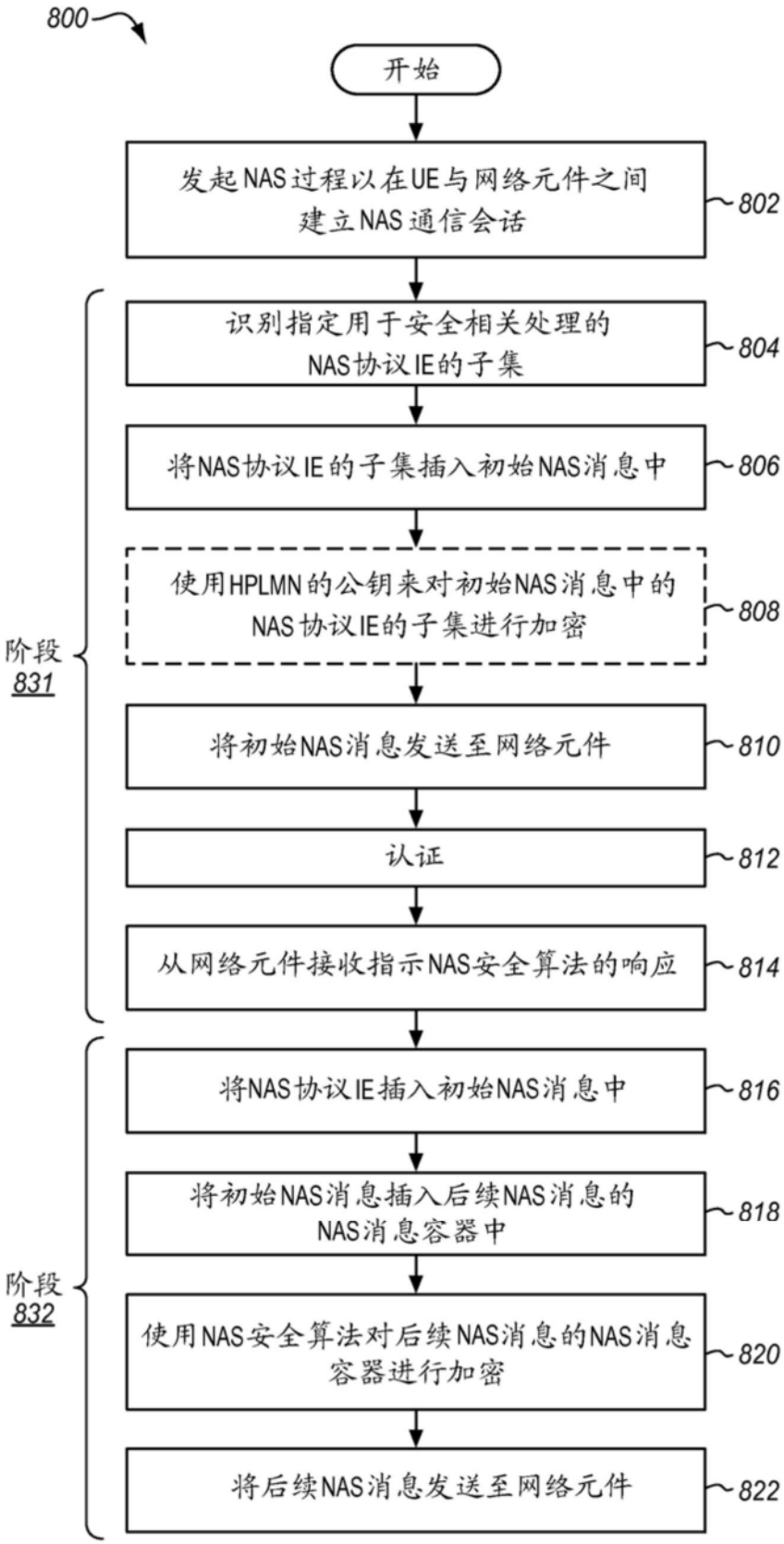

800
开始
发起NAS过程以在UE与网络元件之间建立NAS通信会话
802
识别指定用于安全相关处理的NAS协议IE的子集
804
将NAS协议IE的子集插入初始NAS消息中
806
使用HPLMN的公钥来对初始NAS消息中的NAS协议IE的子集进行加密
808
阶段 831
将初始NAS消息发送至网络元件
810
认证
812
从网络元件接收指示NAS安全算法的响应
814
将NAS协议IE插入初始NAS消息中
816
将初始NAS消息插入后续NAS消息的NAS消息容器中
818
阶段 832
使用NAS安全算法对后续NAS消息的NAS消息容器进行加密
820
将后续NAS消息发送至网络元件
822

