(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102934470 B
(45)授权公告日 2016.06.29

(21)申请号 201180027820.4

(22)申请日 2011.06.16

(30)优先权数据
61/355,423 2010.06.16 US
13/161,336 2011.06.15 US

(85)PCT国际申请进入国家阶段日
2012.12.05

(86)PCT国际申请的申请数据
PCT/US2011/040777 2011.06.16

(87)PCT国际申请的公布数据
WO2011/159952 EN 2011.12.22

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 A·E·艾斯科特 A·帕拉尼格朗德

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 亓云

(51)Int.Cl.
H04W 12/04(2006.01)
H04L 29/06(2006.01)

(56)对比文件
WO 2007/121190 A2,2007.10.25,
CN 101208901 A,2008.06.25,
US 2006/0107036 A1,2006.05.18,
US 2007/0016780 A1,2007.01.18,

审查员 乔莹

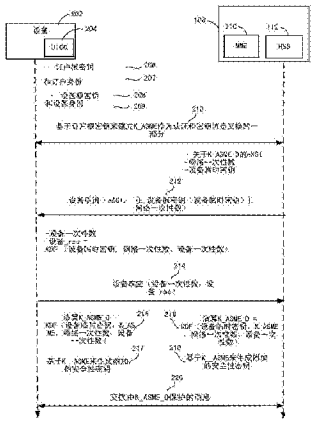
权利要求书4页 说明书15页 附图13页

(54)发明名称

用于在通信系统中将订户认证与设备认证绑定的方法和装置

(57)摘要

提供了设备(例如,客户端设备或接入终端)与网络实体之间的认证方法。可移除存储设备可耦合至该设备并存储可被用于订户认证的因订户而异的密钥。安全存储设备可耦合至该设备并存储用于设备认证的因设备而异的密钥。可以在该设备与网络实体之间执行订户认证。还可以与该网络实体执行对该设备的设备认证。随后,可生成将订户认证与设备认证绑定的安全性密钥。该安全性密钥可被用来保护该设备与服务网络之间的通信。



CN 102934470 B

1.一种在设备中操作的、用于将订户认证与设备认证绑定的方法，包括：

基于订户认证密钥来与网络实体来执行订户认证；

与所述网络实体来执行对所述设备的设备认证并且获得设备认证数据；

基于所述订户认证密钥和所述设备认证数据来生成将所述订户认证与所述设备认证绑定的安全性密钥；以及

使用所述安全性密钥来保护所述设备与服务网络之间的通信。

2.如权利要求1所述的方法，其特征在于，订户认证基于所述设备与所述网络实体之间的认证密钥协定交换。

3.如权利要求1所述的方法，其特征在于，设备认证基于所述设备与所述网络实体之间的质询-响应交换。

4.如权利要求1所述的方法，其特征在于，订户认证由作为所述网络实体的一部分的第一认证服务器执行，并且设备认证由作为所述网络实体的一部分的第二认证服务器执行。

5.如权利要求1所述的方法，其特征在于，所述设备认证通过以下步骤来执行：

从所述网络实体接收用所述设备的公钥加密的数据；

使用对应的私钥来解密经加密的数据；以及

随后向所述网络实体证明所述设备具备所述数据的知识。

6.如权利要求1所述的方法，其特征在于，进一步包括：

从所述设备向所述网络实体发送附连请求，所述附连请求包括对所述设备能够进行设备认证的指示。

7.如权利要求1所述的方法，其特征在于，设备认证是由在所述订户认证期间生成的至少一个密钥来保护的。

8.如权利要求1所述的方法，其特征在于，订户认证和设备认证是在其中组合订户认证和设备认证的消息交换中并发执行的。

9.如权利要求1所述的方法，其特征在于，订户认证是在比所述设备认证早且与之分开的安全性交换中执行的。

10.如权利要求1所述的方法，其特征在于，所述安全性密钥是至少作为从订户认证获得的第一密钥和从设备认证获得的第二密钥的函数来生成的。

11.如权利要求10所述的方法，其特征在于，所述安全性密钥还是网络一次性数和设备一次性数的函数。

12.如权利要求1所述的方法，其特征在于，所述设备是对于所述网络实体而言表现为接入终端并且对于一个或多个接入终端而言表现为网络设备的中继节点。

13.如权利要求1所述的方法，其特征在于，所述安全性密钥是由所述设备和所述网络实体分别生成的。

14.如权利要求1所述的方法，其特征在于，进一步包括：

作为服务协定的一部分提供因订户而异的密钥，其中所述因订户而异的密钥被用于所述订户认证；以及

在制造期间在所述设备中提供因设备而异的密钥，其中所述因设备而异的密钥被用于所述设备认证。

15.一种用于将订户认证与设备认证绑定的设备，包括：

通信接口;以及

耦合至所述通信接口的处理电路,所述处理电路被适配成:

基于订户认证密钥来与网络实体来执行订户认证;

与所述网络实体来执行对所述设备的设备认证并且获得设备认证数据;

基于所述订户认证密钥和所述设备认证数据来生成将所述订户认证与所述设备认证绑定的安全性密钥;以及

使用所述安全性密钥来保护所述设备与服务网络之间的通信。

16.如权利要求15所述的设备,其特征在于,订户认证基于所述设备与所述网络实体之间的认证密钥协定交换。

17.如权利要求15所述的设备,其特征在于,设备认证基于所述设备与所述网络实体之间的质询-响应交换。

18.如权利要求15所述的设备,其特征在于,设备认证通过以下方式执行:

从所述网络实体接收用所述设备的公钥加密的数据;

使用对应的私钥来解密经加密的数据;以及

随后向所述网络实体证明所述设备具备所述数据的知识。

19.如权利要求15所述的设备,其特征在于,进一步包括:

使用所述通信接口从所述设备向所述网络实体发送附连请求,所述附连请求包括对所述设备能够进行设备认证的指示。

20.如权利要求15所述的设备,其特征在于,所述设备认证是由在所述订户认证期间生成的至少一个密钥来保护的。

21.如权利要求15所述的设备,其特征在于,订户认证和设备认证是在其中组合订户认证和设备认证的消息交换中并发执行的。

22.如权利要求15所述的设备,其特征在于,订户认证是在比所述设备认证早且与之分开的安全性交换中执行的。

23.如权利要求15所述的设备,其特征在于,所述安全性密钥是至少作为从订户认证获得的第一密钥和从设备认证获得的第二密钥的函数来生成的。

24.如权利要求15所述的设备,其特征在于,所述设备是对于所述网络实体而言表现为接入终端并且对于一个或多个接入终端而言表现为网络设备的中继节点。

25.如权利要求15所述的设备,其特征在于,进一步包括:

可移除存储设备,其耦合至所述处理电路并存储用于所述订户认证的因订户而异的密钥;以及

安全存储设备,其耦合至所述处理电路并存储用于所述设备认证的因设备而异的密钥。

26.一种用于将订户认证与设备认证绑定的设备,包括:

用于基于订户认证密钥来与网络实体来执行订户认证的装置;

用于与所述网络实体来执行对所述设备的设备认证并且获得设备认证数据的装置;

用于基于所述订户认证密钥和所述设备认证数据来生成将所述订户认证与所述设备认证绑定的安全性密钥的装置;以及

用于使用所述安全性密钥来保护所述设备与服务网络之间的通信的装置。

27.如权利要求26所述的设备，其特征在于，进一步包括：

用于存储用于所述订户认证的因订户而异的密钥的装置；以及

用于存储用于所述设备认证的因设备而异的密钥的装置。

28.一种在网络实体中操作的、用于将订户认证与设备认证绑定的方法，包括：

基于订户认证密钥来与设备来执行订户认证；

执行对所述设备的设备认证并且获得设备认证数据；

基于所述订户认证密钥和所述设备认证数据来生成将所述订户认证与所述设备认证绑定的安全性密钥；以及

使用所述安全性密钥来保护所述网络实体与所述设备之间的通信。

29.如权利要求28所述的方法，其特征在于，订户认证基于所述网络实体与所述设备之间的认证密钥协定交换。

30.如权利要求28所述的方法，其特征在于，设备认证基于所述网络实体与所述设备之间的质询-响应交换。

31.如权利要求28所述的方法，其特征在于，所述设备认证包括：

从所述设备接收证书；

验证与所述设备相关联的所述证书未曾被撤销。

32.如权利要求28所述的方法，其特征在于，进一步包括：

从所述设备接收附连请求，所述附连请求包括对所述设备能够进行设备认证的指示。

33.如权利要求28所述的方法，其特征在于，设备认证是由在所述订户认证期间生成的至少一个密钥来保护的。

34.如权利要求28所述的方法，其特征在于，订户认证和设备认证是在其中组合订户认证和设备认证的消息交换中并发执行的。

35.如权利要求28所述的方法，其特征在于，订户认证是在比所述设备认证早且与之分开的安全性交换中执行的。

36.如权利要求28所述的方法，其特征在于，所述安全性密钥是至少作为从订户认证获得的第一密钥和从设备认证获得的第二密钥的函数来生成的。

37.如权利要求28所述的方法，其特征在于，所述安全性密钥是由所述设备和所述网络实体分别生成的。

38.如权利要求28所述的方法，其特征在于，进一步包括：

作为服务协定的一部分获得因订户而异的密钥，其中所述因订户而异的密钥被用于所述订户认证；以及

获得所述设备的因设备而异的密钥，所述因设备而异的密钥被用于所述设备认证。

39.一种用于将订户认证与设备认证绑定的网络实体，包括：

通信接口；以及

耦合至所述通信接口的处理电路，所述处理电路被适配成：

基于订户认证密钥来与设备来执行订户认证；

执行对所述设备的设备认证并且获得设备认证数据；

基于所述订户认证密钥和所述设备认证数据来生成将所述订户认证与所述设备认证绑定的安全性密钥；以及

使用所述安全性密钥来保护所述网络实体与所述设备之间的通信。

40.如权利要求39所述的网络实体，其特征在于，订户认证基于所述网络实体与所述设备之间的认证密钥协定交换。

41.如权利要求39所述的网络实体，其特征在于，设备认证基于所述网络实体与所述设备之间的质询-响应交换。

42.如权利要求39所述的网络实体，其特征在于，所述处理电路还被配置成：

从所述设备接收附连请求，所述附连请求包括对所述设备能够进行设备认证的指示。

43.如权利要求39所述的网络实体，其特征在于，设备认证是由在所述订户认证期间生成的至少一个密钥来保护的。

44.如权利要求39所述的网络实体，其特征在于，订户认证和设备认证是在其中组合订户认证和设备认证的消息交换中并发执行的。

45.如权利要求39所述的网络实体，其特征在于，订户认证是在比所述设备认证早且与之分开的安全性交换中执行的。

46.如权利要求39所述的网络实体，其特征在于，所述安全性密钥是至少作为从订户认证获得的第一密钥和从设备认证获得的第二密钥的函数来生成的。

47.如权利要求39所述的网络实体，其特征在于，进一步包括：

作为服务协定的一部分获得因订户而异的密钥，其中所述因订户而异的密钥被用于所述订户认证；以及

获得所述设备的因设备而异的密钥，所述因设备而异的密钥被用于所述设备认证。

48.一种用于将订户认证与设备认证绑定的网络实体，包括：

用于基于订户认证密钥来与设备来执行订户认证的装置；

用于执行对所述设备的设备认证并且获得设备认证数据的装置；

用于基于所述订户认证密钥和所述设备认证数据来生成将所述订户认证与所述设备认证绑定的安全性密钥的装置；以及

用于使用所述安全性密钥来保护所述网络实体与所述设备之间的通信的装置。

用于在通信系统中将订户认证与设备认证绑定的方法和装置

[0001] 根据35U.S.C.§119的优先权要求

[0002] 本专利申请要求于2010年6月16日提交且被转让给本申请受让人并由此通过援引明确纳入于此的题为“Apparatus and Method for Device Authentication in 3GPP Systems(用于3GPP系统中的设备认证的方法和装置)的美国临时申请No.61/355,423的优先权。

[0003] 背景

[0004] 领域

[0005] 各种特征涉及通信系统,尤其涉及对有线和/或无线通信系统中采用的诸如中继节点和机对机设备之类的设备的认证。

[0006] 背景

[0007] 现代无线网络可包括中继节点和/或接入终端,它们在本文中被统称为设备。为了使此类设备正确地运行,在使该设备进入操作之前,该设备往往被提供/配置有操作和订户安全性凭证。此类订户安全性凭证可例如被用来在提供无线服务或接入之前认证该设备,并且在一些情形中可被存储在不可移除地耦合至其主机设备的模块中。存在着订户安全性凭证可从经认证设备移除并置于未授权设备中的风险。在中继节点的情形中,这可能允许未授权的中继节点暗中访问例如接入节点与一个或多个接入终端之间的传输和/或获得对网络服务的自由访问。在机对机(M2M)设备的情形中也存在此风险或弱点,因为M2M设备中的有效订户凭证(例如,可移除的通用集成电路卡(UICC)中的认证和密钥协定(AKA)参数)可被转移至另一设备以得到自由的网络访问。存在相关的弱点是因为不必对M2M设备本身进行物理访问。对正越过M2M设备接口(例如,主机设备至UICC接口)的数据(例如,从认证得到的安全性密钥)的访问足以获得对安全性密钥的访问并曝露由所述密钥保护的数据。

