(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111133731 B
(45)授权公告日 2022.06.03

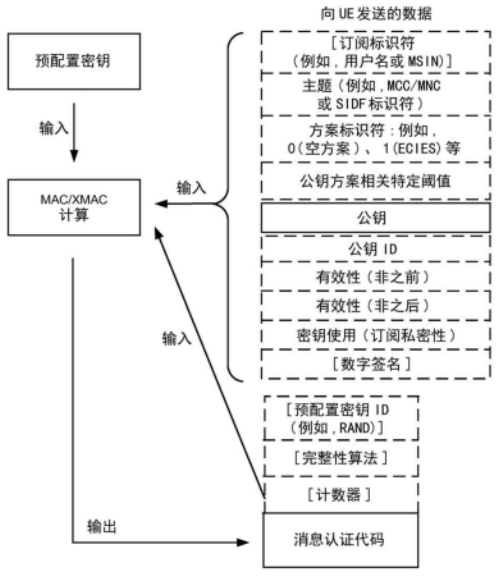
(21)申请号 201880062042.4
(22)申请日 2018.07.17
(65)同一申请的已公布的文献号
申请公布号 CN 111133731 A
(43)申请公布日 2020.05.08
(30)优先权数据
62/536,632 2017.07.25 US
(85)PCT国际申请进入国家阶段日
2020.03.24
(86)PCT国际申请的申请数据
PCT/EP2018/069433 2018.07.17
(87)PCT国际申请的公布数据
WO2019/020440 EN 2019.01.31
(73)专利权人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩
(72)发明人 韦萨·托尔维宁
普拉耶沃·库马·纳卡米
诺阿蒙·本赫达
戴维·卡斯特利亚诺斯萨莫拉
莫尼卡·威弗森 帕西·萨里宁
(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 余婧娜
(51)Int.Cl.
H04W 12/0431(2021.01)
H04W 12/06(2021.01)
H04W 12/72(2021.01)
(56)对比文件
WO 2016209126 A1,2016.12.29
CN 102668501 A,2012.09.12
CN 103370915 A,2013.10.23
US 2013003971 A1,2013.01.03
3GPP."3rd Generation Partnership Project
".《3GPP TR 33.899 V1.2.0 (2017-06)》.2017,
审查员 高露
权利要求书2页 说明书16页 附图14页

(54)发明名称

私钥和消息认证码

(57)摘要

一种由认证服务器执行的用于预配置用户设备UE(1)的方法。该方法包括:基于特定于UE的预配置密钥和UE的归属网络(3)的私钥,获得消息认证码MAC,其中,该预配置密钥是认证服务器(14)与UE之间的共享秘密,以及该私钥包括归属网络的公钥;以及向UE传送该私钥和MAC。还公开了分别由去隐藏服务器和该UE执行的方法、以及认证服务器、去隐藏服务器和UE。还公开了计算机程序和存储器电路(13)。



CN 111133731 B

1.一种由去隐藏服务器(19)执行的用于预配置用户设备UE(1)的方法,所述方法包括:

响应于从认证服务器(14)接收指示所述UE缺少有效私钥的所述UE(1)的订阅隐藏标识符SUCI,生成用于所述UE(1)的订阅永久标识符SUPI和私钥,其中,所述私钥包括所述UE(1)的归属网络(3)的公钥;

基于所述私钥和特定于所述UE的并且是所述去隐藏服务器(19)和所述UE(1)之间的共享秘密的预配置密钥,生成消息认证码MAC;

向所述认证服务器(14)传送所述SUPI、所述MAC和所述私钥。

2.根据权利要求1所述的方法,还包括:通过检测所述SUCI的至少一部分是使用过时的私钥加密的来检测所述SUCI指示所述UE(1)缺少有效私钥。

3.根据权利要求2所述的方法,其中,所述过时的私钥是到期或被破解的私钥。

4.根据权利要求1-3中的任一项所述的方法,其中,生成所述私钥包括:根据对所述UE(1)的订户标识符在无线通信网络(30)中的安全通信进行管理的加密方案策略来生成所述私钥。

5.根据权利要求4所述的方法,其中,根据所述加密方案策略来生成所述私钥包括:生成所述私钥,使得所述私钥适于生成新的SUCI,在所述新的SUCI中所述UE(1)的订户标识符是根据椭圆曲线集成加密方案加密的。

6.根据权利要求1-3中的任一项所述的方法,还包括:响应于接收所述SUCI,生成至少一个附加私钥,并向所述认证服务器(14)传送所述至少一个附加私钥。

7.根据权利要求1-3中的任一项所述的方法,还包括:向所述认证服务器(14)传送所述预配置密钥。

8.根据权利要求1-3中的任一项所述的方法,其中,所述私钥还包括标识在多个加密方案中的哪一个中使用所述公钥的标识符。

9.根据权利要求8所述的方法,其中,所述私钥还包括在使用所述公钥的加密方案中被使用的参数。

10.根据权利要求1-3中的任一项所述的方法,其中,所述私钥包括所述UE(1)的订阅标识符。

11.根据权利要求10所述的方法,其中,所述UE(1)的订阅标识符包括所述UE(1)的移动订阅标识号。

12.根据权利要求1-3中的任一项所述的方法,其中,所述私钥包括所述归属网络(3)的标识符。

13.根据权利要求1-3中的任一项所述的方法,其中,所述私钥包括有效时间信息,所述有效时间信息指示所述私钥为有效的时间。

14.根据权利要求1-3中的任一项所述的方法,其中,所述私钥包括基于所述私钥的一个或多个部分计算的数字签名。

15.根据权利要求1-3中的任一项所述的方法,其中,所述私钥包括明确指示能够使用所述私钥的过程的字段。

16.一种用于预配置用户设备UE(1)的去隐藏服务器(19),所述去隐藏服务器(19)包括:

处理电路(11)和存储器电路(13),所述存储器电路(13)包含可由所述处理电路(11)执

行的指令,从而所述去隐藏服务器(19)操作用于:

响应于从认证服务器(14)接收指示所述UE缺少有效私钥的所述UE(1)的订阅隐藏标识符SUCI,生成用于所述UE(1)的订阅永久标识符SUPI和私钥,其中,所述私钥包括所述UE(1)的归属网络(3)的公钥;

基于所述私钥和特定于所述UE的并且是所述去隐藏服务器(19)和所述UE(1)之间的共享秘密的预配置密钥,生成消息认证码MAC;以及

向所述认证服务器(14)传送所述SUPI、所述MAC和所述私钥。

17.根据权利要求16所述的去隐藏服务器(19),其中所述指令在由所述处理电路(11)执行时还使所述去隐藏服务器(19)实现包括至少一个订阅标识符去隐藏功能(6)和统一数据管理(7)。

私钥和消息认证码

技术领域

[0001] 本公开涉及用于预配置用户设备(UE)的方法、用于获得私钥(privacy key)的方法、认证服务器、去隐藏服务器、UE、存储器电路和用于服务器设备的计算机程序。

背景技术

[0002] 保持用户设备(UE)的长期订阅标识符(例如,IMSI(国际移动订户标识))的机密性很重要。早代3GPP系统(例如,4G/LTE、3G/UMTS、2G/GSM)包括使用一个或多个短期订阅标识符的用于长期订阅标识符机密性的部分机制。GUTI(全球唯一临时ID)和C-RNTI(小区无线网络临时标识符)是4G/LTE系统中短期订阅标识符的示例。然而,传统的部分机制可以通过空中接口以明文形式显示长期订阅标识符。例如,所谓的“IMSI捕获器”可以简单地例如使用标识符请求/响应消息来从UE询问长期标识符。

[0003] 当前,第三代合作伙伴计划(3GPP)讨论了如何在通信网络中改善安全性(例如,私密性)。关于5G,3GPP TS 33.501 V0.2.0提到了订阅永久标识符(SUPI),并且应当指出的是,SUPI可以例如以化名或公钥加密SUPI的形式被隐藏。

发明内容

[0004] 本发明的目的是促进UE与通信网络之间的通信中的安全性。

[0005] 本发明的第一方面涉及一种由认证服务器执行的用于预配置UE的方法。所述方法包括:

[0006] 基于特定于UE的预配置密钥和UE的归属网络的私钥,获得消息认证码MAC,其中,所述预配置密钥是认证服务器与UE之间的共享秘密,以及所述私钥包括归属网络的公钥;以及

[0007] 向UE传送所述私钥和MAC。

[0008] 在一个实施例中,获得MAC包括生成MAC。在另一实施例中,获得MAC包括从去隐藏服务器接收所述MAC。

[0009] 所述方法还可以包括:响应于UE的成功认证,获得所述预配置密钥。在这样的实施例中,获得所述预配置密钥可以包括生成所述预配置密钥。备选地,获得所述预配置密钥可以包括从去隐藏服务器接收所述预配置密钥。

[0010] 所述方法还包括接收预配置UE的请求,其中,所述请求包括私钥。在这样的实施例中,接收预配置UE的请求可以包括:在消息中接收预配置UE的请求和用于对UE进行认证的认证矢量。在任何一个这样的实施例中,预配置UE的请求还包括归属网络的至少一个附加私钥,并且所述方法还包括向UE传送所述至少一个附加私钥。此外,在任何一个这样的实施例中,所述方法还包括:向去隐藏服务器传送指示所述UE缺少有效私钥的所述UE的订阅隐藏标识符SUCI,并且作为响应,从去隐藏服务器接收所述预配置所述UE的请求。在根据后一实施例的实施例中,所述私钥是归属网络的多个私钥之一,并且由去隐藏服务器管理。

[0011] 预配置UE的请求还可以包括UE的订阅永久标识符SUPI。

[0012] 在所述方法的实施例中，向UE传送私钥和MAC可以包括：在注册接受消息传递过程中向UE一起传送所述私钥和MAC。

[0013] 所述方法的实施例还包括：使用用于所述SUCI中包括的订阅标识符的空加密方案来接收UE的订阅隐藏标识符SUCI。所述SUCI可以包括明文部分，所述明文部分具有公钥标识符、加密方案标识符、以及用于根据由所述加密方案标识符标识的加密方案对所述SUCI的加密部分进行解密的加密方案参数。

[0014] 在与UE的注册过程有关的一个或多个非接入层消息中向UE发送所述私钥和MAC。

[0015] 可以经由接入和移动性管理功能AMF完成向UE传送所述私钥和MAC。

[0016] 本发明的第二方面涉及一种由去隐藏服务器执行的用于预配置UE的方法。所述方法包括：

[0017] 响应于从认证服务器接收指示UE缺少有效私钥的UE的SUCI，生成用于UE的SUPI和私钥，其中，所述私钥包括UE的归属网络的公钥；

[0018] 基于所述私钥和特定于UE的并且是去隐藏服务器和UE之间的共享秘密的预配置密钥来生成MAC；

[0019] 向认证服务器传送所述SUPI、MAC和私钥。

[0020] 第二方面的实施例还包括：通过检测所述SUCI的至少一部分是使用过时的(obsolete)私钥加密的来检测所述SUCI指示所述UE缺少有效私钥。在这样的实施例中，过时的私钥可以是到期或被破解的(compromised)私钥。

[0021] 生成所述私钥可以包括：根据对UE的订户标识符在无线通信网络中的安全通信进行管理的加密方案策略来生成所述私钥。在这样的实施例中，根据所述加密方案策略来生成所述私钥包括：生成所述私钥，使得所述私钥适于生成新的SUCI，在所述新的SUCI中所述UE的订户标识符是根据椭圆曲线集成加密方案加密的。

[0022] 根据第二方面的方法可以包括：响应于接收所述SUCI，生成至少一个附加私钥，并向认证服务器传送所述至少一个附加私钥。

[0023] 根据第二方面的方法还可以包括：向认证服务器传送所述预配置密钥。

[0024] 所述私钥可以包括标识在多个加密方案中的哪一个中使用所述公钥的标识符。在这样的实施例中，所述私钥还包括在使用所述公钥的加密方案中被使用的参数。

[0025] 所述私钥可以包括UE的订阅标识符，例如，移动订阅标识号(MSIN)。

[0026] 所述私钥可以包括归属网络的标识符。所述私钥可以包括有效时间信息，所述有效时间信息指示所述私钥为有效的时间。所述私钥可以包括基于所述私钥的一个或多个部分计算的数字签名。所述私钥可以包括明确指示可以使用所述私钥的过程的字段。

[0027] 本发明的第三方面涉及一种由用户UE执行的用于获得私钥的方法。所述方法包括：

[0028] 从认证服务器接收私钥和MAC，其中，所述私钥包括UE的归属网络的公钥；以及

[0029] 通过以下方式验证所述私钥的完整性：

[0030] 生成预配置密钥，所述预配置密钥特定于所述UE，并且是所述UE和认证服务器之间的共享秘密；以及

[0031] 使用所述预配置密钥和所述私钥以重新产生从所述认证服务器接收的MAC。

[0032] 根据第三方面的方法还可以包括：向所述认证服务器传送SUCI，并且作为响应，接

收所述私钥。在该情况下，所述SUCI可以指示UE缺少有效私钥。所述SUCI的传送可以包括：在向无线通信网络注册的请求中传送所述SUCI。在这样的实施例中，根据第三方面的方法还可以包括：经由移动性管理功能并在注册接受消息中从所述认证服务器接收所述私钥和MAC。在这种情况下，所述方法还可以包括：响应于验证所述私钥，

[0033] 从无线通信网络解附着；

[0034] 生成不同的SUCI，在所述不同的SUCI中，所述UE的订阅标识符(例如，MSIN)是由所述私钥的至少一部分加密的；

[0035] 使用所述不同的SUCI，向所述无线通信网络重新注册。

[0036] 第三方面的方法还可以包括：使用所述UE的防篡改安全硬件组件来获得所述SUCI。在这样的实施例中，所述方法还可以包括：将所述私钥存储在防篡改安全硬件组件中。所述方法还可以包括：响应于向UE插入防篡改安全硬件组件，检测UE缺少有效私钥。使用防篡改安全硬件组件来获得SUCI可以包括：使用防篡改安全硬件组件来生成所述SUCI。使用防篡改安全硬件组件来获得SUCI可以包括：在防篡改安全硬件组件上执行读取操作以获得所述SUCI。使用防篡改安全硬件组件来获得SUCI可以包括：向防篡改安全硬件组件发送时间，并且作为响应，从防篡改安全硬件组件接收所述SUCI。