图8

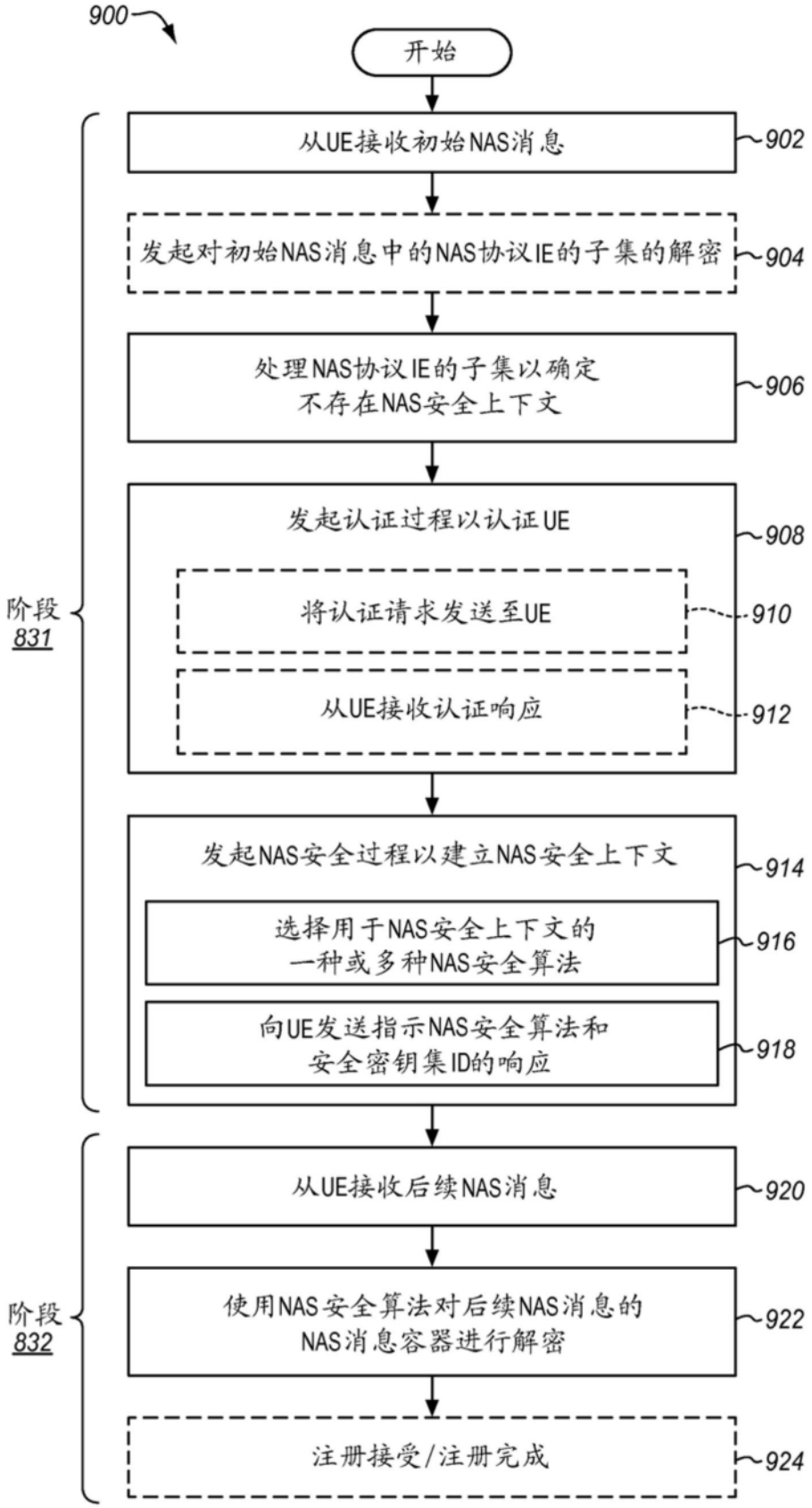

900
开始
从UE接收初始NAS消息
902
发起对初始NAS消息中的NAS协议IE的子集的解密
904
处理NAS协议IE的子集以确定
不存在NAS安全上下文
906
发起认证过程以认证UE
908
将认证请求发送至UE
910
从UE接收认证响应
912
阶段
831
发起NAS安全过程以建立NAS安全上下文
914
选择用于NAS安全上下文的
一种或多种NAS安全算法
916
向UE发送指示NAS安全算法和
安全密钥集ID的响应
918
从UE接收后续NAS消息
920
使用NAS安全算法对后续NAS消息的
NAS消息容器进行解密
922
阶段
832
注册接受/注册完成
924

图9

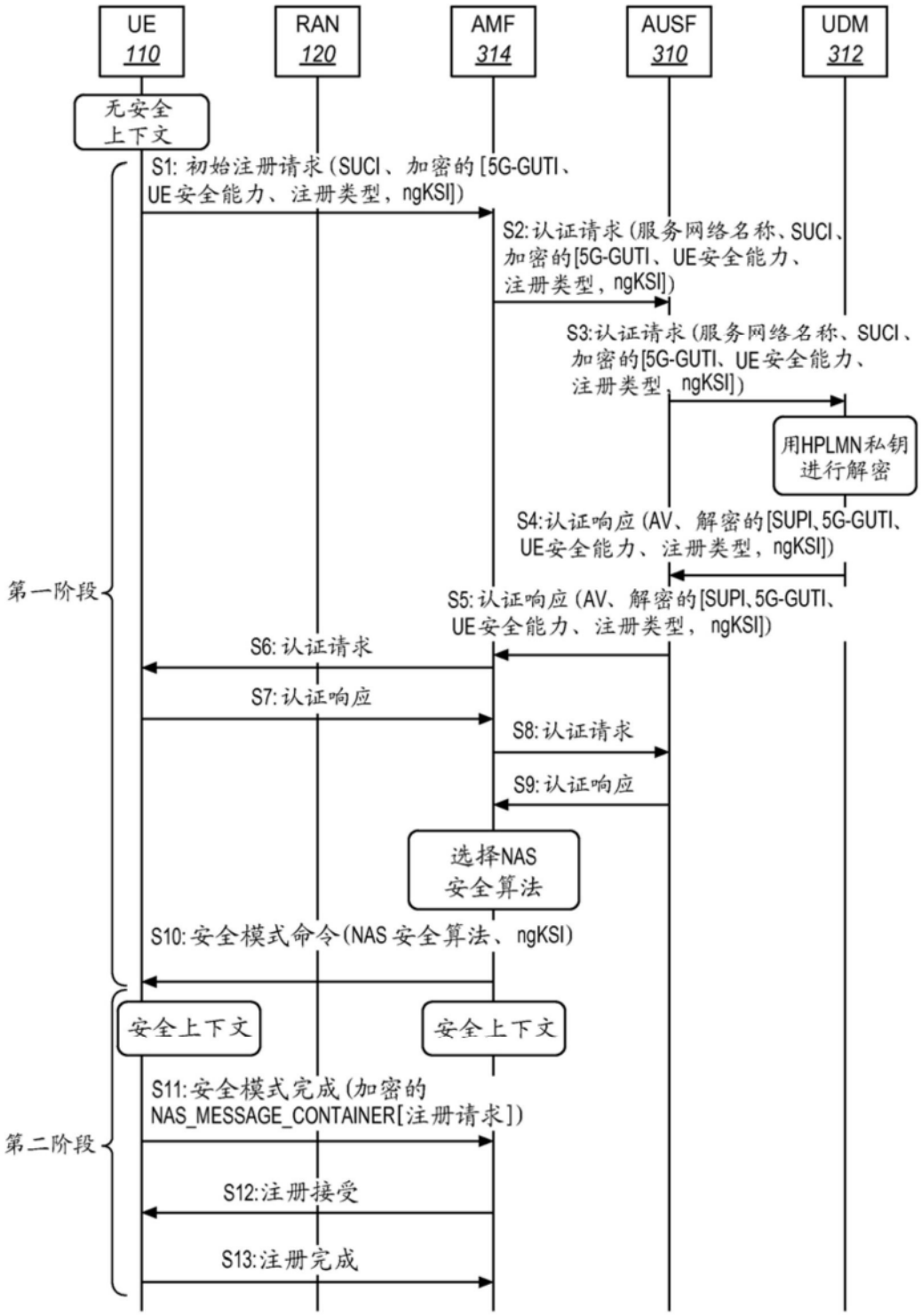

UE
110
RAN
120
AMF
314
AUSF
310
UDM
312
无安全
上下文
S1: 初始注册请求(SUCI、加密的[5G-GUTI、
UE安全能力、注册类型，ngKSI])
S2:认证请求(服务网络名称、SUCI、
加密的[5G-GUTI、UE安全能力、
注册类型，ngKSI])
S3:认证请求(服务网络名称、SUCI、
加密的[5G-GUTI、UE安全能力、
注册类型，ngKSI])
用HPLMN私钥
进行解密
S4:认证响应(AV、解密的[SUPI、5G-GUTI、
UE安全能力、注册类型，ngKSI])
第一阶段
S5:认证响应(AV、解密的[SUPI、5G-GUTI、
UE安全能力、注册类型，ngKSI])
S6:认证请求
S7:认证响应
S8:认证请求
S9:认证响应
选择NAS
安全算法
S10:安全模式命令(NAS安全算法、ngKSI)
安全上下文
安全上下文
S11:安全模式完成(加密的
NAS_MESSAGE_CONTAINER[注册请求])
第二阶段
S12:注册接受
S13:注册完成