[0008] 在运营商希望控制哪些设备被允许接入其网络的情况下也存在类似的问题。

[0009] 因此,需要为设备提供附加的安全性以解决这些以及其他弱点和风险。

[0010] 概述

[0011] 提供了用于通过将订户认证与设备认证绑定以生成安全性密钥的方式来保护设备的方法和装置。

[0012] 根据第一方面,提供一种在设备中操作的用于将订户与设备认证绑定的方法。该设备一开始可向网络实体发送附连请求,该附连请求包括对该设备的设备认证能力的指示。订户认证可由该设备与网络实体执行。例如,订户认证可基于该设备与该网络实体之间的认证密钥协定交换。该设备还可与该网络实体执行设备认证。例如,设备认证可基于该设备与该网络实体之间的质询-响应交换。

[0013] 随后,可以生成将订户认证与设备认证绑定的安全性密钥。该安全性密钥可至少作为从订户认证获得的第一密钥和从设备认证获得的第二密钥的函数来生成。附加地,该安全性密钥还可以是网络一次性数和设备一次性数的函数。随后,可以使用该安全性密钥来保护该设备与服务网络之间的通信。注意,该安全性密钥可以由该设备和该网络实体分别生成,所以该安全性密钥不越空传送。

[0014] 根据一个实现，订户认证可以由作为网络实体的一部分的第一认证服务器执行，而设备认证可以由作为网络实体的一部分的第二认证服务器执行。

[0015] 在一个示例中，可以通过使用共享的机密密钥来加密/解密该设备与网络实体之间的某些交换的方式来执行设备认证。在另一个示例中，可通过如下方式来执行设备认证：(a)从网络实体接收用该设备的公钥加密的数据；(b)使用对应的私钥来解密该经加密数据；和/或(c)随后向该网络实体证明该设备具备该数据的知识。

[0016] 根据一个方面，可以由在订户认证期间生成的至少一个密钥来保护设备认证。

[0017] 在各种实现中，可以在组合的消息交换中并发地执行订户认证和设备认证，或者可以在比设备认证早且与之分开的安全性交换中执行订户认证。

[0018] 根据一个特征，可以在该设备上作为服务协定的一部分提供因订户而异的密钥，其中该因订户而异的密钥被用于订户认证。类似地，可以在制造期间在该设备中提供因设备而异的密钥，其中该因设备而异的密钥被用于设备认证。

[0019] 在一个实现中，设备可以是对于网络实体而言表现为接入终端而对于一个或多个接入终端而言表现为网络设备的中继节点。在另一个实现中，该设备可以是接入终端。

[0020] 根据一个示例，该设备可包括耦合至处理电路的通信接口。该处理电路可被适配成：(a)与网络实体执行订户认证；(b)与该网络实体执行对该设备的设备认证；(c)生成将订户认证与设备认证绑定的安全性密钥；和/或(d)使用该安全性密钥来保护该设备与服务网络之间的通信。

[0021] 根据又一示例，可以提供包括在设备上操作的指令的处理器可读介质。当由处理器执行时，这些指令可使该处理器：(a)与网络实体执行订户认证；(b)与该网络实体执行对该设备的设备认证；(c)生成将订户认证与设备认证绑定的安全性密钥；和/或(d)使用该安全性密钥来保护该设备与服务网络之间的通信。

[0022] 根据另一方面，提供在网络实体中操作的方法。该网络实体可从设备接收附连请求，该附连请求包括对该设备的设备认证能力的指示。该网络实体可与设备执行订户认证。类似地，该网络实体可执行对该设备的设备认证。随后，可由该网络实体生成将订户认证与设备认证绑定的安全性密钥。随后，可以使用该安全性密钥来保护该网络实体与该设备之间的通信。注意，为了防止该安全性密钥的越空传输，该安全性密钥可由该设备和该网络实体分别生成。

[0023] 在一个示例中，订户认证可基于网络实体与设备之间的认证密钥协定交换。设备认证可基于网络实体与设备之间的质询-响应交换。

[0024] 在一个实现中，设备认证可包括：(a)从设备接收证书；以及(b)验证与该设备相关联的该证书尚未被撤销。

[0025] 在一个实现中，为了防止设备认证过程期间的窥探，可以由在较早的订户认证期间生成的至少一个密钥来保护设备认证。

[0026] 根据各种示例，可以在组合的消息交换中并发地执行订户认证和设备认证，或者可以在比设备认证早且与之分开的安全性交换中执行认证。

[0027] 在另一示例中，安全性密钥可至少作为从订户认证获得的第一密钥和从设备认证获得的第二密钥的函数来生成。

[0028] 在一个实现中，网络实体可作为服务协定的一部分获得因订户而异的密钥，该因

订户而异的密钥被用于订户认证。类似地，网络实体可获得该设备的因设备而异的密钥，该因设备而异的密钥被用于设备认证。

[0029] 在一个实现中，网络实体可包括耦合至处理电路的通信接口。该处理电路可被适配成：(a)与设备执行订户认证；(b)执行对该设备的设备认证；(c)生成将订户认证与设备认证绑定的安全性密钥；和/或(d)使用该安全性密钥来保护该网络实体与该设备之间的通信。

[0030] 在一个实现中，提供一种包括在网络实体上操作的指令的处理器可读介质。当由处理器执行时，这些指令可使该处理器：(a)与设备执行订户认证；(b)执行对该设备的设备认证；(c)生成将订户认证与设备认证绑定的安全性密钥；和/或(d)使用该安全性密钥来保护该网络实体与该设备之间的通信。

[0031] 附图简述

[0032] 图1是解说在其中各种类型的无线设备可由核心网认证以获得服务的无线通信系统的框图。

[0033] 图2解说用于将设备认证与订户认证绑定的一般性办法。

[0034] 图3(包括图3A和图3B)解说如何可以修改基于订户认证的密钥阶级以添加设备认证的示例。

[0035] 图4解说可在分组交换网络内工作的设备中实现的示例性协议栈。

[0036] 图5是解说在其中可生成图3和图4中解说的各种认证和/或安全性密钥的网络系统的框图。

[0037] 图6是解说可被适配成将订户认证与设备认证绑定的无线设备的组件选集的框图。

[0038] 图7是解说在无线设备中操作以用于生成将订户认证与设备认证绑定的安全性密钥的方法的示例的流程图。

[0039] 图8是解说可被适配成将订户认证与设备认证绑定的网络实体的组件选集的框图。

[0040] 图9是解说在网络实体中操作以用于生成将订户认证与设备认证绑定的安全性密钥的方法的示例的流程图。

[0041] 图10解说用于通过将订户与设备认证绑定来生成安全性密钥的第一示例性方法。

[0042] 图11解说用于通过将订户与设备认证绑定来生成安全性密钥的第二示例性方法。

[0043] 图12解说用于通过将订户与设备认证绑定来生成安全性密钥的第三示例性方法。

[0044] 详细描述

[0045] 在以下描述中，给出了具体细节以提供对所描述的实现的透彻理解。然而，本领域普通技术人员将理解，没有这些具体细节也可实践各种实现。例如，电路可能以框图形式示出，以免使这些实现湮没在不必要的细节中。在其他实例中，公知的电路、结构和技术可能被详细示出以免湮没所描述的实现。

[0046] 措辞“示例性”在本文中用于表示“用作示例、实例或解说”。本文中描述为“示例性”的任何实现或实施例不必被解释为优于或胜过其他实施例或实现。同样，术语“实施例”并不要求所有实施例都包括所讨论的特征、优点、或工作模式。

[0047] 综述

[0048] 提供在设备(例如,客户端设备或接入终端)与网络实体之间的认证方法。可移除的存储设备可耦合至该设备并存储可被用于订户认证的因订户而异的密钥。安全的存储设备可耦合至该设备并存储被用于设备认证的因设备而异的密钥。订户认证可以在该设备与网络实体之间执行。还可以与该网络实体执行对该设备的设备认证。随后,可以生成将订户认证与设备认证绑定的安全性密钥。即,来自订户认证过程的密钥、数据、和/信息和来自设备认证过程的密钥、数据、和/或信息可被组合以生成(复合)安全性密钥。可以使用该安全性密钥来保护该设备与服务网络之间的通信。

[0049] 示例性网络环境

[0050] 图1是解说在其中各种类型的无线设备可由核心网认证以获得服务的无线通信系统的框图。此无线通信系统可以例如是通用移动电信系统(UMTS)顺应性网络或兼容网络、或全球移动通信系统(GSM)兼容网络、或全球移动通信系统(GSM)兼容网络。虽然本文中所描述的示例中的一些示例可能涉及长期演进(LTE)网络,但是本文中所描述的各种特征也可在其他网络中实现。

[0051] 该系统可包括与接入节点106通信的诸如接入终端103/104和中继节点102之类的一个或多个设备101。中继节点102可促成无线通信网络106/108与一个或多个接入终端104之间的无线传输。无线通信系统(例如,长期演进(LTE)网络,高级LTE网络等)可包括核心网108和一个或多个接入节点106。接入节点106可经由回程链路(例如,有线连接)耦合至核心网108。核心网108可以包括例如移动管理实体(MME)110、归属订户服务器(HSS)112、和/或其他组件。

[0052] 在一个示例中,移动管理实体(MME)110可参与对设备101、中继节点102和/或接入终端103/104(下文中普遍称为“设备”)的承载激活/停用并通过与归属订户服务器(HSS)112交互来辅助认证。MME 110还可生成临时身份和/或向设备(例如,设备101、中继节点102、接入终端103/104等)分配这些临时身份。MME 110可检查对设备宿营于服务供应商的公众陆地移动网络(PLMN)(例如,从该PLMN获得服务,连接至该PLMN,建立与该PLMN的通信链路)的授权并可强制实施对该设备的漫游约束。MME 110可以是网络中用于对非接入阶层(NAS)信令进行密码化/完好性保护并处置安全性密钥管理的终接点。MME 110还可对耦合至核心网108的设备执行跟踪和/或寻呼规程(包括重传)。

[0053] 归属订户服务器(HSS)112是支持实际处置设备的网络实体的主订户数据库。该HSS可包含与订阅有关的信息(订户概况),帮助执行对订阅的认证和授权,并可提供关于订户位置的信息。该HSS类似于GSM归属位置注册器(HLR)和认证中心(AuC)。归属位置注册器(HLR)可以是包含被授权使用核心网的每个订户的详情的数据库。HLR可辅助AuC认证订户(即,使用用户终端)。

[0054] 中继节点102可被适配成在接入终端104与接入节点106之间放大和/或转发信号。一般而言,中继节点102可以对于接入终端104而言表现为接入节点(AN)并可对于接入节点106而言表现为接入终端(AT)。例如,中继节点102可包括藉以与接入节点106通信的接入终端接口105,并还可包括藉以与接入终端104通信的接入节点接口107。即,接入终端接口105可使中继节点对于接入节点106而言表现为接入终端。类似地,接入节点接口107可使中继节点102对于接入终端104而言表现为接入节点。在一些实现中,中继节点102可将接入终端接口105与接入节点接口107之间的信号从第一格式转换成第二格式。中继节点102可置于

蜂窝小区的边缘附近，以使得接入终端104能与中继节点102通信而不是直接与接入节点106通信。

[0055] 在无线电系统中，蜂窝小区是接收和发射覆盖的地理区域。蜂窝小区可彼此交叠。在典型示例中，与每个蜂窝小区有一个相关联的接入节点。蜂窝小区的大小是由诸如频带、功率电平和信道状况之类的因素决定的。诸如中继节点102之类的中继节点可被用于增强蜂窝小区内或蜂窝小区附近的覆盖，或扩展蜂窝小区的覆盖大小。附加地，中继节点102的使用能够增强蜂窝小区内的信号的吞吐量，因为接入终端104能以比接入终端104在与该蜂窝小区的接入节点106直接通信时所可使用的数据率或者发射功率更高的数据率或者更低的发射功率来访问中继节点102。较高数据率下的传输创生较高的频谱效率，并且较低的功率例如通过消耗较少的电池功率来使接入终端104受益。

[0056] 在一些示例中，中继节点102可被实现为三种中继类型之一：第1层中继节点、第2层中继节点、和/或第3层中继节点。第1层中继节点实质上是能在除了放大和略微延迟之外不作任何修改的情况下重传传输的中继器。第2层中继节点可解码其接收的传输，重新编码该解码的结果，并随后传送经重新编码的数据。第3层中继节点可具有全无线电资源控制能力并因此能以类似于接入节点的方式起作用。由中继节点使用的无线电资源控制协议可以与由接入节点使用的那些无线电资源控制协议相同，并且中继节点可具有典型情况下由接入节点使用的唯一性蜂窝小区身份。为了本公开的目的，中继节点102因以下事实而区别于接入节点106：中继节点102可依赖至少一个接入节点106(和与该接入节点相关联的蜂窝小区)或其他接入节点的存在来访问电信系统(例如，网络108)中的其他组件。即，中继节点102可以对于网络而言表现为订户设备、客户端设备、或接入终端，因此中继节点102连接至接入节点以在网络108上通信。然而，对于其他订户设备、用户设备、和/或接入终端104而言，中继节点102可以表现为网络设备(例如，接入节点)。因此，中继节点102可实现一个或多个通信接口以与接入节点和/或一个或多个接入/订户/用户终端通信。在一个示例中，相同的发射机/接收机(例如，在一个或多个无线信道中)可由中继节点102用来与其接入节点和/或一个或多个接入终端通信。在另一示例中，中继节点102可利用两个或更多个不同的发射机/接收机来与接入节点和/或该一个或多个接入终端通信。