[0037] 使用防篡改安全硬件组件来获得SUCI可以包括：使用从防篡改安全硬件组件获得的不同的私钥来生成所述SUCI。在这种实施例中，如果所述不同的私钥到期，所述方法还可以包括用所述私钥替换所述不同的私钥。

[0038] 在第三方面的方法的实施例中，可以经由接入和移动性管理功能(AMF)接收从认证服务器接收的所述私钥和MAC。

[0039] 本发明的第四方面涉及一种用于预配置UE的认证服务器。所述认证服务器包括处理电路和存储器电路。所述存储器电路包含可由处理电路执行的指令，从而所述认证服务器操作用于：

[0040] 基于特定于UE的预配置密钥和UE的归属网络的私钥，获得MAC，其中，所述预配置密钥是认证服务器与UE之间的共享秘密，以及所述私钥包括归属网络的公钥；

[0041] 向UE传送所述私钥和MAC。

[0042] 第五方面涉及一种用于预配置UE的认证服务器。所述认证服务器包括：

[0043] 获取模块，被配置为：基于特定于UE的预配置密钥和UE的归属网络的私钥，获得MAC，其中，所述预配置密钥是认证服务器与UE之间的共享秘密，以及所述私钥包括归属网络的公钥；

[0044] 传送模块，被配置为向所述UE传送所述私钥和MAC。

[0045] 根据第四或第五方面，所述认证服务器可以被配置为：根据其实施例中的任何一个，执行第一方面的方法。

[0046] 根据第四或第五方面的认证服务器可以包括认证服务器功能。

[0047] 第六方面涉及一种用于预配置UE的去隐藏服务器。所述去隐藏服务器包括处理电路和存储器电路。所述存储器电路包含可由所述处理电路执行的指令，从而所述去隐藏服务器操作用于：

[0048] 响应于从认证服务器接收指示UE缺少有效私钥的UE的SUCI，生成用于UE的SUPI和私钥，其中，所述私钥包括UE的归属网络的公钥；

[0049] 基于所述私钥和特定于UE的并且是去隐藏服务器和UE之间的共享秘密的预配置密钥来生成MAC;以及

[0050] 向认证服务器传送所述SUPI、MAC和私钥。

[0051] 第七方面涉及一种用于预配置UE的去隐藏服务器。所述去隐藏服务器被配置为:

[0052] 响应于从认证服务器接收指示UE缺少有效私钥的UE的SUCI,生成用于UE的SUPI和私钥,其中,所述私钥包括UE的归属网络的公钥;

[0053] 基于所述私钥和特定于UE的并且是去隐藏服务器和UE之间的共享秘密的预配置密钥来生成MAC;以及

[0054] 向所述认证服务器传送所述SUPI、MAC和私钥。

[0055] 根据第六或第七方面的去隐藏服务器可以被配置为:根据任何一个实施例中的其实施例中的任何一个,执行第二方面的方法。

[0056] 根据第六或第七方面的去隐藏服务器可以包括至少一个订阅标识符去隐藏功能和统一数据管理。

[0057] 第八方面涉及一种用于获得私钥的UE。所述UE包括处理电路和存储器电路。所述存储器电路包含可由所述处理电路执行的指令,从而所述UE操作用于:

[0058] 从认证服务器接收私钥和MAC,所述私钥包括UE的归属网络的公钥;

[0059] 通过以下方式验证所述私钥的完整性:

[0060] 生成预配置密钥,所述预配置密钥特定于所述UE,并且是所述UE和认证服务器之间的共享秘密;以及

[0061] 使用所述预配置密钥和所述私钥以重新产生从所述认证服务器接收的MAC。

[0062] 第九方面涉及一种用于获得私钥的UE。所述UE被配置为:

[0063] 从认证服务器接收私钥和MAC,所述私钥包括UE的归属网络的公钥;

[0064] 通过以下方式验证所述私钥的完整性:

[0065] 生成预配置密钥,所述预配置密钥特定于所述UE,并且是所述UE和认证服务器之间的共享秘密;以及

[0066] 使用所述预配置密钥和所述私钥以重新产生从所述认证服务器接收的MAC。

[0067] 第十方面涉及用于获得私钥的UE。所述UE包括:

[0068] 接收模块,被配置为:从认证服务器接收私钥和MAC,所述私钥包括UE的归属网络的公钥;

[0069] 验证模块,被配置为:通过以下方式来验证所述私钥的完整性:生成预配置密钥,所述预配置密钥特定于所述UE,并且是所述UE和所述认证服务器之间的共享秘密;以及使用该预配置密钥和私钥以重新产生从所述认证服务器接收的MAC。

[0070] 第十一方面涉及一种包括指令的计算机程序,所述指令当在服务器设备的至少一个处理电路上执行时,使所述至少一个处理器执行根据第一、第二和第三方面中的任何一个的方法。

[0071] 第十二方面涉及一种包括所述计算机程序的存储器电路。

附图说明

[0072] 图1示出了示例性无线通信网络。

[0073] 图2示出了UE对其长期订阅标识符进行加密作为附着过程的一部分的示例。

[0074] 图3示出了订阅隐藏标识符(SUCI)的示例。

[0075] 图4示出了私钥的示例。

[0076] 图5示出了3GPP公钥私密性方案。

[0077] 图6示出了注册过程的示例。

[0078] 图7示出了UE的5G-USIM/UICC生成SUCI的示例。

[0079] 图8示出了5G-USIM/UICC不具有私钥的示例。

[0080] 图9示出了ME生成SUCI的示例。

[0081] 图10示出了向ME通知更新私钥的示例。

[0082] 图11示出了ME检测到5G-USIM/UICC已被替换的示例。

[0083] 图12示出了私钥验证数据的示例。

[0084] 图13示出了UE没有有效私钥的示例UE注册过程。

[0085] 图14示出了需要更新UE的私钥的示例UE注册过程。

[0086] 图15示出了私钥和私钥验证数据如何相互相关的示例。

[0087] 图16示出了用于例如认证服务器的硬件实施例。

[0088] 图17示出了认证服务器的实施例。

[0089] 图18示出了认证服务器的实施例。

[0090] 图19示出了用于例如去隐藏服务器的实施例。

[0091] 图20示出了去隐藏服务器的实施例。

[0092] 图21示出了UE的实施例。

[0093] 图22示出了UE的实施例。

具体实施方式

[0094] 图1示出了示例无线通信网络30,其包括UE 1、服务网络2和归属网络3。该UE和归属网络都与服务网络通信地连接,并且经由该服务网络彼此交换信号。该UE被配置为具有标识由归属网络支持的订阅的订阅标识符,并且使用服务网络访问该归属网络。

[0095] UE的典型示例包括:移动设备(ME)、移动终端、智能手机、个人计算机、膝上型计算机、台式计算机、工作站、平板计算机、可穿戴计算机和/或智能家电。根据UE 1的特定实施例,该UE可以包括作为ME的一部分的通用存储器存储装置,以及提供安全存储器(例如,5G-USIM(通用订户标识模块)、例如上面安装了5G-USIM的UICC(通用集成电路卡)和/或其他安全存储设备)的防篡改安全硬件组件8。根据这样的实施例,通常可以使用该UE的防篡改安全硬件组件来执行归于该UE的任何能力。

[0096] 服务网络2包括能够与UE 1和归属网络3交换通信信号的一个或多个物理设备和/或信令介质。特别地,该服务网络可以包括硬件,该硬件提供一个或多个:接入点(例如,基站、eNodeB、毫微微小区和/或无线接入点)、接入网络、认证服务器、接入和移动性管理功能(AMF)、安全锚点功能(SEAF)、认证服务器功能(AUSF)和/或其任意组合(未示出)。特别地,认证服务器可以提供一个或多个AMF、SEAF、AUSF和/或其任意组合。这些网络实体的细节将在下文进一步详细讨论。

[0097] 归属网络3包括能够经由服务网络2与UE 1交换通信信号的一个或多个物理设备

和/或信令介质。特别地，该归属网络可以包括一个或多个：去隐藏服务器、认证服务器(例如，如上所述的)、密钥预配置(provisioning)服务器、订阅标识符去隐藏功能(SIDF)、私钥预配置功能(PKPF)、统一数据管理(UDM)和/或其任意组合(未示出)。特别地，去隐藏服务器可以提供一个或多个SIDF、PKPF和/或其任意组合。这些网络实体中的特定实体也将在下文进一步详细讨论。

[0098] 该服务和/或归属网络的示例包括(但不限于)一个或多个：局域网；无线网络；蜂窝网络；基于互联网协议的网络；以太网；光网络；和/或电路交换网。这些网络可以包括任意数量的支持这种通信信号的交换的连网设备，例如，路由器、网关、交换机、集线器、防火墙、诸如此类(未示出)。

[0099] 尽管图1示出了独立的服务网络和归属网络，但是在本公开的一些实施例中，归属网络3是服务网络2，即，在UE不漫游的情况下。此外，尽管上文指定了归属网络或服务网络中的特定功能的示例，但是根据特定实施例，那些特定功能可以在归属网络或服务网络中的另一个中。此外，尽管在图1中仅示出了一个UE 1，但是根据特定实施例，服务网络和归属网络可以支持多个UE。

[0100] 保持UE的长期订阅标识符的机密性的一种示例方式是使用归属网络公钥来保护该长期订阅标识符。可以在没有证书的情况下在UE 1内预配置该归属网络公钥，从而不需要全球公钥基础设施(PKI)或证书颁发机构(CA)(即，因为该技术在该UE和归属网络3中的功能之间非对称使用)。在这样的示例中，可以期望UE使用归属网络公钥对长期订阅标识符进行加密，然后向归属网络传送该长期订阅标识符。

[0101] 图2示出了一个这样的特定示例，其中，UE对其长期订阅标识符进行加密，作为附着过程的一部分。根据图2的示例，UE 1对其IMSI进行加密，以明文形式保留其MCC(移动国家代码)和MNC(移动网络代码)部分，并以加密IMSI作为其标识符向服务网络2发送附着请求(步骤1)。该服务网络使用明文MCC/MNC识别UE的归属网络3，并使用加密IMSI作为该UE的标识符向该UE的归属网络请求认证信息(步骤2)。该归属网络从加密IMSI中解密IMSI，并获取相应的认证信息。响应于该认证信息请求，该归属网络向服务网络发送该UE的认证信息和明文IMSI(步骤3)。该服务网络与该UE执行认证过程以认证该UE(步骤4)。如果认证过程成功，则该服务网络向该UE发送附着接受消息(步骤5)。

[0102] 在这样的方法中，归属网络公钥可以在USIM中被预先配置和/或可以使用OTA(空中)预配置程序来预配置。尽管在至少一些实施例中，图2所示的方法确实保护了长期订阅标识符，但是一些这样的实施例可能包括一个或多个缺陷。例如，图2所示的方法可能会因无法可行地更改的传统USIM、某些可能不支持OTA预配置的归属运营商、和/或可能不可更新的USIM(例如，由于技术限制、存储空间缺乏或其他限制)而受挫。

[0103] 本公开的各种实施例向图2所示的特定实施例的至少一些方面提供了备选方案，该备选方案对应于图3-8：文献“Deliverable D3.6 5G-PPP Security enablers open specifications(v2.0)”中的组件之间的交互。特定实施例使归属网络3的公钥能够被预配置(例如，新近地或被刷新)并存储在UE 1中，使得UE 1能够使用该公钥对其订阅标识符进行加密。此外，在特定实施例中，核心网(例如，5GC(5G核心)网)触发通过3GPP定义的现有业务过程(例如，注册/认证信令，例如，与注册过程有关的UE与AMF/SEAF节点之间的非接入层消息)预配置归属网络公钥，而无需依赖附加的基础设施和带外过程，例如，执行OTA更新过

程。

[0104] 尽管本文的各种实施例将描述由UE 1执行的某些特征或动作，但是除非另有说明，否则不应假设这些特征或动作由该UE的任何特定组件执行。例如，取决于特定实施例，这种功能可以或不可以由UICC、USIM、嵌入式UICC、集成UICC或UE的其他电路和/或软件(例如，ME中的基带电路)执行。

[0105] 特定实施例包括订阅永久标识符(SUPI)。SUPI是分配给5G系统中每个用户的明文、全球唯一5G永久标识符。SUPI可以是基于IMSI的或非基于IMSI的。包括基于IMSI的SUPI的实施例可以使用例如3GPP TS 23.003 V15.0.0中描述的IMSI。包括非基于IMSI的SUPI的实施例可以基于根据在3GPP TS 23.003 V15.0.0中描述的基于NAI IETF RFC 4282的用户标识的网络接入标识符(NAI)。在一些实施例中，该SUPI包含归属网络的地址(例如，在基于IMSI的SUPI的情况下的MCC和MNC)。这样的实施例可以例如通过向服务网络2提供对于识别该UE的归属网络3有用的信息来实现某些漫游场景。如果SUPI是NAI，则它也可以包含IMSI，但也可以是非基于IMSI的。

[0106] 特定实施例附加地或备选地包括订阅隐藏标识符(SUCI)，例如图3的示例中所示。SUCI是SUPI的受保护版本。SUCI包括明文部分和加密部分。

[0107] 该明文部分包括标识UE 1的归属网络的归属网络标识符。例如，SUCI可以包括该归属网络的MCC和MNC。该明文部分还可以包括对于根据加密方案对该SUCI的加密部分进行解密有用的公钥标识符、加密方案标识符和/或方案相关参数(例如，该UE的临时公钥或在椭圆曲线集成加密方案(ECIES)或其他加密方案中使用的其他参数)。术语临时密钥是本领域技术人员已知的，并且被定义为一种密钥，该密钥的使用被限制在较短时间段内，例如，单个电信连接(或会话)，在此之后，其所有痕迹被消除。如下文将要时论的，公钥标识符是可以在归属网络内用于识别包括多个SIDF的归属网络中的正确SIDF的标识符。ECIES、公钥标识符和SIDF将在下文更详细地描述。技术人员理解，SUCI上下文中的“明文部分”表示其中的信息是非隐藏/未加密的信息。