图10

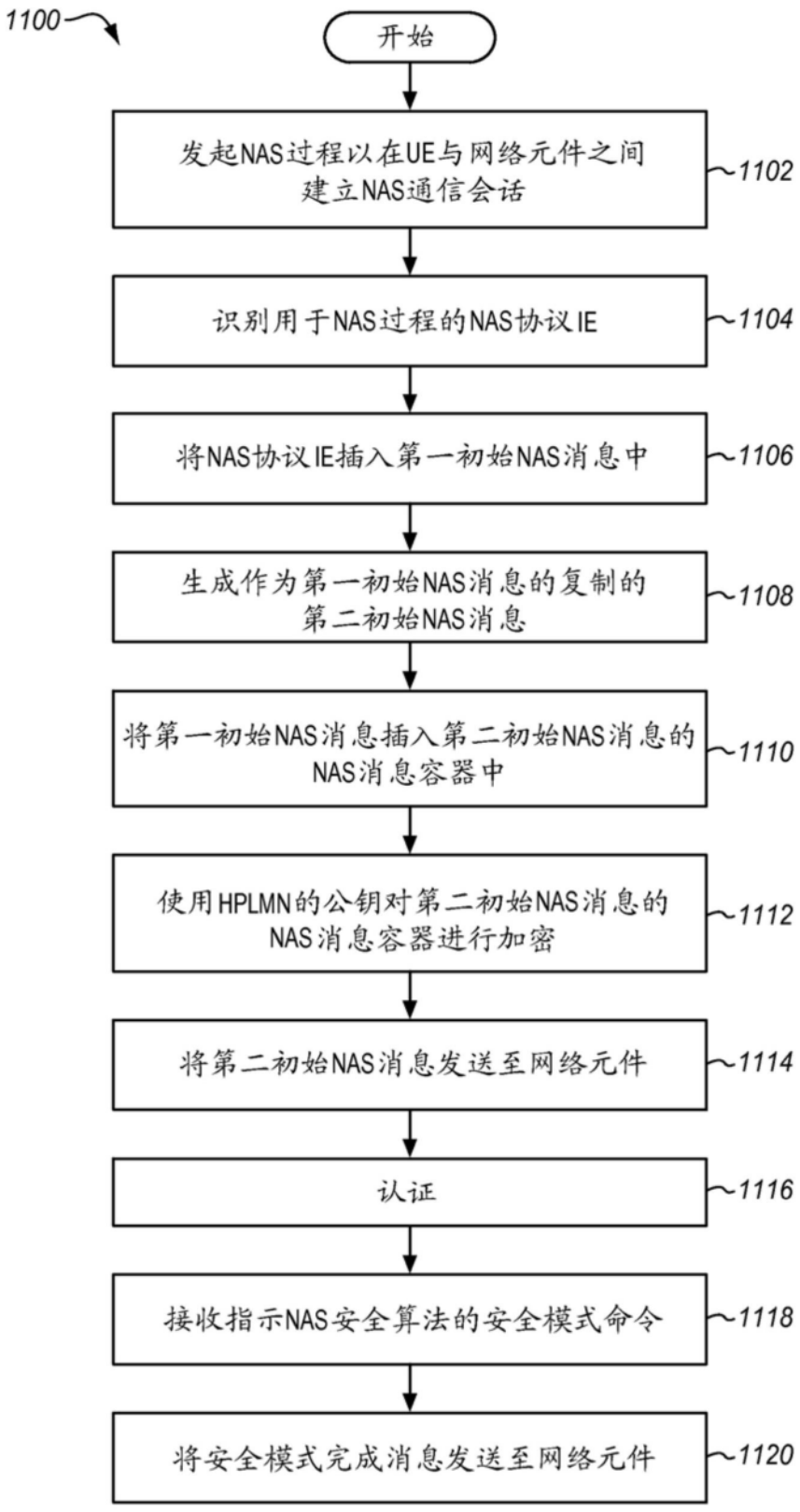

1100
开始
发起NAS过程以在UE与网络元件之间建立NAS通信会话
1102
识别用于NAS过程的NAS协议IE
1104
将NAS协议IE插入第一初始NAS消息中
1106
生成作为第一初始NAS消息的复制的第二初始NAS消息
1108
将第一初始NAS消息插入第二初始NAS消息的NAS消息容器中
1110
使用HPLMN的公钥对第二初始NAS消息的NAS消息容器进行加密
1112
将第二初始NAS消息发送至网络元件
1114
认证
1116
接收指示NAS安全算法的安全模式命令
1118
将安全模式完成消息发送至网络元件
1120

图11

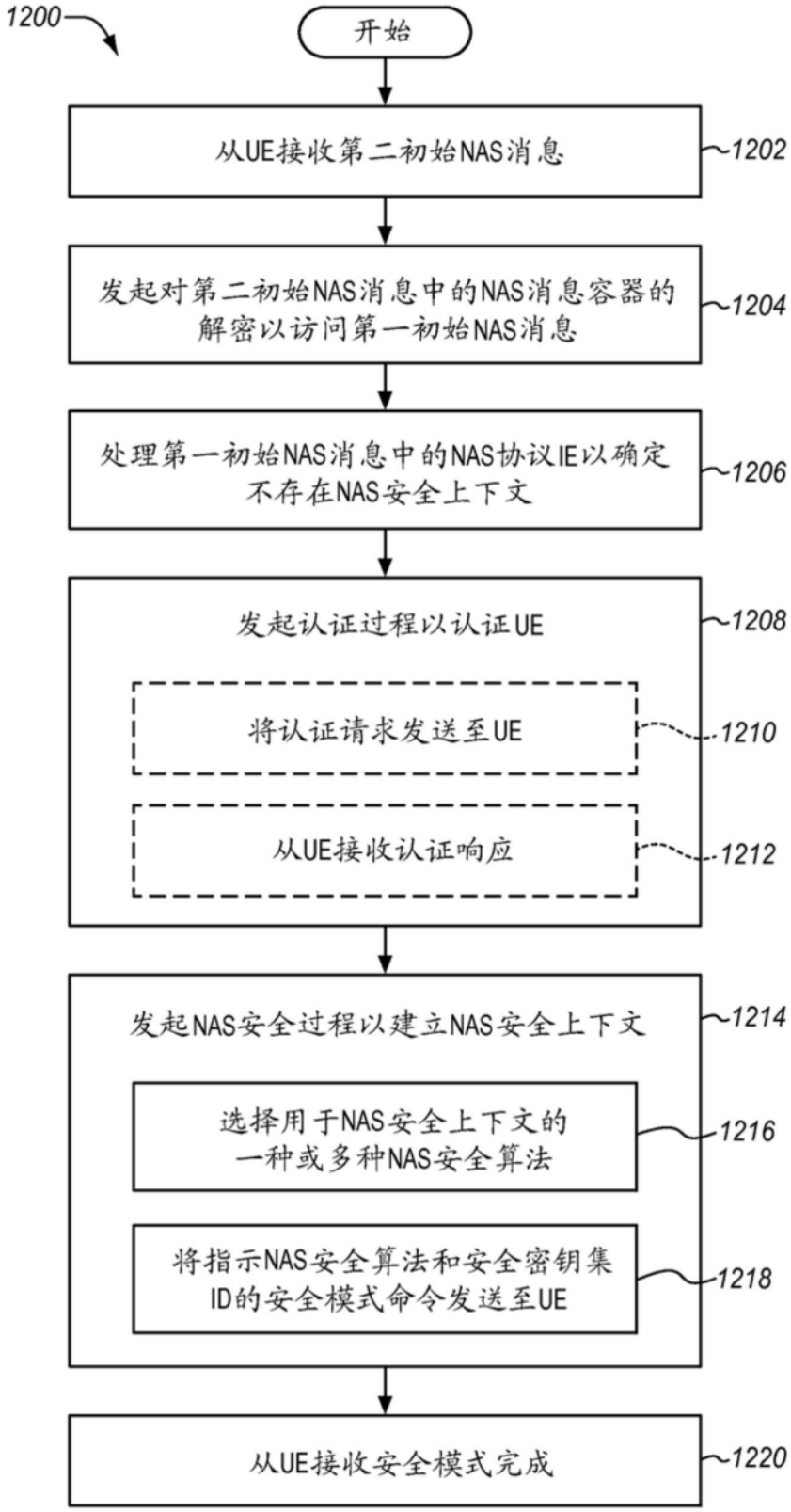

1200
开始
从UE接收第二初始NAS消息
1202
发起对第二初始NAS消息中的NAS消息容器的解密以访问第一初始NAS消息
1204
处理第一初始NAS消息中的NAS协议IE以确定不存在NAS安全上下文
1206
发起认证过程以认证UE
1208
将认证请求发送至UE
1210
从UE接收认证响应
1212
发起NAS安全过程以建立NAS安全上下文
1214
选择用于NAS安全上下文的一种或多种NAS安全算法
1216
将指示NAS安全算法和安全密钥集ID的安全模式命令发送至UE
1218
从UE接收安全模式完成
1220