[0057] 为了减轻对接入网服务的订阅的滥用，这些设备可将设备认证与订户认证绑定。设备认证可协同例如基于存储在可移除地耦合至该设备的通用集成电路卡(UICC)109、111、113和116或通用订户标识模块(例如，USIM)中的凭证(诸如订户根密钥K)的标准3GPP AKA(认证和密钥协定)接入认证来工作。在一些实施例中，可以在被用于AKA认证的相同的非接入阶层(NAS)消息中执行设备认证。以此方式，该设备(例如，中继节点102、接入终端103/104等)可被绑定至自己的订阅(即，向核心网108的服务订阅)以便防止他人在未授权设备中使用其订户凭证(即，用于订阅服务的订户凭证)。

[0058] 一种针对订户凭证的未授权使用的风险的解决方案在于，由该设备(例如，设备101、中继节点102或接入终端103/104)和UICC 109彼此相互认证(例如，使用主机设备与UICC之间的安全信道)，但这会要求向UICC 109、111、113和116和/或主机设备(例如，设备101、中继节点102或接入终端103/104)预先提供用以执行此类相互认证的信息。

[0059] 另一解决方案可以是要求用于网络接入的密钥(例如，被用来保护该设备与网络之间的话务的密钥)取决于存储在UICC 109、111、113和116上的凭证以及存储在该设备(例

如，设备101、中继节点102或接入终端103/104)上的凭证两者。这可通过以某种方式将AKA认证密钥与设备认证绑定的方式达成。这种解决方案在国际移动装备身份(IMEI)认证(该认证例如可允许运营商阻止未授权设备附连至其网络)的情形中也是有用的。这是因为，通过将从AKA认证得到的用于网络接入的密钥与用于设备认证的密钥绑定，就确保了源自该设备去往网络108的所有消息确实源自此经认证的设备。在假定被绑定的密钥(和所有其他从被绑定的密钥推导出来的后续密钥)被安全地存储在该设备(例如，设备101、中继节点102、或接入终端103/104)上的情况下，将来自AKA认证的密钥与设备认证绑定便提供比单独将基于质询/响应的机制用于设备认证的方式更强的安全性。单独将质询/响应机制用于设备认证仅证明该设备曾在场以生成认证响应，但不能证明该设备在后续时间仍然在场。

[0060] 图2解说用于将设备认证与订户认证绑定的一般性办法。可为设备202(例如，设备101、中继节点102或接入终端103/104)提供订户根密钥206和/或订户身份207，该订户根密钥206和/或订户身份207可被用来认证向核心网108的订阅和/或生成被用来访问发送给设备202的经加密话务的安全性密钥。订户根密钥206可以唯一性地与订户身份207相关联。在一个示例中，订户根密钥206和/或订户身份207可被存储在UICC 204中，和/或订户认证可由UICC 204来处理。类似地，可为设备202提供(或其可存储)可被用来与核心网108认证该设备的设备根密钥208和/或设备身份209。设备根密钥208可以唯一性地与设备身份209相关联。

[0061] 在一个示例中，设备身份209可以是设备202(例如，设备101、中继节点102或接入终端103/104)的国际移动装备身份(IMEI)，但是其他形式的与该设备相关联的身份(例如，诸如EUI-48或EUI-64之类的IEEE硬件地址)也可被使用。

[0062] 在一些实现中，设备根密钥208可以是由设备202仅与核心网108共享但不越空传送的机密密钥。设备身份209可由设备202向核心网108传送，以使得核心网108能够获得在设备认证中使用的正确的设备根密钥。替换地，设备根密钥208可以是公钥/私钥对中的公钥，其中诸证书被用于设备认证。例如，设备可从网络接收一些数据，其中这些数据是用公钥来加密的。设备可随后使用自己的私钥来解密经加密数据并随后向网络证明它知道该数据。证书(例如，设备凭证)可由核心网108来验证。设备202的相关联的私钥可被安全地存储在设备202中。设备凭证可以指代设备证书或指向设备证书的指针。这些设备凭证可允许有关的网络实体形成设备质询并检查设备202的撤销状态(例如，检查与设备相关联的诸如私钥或共享密钥之类的凭证是否泄密)。进一步假定，设备的安全部分(诸如在3GPP技术规范33.320中定义的受信任环境或即TrE)存储诸如设备根密钥和/或与证书相关联的私钥之类的敏感的设备密钥。另外，假定，TrE执行利用这些密钥的所有密码术操作。

[0063] 最初，订户认证可在设备202与网络108之间进行。例如，设备202与网络108之间的认证和密钥协定(AKA)交换210可导致建立密钥K_ASME。此类AKA交换210可例如基于订户根密钥206和/或订户身份207以认证与设备202相关联的订户。例如，此类订阅信息或凭证可安全地存储在可移除地耦合至主机设备202的UICC 204中。

[0064] 网络108还可对设备202执行设备认证。设备身份209可由设备202提供给核心网108，以使得核心网108可查找或获得正确的对应设备根密钥208。网络108可创建设备质询212并向设备202发送该设备质询212(例如，作为有关的NAS消息的一部分)。作为响应，设备202计算设备响应214(例如，基于设备质询和设备根密钥208或其衍生物)并向网络108返回

该设备响应214。设备202可使用设备质询和设备响应中的数据来演算复合安全性密钥K_ASME_D 216。注意，在设备202的情形中，可以要么在设备响应214被发送之前要么在设备响应214被发送之后生成复合安全性密钥K_ASME_D 216。在一个示例中，复合安全性密钥K_ASME_D可以是在3GPP技术规范33.401中定义的演进型通用地面无线电接入网E-UTRAN(E-UTRAN)中定义的安全性密钥K_ASME的等效密钥，区别仅在于该密钥K_ASME_D被绑定至设备身份209还绑定至从AKA认证得到的诸如K_ASME密钥之类的密钥。如果网络108接收到有效的设备响应，则网络108还演算复合安全性密钥K_ASME_D218。

[0065] 设备质询212、设备响应214和复合安全性密钥K_ASME_D的演算可如下进行。设备质询212可被演算为：

[0066] 设备质询=eKSI,[E_设备根密钥(设备临时密钥),网络一次性数]，

[0067] 其中eKSI是将与K_ASME_D相关联的演进/扩展密钥集标识符，[..]表示可任选的参数，E_k(数据)表示用密钥k加密的数据，并且网络一次性数是由网络选择的合适大小的随机数(例如，128位)。加密算法可以是非对称的(在设备根密钥是与设备证书相关联的公钥的情形中)或者是对称的(在设备根密钥是共享密钥的情形中)。设备临时密钥可以是作为设备认证的一部分获得或生成的密钥。在一个示例中，设备临时密钥可由网络108(例如，随机地)选择，以经加密的形式发送给设备202，并具有恰适的长度(例如，256位或128位值)。

[0068] 设备202和网络108两者可为了优化目的而在网络接入之间保持设备临时密钥。如果不是这种情形，那么设备质询212中的第二个参数([E设备根密钥(设备临时密钥)])就不是可任选的。

[0069] 设备响应214可被演算为：

[0070] 设备响应=设备一次性数，设备_res。

[0071] 其中设备一次性数是由设备选择的合适大小的随机数(例如，128位)，并且

[0072] 设备_res=KDF(设备临时密钥，网络一次性数，设备一次性数)

[0073] 其中KDF是适于生成响应设备_res的密码术函数。

[0074] 在先前已获得认证密钥K_ASME(例如，作为AKA交换210的一部分)的情况下，复合安全性密钥K_ASME_D 216和218的演算(即，将设备认证与订户认证绑定)可如下进行：

[0075] K_ASME_D=KDF(设备临时密钥，K_ASME，网络一次性数，设备一次性数)

[0076] 其中K_ASME可以是在设备与网络之间的订户认证期间获得的密钥或值(作为AKA认证交换210的结果)。在一个示例中，K_ASME密钥可以是先前在设备202与网络108之间生成和/或使用的密钥。替换地，如果设备认证过程212和214是正使用与用于AKA规程210的NAS消息相同的NAS消息来执行的，那么K_ASME密钥可被重新或并发地生成。类似地，设备临时密钥可以是在设备202与网络108之间的设备认证期间获得的密钥或值。

[0077] 复合安全性密钥可随后被用作用于演算附加的安全性密钥217和219的基础和/或根。这些附加的安全性密钥可用于保护例如NAS级和/或AS级通信。

[0078] 与安全性参数相关联的复合安全性密钥K_ASME_D和从K_ASME_D推导出来的所有密钥可被安全地保持在设备202上并且不被存储在UICC 204上。复合安全性密钥K_ASME_D可随后被用来保护设备202与核心网108之间交换的消息220。

[0079] 图3(包括图3A和图3B)解说可以如何将基于订户认证的密钥阶级修改成还包括设

备认证的示例。密钥阶级可被实现成建立在设备与网络之间的通信的加密/解密中使用的安全性参数(例如,安全性密钥)。在此示例中,可以在设备322与网络实体324之间执行订户和设备认证。设备322可以例如是接入终端(AT)、用户装备(UE)、移动电话、和/或中继节点。网络实体324可以是诸如移动性管理实体(MME)和/或归属订户服务器(HSS)之类的一个或多个网络设备。

[0080] 此示例解说如何修改基于订户认证的第一密钥阶级300以获得基于订户认证和设备认证两者的第二密钥阶级300'。

[0081] 为了如在第一密钥阶级300中解说的订户认证的目的,通用集成电路卡(设备322中的UICC)、和网络实体324(例如,图1中的MME 110、HSS 112、或是其他网络实体)可使用主密钥K 302来生成密码密钥(CK)304和完好性密钥(IK)306。密码密钥(CK)304和完好性密钥(IK)306可随后由设备322和网络实体324用作认证和密钥协定(AKA)交换的一部分以生成接入安全性管理实体密钥K_ASME 308(在本文中亦被称为订户认证密钥)。设备202的安全性激活可通过认证和密钥协定规程(AKA)、非接入阶层(NAS)安全性模式配置(NAS SMC)规程和接入阶层(AS)安全性模式配置(AS SMC)规程来达成。

[0082] 在此示例中,订户认证可包括结果得到K_ASME 308的AKA交换326。AKA交换236可包括订户认证请求340和订户认证响应342。在此示例中,生成K_ASME密钥308的订户认证过程还可生成相关联的NAS级密钥(例如,K_NAS-enc 305和K_NAS-int 311)和/或AS级密钥(例如,K_UP-enc 315、K_RRC-enc 317、和K_RRC-int 319)。注意,在一些实现中,如果不使用这些版本的NAS级密钥和AS级密钥,那么这些密钥的生成可以是在订户认证期间已先期进行了的。

[0083] 第二密钥阶级300'解说设备认证可如何绑定至订户认证以生成NAS级和AS级安全性密钥。与订户认证(以及生成其对应的K_ASME密钥308)并发地,在其之前或之后,可以至少部分地基于因设备而异的根密钥来执行设备认证328。设备认证328可包括设备认证请求344和设备认证响应346。在一个实现中,设备认证307可独立于订户认证;仅当订户和设备认证两者均被满足时才生成复合安全性密钥K_ASME_D 309。在替换实现中,可以在订户认证之前执行设备认证。

[0084] 复合安全性密钥K_ASME_D 309可被用作用于例如NAS(非接入阶层)密钥310和312以及AS(接入阶层)密钥314、316、318和320的演算的基密钥。即,设备322和网络实体324可随后使用K_ASME_D密钥309来生成一个或多个安全性密钥。

[0085] 分组交换网络可被结构化成多个阶级式协议层,其中各下协议层向各上层提供服务,并且每一层负责不同的任务。例如,图4解说可在分组交换网络中工作的设备中实现的示例性协议栈。在此示例中,协议栈402包括物理(PHY)层404、媒体接入控制(MAC)层406、无线电链路控制(RLC)层408、分组数据汇聚协议(PDCP)层410、无线电资源控制(RRC)层412、非接入阶层(NAS)层414、和应用(APP)层416。

[0086] NAS层414以下的各层常被称为接入阶层(AS)层418。RLC层408可包括一个或多个信道420。RRC层412可为接入终端实现各种监视模式,包括连通状态和空闲状态。非接入阶层(NAS)层414可维护通信设备的移动性管理上下文、分组数据上下文和/或它的IP地址。注意,其他层可存在于协议栈402中(例如,在所解说的层之上、之下和/或之间),但为了解说的目的而已被省去。

[0087] 参照图4，无线电/会话承载422可以例如被建立在RRC层412和/或NAS层414处。结果，NAS层414可由设备202和核心网108用来生成图3中所示的安全性密钥K_NAS-enc 310和K_NAS-int 312。类似地，RRC层412可由设备202和接入节点108用来生成接入阶层(AS)安全性密钥K_UP-enc 316、K_RRC-enc 318、和K_RRC-int 320。虽然安全性密钥K_UP-enc 316、K_RRC-enc318、和K_RRC-int 320可在RRC层312处生成，但是这些密钥可由PDCP层410用来保护信令和/或用户/数据通信。例如，密钥K_UP-enc 316可由PDCP层410用来保护用户/数据面(UP)通信，而密钥K_RRC-enc 318和K_RRC-int320可被用来保护PDCP层410处的信令(即，控制)通信。