[0108] 如果SUCI中包括加密部分，则该SUCI是SUPI的受保护版本。该加密部分包括加密订阅标识符，例如，MSIN(移动订阅标识号)或用户名(username)。用户名可以是NAI中“@”之前的全部或部分字符，例如，username@mnc<MNC>.mcc<MCC>.3gppnetwork.org。在此示例中，“@”之前的所有字符均被加密。在具有形式“homerealm!username@otherrealm”的装饰NAI的情况下，由于“homerealm”可用作路由信息，因此仅对“@”左侧文本的username部分进行加密。因此，可以执行对SUCI的加密部分进行解密以学习相应的SUPI。ECIES是可用于根据SUPI生成SUCI和/或根据SUCI生成SUPI的公钥加密方案的示例。如将在下文进一步讨论的，例如，如果UE 1尚未被预配置有归属网络的公钥，则SUCI的加密部分可以使用空(null)加密方案。

[0109] SIDF是位于归属网络中的负责对SUCI进行解密的功能。特别是在5G架构中，SIDF可以协同定位在UDM(统一数据管理)中。SIDF可以备选地被称为UDM的一部分或由UDM提供。附加地或备选地，SIDF可以是与UDM分离的实体和/或与AUSF(认证服务器功能)协同定位。

[0110] 图4示出了私钥的示例。该私钥的特定示例包括归属网络的公钥。在一些实施例中，私钥还包括：一个或多个公钥方案相关参数、长期订阅标识符、指示该私钥所属的网络、域或上下文的主题字段(例如，该主题可以是归属网络标识符，例如，MCC/MNC)、公钥方案标

识符、公钥方案相关域特定值(例如,在ECIES方案的情况下用于椭圆曲线域的值)、将在下文进行详细讨论的公钥标识符、指定何时私钥有效的有效时间指示(例如,之前无效和/或之后无效时间)、指示可以使用密钥的一种或多种方式的密钥用途字段(例如,订阅标识符私密性、切片选择私密性等)、和/或基于私钥的一些或全部内容计算的数字签名。

[0111] 具体地,根据本公开的实施例,可以将该密钥用途字段设置为指示该密钥对于"订阅私密性"是有用的。超出本公开范围的私密性的使用可以附加地或备选地指示私钥的其他使用。例如,私钥可以用于"网络切片选择辅助信息(NSSAI)私密性"目的而不是"订阅私密性"目的,或除了"订阅私密性"目的,私钥还可以用于"网络切片选择辅助信息(NSSAI)私密性"目的。实际上,这样的其他目的可以包括UE 1和/或归属网络中的类似方法、设备和系统,以用于如本文所述的初始预配置、刷新和其他特征。尽管在一些实施例中一个私钥可以指示多种用途,但是其他实施例可以包括用于各个用途的各个私钥,每个私钥的密钥用途字段指示单个密钥用途(例如,私钥之一可以指示"订阅私密性",另一个可以指示"NSSAI私密性")。该密钥用途字段可以被格式化为整数、一个或多个枚举值、字母数字字符串、比特字符串、定界字符串和/或任何上述格式的阵列等。

[0112] 3GPP公钥私密性方案(3GPK方案)是标准化公钥方案,其中UE 1可以支持该UE与例如移动运营商之间的互操作性。在没有标准化方案的情况下,UE供应商可能会需要与此类运营商协调以实现私密性机制。根据特定实施例,UE应当支持被允许和/或标准化的方案中的任何一个,使得归属网络能够自由地选择方案而不产生任何互操作性困难。一种这样的方案例如具体是ECIES。特定的方案可以作为标准被采用,并且被赋予用于互操作性的标识符(也被称为"寄存器")。对于每个这样的方案,也可以指定需要支持的任何特定算法。例如,在ECIES的情况下,可以指定密钥协议(KA)、密钥导出(KD)函数(KDF)、对称完整性和对称加密。也可以指定与这样的方案有关的一个或多个参数,以及(在一种或多种情况下)其可能的静态值。例如,在ECIES中,可以指定用于素域上曲线的椭圆曲线域参数(p,a,b,G,n,h)和/或用于二进制域上曲线的(m,f(x),a,b,G,n,h)。

[0113] 图5说明了示例3GPK方案。可以为采用为标准的每个方案分配特定标识符。例如,可以为空(null)方案分配0,为ECIES分配1,依此类推。其他实施例可以以其他方式格式化该方案标识符,包括但不限于一个或多个整数、数字字符串、字母数字字符串、比特字符串和/或其他数据类型。

[0114] 根据本文的实施例,UE根据注册过程(例如,图6所示的示例注册过程)向无线通信网络30注册。根据图6所示的示例注册过程,UE使用归属网络的公钥来隐藏长期订阅标识符。尽管图6所示的一个或多个特定接口(例如,由N后跟数字标记(例如,N1、N12、N13)指定的接口)符合3GPP TS 23.501,但在本文所述的这样的接口上执行的信令以及其他接口本身(例如,Nxx)在任何已知技术中都是未知的或未描述的。

[0115] 根据图6的示例,UE 1在注册请求中包括临时标识符(例如,5G-GUTI),并向AMF/SEAF 4发送该注册请求(步骤1)。AMF/SEAF(无法识别5G-GUTI)向UE传送标识符请求消息以请求该UE的标识符(步骤2)。UE用包括SUCI的标识符响应消息来响应该标识符请求消息(步骤3)。AMF/SEAF向归属网络3中的AUSF 5请求UE的认证,并将SUCI包括在认证请求中(步骤4)。AUSF使用在SUCI中编码的信息来确定使用多个SIDF中的哪一个来对SUCI的至少一部分进行解密(步骤5)。具体地,AUSF可以使用SUCI中携带的(或以其他方式存在于认证请求消

息中的)公钥标识符来识别正确的SIDF 6。在一些实施例中,AUSF可以附加地或备选地使用方案标识符来识别正确的SIDF。换句话说,不同的SIDF可以处理不同的加密方案(例如,第一SIDF可以处理ECIES,第二SIDF可以处理RSA),并且AUSF可以基于通过SUCI识别的方案来选择合适的SIDF。在又一备选实施例中,用于识别正确的SIDF 6的信息可以是指示SIDF 6的参数或ID,并且所述参数/ID被存储到或预配置给防篡改安全硬件。

[0116] 例如,本公开的实施例可以包括多个SIDF,以避免对于具有大量用户的网络具有单个故障点。因此,分布式SIDF部署可以有利于提高网络的容错性、负载平衡和/或整体容量。附加地或备选地,可以部署不同的SIDF实例以处理不同的归属网络公钥集。因此,根据本文的一个或多个实施例,SUCI中的公钥标识符可以用于选择适合的SIDF实例。备选地,在仅部署有一个SIDF的特定实施例中,可以从SUCI中省略公钥标识符。

[0117] AUSF 5向所选的SIDF 6发送SUCI(步骤6)。如果SIDF协同位于UDM 7中(例如,使得图6的步骤6中的Nxx消息是N13消息),则可以使用同一消息从UDM请求认证矢量或认证证书。SIDF对SUCI进行解密以获得相应的SUPI,并向AUSF返回SUPI(步骤7)。如果SIDF协同位于UDM中,则可以使用相同的消息向AUSF返回认证矢量/证书。

[0118] AUSF 5和UE 1使用从UDM 7接收的认证矢量/证书来交换认证消息(步骤8)。如果AUSF尚未从UDM接收到所需的认证矢量/证书(例如,在上述步骤7中),则AUSF可以在发起与UE的认证之前向UDM请求认证矢量/证书(未示出)。备选地,AUSF可能已向SEAF委托了认证。在这样的实施例中,AUSF可以在该步骤中简单地向SEAF转发SUPI,并且在下一步骤中依靠SEAF来执行认证。

[0119] 继续AUSF 5成功认证了UE 1的示例,AUSF向AMF/SEAF 4返回SUPI(步骤9)。AMF/SEAF接受UE的注册,并向UE传送注册接受消息(步骤10)。

[0120] 如以上简要讨论的,UE 1的特定特征可以由UE的防篡改安全硬件组件8执行。图7示出了UE的5G-USIM/UICC 8a生成SUCI的特定示例。尽管该特定示例使用了术语5G-USIM/UICC,但不应将该术语视为对USIM或UICC技术的任何版本或供应商的限制,也不应将该术语视为对任何一代移动网络(例如,2G/3G/4G/5G)进行限制。

[0121] 根据图7的示例,ME 9请求SUCI(步骤1)。在一些这样的实施例中,该SUCI请求可以包括时间。在其他这样的实施例中,该请求可以仅仅是从5G-USIM/UICC 8a的读取操作。根据存在多个归属网络公钥的这样的实施例,5G-USIM/UICC选择正确的对应私钥(例如,基于时间),并使用所选的私钥生成SUCI(步骤2)。备选地,如果这样的实施例中只有一个私钥,则5G-USIM/UICC仅使用该私钥。然后,5G-USIM/UICC向ME返回SUCI(步骤3)。

[0122] 图8示出了5G-USIM/UICC不具有私钥或不支持该功能的示例。

[0123] 根据图8的示例,ME 9以与以上参考图7所述的类似方式的请求(在一些实施例中可以包括时间)来请求SUCI。然而,在该示例中,5G-USIM/UICC 8a不具有私钥或不能识别该命令,因为它确实支持该功能(步骤2)。因此,5G-USIM/UICC向ME返回错误消息(或空数据)(步骤3)。

[0124] 根据特定实施例,作为图8的示例的备选,ME 9可以通过其他方式知道5G-USIM/UICC 8a不具有私钥或不支持私钥。例如,ME可以获取5G-USIM/UICC的版本和/或供应商信息,并基于该信息确定不支持或不存在私钥。作为另一示例,ME可以基于来自5G-USIM/UICC的一些其他响应消息来确定在5G-USIM/UICC中不支持或不存在私钥。

[0125] 图9示出了ME 9生成SUCI、但是私钥本身被存储在5G-USIM/UICC 8a中的示例。

[0126] 根据图9的示例,ME 9不具有私钥,并向5G-USIM/UICC 8a请求私钥(步骤1)。在一些实施例中,该请求包括时间。在其他实施例中,该请求是从5G-USIM/UICC存储器的直接读取操作。然后,5G-USIM/UICC选择私钥(例如,基于时间(如果在请求中被提供))(步骤2)。5G-USIM/UICC向ME返回该私钥(步骤3)。此时,在一些实施例(但不一定是所有实施例)中,ME可以将该私钥和/或SUPI存储到ME的非易失性存储器中(步骤4)。然后,ME基于SUPI和该私钥生成SUCI(步骤5)。

[0127] 图10示出了如果在5G-USIM/UICC 8a中更新私钥则ME 9得到通知的示例。在该场景中,ME订阅私钥的改变,并在更新可用时得到通知。该场景假设ME存储私钥或根据需要向5G-USIM/UICC请求私钥以获得最新私钥。

[0128] 根据图10的示例,ME 9向5G-USIM/UICC 8a发送请求订阅私钥更新的请求(步骤1)。在一些实施例中,该请求可以包括SUPI。5G-USIM/UICC接受订阅并向ME传送确认作为响应(步骤2)。当归属网络更新私钥或向5G-USIM/UICC交付一个或多个新私钥时(步骤3),5G-USIM/UICC通知ME一个或多个新私钥可用(步骤4)。尽管图10描绘了包括私钥的通知消息,但是根据其他实施例,ME可以备选地基于该通知从5G-USIM/UICC中读取密钥。ME确认该通知(步骤5)。然后,ME将新私钥存储到ME的非易失性存储器中(步骤6)。如果先前存储的私钥数据中的MCC/MNC/MSID相同,则ME可以替换现有的私钥数据。

[0129] 图11示出了根据各种实施例,UE被通电并且ME 9检测到5G-USIM/UICC 8a已经被替换(例如,被替换为不同的5G-USIM/UICC,或者仅仅被移除并重新插入)的示例。尽管特定实施例可以将用不同的5G-USIM/UICC进行的替换等同于移除并重新插入(例如,出于安全性原因),但是其他实施例可以基于检测到这两种情况中的哪一种来做出不同的响应。

[0130] 根据图10的示例,UE 1被通电(步骤1)。ME 9向5G-USIM/UICC 8a发送消息(步骤2),并且5G-USIM/UICC以与UE先前被通电时不一致的方式进行响应(步骤3)。例如,响应消息可以包括与ME先前看到的任一SUPI不同的SUPI。

[0131] ME 9确定5G-USIM/UICC 8a已被替换(步骤4)。例如,5G-USIM/UICC可以与前一次UE 1被通电时有某种不同,指示该5G-USIM/UICC已被不同的5G-USIM/UICC替换。备选地,ME可以使用非易失性存储器检测5G-USIM/UICC已被替换,该非易失性存储器通过机械、电气或软件机制(例如,光学传感器、开关、重量传感器、压力传感器、和/或在移除和/或插入5G-USIM/UICC(例如,无论是已移除并重新插入相同的5G-USIM/UICC还是不同的5G-USIM/UICC)时触发的电路)更新。

[0132] ME 9从非易失性存储器(如果有的话)中移除其先前存储的私钥。附加地或备选地,如果ME将旧的5G-USIM/UICC的SUPI与私钥一起存储到其存储器中,则ME可以基于由新的5G-USIM/UICC 8a返回的SUPI和与旧私钥一起存储的SUPI的比较来决定从非易失性存储器中移除该私钥。

[0133] 上文所述的特定实施例描述了无线通信系统内的设备可以安全地交换订阅标识符的方式,包括特定数据结构和相应的加密/解密方案的生成和使用。特别地,上述实施例允许该安全交换作为向无线通信网络30注册UE 1的一部分来执行。许多这样的实施例假设为UE预配置有效的私钥。