图12

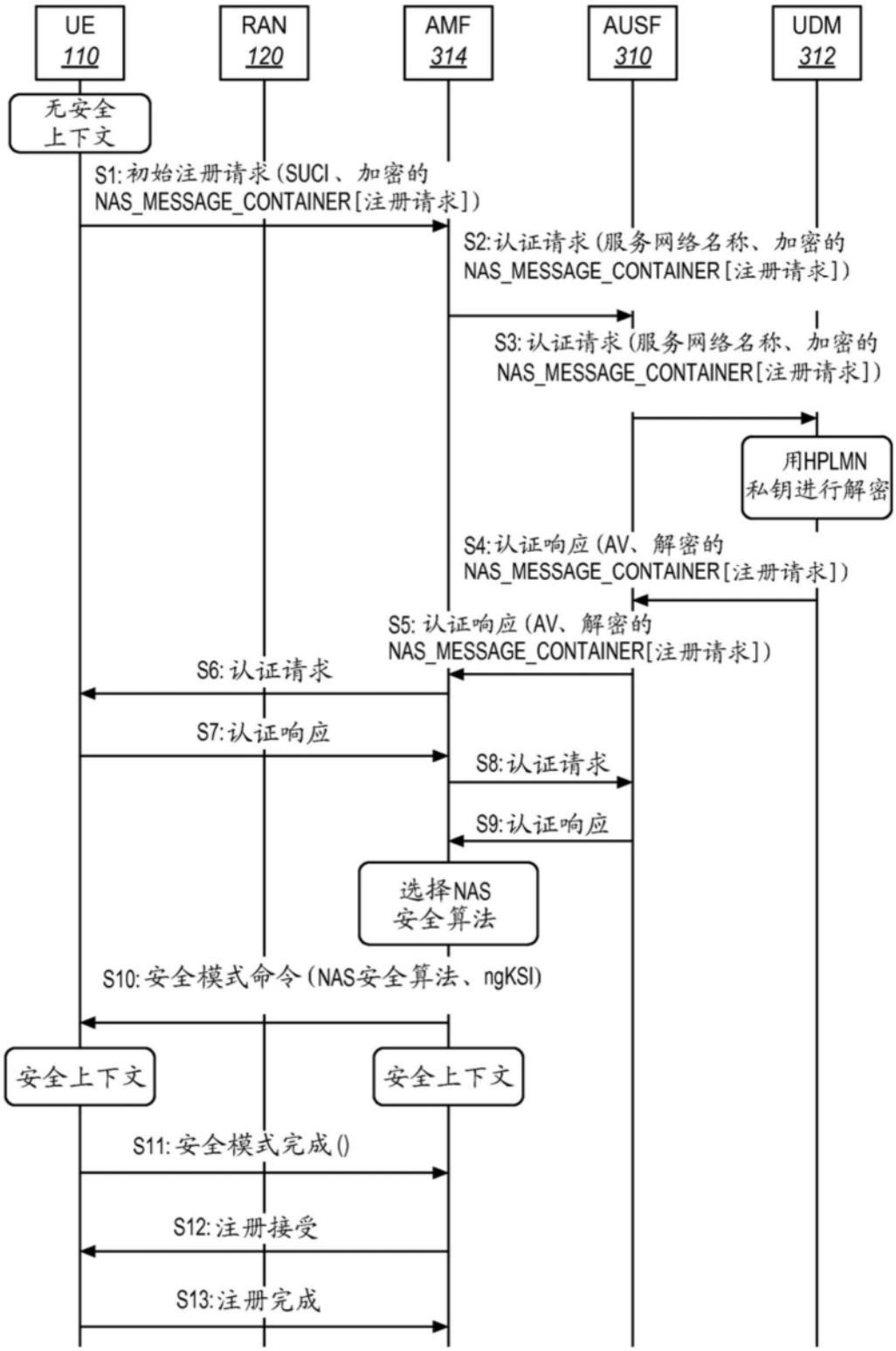

UE
110
RAN
120
AMF
314
AUSF
310
UDM
312
无安全
上下文
S1:初始注册请求(SUCI、加密的
NAS_MESSAGE_CONTAINER[注册请求])
S2:认证请求(服务网络名称、加密的
NAS_MESSAGE_CONTAINER[注册请求])
S3:认证请求(服务网络名称、加密的
NAS_MESSAGE_CONTAINER[注册请求])
用HPLMN
私钥进行解密
S4:认证响应(AV、解密的
NAS_MESSAGE_CONTAINER[注册请求])
S5:认证响应(AV、解密的
NAS_MESSAGE_CONTAINER[注册请求])
S6:认证请求
S7:认证响应
S8:认证请求
S9:认证响应
选择NAS
安全算法
S10:安全模式命令(NAS安全算法、ngKSI)
安全上下文
安全上下文
S11:安全模式完成()
S12:注册接受
S13:注册完成

图13

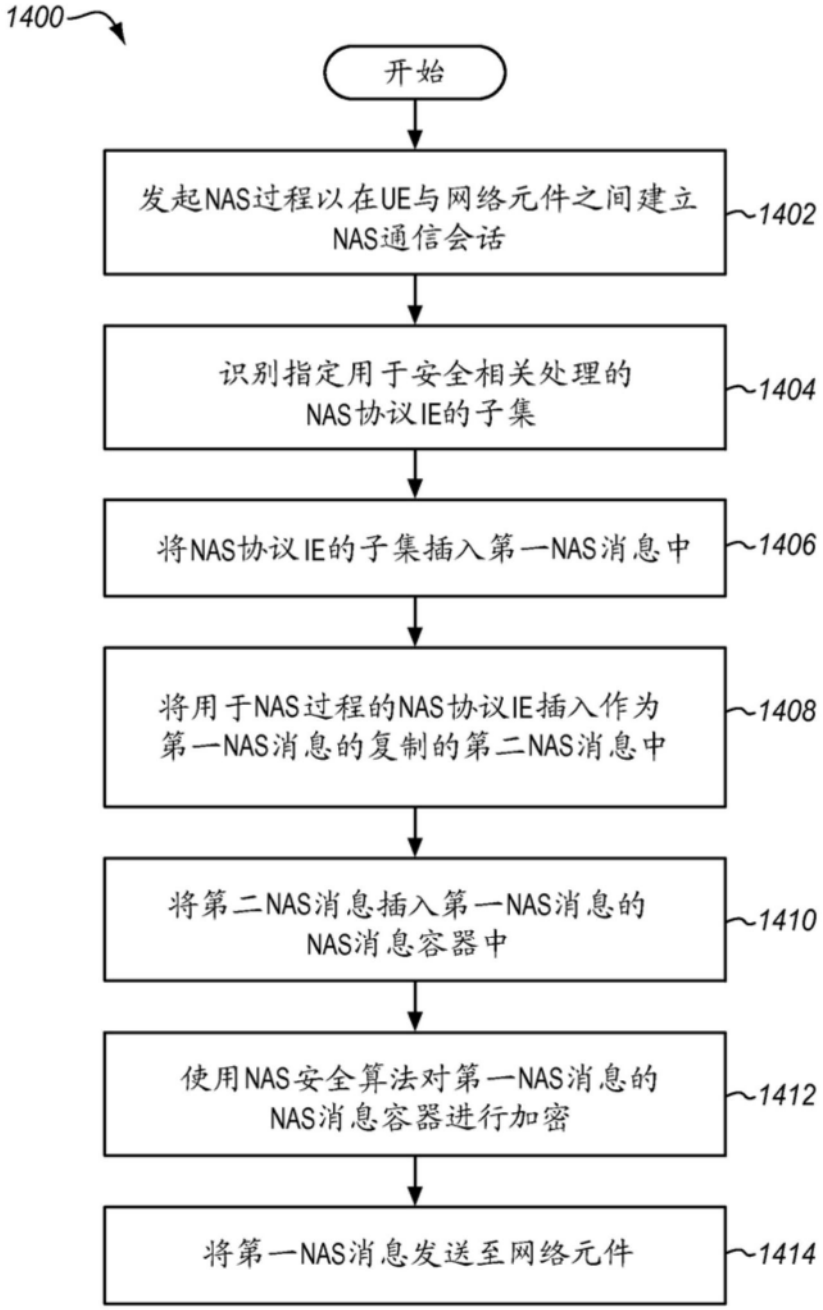

1400
开始
发起NAS过程以在UE与网络元件之间建立NAS通信会话
1402
识别指定用于安全相关处理的NAS协议IE的子集
1404
将NAS协议IE的子集插入第一NAS消息中
1406
将用于NAS过程的NAS协议IE插入作为第一NAS消息的复制的第二NAS消息中
1408
将第二NAS消息插入第一NAS消息的NAS消息容器中
1410
使用NAS安全算法对第一NAS消息的NAS消息容器进行加密
1412
将第一NAS消息发送至网络元件
1414