[0088] 在被用于密码化和完好性算法的这些安全性密钥的推导中，在AS(用户面和RRC)和NAS两者处均要求提供个体算法身份作为输入之一。在AS级处，要使用的算法由无线电资源控制(RRC)安全性模式命令提供。

[0089] 图5是解说在其中可生成图3和图4中解说的各种认证和/或安全性密钥的网络系统的框图。此处，设备322可实现包括各种层(例如，APP、NAS、RRC、RLC、MAC和PHY)的通信栈。接入网504(例如，图1中的接入节点106)可向设备322提供无线连通性，以使得设备322可与网络108通信。归属订户服务器506和设备322可双方均知晓或有途径访问可被用来生成或获得密码密钥(CK)和/或完好性密钥(IK)的根密钥(K)。设备322和/或HSS506可随后使用密码密钥(CK)和/或完好性密钥(IK)来生成接入安全性管理实体密钥K_ASME。设备认证也可被执行并与K_ASME密钥相组合或基于K_ASME密钥以生成复合安全性密钥K_ASME_D，由此将订户与设备认证组合成一个密钥。使用该K_ASME_d密钥，设备322和移动性管理实体(MME)510可随后生成密钥K_NAS-enc和K_NAS-int。设备322和MME 510还可生成因接入网而异的密钥K_eNB/NH。使用此因接入网而异的密钥K_eNB/NH，设备322和接入网504可生成密钥K_UP-enc以及K_RRC-enc和K_RRC-int。

[0090] 关于这些密钥的推导的详情在3GPP STD-T63-33.401“(System Architecture Evolution(SAE):Security Architecture)系统构架演进(SAE):安全性架构”(称为3GPP TS 33.401)第八版中提供，其通过援引纳入于此。注意，虽然图3-图5描述了在其中可实现设备和订户认证及绑定的特定环境/上下文，但是这并非旨在对此特征构成限定，该特征可在各种其他类型的网络中实现。

[0091] 示例性无线设备

[0092] 图6是解说可被适配成将订户认证与设备认证绑定的无线设备600的组件选集的框图。无线设备600一般包括耦合至一个或多个无线通信接口604的处理电路602。例如，无线设备600可以是中继节点和/或接入终端。

[0093] 处理电路602可被安排成获得、处理和/或发送数据、控制数据访问和存储、发布命令、以及控制其他期望的操作。在至少一个实施例中，处理电路602可包括被配置成实现由恰适的介质提供的期望编程的电路系统。例如，处理电路602可被实现为处理器、控制器、多个处理器和/或被配置成执行包括例如软件和/或固件指令的可执行指令的其他结构、和/或硬件电路系统中的一者或多者。处理电路602的实施例可包括被设计成执行本文中所描述的功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他可编程逻辑组件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合。通用处理器可以是微处理器，但在替换方案中，处理器可以是任何常规的处理器、控制器、

微控制器、或状态机。处理器还可以实现为计算组件的组合，诸如DSP与微处理器的组合、数个微处理器、与DSP核心协作的一个或多个微处理器、或任何其他此类配置。处理电路602的这些示例是为了解说，并且本公开范围内的其他合适的配置也是构想到的。

[0094] 无线通信接口604可被配置成促成无线设备600的无线通信。例如，通信接口604可被配置成关于诸如接入终端、接入点、其他中继节点等之类的其他无线设备双向地传达信息。通信接口604可耦合至天线(未示出)并可包括无线收发机电路系统，该无线收发机电路系统包括用于无线通信的至少一个发射机和/或至少一个接收机(例如，一个或多个发射机/接收机链)。

[0095] 处理电路602可包括订户与设备认证绑定模块610。订户与设备认证模块610可包括适配成使用订户安全性凭证(例如，存储在通用集成电路卡608中的因订户而异的密钥607和/或订户身份609)来执行订户认证规程、适配成使用因设备而异的凭证(例如，因设备而异的密钥605和/或设备身份611)来(在受信任环境606内)执行设备认证规程、并将订户认证与设备认证绑定在一起的电路系统和/或编程。此类“绑定”可涉及将来自订户认证和设备认证两者的一些结果相组合。例如，从订户认证获得的第一安全性密钥可与从设备认证获得的第二安全性密钥相组合以获得第三(复合)安全性密钥。

[0096] 在一些实施例中，无线设备600可包括受信任环境(TrE)606。受信任环境606可被适配成满足TS 33.320处的3GPP规范详情中针对受信任环境的规范。可为受信任环境606预先提供(或安全地嵌入)至少一些安全性凭证(例如，因设备而异的密钥605和/或设备身份6111)。例如，受信任环境606可具有与设备认证有关的安全性凭证。

[0097] 在一些实施例中，无线设备600可包括通用集成电路卡(UICC)608内的受保护处理。UICC 608可被可移除地耦合至无线设备600。可为UICC 608预先提供订户安全性凭证(例如，因订户而异的密钥607和/或订户身份609)，诸如初始认证和密钥协定(AKA)凭证。替换地，可以在通用订户身份模块(USIM)内执行受保护处理。

[0098] 根据无线设备600的一个或多个特征，处理电路602可被适配成执行图2-5、7、10、11和12中解说的有关的过程、功能、步骤和/或例程中的任何一者或全部。如本文中使用的，涉及处理电路602的术语“适配成”可指处理电路602被配置、采用、实现和/或编程为执行根据本文中所描述的各种特征的特定过程、功能、步骤和/或例程。

[0099] 图7是解说在无线设备中操作以用于生成将订户认证与设备认证绑定的安全性密钥的方法的示例的流程图。可为无线设备预先提供因设备而异的密钥702。例如，此类因设备而异的密钥可在该无线设备的制造期间被嵌入芯片中或被配置。无线设备还可包括与该因设备而异的密钥相关联的设备标识符。附加地，可为无线设备预先提供因订户而异的密钥704。例如，此类因订户而异的密钥可以是指派给订户的根密钥并可被存储在耦合至该无线设备的固定或可移除模块(例如，UICC或USIM)内。无线设备还可包括与该因订户而异的密钥相关联的订阅身份。无线设备可与网络实体(例如，使用因订户而异的密钥)来执行订户认证706。这可包括例如与该网络实体的认证和密钥协定交换。无线设备还可与网络实体(例如，使用因设备而异的密钥)来执行设备认证708。订户认证和设备认证可在相同或不同的时间并且与相同网络实体或与不同网络实体来执行。安全性密钥(例如，K_ASME_D等)可随后由该无线设备生成，此类安全性密钥将订户认证与设备认证绑定710。例如，在一个示例中，来自设备认证的数据(例如，一个或多个结果得到的密钥、证书、标识符等)和来自订

户认证的数据(例如,一个或多个结果得到的密钥、证书、标识符等)可被组合以生成安全性密钥。例如,在图1中,来自订户认证210的K_ASME密钥和来自图1中的设备认证的设备临时密钥可被组合以生成安全性密钥K_ASME_D。该安全性密钥可随后被用来保护该无线设备与网络实体之间的无线通信712。例如,该安全性密钥可被用来生成可用于加密/解密该无线设备与网络之间的通信(例如,数据和信令)的其他密钥和/或证书(例如,NAS级和/或AS级安全性密钥)。

[0100] 示例性网络实体

[0101] 图8是解说可被适配成将订户认证与设备认证绑定的网络实体800的组件选集的框图。网关实体800可包括耦合至通信接口804的处理电路802。处理电路802被安排成获得、处理和/或发送数据、控制数据访问和存储、发布命令、以及控制其他期望的操作。在至少一个实施例中,处理电路802可包括被配置成实现由恰适的介质提供的期望编程的电路系统。例如,处理电路802可被实现为处理器、控制器、多个处理器和/或被配置成执行包括例如软件和/或固件指令的可执行指令的其他结构、和/或硬件电路系统中的一者或多者。处理电路802的实施例可包括被设计成执行本文中所描述的功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他可编程逻辑组件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合。通用处理器可以是微处理器,但在替换方案中,处理器可以是任何常规的处理器、控制器、微控制器、或状态机。处理器还可以实现为计算组件的组合,诸如DSP与微处理器的组合、数个微处理器、与DSP核心协作的一个或多个微处理器、或任何其他此类配置。处理电路802的这些示例是为了解说,并且本公开范围内的其他合适的配置也是构想到的。

[0102] 处理电路802包括订户与设备认证绑定模块806。订户与设备认证绑定模块806可包括适配成执行用于基于订户安全性凭证(例如,因订户而异的密钥和/或订户标识符)来认证订阅的订户认证规程、执行用于基于因设备而异的凭证(例如,因设备而异的密钥和/或设备标识符)来认证设备的设备认证规程、以及将来自设备认证和订户认证的数据(例如,密钥、值、证书等)绑定以生成安全性密钥的电路系统和/或编程。

[0103] 通信接口804被配置成促成网络实体800的通信以直接地或间接地(例如,通过一个或多个其他网络实体)与诸如中继节点和接入终端之类的其他设备通信。

[0104] 根据网络实体800的一个或多个特征,处理电路802可被适配成执行与诸如移动管理实体(MME)110和归属订户服务器(HSS)112之类的各种网络实体有关的过程、功能、步骤和/或例程中的任一者或全部。此外,网络实体800可包括单个实体,或网络中的两个或更多个实体的组合。作为示例而非限定,网络实体800可尤其包括移动管理实体(MME)、归属订户服务器(HSS)、设备认证服务器,等等。如本文中使用的,涉及处理电路802的术语“适配成”可指处理电路802被配置、采用、实现和/或编程为执行根据本文中所描述的各种特征的特定过程、功能、步骤和/或例程中的一者或多者。

[0105] 图9是解说在网络实体中操作以用于生成将订户认证与设备认证绑定的安全性密钥的方法的示例的流程图。网络实体可获得无线设备的因设备而异的密钥902。例如,此类因设备而异的密钥可在该无线设备的制造期间被嵌入芯片中或被配置,并且此信息可被存储在网络实体可访问的数据库中。设备标识符可与该因设备而异的密钥相关联,并可被用来标识该设备及其密钥。附加地,网络实体可获得与无线设备的订阅相关联的因订户而异

的密钥904。例如，此类因订户而异的密钥可以是指派给订户的根密钥，并可被存储在耦合至该无线设备的固定或可移除模块(例如，UICC或USIM)内。网络实体可与无线设备(例如，使用因订户而异的密钥)来执行订户认证906。这可包括例如与该网络实体的认证和密钥协定交换。网络实体还可与无线设备(例如，使用因设备而异的密钥)来执行设备认证908。订户认证和设备认证可在相同或不同的时间执行。(复合)安全性密钥(例如，K_ASME_D等)可随后由网络实体生成，此类安全性密钥将订户认证与设备认证绑定910。例如，在一个示例中，来自设备认证的数据(例如，一个或多个结果得到的密钥、证书、标识符等)和来自订户认证的数据(例如，K_ASME等)可被组合以生成安全性密钥。随后，可以使用该安全性密钥来保护该网络实体与该无线设备之间的无线通信912。例如，该安全性密钥可被用来生成可用于加密/解密该无线设备与网络之间的通信的其他密钥和/或证书。

[0106] 订户-设备认证的第一示例性方法

[0107] 图10解说用于通过将订户与设备认证绑定来生成安全性密钥的第一示例性方法。在此示例中，设备1002可以例如是中继节点或接入终端。在其中设备1102可寻求附连至无线网络(例如，该无线网络包括MME 1002和HSS1006)的附连阶段期间，越空泄露设备身份或其他有关的设备信息可能(例如，对于设备1002而言)是安全性问题所在。结果，在此方法中，设备1002不越空呈现其设备凭证(例如，诸如国际移动装备身份(IMEI)等的因设备而异的标识符)，直至由网络安全地请求，以防止对设备身份的被动攻击。

[0108] 设备一开始可向网络发送附连请求1010，该附连请求1010包括对该设备能够进行设备认证的指示。一旦接收到附连请求1010，移动性管理实体(MME)1004即可向归属订阅服务器(HSS)1006请求并从其接收(例如，与基于订阅的账户或设备1002的用户相关联的)订阅和认证信息1012。MME 1004随后发送包括AKA质询的认证请求1014以执行AKA认证。一旦接收到AKA认证请求1014，设备1002即发送包括AKA响应的认证响应1016。AKA认证请求1014和响应1016用于执行订阅认证。此类AKA认证规程可导致由设备1002和MME生成订户认证密钥(例如，K_ASME)。