[0134] 为了确保UE 1实际上具有有效的私钥,本公开的其他实施例描述了预配置UE的方

式。与预配置有关的特定实施例可以包括私钥验证数据(MAC-P)。如图12的示例所示,MAC-P包括消息认证码(MAC)。基于私钥和预配置密钥(将在下文更详细地解释)计算MAC。例如,可以结合预配置密钥,基于私钥的各字段(包括但不限于如上所述的归属网络公钥及其相关参数)计算MAC。

[0135] 根据一些实施例,MAC-P还可以包括预配置密钥标识符(例如,RAND)和/或完整性保护算法标识符。根据其中MAC-P不包括完整性保护算法标识符的一些实施例,要使用的完整性保护算法可以与MAC-P分开识别,或可以使用预定义的密钥导出函数(KDF),例如,HMAC-SHA-256。MAC-P可以附加地或备选地包括计数器字段,该计数器字段可以用于从多个MAC-P中识别该MAC-P(例如,在使用相同的预配置密钥来计算一个以上MAC-P的情况下)。下文参照图15进一步解释私钥(例如,如图4所示)和MAC-P(例如,如图12所示)之间的关系。

[0136] 预配置密钥是在UE 1和PKPF 10(参见图13)之间共享的秘密,这将在下文进一步详细描述。预配置密钥是UE特定的,即,它是在归属网络3中与UE和/或5G USIM、UICC 8a或在允许SIM/USIM存储在其中的UE/ME中的任何其他硬件相关联的密钥。在一些实施例中,预配置密钥可以从归属网络主密钥(例如,在5G或未来网路中如例如在5G AKA、EAP-AKA'和EAP-TLS(可扩展认证协议-传输层安全性)中创建的KAUSF)中导出,该归属网络主密钥是在UE 1向网络进行认证时创建的。在一些这样的实施例中,AUSF可以具有归属网络主密钥。此外,当UE重新认证时,可以创建新的归属网络主密钥。

[0137] 根据一个示例,可以(例如,通过应用诸如HMAC-SHA-256的KDF、或诸如SHA-256的其他安全单向哈希函数、或CK和IK的串联)根据CK(密码密钥)、IK(完整性密钥)创建预配置密钥。除了根据主密钥或CK/IK直接生成之外,预配置密钥还可以根据如在EAP-AKA'方法中根据CK和IK生成的CK'和IK'生成。在另一备选方案中,如在RFC5216中规定的,在EAP-TLS情况下,可以根据EMSK(扩展主会话密钥)生成预配置密钥。由于相同的归属网络主密钥可以用于导出许多密钥,因此本公开的实施例将至少一个另外的标准参数与归属网络主密钥结合使用作为用于导出预配置密钥的输入。例如,当使用标准KDF时,FC(功能代码)可以用作输入(例如,如TS 33.220(例如,TS33.220 V15.0.0)中规定的),以产生可与使用归属网络主密钥产生的其他密钥区分开的预配置密钥。

[0138] 根据另一示例,预配置密钥可以是与SIDF 6和UE 1之间共享的临时共享密钥相同或从其导出的密钥,特别是当使用的加密方案是混合公钥方案(例如,ECIES)时。例如,ECIES将公钥机制(例如,Diffie-Hellman)用作导致SIDF和UE之间的共享密钥(临时的)的密钥协议。为了安全性目的,通常进一步通过密钥导出函数(例如,SHA-256)处理该临时共享密钥,以在SIDF和UE之间导出其他导出共享密钥(例如,ECIES中的加密密钥和MAC密钥)。这些其他导出的共享密钥之一通常用于加密,并被称为临时加密密钥。如应用于本公开的实施例,可以使用这些其他导出共享密钥之一,以例如根据SUPI生成SUCI。此外,在一些实施例中,可以使用导出共享密钥中的另一个(例如,ECIES中的MAC密钥)、进一步从导出共享密钥之一中导出的新密钥、或者从临时共享密钥中导出的另一个密钥作为预配置密钥。在其中SIDF具有或能够获得/导出预配置密钥的一些实施例中,SIDF也可以计算MAC或MAC-P。

[0139] PKPF 10是位于归属网络3中的功能,负责预配置私钥。根据特定实施例,PKPF可以与AUSF 5协同定位,特别是在至少一些实施例中,其中,预配置密钥是从基于UE与网络之间的主(primary)认证而创建的归属网络主密钥中导出的。在其他实施例中,PKPF可以与其他

5GC实体(例如,UDM 7)协同定位。根据其他实施例,PKPF是其自己的单独实体。在一些实施例中,SIDF 6和PKPF一起被实现为单个功能,并且不需要传送预配置密钥。在一些其他实施例中,PKPF可以从SIDF中获得预配置密钥。PKPF还可以从SIDF获得MAC/MAC-P。

[0140] 图13示出了UE 1没有有效私钥的示例UE注册过程。例如,终端用户可能已将新的USIM/UICC插入到UE中,并且该新的USIM/UICC不包含私钥。

[0141] 根据图13所示的示例,UE 1向AMF/SEAF 4发送注册请求,该请求中包括SUCI(步骤1)。因为在这种场景中,UE最初不具有私钥,所以UE使用空(null)方案或空(null)加密方法来创建SUCI。此外,根据特定实施例,因为UE不具有将指示空(null)方案或空(null)加密方法(根据实施例,归属网络可以自由选择)的私钥,所以可以使用UE中缺少实际私钥的显式或隐式指示符。例如,如上所述,SUCI可以对加密部分使用空(null)加密方案,这可以隐式地发信号通知缺少私钥。备选地,“缺少私钥”指示符可以是例如标准化的或众所周知的公钥标识符值、标志和/或消息类型指示符(例如,类型为“私密性预配置”或“预先初始注册”的注册请求)。

[0142] 已经接收到该注册请求的AMF/SEAF 4向AUSF 5/PKPF 10请求UE认证(步骤2)。AUSF向SIDF 6发送SUCI(和“缺少私钥”指示符,如果认证请求中包括“缺少私钥”指示符)(步骤3)。根据SIDF协同位于UDM 7中的实施例(例如,Nxx消息是N13消息),可以使用相同的消息向UDM请求认证矢量/证书。

[0143] SIDF 6看到SUCI是明文的并且UE 1缺少私钥。根据该示例,SIDF具有必须使用ECIES保护所有SUCI的本地策略。因此,SIDF将SUPI连同向UE预配置ECIES私钥的请求一起向AUSF返回(步骤4)。在一些实施例中,该响应包括要向UE预配置的多个私钥。根据SIDF协同位于UDM 7中的实施例,相同的消息可以用于向AUSF 5返回认证矢量/证书。

[0144] 根据AUSF 5尚未从UDM 7接收到认证矢量/证书的实施例,在发起与UE的认证之前,AUSF 5可以向UDM请求所述认证矢量/证书(未示出)。备选地,根据其中AUSF已经从UDM接收到认证矢量/证书的实施例,AUSF和UE使用所述认证矢量/证书来交换认证消息(步骤5)。备选地,AUSF可能已经向AMF/SEAF 4委托了认证。

[0145] 根据该示例,PKPF 10与AUSF 5协同定位。因此,在成功认证之后,AUSF/PKPF创建可用于保护到UE 1的私钥预配置消息的预配置密钥,即,无需交换信令以传送预配置密钥。根据其中AUSF和PKPF非协同定位的其他实施例,AUSF可以请求由PKPF生成预配置密钥,并且作为响应,PKPF可以向AUSF传送该预配置密钥(未示出)。

[0146] AUSF 5/PKPF 10通过计算MAC(例如,如上文关于图12所述)并构造MAC-P,用预配置密钥保护(在步骤4中从SIDF 6接收的)私钥(步骤6)。在一些实施例中,私钥也可以被加密。在一些实施例中,如上所述,特别是在预配置密钥基于例如EICES方案的临时共享密钥的至少一些实施例中,AUSF/PKPF可以从SIDF接收MAC和/或MAC-P。特别地,如上所述,SIDF可能已经生成了MAC和/或MAC-P。

[0147] 然后,AUSF 5向AMF/SEAF 4返回SUPI、私钥和MAC-P(步骤7)。在一些实施例中,在相同的注册相关消息流中向AMF/SEAF传送SUPI、私钥和/或MAC-P,用于向无线通信网络30注册UE 1。在一些实施例中,在单独的消息流(未示出)中向AMF/SEAF发传送SUPI、私钥和/或MAC-P。

[0148] 根据其中AUSF 5向AMF/SEAF 4委托了UE 1的认证的实施例,AMF/SEAF可以在此时

认证UE(未示出)。在这样的实施例中,AMF/SEAF可能已经例如先前在步骤4中直接从SIDF 6接收到SUPI、私钥和MAC-P。

[0149] AMF/SEAF 4接受UE 1的注册,并且例如在注册接受消息中向UE转发私钥和MAC-P(步骤8)。然后,UE尝试验证MAC,并且如果成功,则存储该私钥。为了验证MAC,UE创建与AUSF 5/PKPF 10先前所创建的相同的预配置密钥。换句话说,当UE生成期望的MAC并且然后将其与接收的MAC进行比较时,如果期望的MAC被认为与接收的MAC相同,则MAC被验证。

[0150] 在一些实施例中,根据上述实施例之一,然后UE 1从网络解附着(步骤9),例如以使用预配置私钥隐藏其用户标识来开始新的注册过程。例如,以这种方式解附着和重新注册可以防止攻击者将SUPI与UE的临时标识符链接。

[0151] 在一些实施例中,由于先前向UE预配置的私钥到期或无效,可能需要为UE 1预配置私钥。图14示出了例如出于某种安全性或操作原因,需要更新UE的私钥的示例UE注册过程。根据各种实施例,可能需要更新先前预配置的私钥的一些原因可能是该先前预配置的私密性可能已经达到(或正在达到)其到期日,无线通信网络30中的安全性已经以某种方式受到危害,和/或该私钥要定期更新。

[0152] 根据图14的示例,UE 1向AMF/SEAF 4发送注册请求(步骤1)。该注册请求包括SUCI。在该示例中,由于UE具有私钥,因此例如根据上述实施例之一,UE使用加密方案或方法(例如,ECIES)创建SUCI。

[0153] AMF/SEAF 4向AUSF 5/PKPF 10请求UE认证(步骤2)。AUSF向SIDF 6发送SUCI(步骤3)。如在先前的示例中,根据SIDF与UDM 7协同定位的一些实施例,相同的消息可以用于向UDM请求认证矢量/证书。

[0154] SIDF 6看到SUCI用需要更新的私钥加密。例如,SIDF可以检测到私钥到期或即将到期,或者私钥由于如前所述的任何其他原因而无效。SIDF将SUPI连同向UE预配置更新的ECIES私钥的请求一起向AUSF 5返回(步骤4)。根据一些实施例,该响应可以包括几个私钥。此外,如先前所讨论的,根据SIDF协同位于UDM中的一些实施例,相同的消息可以用于向AUSF返回认证矢量/证书。

[0155] AUSF 5和UE 1使用从UDM 7接收的认证矢量/证书来交换认证消息(步骤5)。如先前示例中所讨论的,AUSF可能已经在步骤4中从UDM接收了所需的认证矢量/证书(例如,在SIDF 6协同位于UDM中的一些实施例中),或者AUSF在发起与UE的认证之前,可以向UDM请求这种认证矢量/证书。

[0156] 根据PKPF 10与AUSF 5协同定位的实施例,作为成功认证的结果,AUSF/PKPF可以创建用于保护到UE 1的私钥预配置消息的预配置密钥。例如,认证过程可以包括产生可用于导出预配置密钥的归属网络主密钥。备选地,在PKPF和AUSF没有协同定位的实施例中,AUSF和PKPF可以通过适合的消息传送(未示出)交换预配置密钥。

[0157] 例如根据图14所示的示例,AUSF 5/PKPF 10通过计算MAC并构造MAC-P,用预配置密钥来保护(在步骤4中从SIDF 6接收到的)私钥(步骤6)。如上所述,在一些实施例中,特别是在预配置密钥基于例如EICES方案的临时共享密钥的至少一些实施例中,AUSF/PKPF可以从SIDF接收MAC和/或MAC-P。特别地,如上所述,SIDF可能已经生成了MAC和/或MAC-P。

[0158] 在成功认证之后,AUSF 5例如在相同的注册相关消息流中向AMF/SEAF 4发送SUPI、私钥和MAC-P(步骤7)。其他实施例可以针对SUPI、私钥或MAC-P中的一个或多个使用

单独的消息流。此外，如前所述，AUSF可能已经向SEAF委托了UE的认证，在这种情况下，可能已经在步骤4中向SEAF返回SUPI、私钥和MAC-P，并且AUSF如先前所述执行认证。

[0159] AMF/SEAF 4接受UE 1的注册，并且例如在注册接受消息中向UE转发私钥和MAC-P(步骤8)。UE从主认证中创建与AUSF 5/PKPF 10所创建的相同的预配置密钥，并验证消息中的MAC。如果验证成功，则UE存储该私钥。也可以移除旧的私钥。

[0160] 根据又一示例，AUSF 5生成MAC和MAC-P，并且经由UDM 7向UE 1发送私钥和MAC-P，其中UDM 7向AMF转发私钥和MAC-P，然后AMF向UE 1转发私钥和MAC-P。在这样的示例中，AUSF可以是归属公共陆地移动网络AUSF，并且在这种情况下，AMF可以是访问公共陆地移动网络(VPLMN)AMF。在这种情况下，AUSF可能已经向VPLMN AMF委托了认证。

[0161] 如之前所讨论的，可以基于私钥(例如，如图4所示)和预配置密钥来计算MAC，以生成MAC-P(例如，如图12所示)。在向UE 1预配置多个私钥的一些实施例中，可以基于同一消息中发送的所有私钥计算相同的MAC。

[0162] 图15示出了私钥和MAC-P如何相互关联、以及将什么参数用作MAC计算(或适当地为期望的MAC(XMAC))的输入的示例。如图15所示，预配置密钥和私钥都用于生成MAC，然后可以将其与另一个私钥结合使用以更新该MAC，依此类推，直到处理完所有私钥为止。一旦所有私钥被处理，就可以向UE发送私钥和MAC。