图14

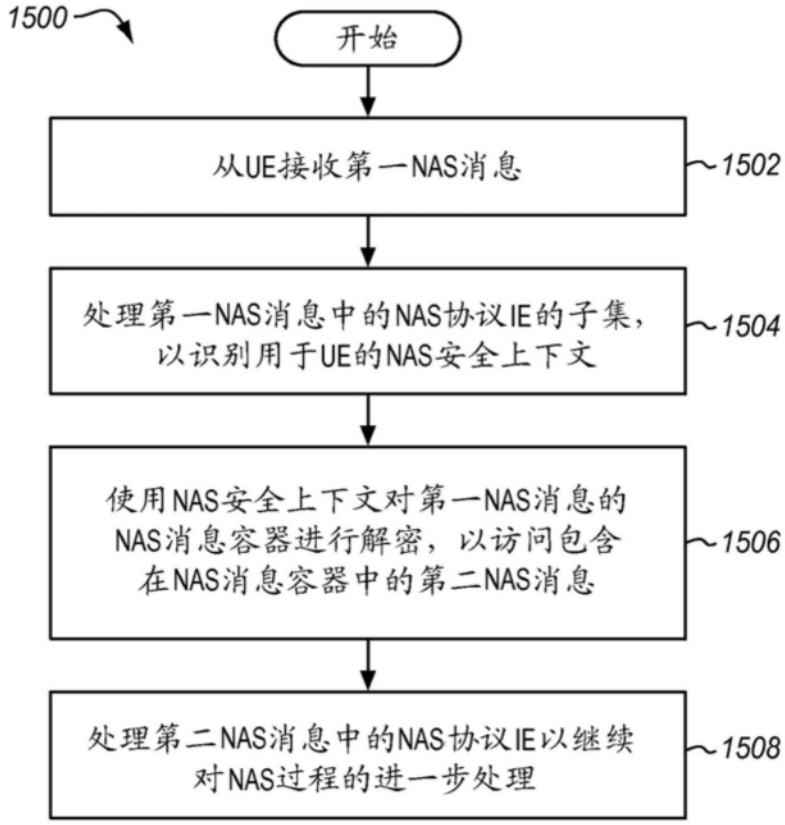

1500
开始
从UE接收第一NAS消息
1502
处理第一NAS消息中的NAS协议IE的子集，以识别用于UE的NAS安全上下文
1504
使用NAS安全上下文对第一NAS消息的NAS消息容器进行解密，以访问包含在NAS消息容器中的第二NAS消息
1506
处理第二NAS消息中的NAS协议IE以继续对NAS过程的进一步处理
1508

图15

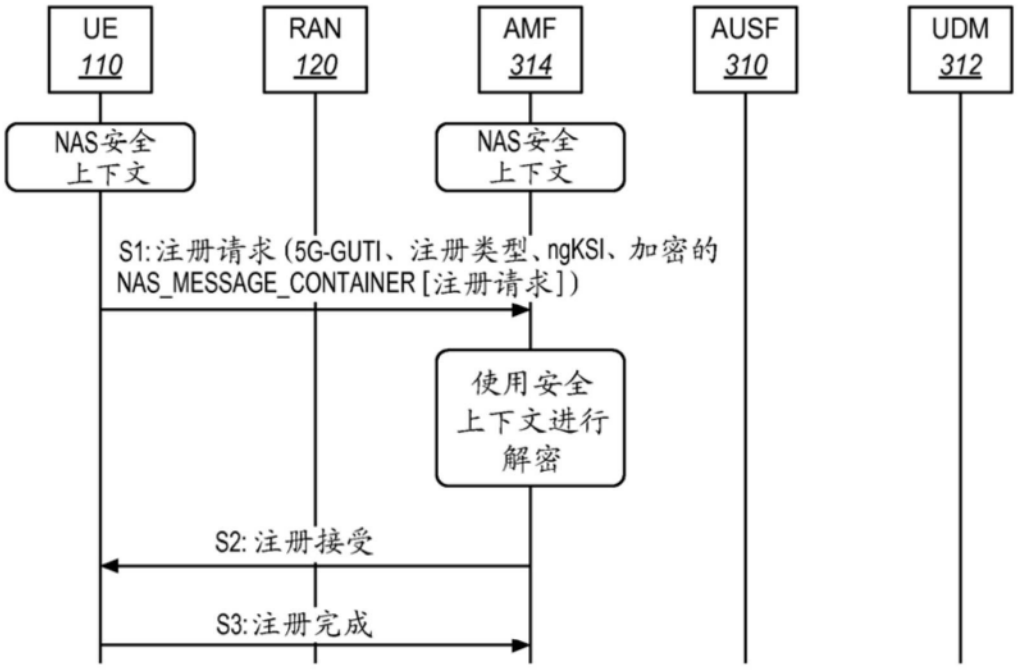

UE
110
RAN
120
AMF
314
AUSF
310
UDM
312
NAS安全上下文
NAS安全上下文
S1:注册请求(5G-GUTI、注册类型、ngKSI、加密的NAS_MESSAGE_CONTAINER[注册请求])
使用安全上下文进行解密
S2:注册接受
S3:注册完成

图16

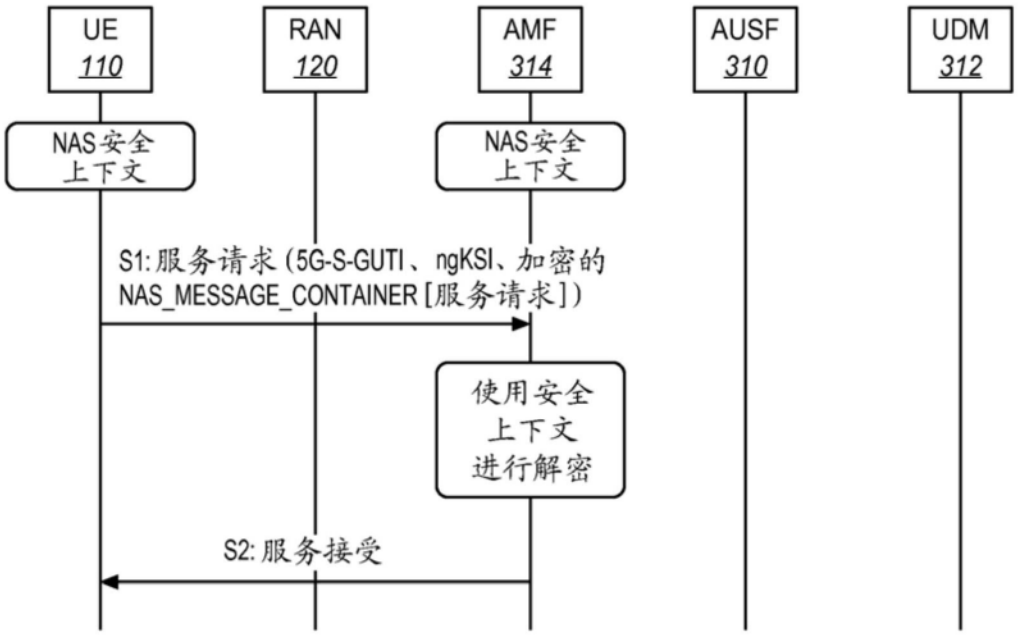

UE
110
RAN
120
AMF
314
AUSF
310
UDM
312
NAS安全
上下文
NAS安全
上下文
S1:服务请求(5G-S-GUTI、ngKSI、加密的
NAS_MESSAGE_CONTAINER[服务请求])
使用安全
上下文
进行解密
S2:服务接受