[0109] 设备认证可在此安全性激活过程期间的各种阶段执行。在此示例中，可以在NAS级安全性消息上背载设备认证。例如，MME 1004可发送包括对设备身份的请求(例如，对IMEI软件版本(IMEISV)的请求和/或对设备凭证的请求)的NAS安全性模式命令1018。作为响应，设备1002可在设备认证将被执行的安全性模式完成1020消息内提供设备身份或凭证。注意，为了避免在传输期间越空曝露设备身份或凭证，安全性模式完成1020中的设备身份或凭证可由先前计算的订户认证密钥(例如，K_ASME)来保护。一旦接收到设备身份或凭证，MME 1004就可发送带有演进/扩展密钥集标识符(eKSI)和设备质询的身份请求1022消息。eKSI可与待生成的K_ASME_D相关联。因此，在身份请求1022中使用的eKSI可以不同或相异于可能已被例如用于AKA(即，订户认证)的任何其他eKSI。一旦接收到身份请求1022消息，设备1002就可基于设备质询来生成设备响应并将该设备响应作为身份响应1024消息的一部分来发送。该设备响应可基于设备质询以及设备身份或凭证。设备1002可随后基于认证密钥(例如，K_ASME)和设备认证数据(例如，设备响应等)来演算(复合)安全性密钥(K_ASME_D)1025。MME 1004例如通过使用设备1002的设备身份或证书以及使用设备质询来检查设备响应。如果设备1002由MME 1004成功认证，那么MME 1004还生成安全性密钥(K_ASME_D)1027。此时，设备1002和MME 1004共享该安全性密钥(K_ASME_D)及其相关联的标识

符eKSI。

[0110] MME 1004可随后发送带有与该安全性密钥(K_ASME_D)相关联的演进/扩展密钥集标识符eKSI的安全性模式命令1026。这允许设备1002基于该安全性密钥(K_ASME_D)来计算一个或多个安全性密钥。设备1002可向MME1004发送安全性模式完成1028消息，由此允许MME 1004发送附连完成1030消息。

[0111] 订户-设备认证的第二示例性方法

[0112] 图11解说了用于通过将订户与设备认证绑定来生成安全性密钥的第二示例性方法。在此示例中，在越空传输中泄露设备身份或证书(或其他有关的凭证信息)不是安全性问题所在。不同于图10的方法，在这种情形中，假定在开头就呈现设备身份将不会导致任何隐私问题或风险。

[0113] 设备已具有MME将接受的设备标识符或凭证(例如，IMEI)但不具有MME愿意使用的E-UTRAN安全性上下文。

[0114] 设备1102向MME 1104发送包括自己的设备标识符或凭证的附连请求1108。MME 1104可从HSS 1106获得订阅和认证信息1110并发送包括例如AKA质询(针对订阅认证)和/或设备质询(针对设备认证)的认证请求1112。注意，设备1102可通过发送可包括AKA响应和/或设备响应的认证响应1114来响应。AKA响应可至少部分地基于订户标识符。设备响应可基于设备标识符和/或凭证以及设备质询。设备1104可随后通过将订户认证信息与设备认证信息相组合的方式来生成(复合)安全性密钥K_ASME_D。类似地，一旦成功验证了AKA响应和设备响应，MME 1104就还可通过将订户认证信息与设备认证信息相组合的方式来生成安全性密钥K_ASME_D。

[0115] MME发送安全性模式命令1116消息来开始使用基于安全性密钥K_ASME_D的安全性上下文。设备1102用安全性模式完成1118消息来响应。即，设备1102和MME 1104可使用安全性密钥K_ASME_D来生成一个或多个附加的安全性密钥(或以其他方式保护设备1102与MME 1104之间的通信)。MME 1104可随后向设备1102发送附连完成1120消息。

[0116] 此处观察到，如果设备标识符和/或凭证(或先前获得/生成的设备密钥)被与订户标识符一起存储在HSS 1106或网络中的另一服务器中，那么设备1102可使用此流程来执行附连。为了在那里进行此举，设备1102可指示(例如，在附连请求1108中)其设备标识符和/或凭证可从HSS 1106或其他网络服务器获得。替换地，MME 1104可向设备1102指示设备质询与特定的设备标识符相关联(例如，通过以某种形式将诸如IMEI之类的设备标识符随设备质询而包括)。以此方式，设备1102可知晓(认证请求1112中的)该设备质询与自己的设备标识符相关联。

[0117] 订户-设备认证的第三示例性方法

[0118] 图12解说了用于通过将订户与设备认证绑定来生成安全性密钥的第三示例性方法。在此示例中，先前已执行了订户认证，所以订户安全性上下文1206(例如，K_ASME密钥)已存在。经组合的订户和设备认证可由网络发起以替代现有的安全性上下文。此实施例可以有益于可能需要建立初始的基于AKA的安全性上下文以从运营商获得有完全资格的或起作用的凭证的设备。

[0119] 此办法假定MME已知晓设备标识符(例如，IMEI)和/或设备凭证。

[0120] MME 1204向设备1202发送包括设备质询的认证请求1208。作为响应，设备1202向

MME 1204发送包括设备响应的认证响应1210。该设备响应可基于设备质询以及设备身份和/或证书。此时，设备1202和MME 1204两者都可具有足以(例如，在基于AKA的安全性上下文和设备认证信息的基础上来)演算(复合)安全性密钥K_ASME_D的信息。

[0121] MME 1204可向设备1202发送NAS安全性模式命令1212以将现有的安全性上下文1206替换成基于新的安全性密钥K_ASME_D的安全性上下文(例如，该安全性上下文纳入订户认证和设备认证两者)。作为响应，设备1202可基于安全性密钥K_ASME_D来生成新的安全性上下文并可作为响应而发送NAS安全性模式完成1214消息。

[0122] 注意，虽然本文中的各种示例解说可经由MME来执行订户认证和设备认证两者，但是其他网络实体也可与MME相组合地或替代MME来执行这些功能中的一些功能。

[0123] 图1、2、3、4、5、6、7、8、9、10、11、和/或12中解说的组件、步骤、特征和/或功能之中的一个或更多个可以被重新安排和/或组合成单个组件、步骤、特征或功能，或可以实施在数个组件、步骤、或功能中。还可添加附加的元件、组件、步骤、和/或功能而不会脱离本公开。图1、5、6和/或8中解说的装置、设备、和/或组件可被配置成执行图2、3、4、7和/或9-12中描述的方法、特征、或步骤中的一者或多者。本文中描述的新颖算法还可以高效率地实现在软件中和/或嵌入硬件中。

[0124] 还应注意，至少一些实现是作为被描绘为流图、流程图、结构图、或框图的过程来描述的。尽管流图可能把诸操作描述为顺序过程，但是这些操作中有许多可以并行或并发执行。另外，这些操作的次序可以被重新安排。过程在其操作完成时终止。过程可对应于方法、函数、规程、子例程、子程序等。当过程对应于函数时，它的终止对应于该函数返回调用方函数或主函数。

[0125] 此外，诸实施例可由硬件、软件、固件、中间件、微代码、或其任何组合来实现。当在软件、固件、中间件或微码中实现时，执行必要任务的程序代码或代码段可被存储在诸如存储介质或其它存储之类的机器可读介质中。处理器可以执行这些必要的任务。代码段可以代表规程、函数、子程序、程序、例程、子例程、模块、软件包、类、或是指令、数据结构、或程序语句的任何组合。通过传递和/或接收信息、数据、自变量、参数、或存储器内容，一代码段可被耦合到另一代码段或硬件电路。信息、自变量、参数、数据等可以经由包括存储器共享、消息传递、令牌传递、网络传输等任何合适的手段被传递、转发、或传输。

[0126] 术语“机器可读介质”、“计算机可读介质”和/或“处理器可读介质”可包括，但不限于，便携或固定的存储设备、光存储设备、以及能够存储、包含或承载指令和/或数据的各种其他非瞬态介质。因此，本文中描述的各种方法可部分或完全地由可存储在“机器可读介质”、“计算机可读介质”和/或“处理器可读介质”中并由一个或多个处理器、机器和/或设备执行的指令和/或数据来实现。

[0127] 结合本文中公开的示例描述的方法或算法可直接在硬件中、在能由处理器执行的软件模块中、在这两者的组合中，以处理单元、编程指令、或其他指示的形式实施，并且可包含在单个设备中或跨多个设备分布。软件模块可驻留在RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动盘、CD-ROM、或本领域中所知的任何其他形式的非瞬态存储介质中。存储介质可耦合到处理器以使得该处理器能从/向该存储介质读写信息。在替换方案中，存储介质可以被整合到处理器。

[0128] 本领域技术人员将可进一步领会，结合本文中公开的实施例描述的各种解说性逻

辑框、模块、电路、和算法步骤可被实现为电子硬件、计算机软件、或两者的组合。为清楚地解说硬件与软件的这一可互换性，各种解说性组件、框、模块、电路、和步骤在上面是以其功能性的形式作一般化描述的。此类功能性是被实现为硬件还是软件取决于具体应用和施加于整体系统的设计约束。

[0129] 本文中所描述的本发明的各种特征可实现于不同系统中而不脱离本发明。应注意，以上实施例仅是示例，且并不应被解释成限定本发明。这些实施例的描述旨在解说，而并非旨在限定本公开的范围。由此，本发明的教导可以现成地应用于其他类型的装置，并且许多替换、修改、和变形对于本领域技术人员将是显而易见的。

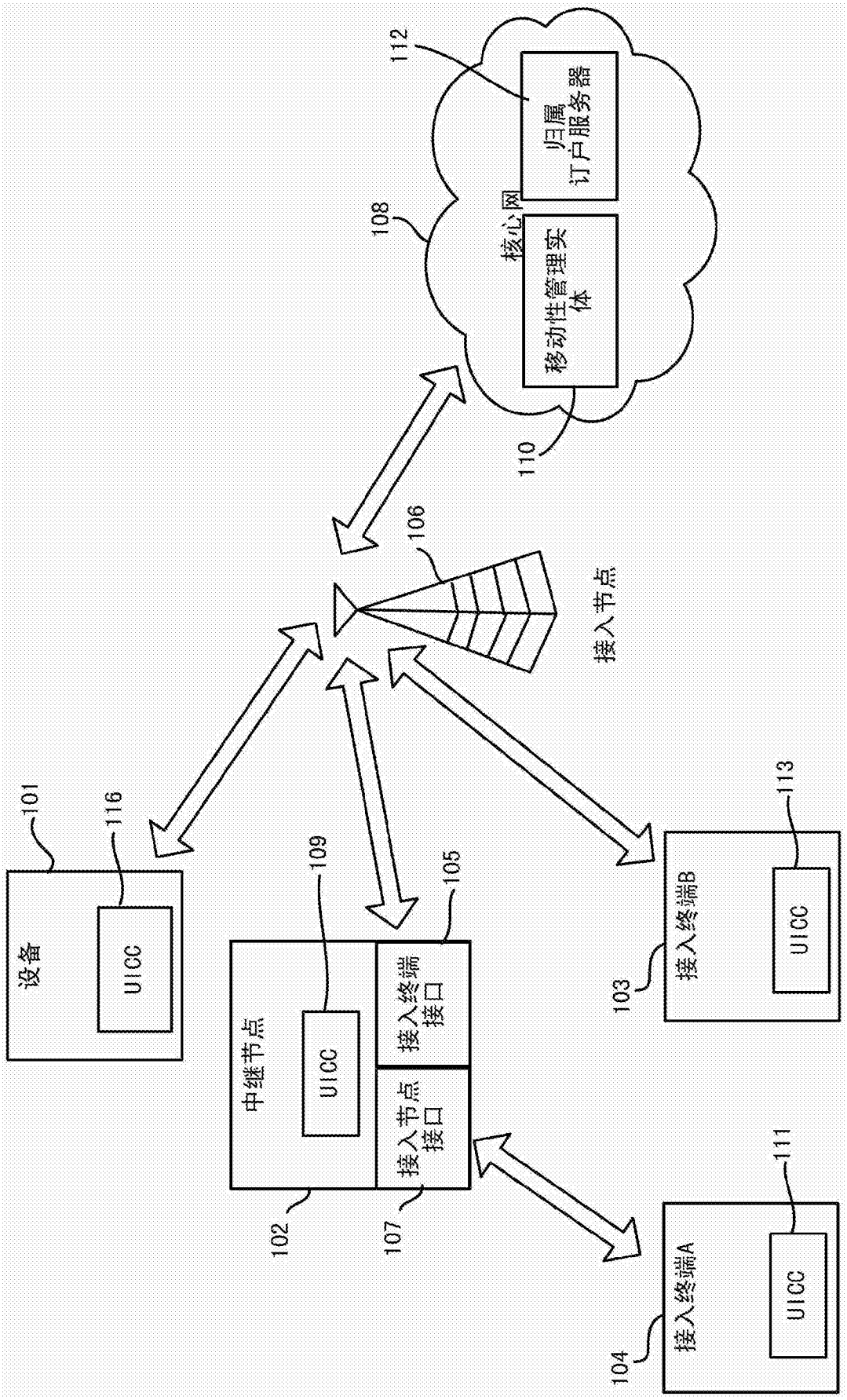

112
归属
订户服务器
核心网
108
移动性管理实
体
110
106
接入节点
101
116
设备
UICC
109
105
中继节点
UICC
接入终端
接口
接入节点
接口
102
107
103
接入终端B
UICC
113
104
接入终端A
UICC
111