[0163] 鉴于以上所有内容，可以使用图16所示的示例硬件来实现上述设备或功能中的一个或多个。该示例硬件包括处理电路11和通信电路12。该处理电路例如经由一个或多个总线与通信电路通信地耦接。该处理电路可以包括一个或多个微处理器、微控制器、硬件电路、离散逻辑电路、硬件寄存器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、专用集成电路(ASIC)或其组合。例如，该处理电路可以是能够执行软件指令的可编程硬件，该软件指令被存储为例如存储器电路13中的机器可读计算机程序133。各种实施例的存储器电路可以包括本领域已知的或可以开发的任何非暂时性机器可读介质，无论是易失性还是非易失性的，包括但不限于固态介质(例如，SRAM、DRAM、DDRAM、ROM、PROM、EPROM、闪存、固态驱动器等)、可移除存储设备(例如，安全数字(SD)卡、miniSD卡、microSD卡、记忆棒、拇指驱动器、USB闪存驱动器、ROM卡盒、通用介质盘)、固定驱动器(例如，磁性硬盘驱动器)等，完全地或以任意组合的形式。根据使用硬件来实现UE 1的特定实施例，该存储器电路可以包括提供安全存储器(例如，5G-USIM和/或UICC 8a)的防篡改安全硬件组件8。

[0164] 通信电路12可以是被配置为控制硬件的输入和输出(I/O)数据路径的控制器中心(hub)。这样的I/O数据路径可以包括用于通过无线通信网络30交换信号的数据路径。例如，该通信电路可以包括收发机，该收发机被配置为例如通过空中、电气和/或光学介质在UE 1、服务网络2和/或归属网络3之内和/或之间发送和接收通信信号。

[0165] 通信电路12可以被实现为单一的物理组件，或者被实现为连续或分开布置的多个物理组件，其中的任意一个可以与任何其他组件通信耦接，或者可以经由处理电路11与任何其他组件通信。例如，该通信电路可以包括：发射机，被配置为发送通信信号；以及接收机，被配置为接收通信信号(未示出)。

[0166] 根据特定实施例，图16所示的硬件可以配置有多个组件。这些组件可以包括多个通信耦接的硬件单元和/或软件模块。一个或多个硬件单元可以是例如处理电路11的一部分。一个或多个软件单元可以例如被存储在存储器电路13中并且由处理电路执行。

[0167] 例如,诸如图16所示的硬件可以用于实现UE 1的归属网络3中的认证服务器14(例如,AMF、SEAF 4、AUSF 5),并被配置有图17所示的示例组件,以获得UE的订阅标识符。图17的组件包括确定单元或模块15、以及接口单元或模块16。该确定单元或模块被配置为:基于从UE接收的信息,确定要用多个去隐藏服务器中的哪一个来对其中订阅标识符被加密的订阅隐藏标识符(SUCI)的至少一部分进行解密。该接口单元或模块被配置为向确定的去隐藏服务器发送SUCI,并且作为响应,接收订阅标识符。

[0168] 这样的认证服务器14可以附加地或备选地被配置有图18所示的示例组件以预配置UE 1。图18的组件包括获取单元或模块17,以及传送单元或模块18。该获取单元或模块被配置为基于特定于UE 1的预配置密钥和UE的归属网络3的私钥来获取消息认证码(MAC)。该传送单元或模块被配置为向UE传送私钥和MAC。

[0169] 这样的认证服务器14还可以被配置为:例如使用上述认证服务器硬件或软件组件中的任何一个来附加地或备选地执行本文所述的关于认证服务器的任一方法。

[0170] 根据图16所示的示例所述的其他硬件可以用于实现去隐蔽服务器19(例如,SIDF 6),以用于向认证服务器14提供UE 1的订阅标识符,并且可以配置有图19所示的示例组件。图19的组件包括接收单元或模块20、解密单元或模块21、以及发送单元或模块22。该接收单元或模块被配置为:从认证服务器接收订阅隐藏标识符(SUCI),在所述SUCI中订阅标识符被加密。该解密单元或模块被配置为:使用根据从UE接收的信息识别的解密密钥对所述SUCI的至少一部分进行解密,以获得订阅标识符。该发送单元或模块被配置为向认证服务器发送该订阅标识符。

[0171] 这样的去隐藏服务器19可以附加地或备选地被配置有图20所示的示例组件以预配置UE 1。图20的组件包括生成单元或模块23、以及传送单元或模块24。该生成单元或模块被配置为:响应于从认证服务器14接收指示UE缺少有效私钥的UE的订阅隐藏标识符(SUCI),来生成用于所述UE的订阅永久标识符(SUPI)和私钥。该传送单元或模块被配置为向认证服务器发送所述SUPI和私钥。因此,术语“去隐藏服务器”也可以被称为SUCI去隐藏服务器。

[0172] 这样的去隐藏服务器19还可以被配置为:例如使用任何上述去隐藏服务器硬件或软件组件来附加地或备选地执行本文所述的关于去隐藏服务器的任一方法。

[0173] 根据图16所示的示例所述的其他硬件可以用于实现用于向无线通信网络30安全地通知订阅标识符的UE 1,并且被配置有图21所示的示例组件。图21的组件包括生成单元或模块25、以及传送单元或模块26。该生成单元或模块被配置为生成订阅隐藏标识符(SUCI),在所述SUCI中UE的订阅标识符被加密。该传送单元或模块被配置为:向认证服务器14传送SUCI和识别能够对该订阅标识符进行解密的去隐藏服务器19的信息。

[0174] 这样的UE 1可以附加地或备选地被配置有图22所示的示例组件以获得私钥。图22的组件包括接收单元或模块27、以及验证单元或模块28。该接收单元或模块被配置为从认证服务器14接收私钥和消息认证码(MAC)。该验证单元或模块被配置为:通过生成预配置密钥并使用所述预配置密钥和私钥再现从认证服务器接收的MAC来验证私钥的完整性,所述预配置密钥是UE和认证服务器之间的共享秘密。

[0175] 这样的UE 1还可以被配置为:例如使用上述UE硬件或软件组件中的任何一个来附加地或备选地执行本文所述的关于UE的任一方法。

[0176] 本文描述的各种方法和过程可以以与上文给出的广义描述在某些细节上不同的方式来实现。例如，尽管本文描述的各种过程或方法的步骤可以被示出和描述为以次序或时间顺序，但是任何这样的过程或方法的步骤不限于以任何特定的次序或顺序来执行，除非另有说明。实际上，这样的过程或方法中的步骤通常可以以各种不同的次序和顺序来执行，同时仍然落入本公开的范围内。本文描述的实施例在所有方面都应被认为是说明性的而非限制性的。特别地，在以下所附列举的实施例的含义和等效范围内的所有改变都旨在包含在其中。

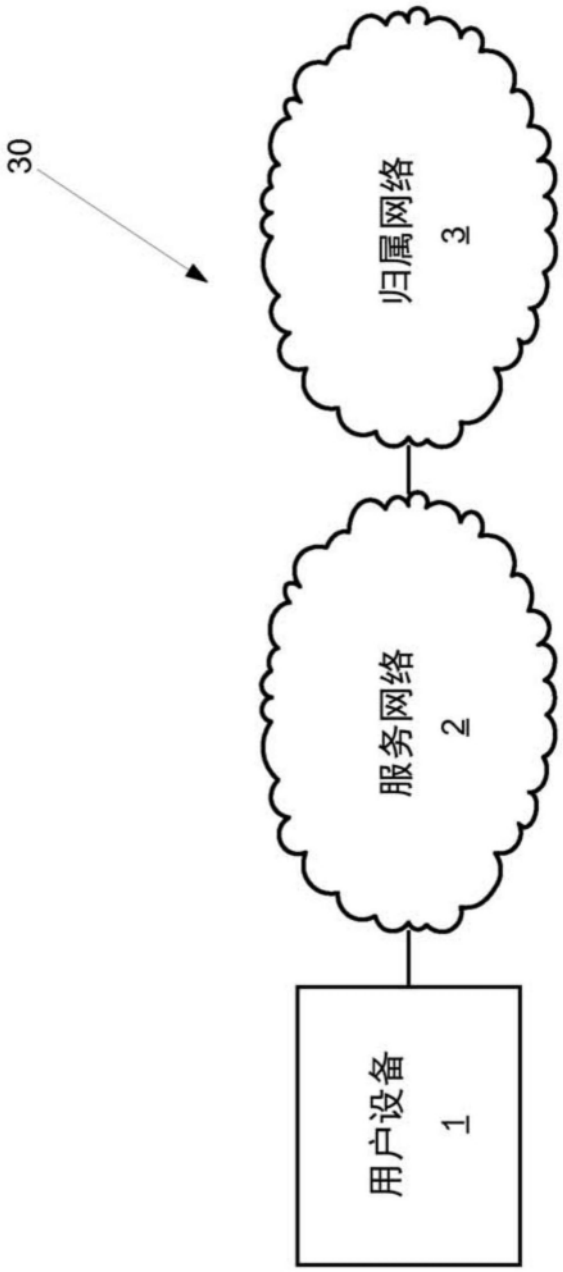


图1

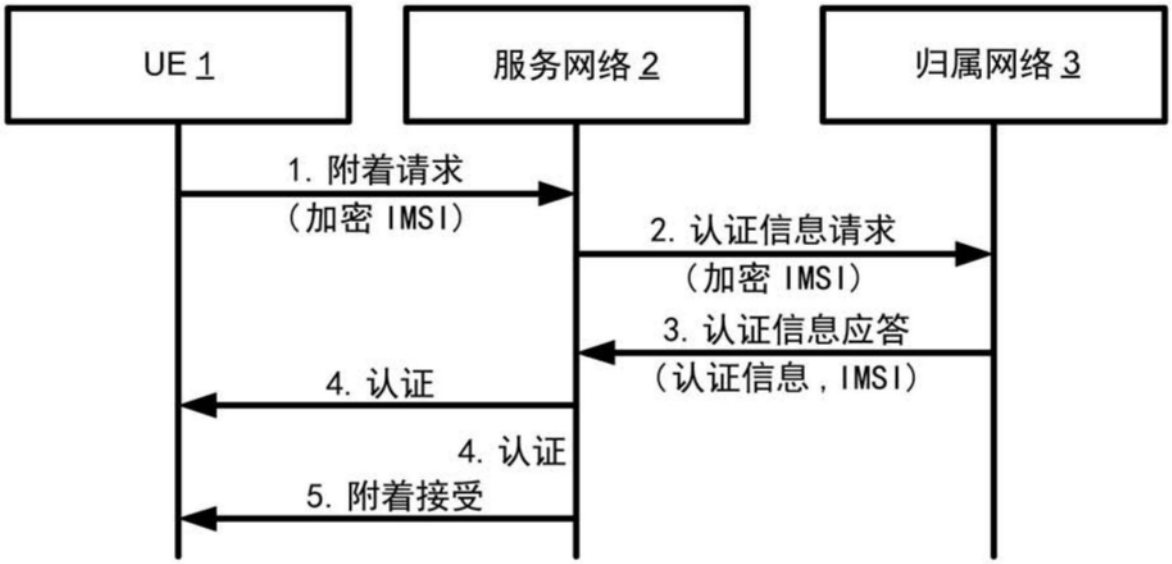

UE 1
服务网络 2
归属网络 3
1. 附着请求
（加密 IMSI）
2. 认证信息请求
（加密 IMSI）
3. 认证信息应答
（认证信息，IMSI）
4. 认证
4. 认证
5. 附着接受

图2

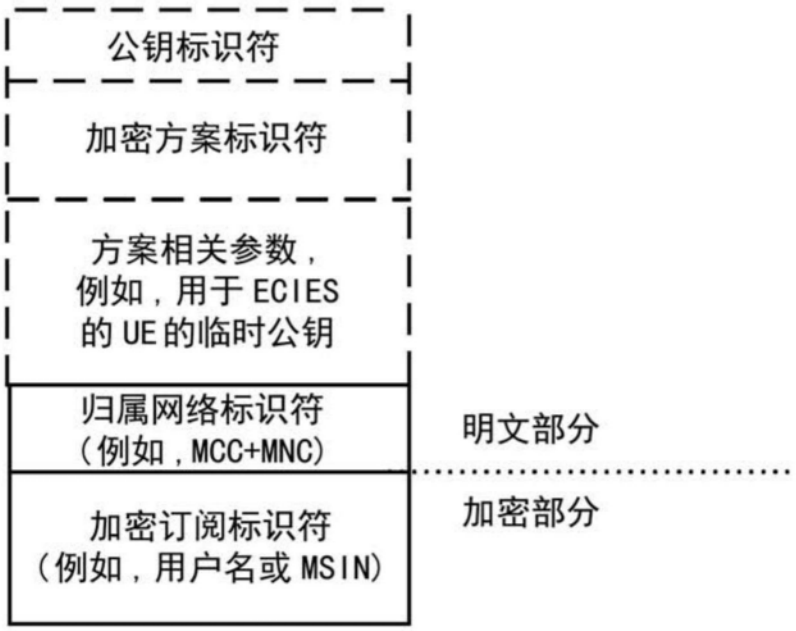

公钥标识符
加密方案标识符
方案相关参数，
例如，用于 ECIES
的 UE 的临时公钥
归属网络标识符
（例如，MCC+MNC）
加密订阅标识符
（例如，用户名或 MSIN）
明文部分
加密部分