图17

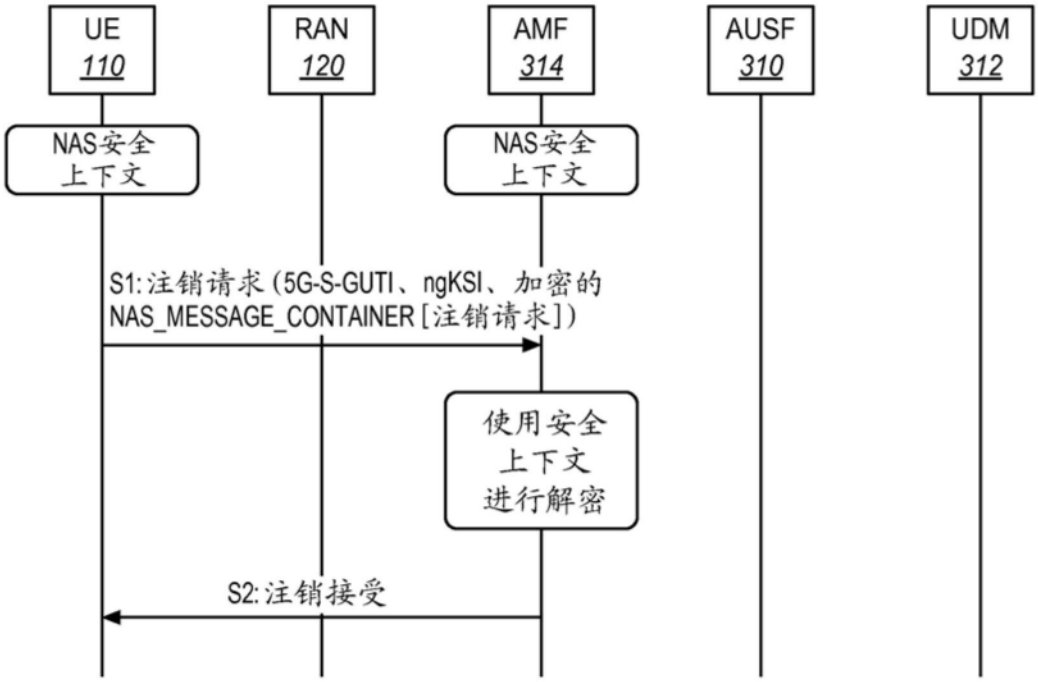

UE
110
RAN
120
AMF
314
AUSF
310
UDM
312
NAS安全
上下文
NAS安全
上下文
S1:注销请求(5G-S-GUTI、ngKSI、加密的
NAS_MESSAGE_CONTAINER[注销请求])
使用安全
上下文
进行解密
S2:注销接受

图18

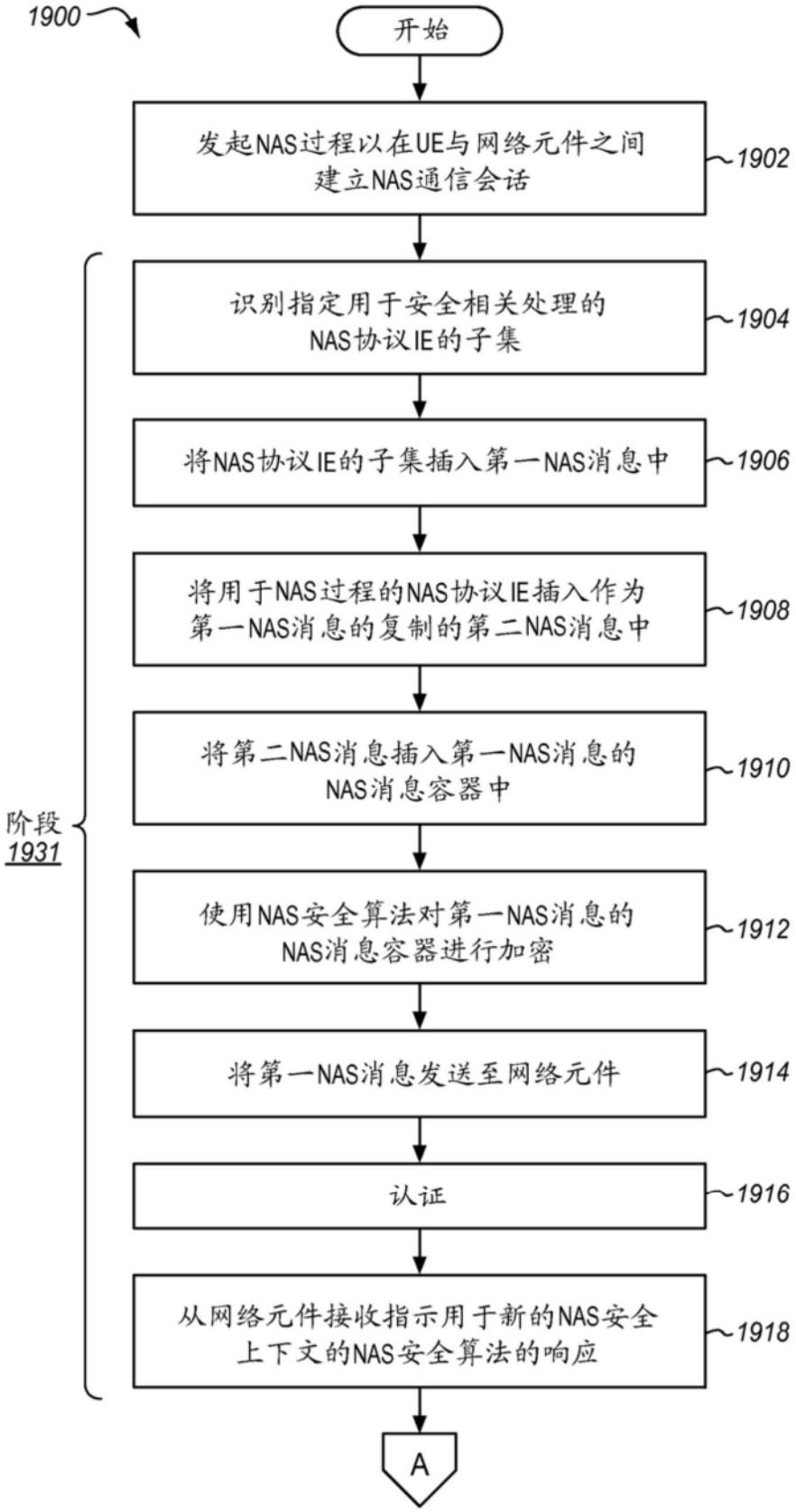

1900
开始
发起NAS过程以在UE与网络元件之间建立NAS通信会话
1902
识别指定用于安全相关处理的NAS协议IE的子集
1904
将NAS协议IE的子集插入第一NAS消息中
1906
将用于NAS过程的NAS协议IE插入作为第一NAS消息的复制的第二NAS消息中
1908
将第二NAS消息插入第一NAS消息的NAS消息容器中
1910
使用NAS安全算法对第一NAS消息的NAS消息容器进行加密
1912
将第一NAS消息发送至网络元件
1914
认证
1916
从网络元件接收指示用于新的NAS安全上下文的NAS安全算法的响应
1918
阶段 1931
A