图1

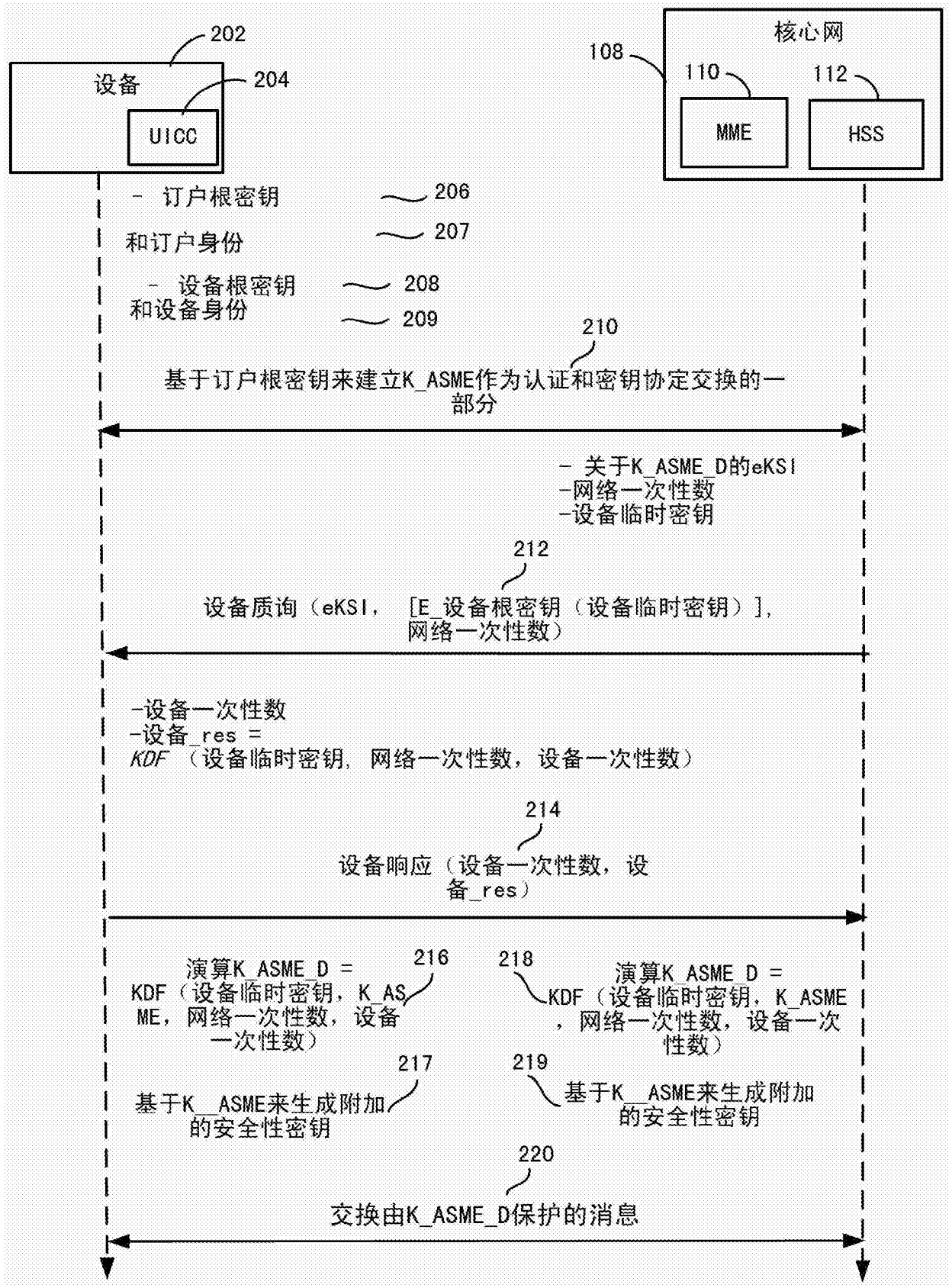

202
设备
204
UICC
核心网
108
110
MME
112
HSS
- 订户根密钥
206
和订户身份
207
- 设备根密钥
208
和设备身份
209
210
基于订户根密钥来建立K_ASME作为认证和密钥协定交换的一部分
- 关于K_ASME_D的eKSI
-网络一次性数
-设备临时密钥
212
设备质询（eKSI，[E_设备根密钥（设备临时密钥）]，网络一次性数）
-设备一次性数
-设备_res =
KDF（设备临时密钥，网络一次性数，设备一次性数）
214
设备响应（设备一次性数，设备_res）
演算K_ASME_D =
216
KDF（设备临时密钥，K_ASME，网络一次性数，设备一次性数）
218
演算K_ASME_D =
KDF（设备临时密钥，K_ASME，网络一次性数，设备一次性数）
217
基于K_ASME来生成附加的安全性密钥
219
基于K_ASME来生成附加的安全性密钥
220
交换由K_ASME_D保护的消息

图2

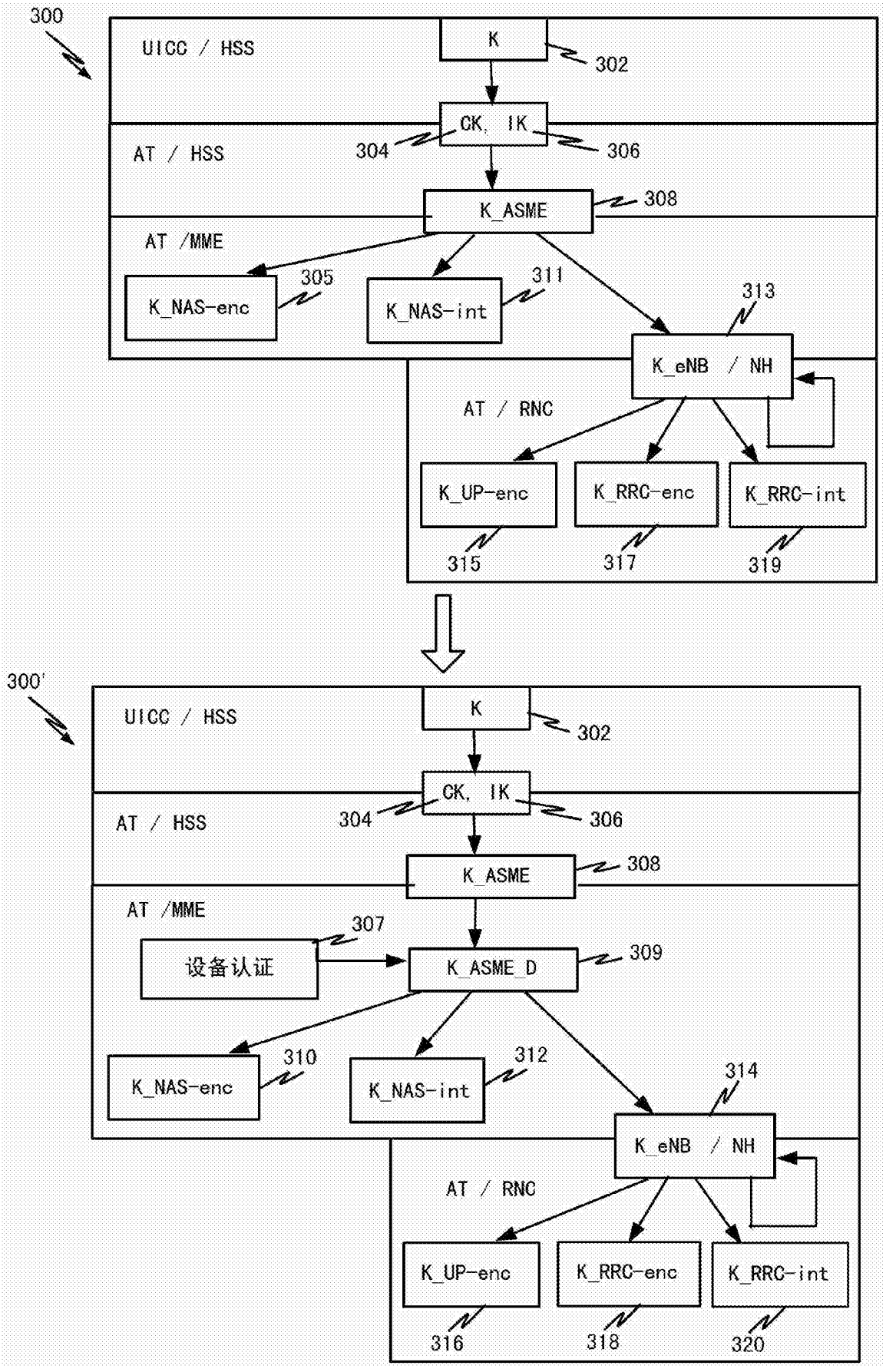

300
UICC / HSS
K
302
CK, IK
304
306
AT / HSS
K_ASME
308
AT /MME
K_NAS-enc
305
K_NAS-int
311
313
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
315
317
319
300'
UICC / HSS
K
302
CK, IK
304
306
AT / HSS
K_ASME
308
AT /MME
设备认证
307
K_ASME_D
309
K_NAS-enc
310
K_NAS-int
312
314
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
316
318
320

图3A

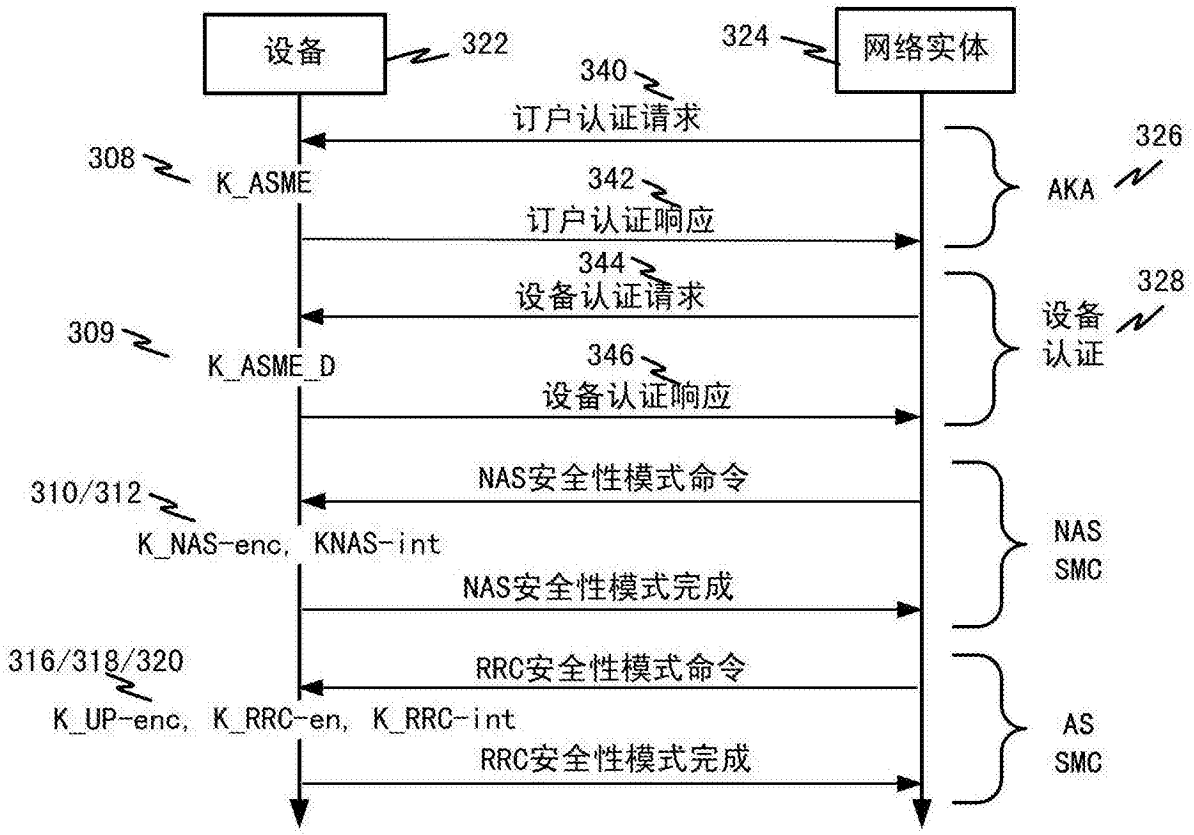

设备
322
324
网络实体
340
订户认证请求
326
308
K_ASME
342
订户认证响应
AKA
344
设备认证请求
328
设备
认证
309
K_ASME_D
346
设备认证响应
NAS安全性模式命令
310/312
K_NAS-enc, KNAS-int
NAS
SMC
NAS安全性模式完成
316/318/320
RRC安全性模式命令
K_UP-enc, K_RRC-en, K_RRC-int
AS
SMC
RRC安全性模式完成