图3

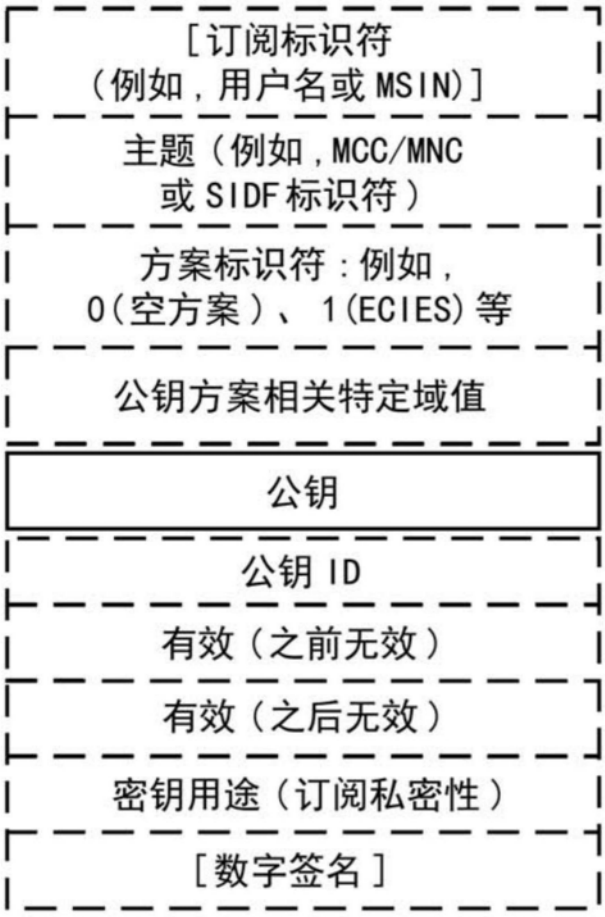

[订阅标识符
(例如，用户名或MSIN)]
主题（例如，MCC/MNC
或SIDF标识符）
方案标识符：例如，
0(空方案)、1(ECIES)等
公钥方案相关特定域值
公钥
公钥ID
有效（之前无效）
有效（之后无效）
密钥用途（订阅私密性）
[数字签名]

图4


方案标识符：例如，
0(空方案)、
1(ECIES)等
方案特定算法：
例如，KA、KDF、
对称完整性算法、
对称加密算法
公钥方案相关
参数及其静态值

图5

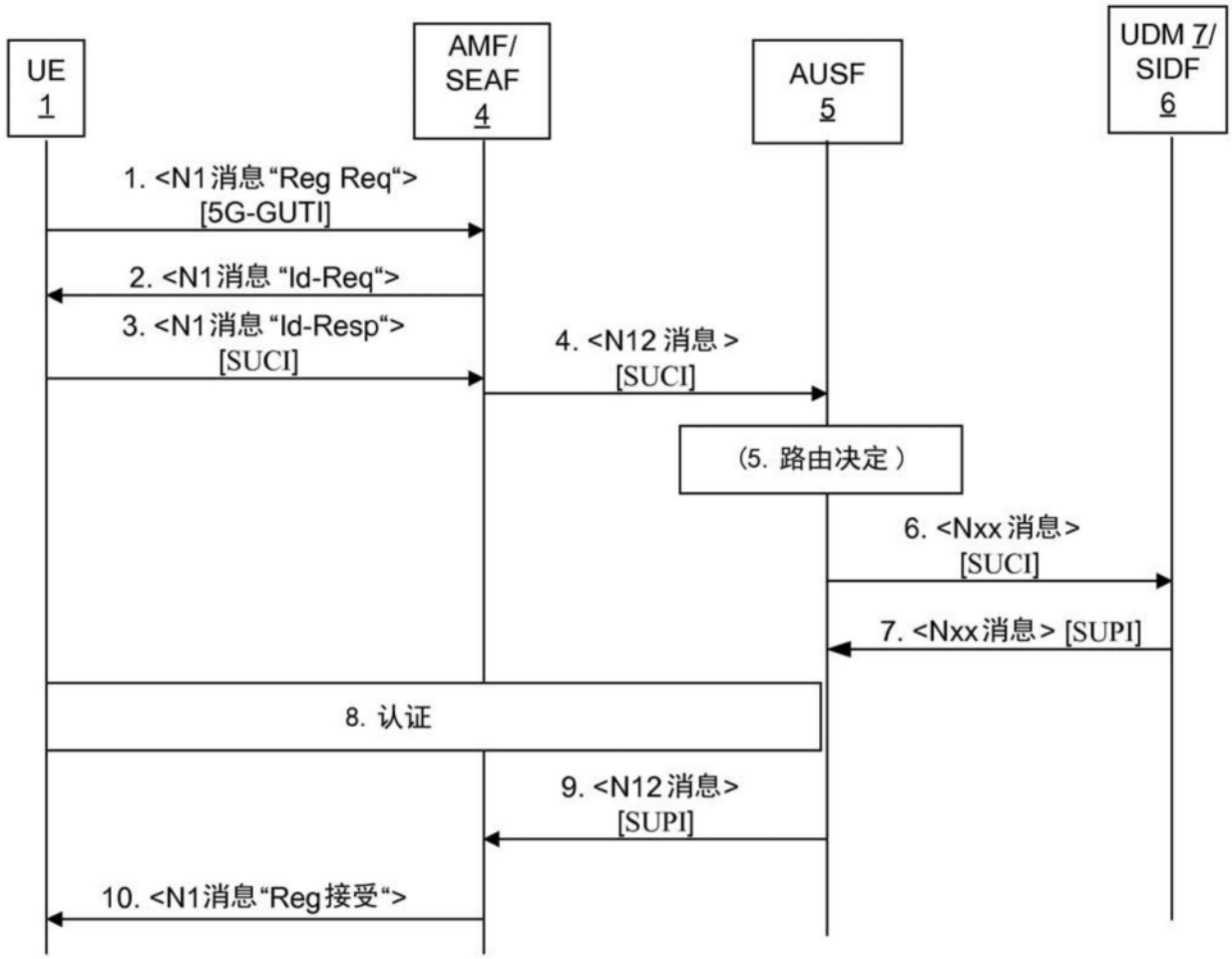

UE
1
AMF/
SEAF
4
AUSF
5
UDM 7/
SIDF
6
1. <N1消息“Reg Req“>
[5G-GUTI]
2. <N1消息 “Id-Req“>
3. <N1消息 “Id-Resp“>
[SUCI]
4. <N12 消息 >
[SUCI]
(5. 路由决定)
6. <Nxx 消息 >
[SUCI]
7. <Nxx消息> [SUPI]
8. 认证
9. <N12消息>
[SUPI]
10. <N1消息“Reg接受“>

图6

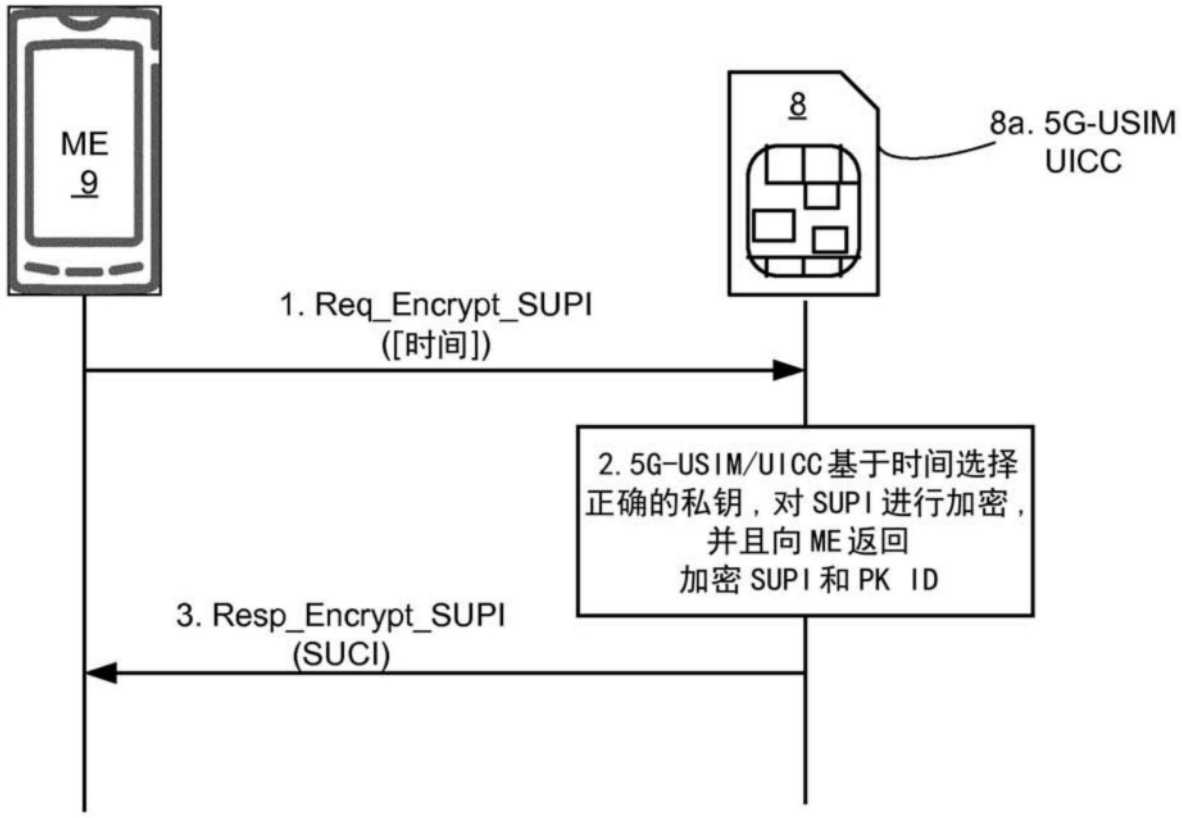

ME
9
8
8a. 5G-USIM
UICC
1. Req_Encrypt_SUPI
([时间])
2. 5G-USIM/UICC基于时间选择
正确的私钥，对SUPI进行加密，
并且向ME返回
加密SUPI和PK ID
3. Resp_Encrypt_SUPI
(SUCI)

图7

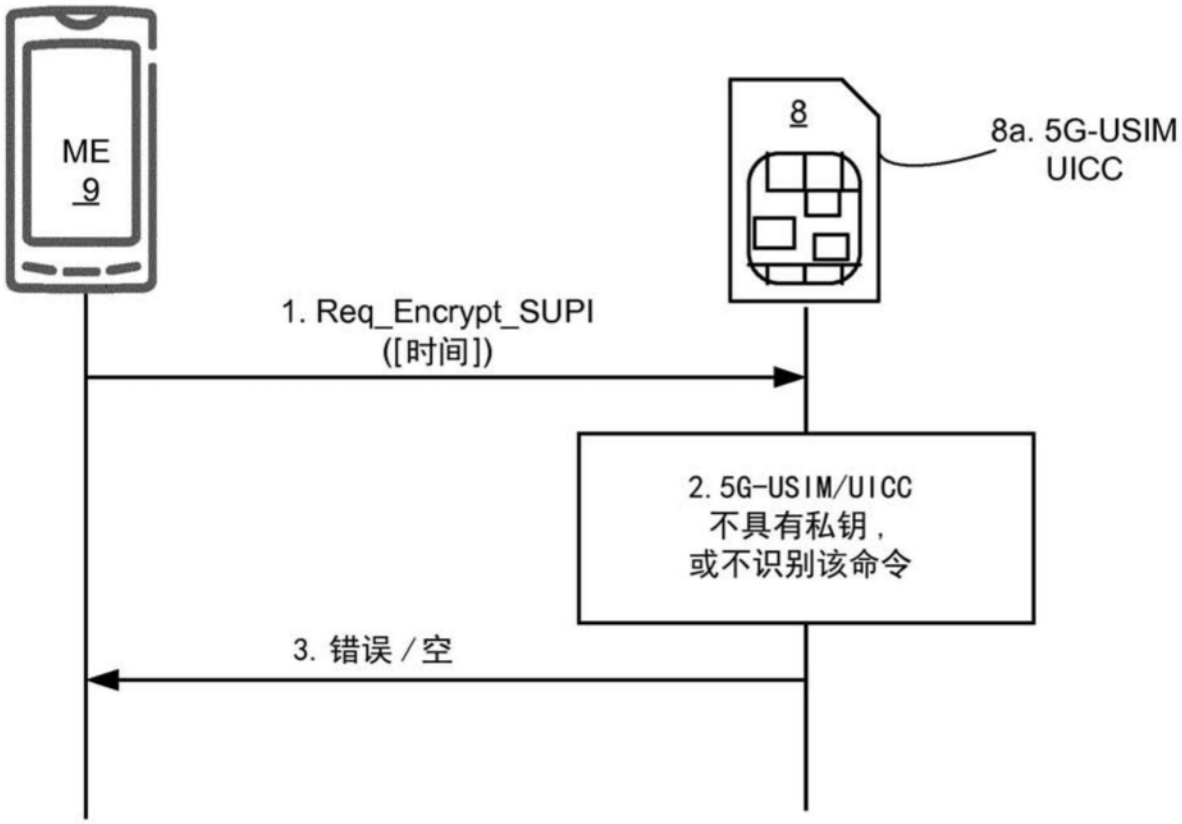

ME
9
8
8a. 5G-USIM
UICC
1. Req_Encrypt_SUPI
([时间])
2. 5G-USIM/UICC
不具有私钥，
或不识别该命令
3. 错误/空