图19A

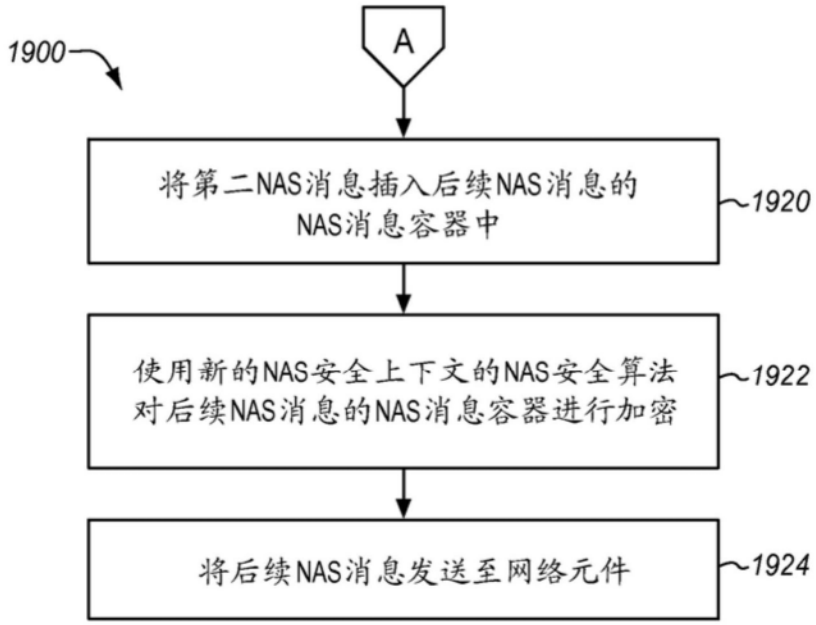

1900
A
将第二NAS消息插入后续NAS消息的NAS消息容器中
1920
使用新的NAS安全上下文的NAS安全算法对后续NAS消息的NAS消息容器进行加密
1922
将后续NAS消息发送至网络元件
1924

图19B

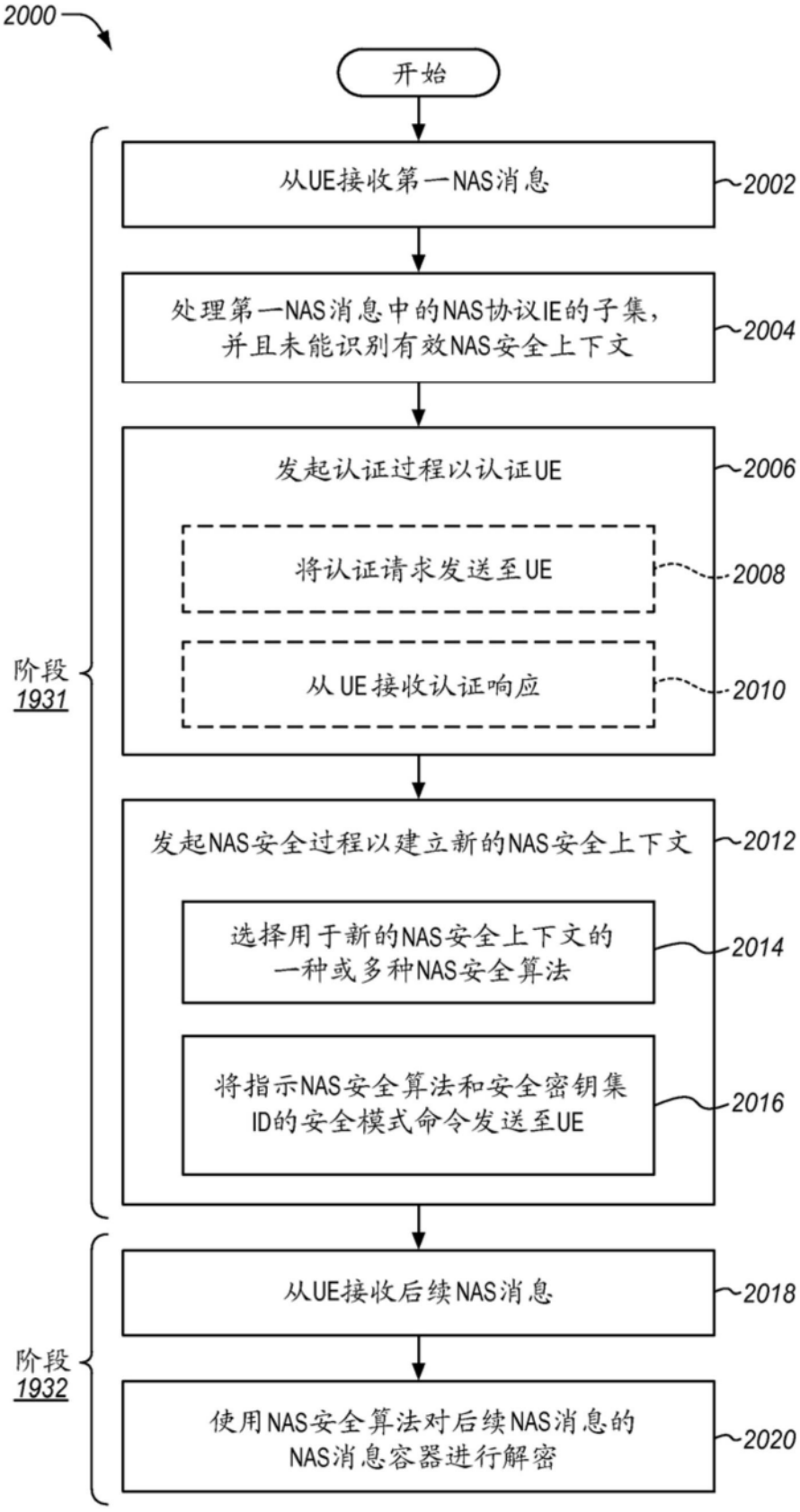

2000
开始
从UE接收第一NAS消息
2002
处理第一NAS消息中的NAS协议IE的子集，并且未能识别有效NAS安全上下文
2004
发起认证过程以认证UE
2006
将认证请求发送至UE
2008
从UE接收认证响应
2010
阶段1931
发起NAS安全过程以建立新的NAS安全上下文
2012
选择用于新的NAS安全上下文的一种或多种NAS安全算法
2014
将指示NAS安全算法和安全密钥集ID的安全模式命令发送至UE
2016
从UE接收后续NAS消息
2018
阶段1932
使用NAS安全算法对后续NAS消息的NAS消息容器进行解密
2020