图3B

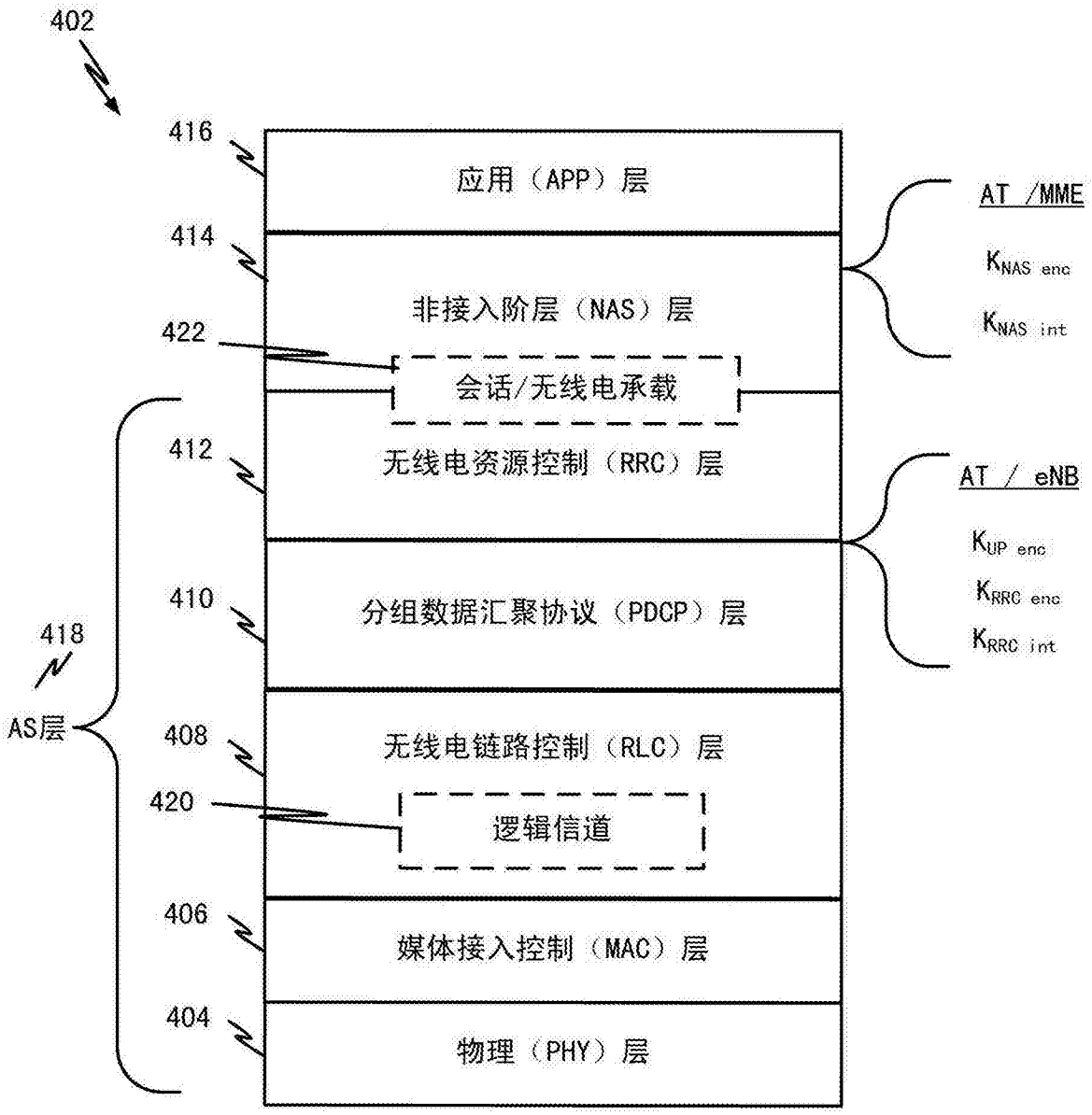

402
416
应用（APP）层
414
非接入阶层（NAS）层
422
会话/无线电承载
412
无线电资源控制（RRC）层
410
分组数据汇聚协议（PDCP）层
418
AS层
408
无线电链路控制（RLC）层
420
逻辑信道
406
媒体接入控制（MAC）层
404
物理（PHY）层
AT /MME
$K_{NAS\ enc}$
$K_{NAS\ int}$
AT / eNB
$K_{UP\ enc}$
$K_{RRC\ enc}$
$K_{RRC\ int}$

图4

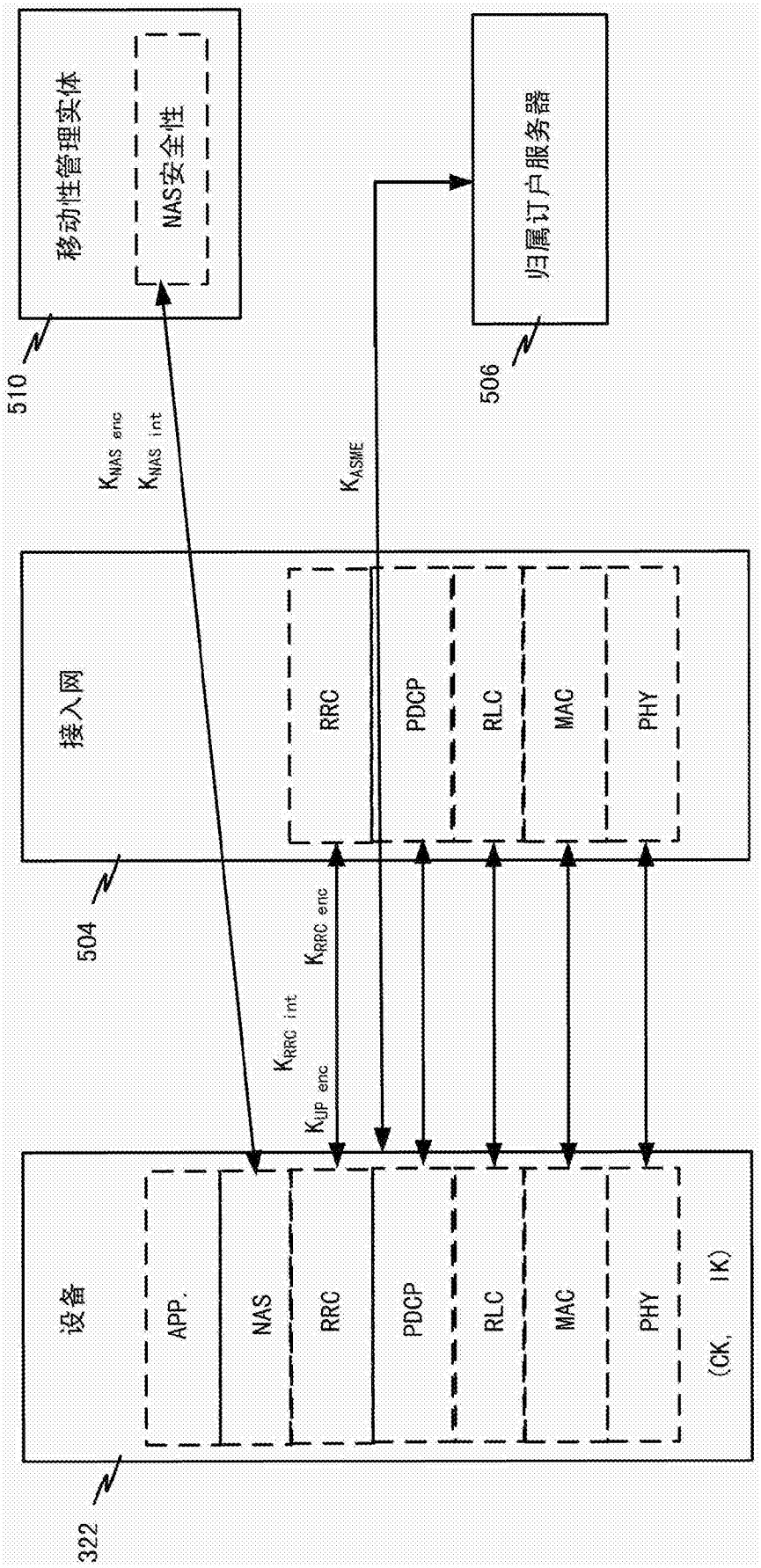

移动性管理实体
NAS安全性
510
归属订户服务器
506
$K_{NAS\ enc}$
$K_{NAS\ int}$
K_{ASME}
接入网
RRC
PDCP
RLC
MAC
PHY
504
$K_{RRC\ enc}$
$K_{RRC\ int}$
$K_{UP\ enc}$
设备
APP.
NAS
RRC
PDCP
RLC
MAC
PHY
(CK, IK)
322

图5

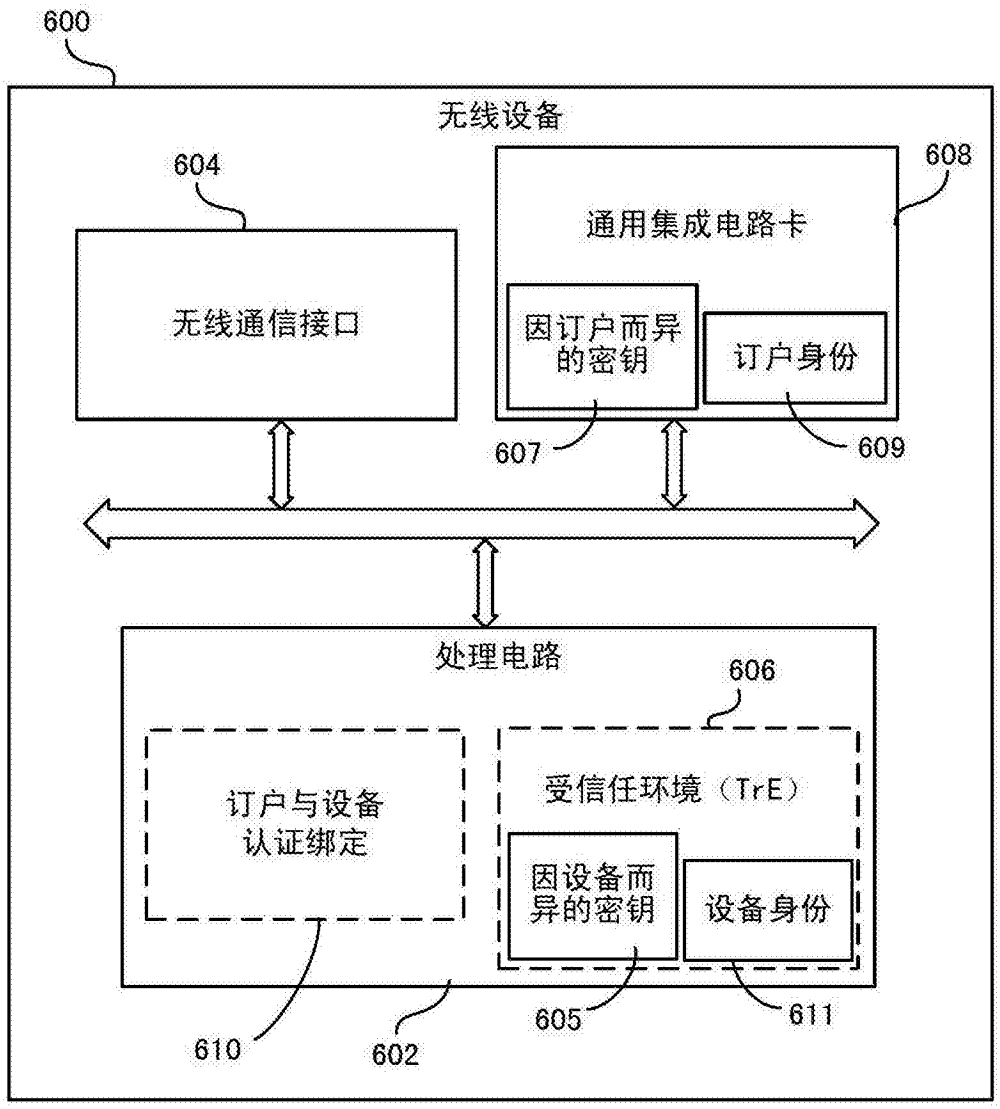

600
无线设备
604
608
通用集成电路卡
无线通信接口
因订户而异的密钥
订户身份
607
609
处理电路
606
订户与设备认证绑定
受信任环境（TrE）
因设备而异的密钥
设备身份
610
602
605
611