图8

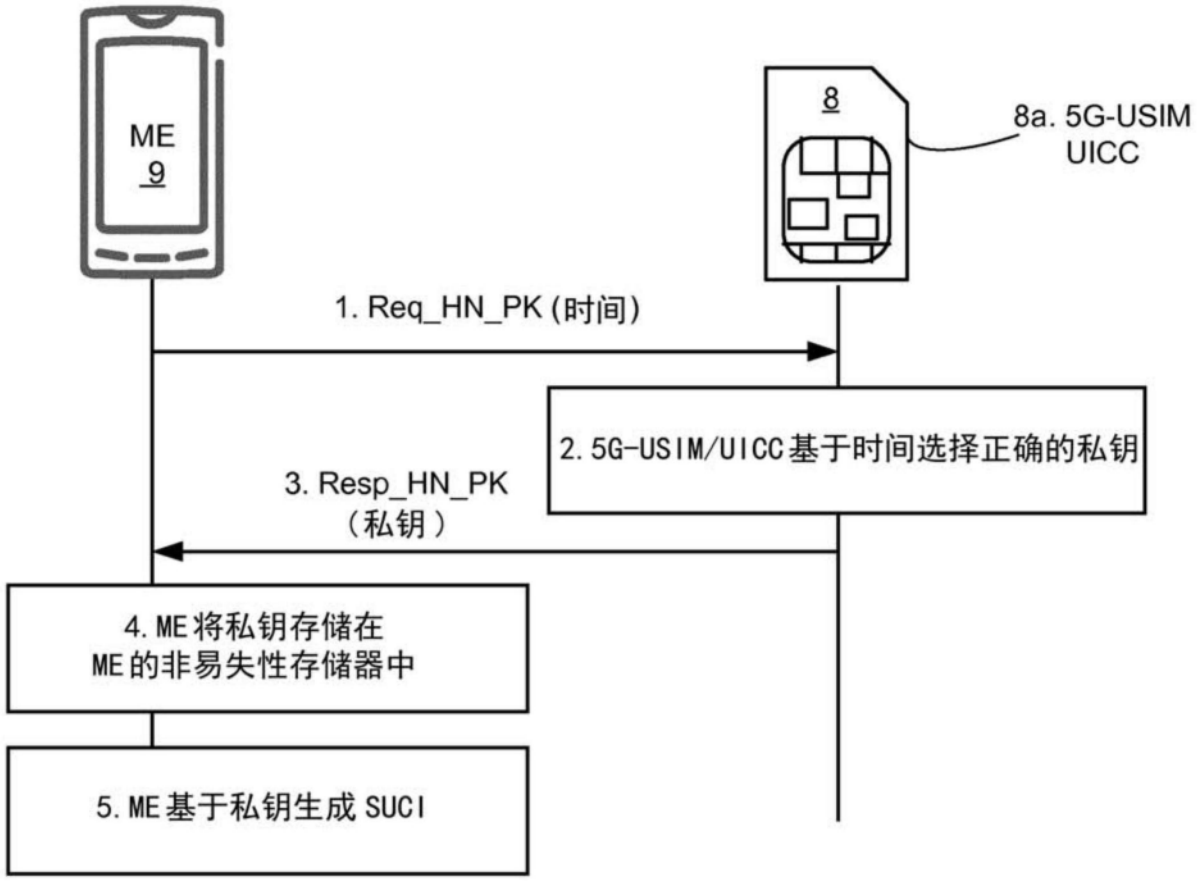

ME
9
8
8a. 5G-USIM
UICC
1. Req_HN_PK (时间)
2. 5G-USIM/UICC基于时间选择正确的私钥
3. Resp_HN_PK
（私钥）
4. ME将私钥存储在
ME的非易失性存储器中
5. ME基于私钥生成 SUCI

图9

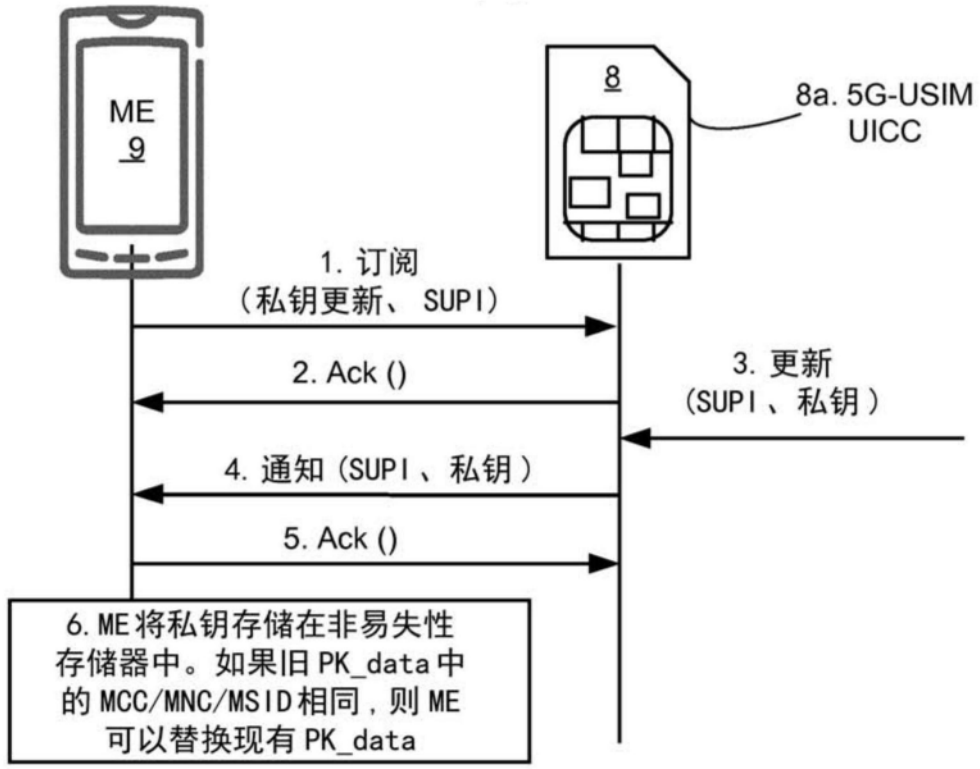

ME
9
8
8a. 5G-USIM
UICC
1. 订阅
（私钥更新、 SUPI）
2. Ack ()
3. 更新
（SUPI 、私钥）
4. 通知（SUPI 、私钥）
5. Ack ()
6. ME将私钥存储在非易失性
存储器中。如果旧PK_data中
的MCC/MNC/MSID相同，则ME
可以替换现有PK_data

图10

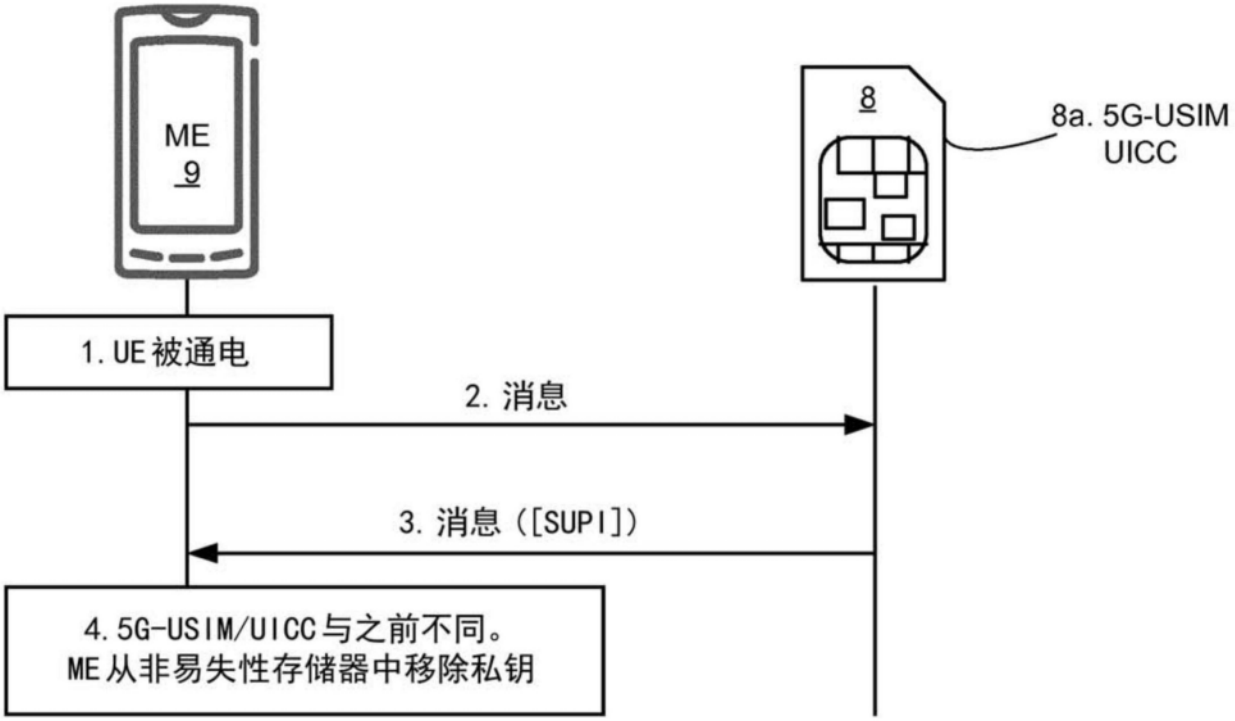

ME
9
8
8a. 5G-USIM
UICC
1. UE被通电
2. 消息
3. 消息（[SUPI]）
4. 5G-USIM/UICC与之前不同。
ME从非易失性存储器中移除私钥

图11


[预配置密钥 ID
(例如，RAND)]
[完整性算法]
[计数器]
消息认证代码

图12

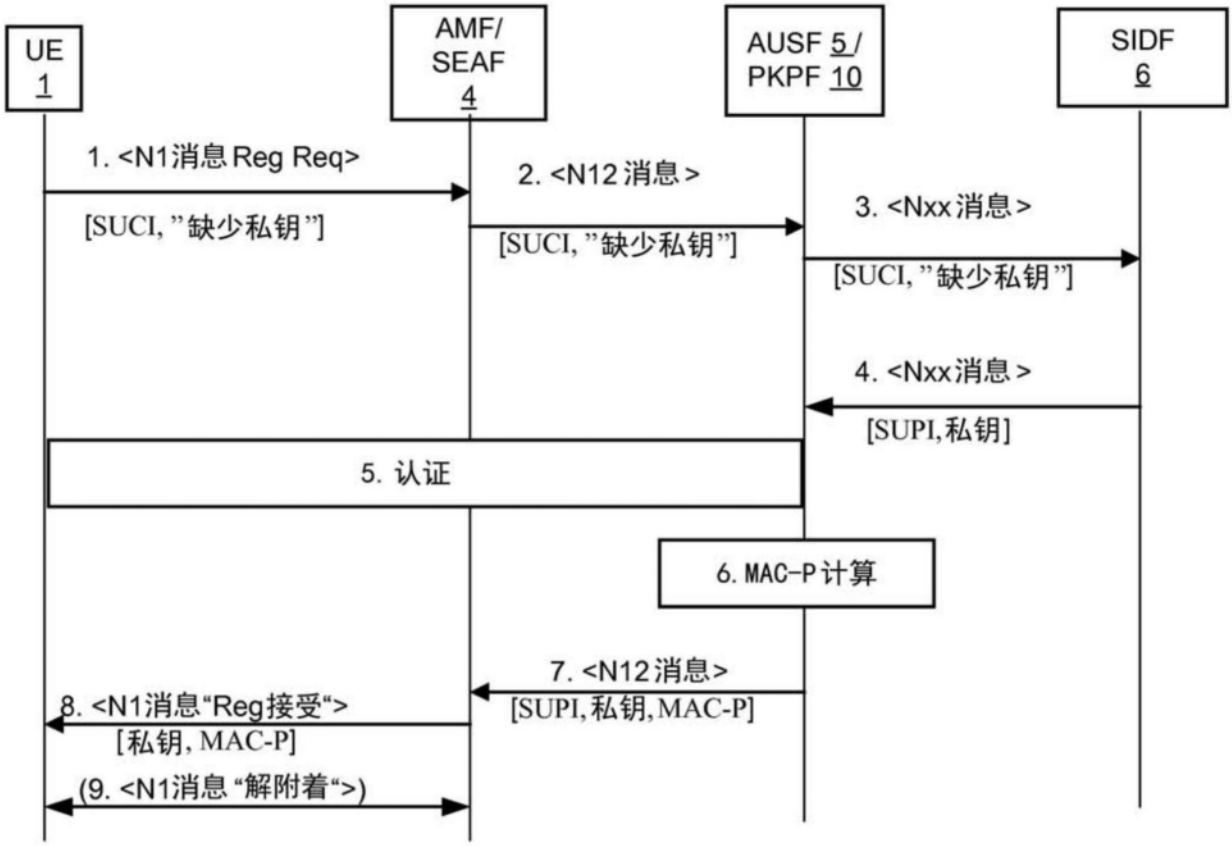

UE
1
AMF/
SEAF
4
AUSF 5 /
PKPF 10
SIDF
6
1. <N1消息 Reg Req>
[SUCI, "缺少私钥"]
2. <N12 消息>
[SUCI, "缺少私钥"]
3. <Nxx 消息>
[SUCI, "缺少私钥"]
4. <Nxx消息>
[SUPI,私钥]
5. 认证
6. MAC-P 计算
7. <N12 消息>
[SUPI,私钥,MAC-P]
8. <N1消息"Reg接受">
[私钥, MAC-P]
(9. <N1消息 "解附着">)

图13

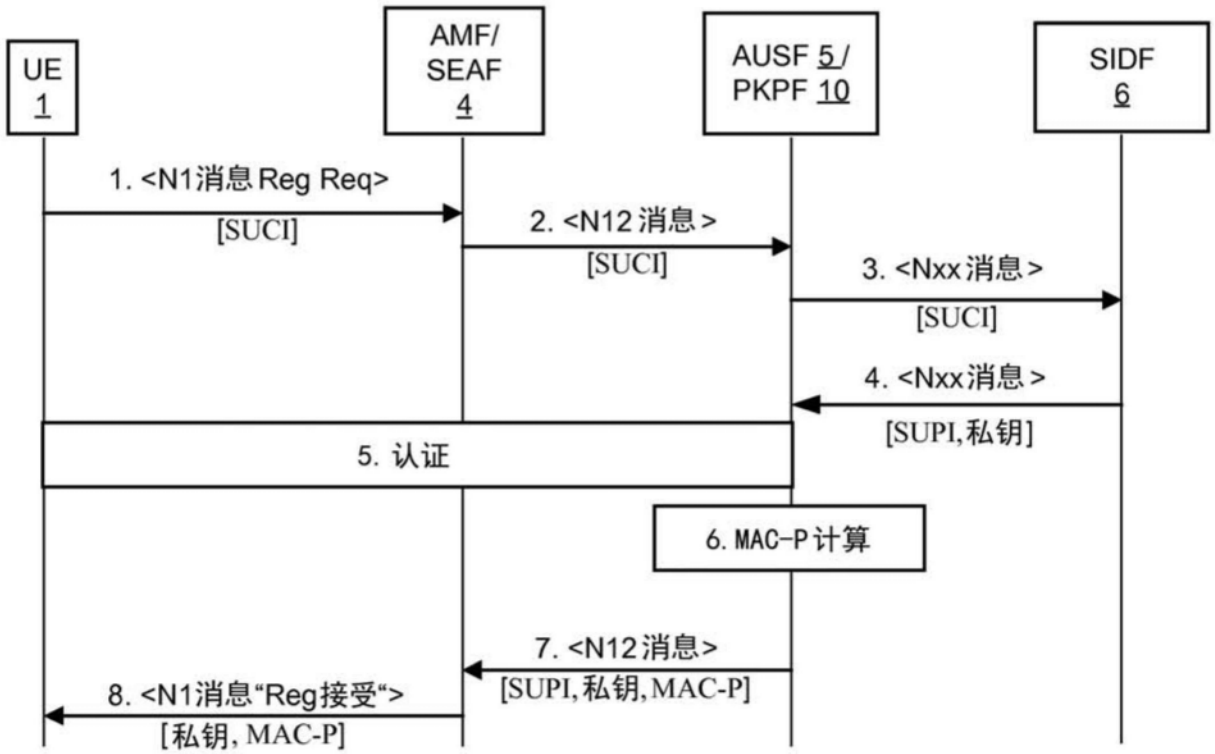

UE
1
AMF/
SEAF
4
AUSF 5/
PKPF 10
SIDF
6
1. <N1消息 Reg Req>
[SUCI]
2. <N12 消息>
[SUCI]
3. <Nxx消息>
[SUCI]
4. <Nxx消息>
[SUPI,私钥]
5. 认证
6. MAC-P计算
7. <N12消息>
[SUPI,私钥,MAC-P]
8. <N1消息“Reg接受“>
[私钥, MAC-P]