图20

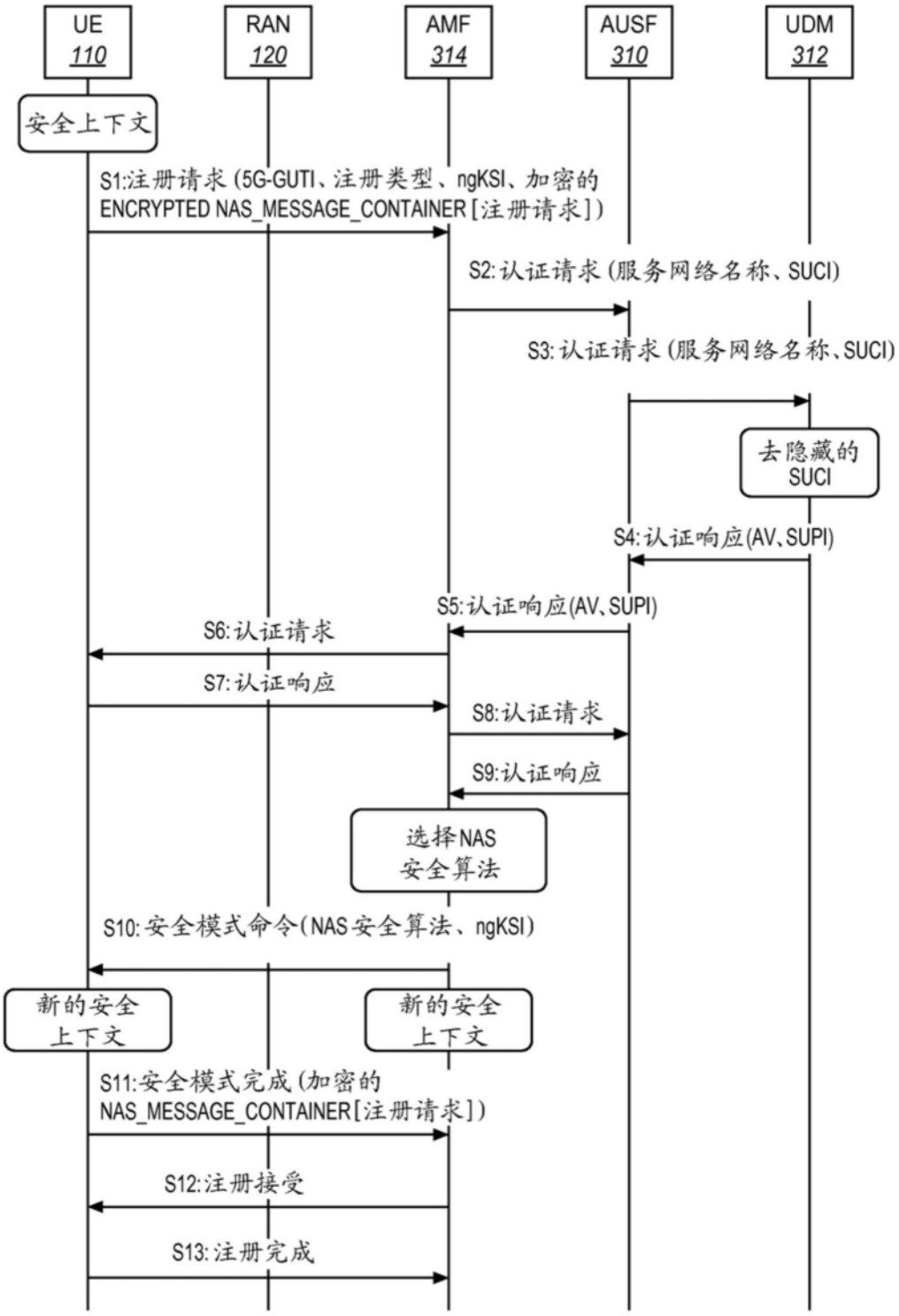

UE
110
RAN
120
AMF
314
AUSF
310
UDM
312
安全上下文
S1:注册请求(5G-GUTI、注册类型、ngKSI、加密的
ENCRYPTED NAS_MESSAGE_CONTAINER[注册请求])
S2:认证请求(服务网络名称、SUCI)
S3:认证请求(服务网络名称、SUCI)
去隐藏的
SUCI
S4:认证响应(AV、SUPI)
S5:认证响应(AV、SUPI)
S6:认证请求
S7:认证响应
S8:认证请求
S9:认证响应
选择NAS
安全算法
S10:安全模式命令(NAS安全算法、ngKSI)
新的安全
上下文
新的安全
上下文
S11:安全模式完成(加密的
NAS_MESSAGE_CONTAINER[注册请求])
S12:注册接受
S13:注册完成

图21

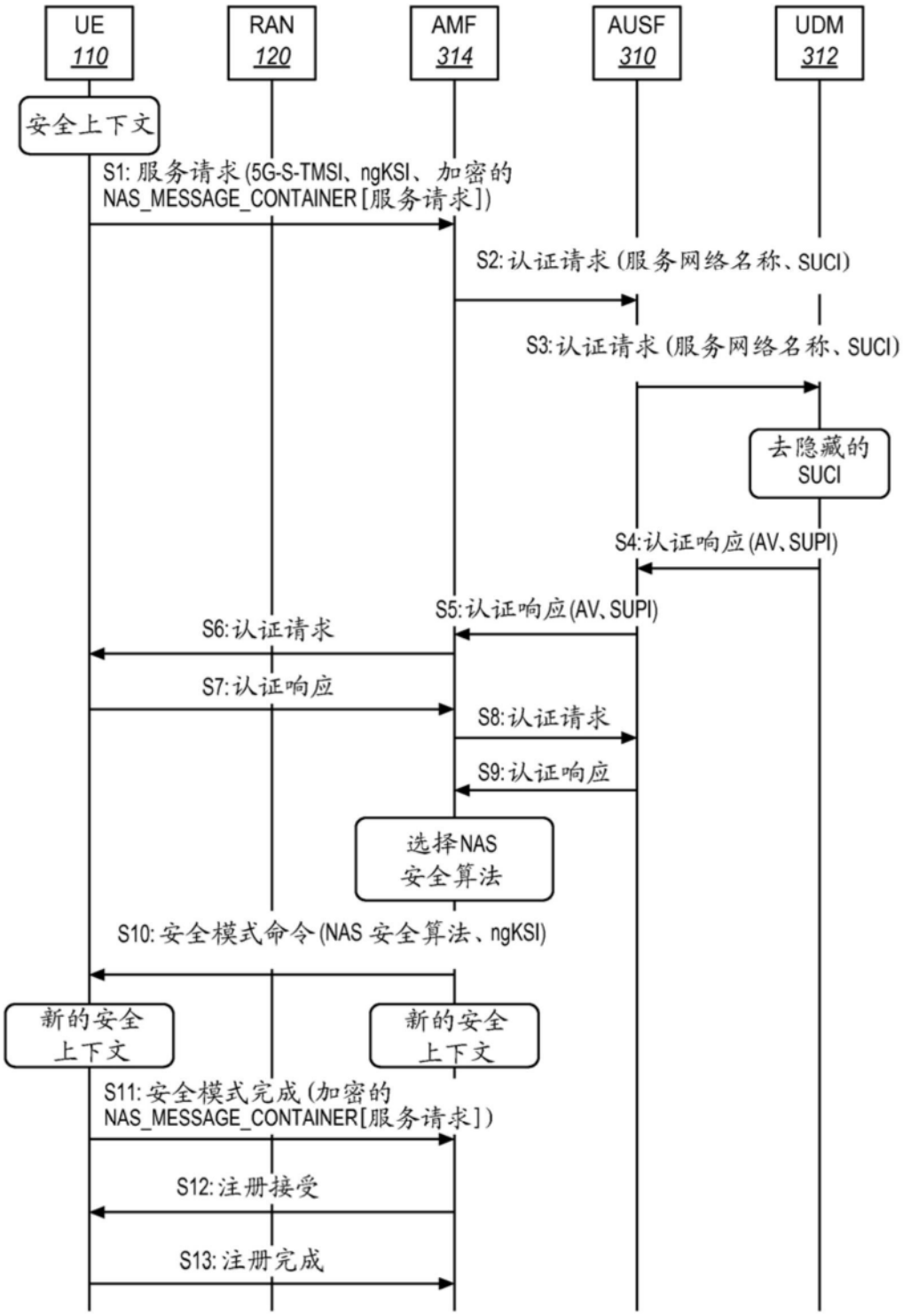

UE
110
RAN
120
AMF
314
AUSF
310
UDM
312
安全上下文
S1: 服务请求(5G-S-TMSI、ngKSI、加密的NAS_MESSAGE_CONTAINER[服务请求])
S2:认证请求(服务网络名称、SUCI)
S3:认证请求(服务网络名称、SUCI)
去隐藏的SUCI
S4:认证响应(AV、SUPI)
S5:认证响应(AV、SUPI)
S6:认证请求
S7:认证响应
S8:认证请求
S9:认证响应
选择NAS安全算法
S10: 安全模式命令(NAS 安全算法、ngKSI)
新的安全上下文
新的安全上下文
S11: 安全模式完成(加密的NAS_MESSAGE_CONTAINER[服务请求])
S12:注册接受
S13:注册完成

图22