图14

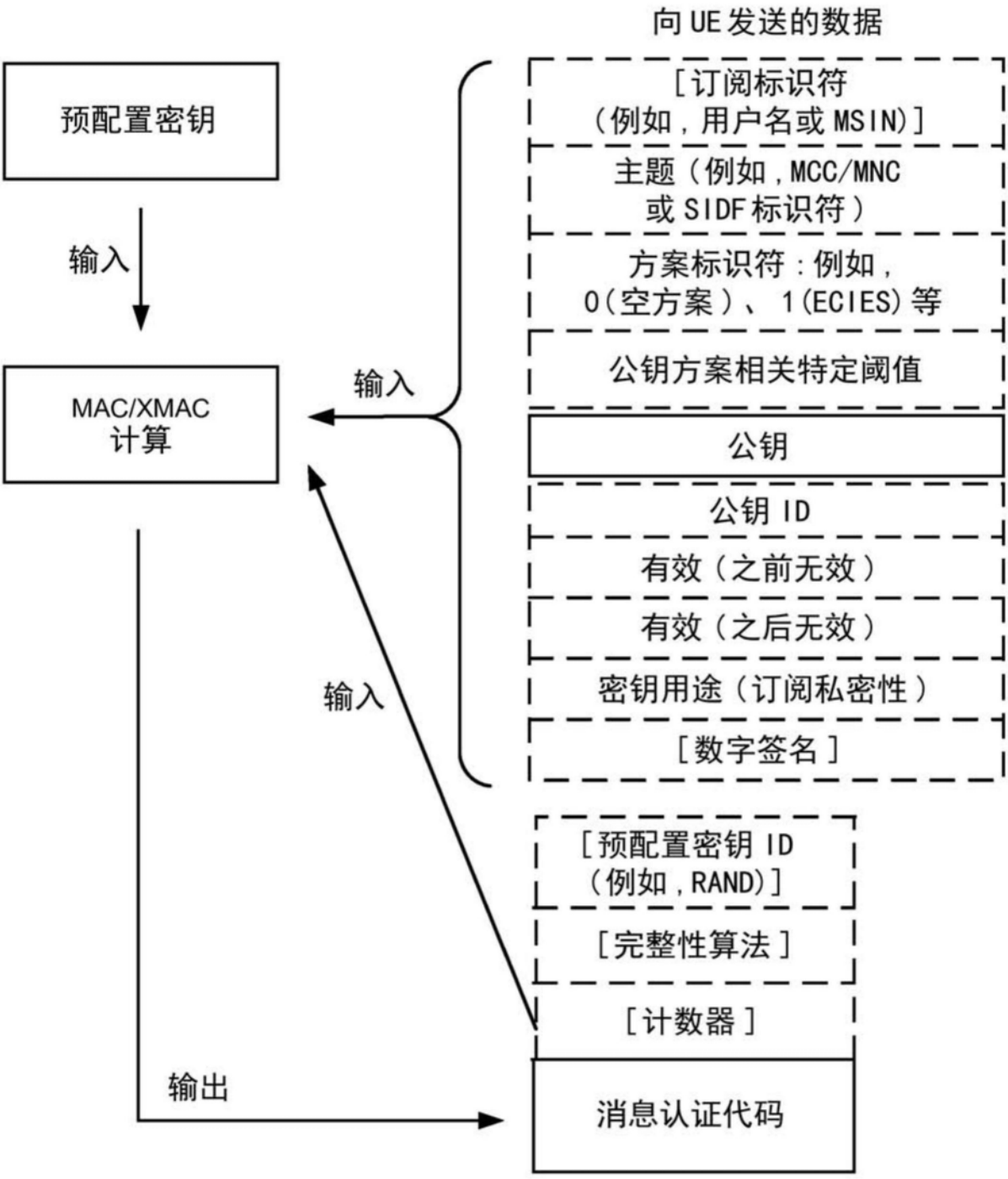

向UE发送的数据
预配置密钥
输入
MAC/XMAC
计算
输入
输入
输出
[订阅标识符
(例如，用户名或MSIN)]
主题（例如，MCC/MNC
或SIDF标识符）
方案标识符：例如，
0(空方案）、1(ECIES)等
公钥方案相关特定阈值
公钥
公钥ID
有效（之前无效）
有效（之后无效）
密钥用途（订阅私密性）
[数字签名]
[预配置密钥ID
(例如，RAND)]
[完整性算法]
[计数器]
消息认证代码

图15

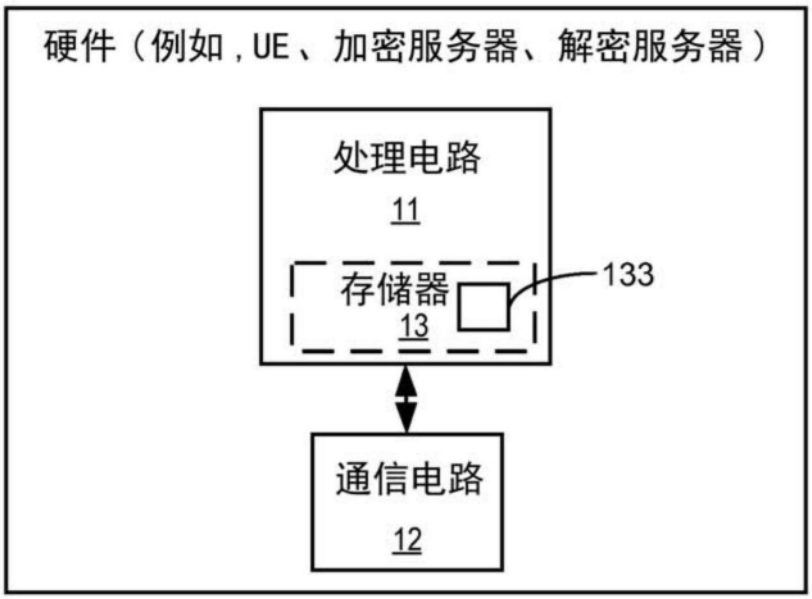

硬件（例如，UE、加密服务器、解密服务器）
处理电路
11
存储器
13
133
通信电路
12

图16

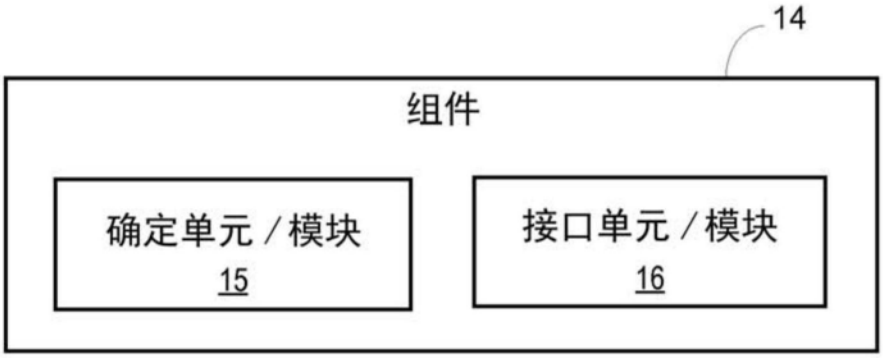

14
组件
确定单元／模块
15
接口单元／模块
16

图17

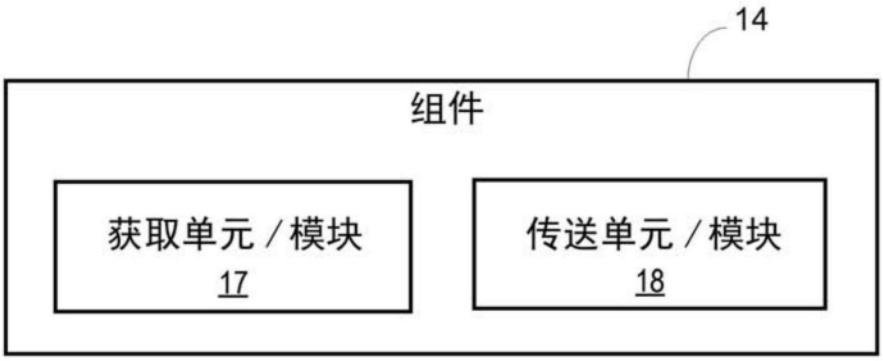

14
组件
获取单元／模块
17
传送单元／模块
18

图18

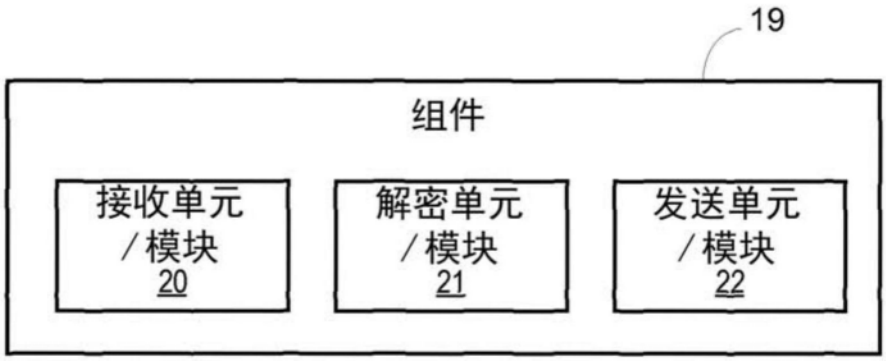

19
组件
接收单元/模块
20
解密单元/模块
21
发送单元/模块
22

图19

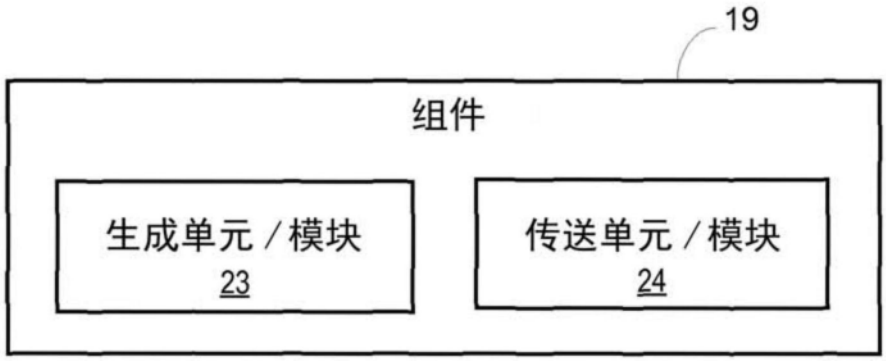

19
组件
生成单元/模块
23
传送单元/模块
24

图20

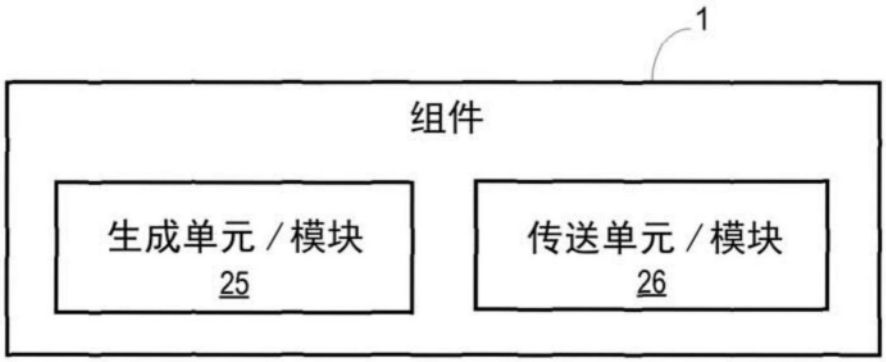

1
组件
生成单元/模块
25
传送单元/模块
26

图21

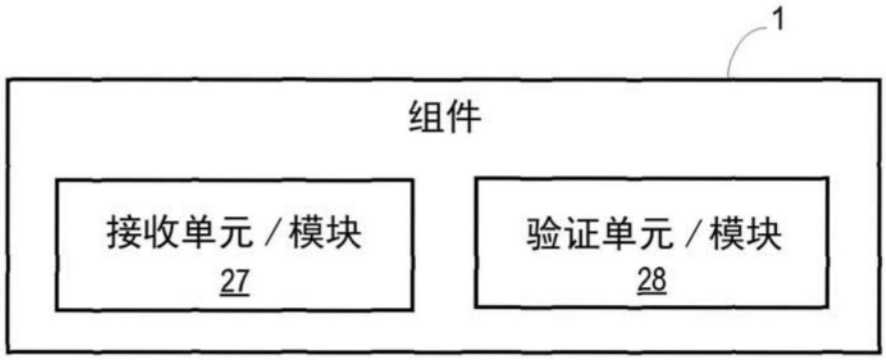


图22