图6

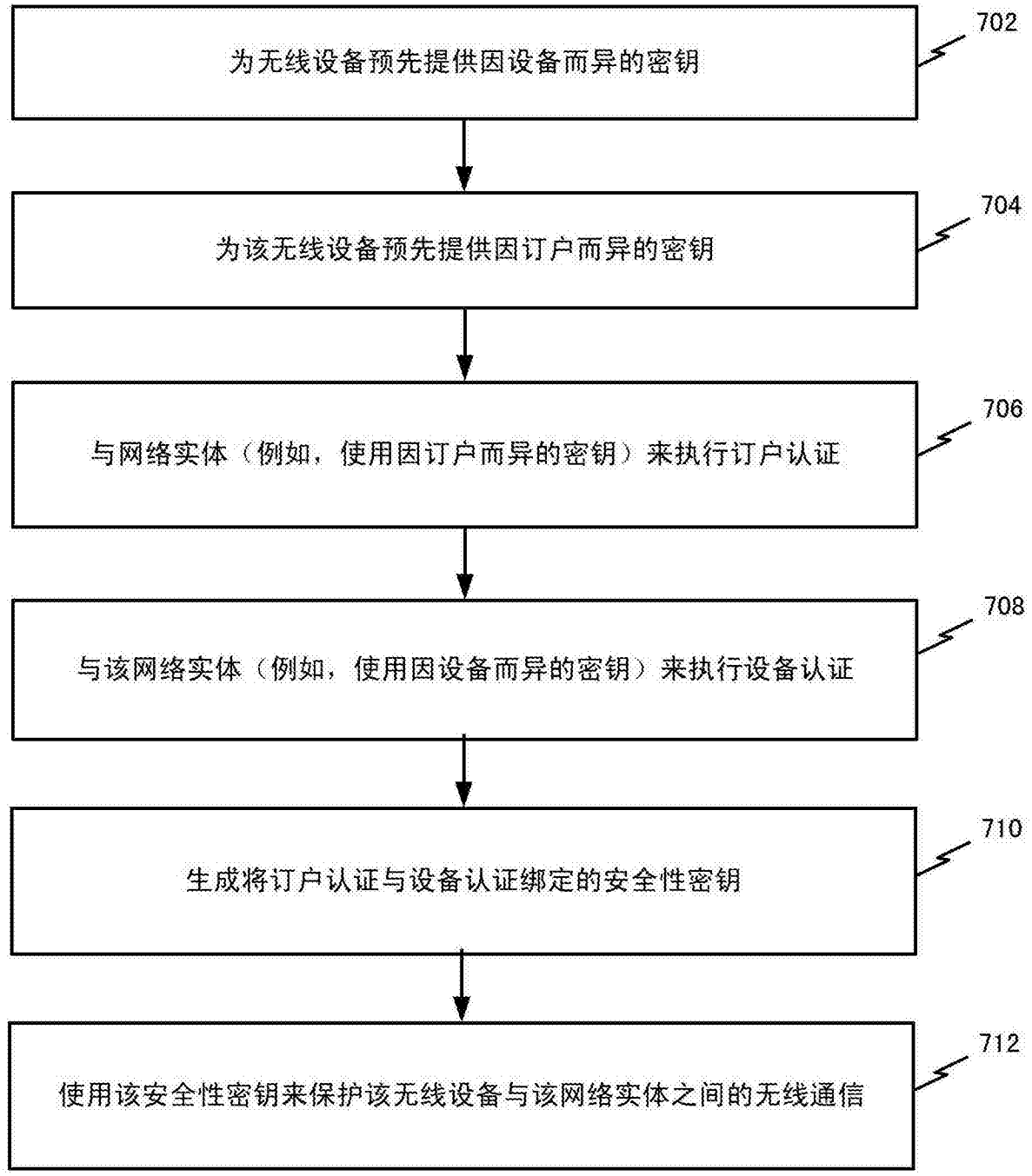

为无线设备预先提供因设备而异的密钥
702
为该无线设备预先提供因订户而异的密钥
704
与网络实体（例如，使用因订户而异的密钥）来执行订户认证
706
与该网络实体（例如，使用因设备而异的密钥）来执行设备认证
708
生成将订户认证与设备认证绑定的安全性密钥
710
使用该安全性密钥来保护该无线设备与该网络实体之间的无线通信
712

图7

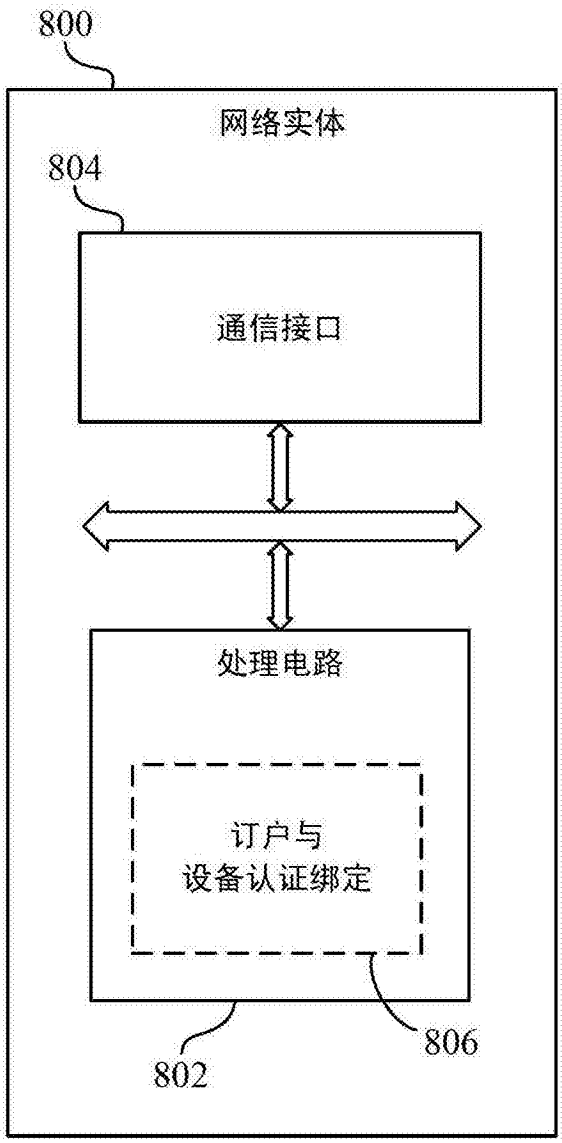


图8

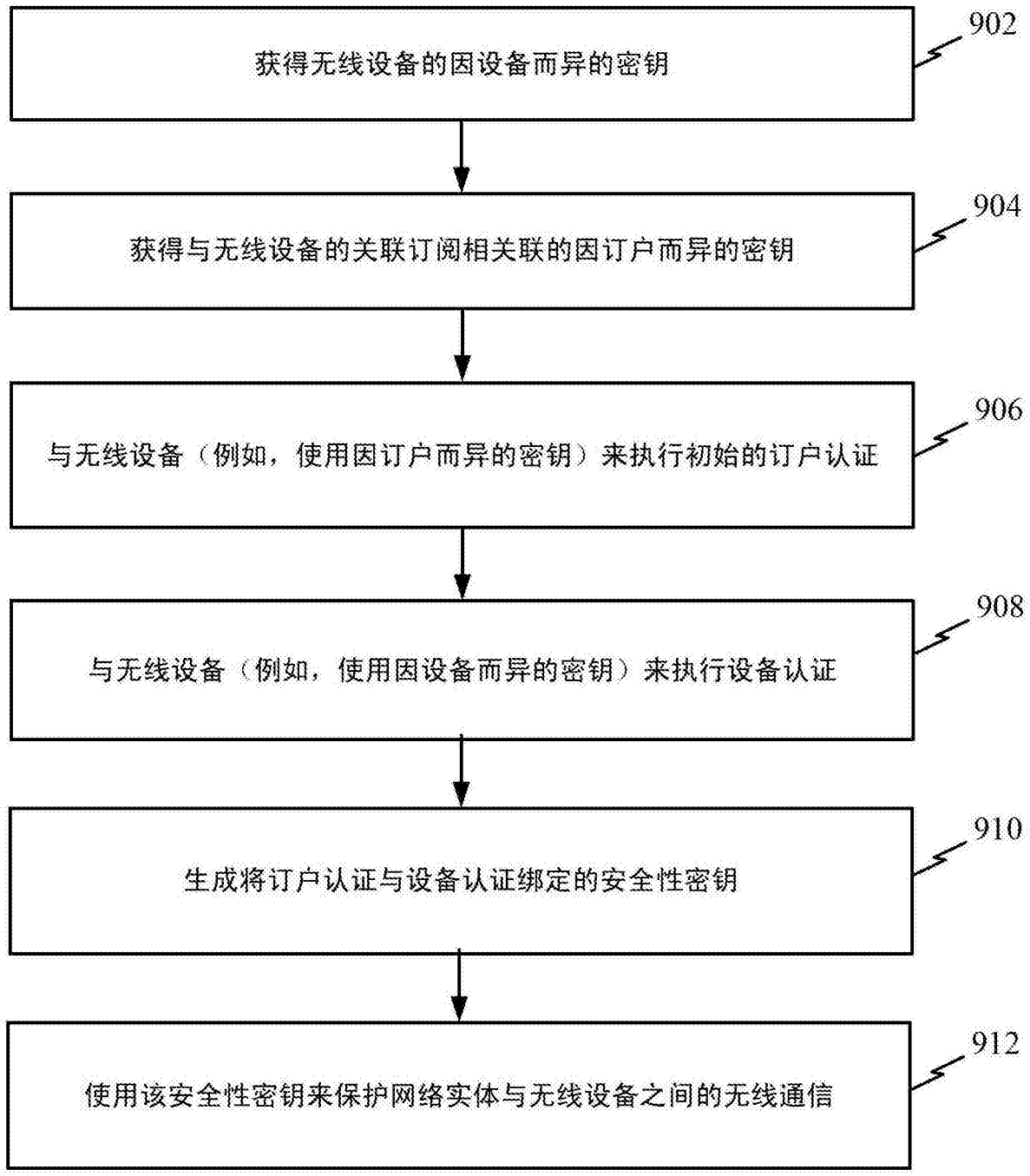

902
获得无线设备的因设备而异的密钥
904
获得与无线设备的关联订阅相关联的因订户而异的密钥
906
与无线设备（例如，使用因订户而异的密钥）来执行初始的订户认证
908
与无线设备（例如，使用因设备而异的密钥）来执行设备认证
910
生成将订户认证与设备认证绑定的安全性密钥
912
使用该安全性密钥来保护网络实体与无线设备之间的无线通信

图9

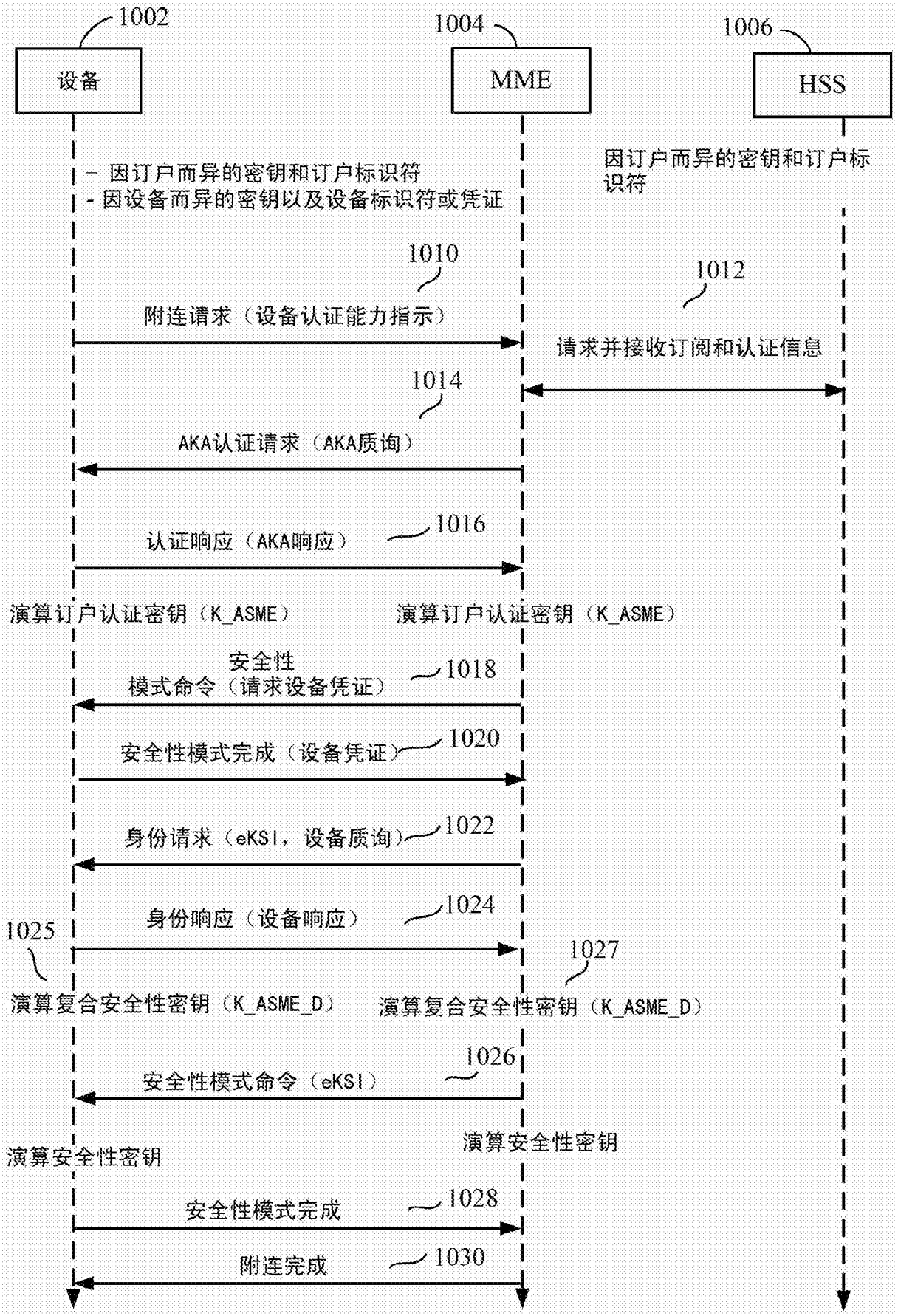

1002
设备
1004
MME
1006
HSS
- 因订户而异的密钥和订户标识符
- 因设备而异的密钥以及设备标识符或凭证
因订户而异的密钥和订户标识符
1010
附连请求（设备认证能力指示）
1012
请求并接收订阅和认证信息
1014
AKA认证请求（AKA质询）
认证响应（AKA响应）
1016
演算订户认证密钥（K_ASME）
演算订户认证密钥（K_ASME）
安全性模式命令（请求设备凭证）
1018
安全性模式完成（设备凭证）
1020
身份请求（eKSI，设备质询）
1022
身份响应（设备响应）
1024
1025
1027
演算复合安全性密钥（K_ASME_D）
演算复合安全性密钥（K_ASME_D）
1026
安全性模式命令（eKSI）
演算安全性密钥
演算安全性密钥
安全性模式完成
1028
附连完成
1030

图10

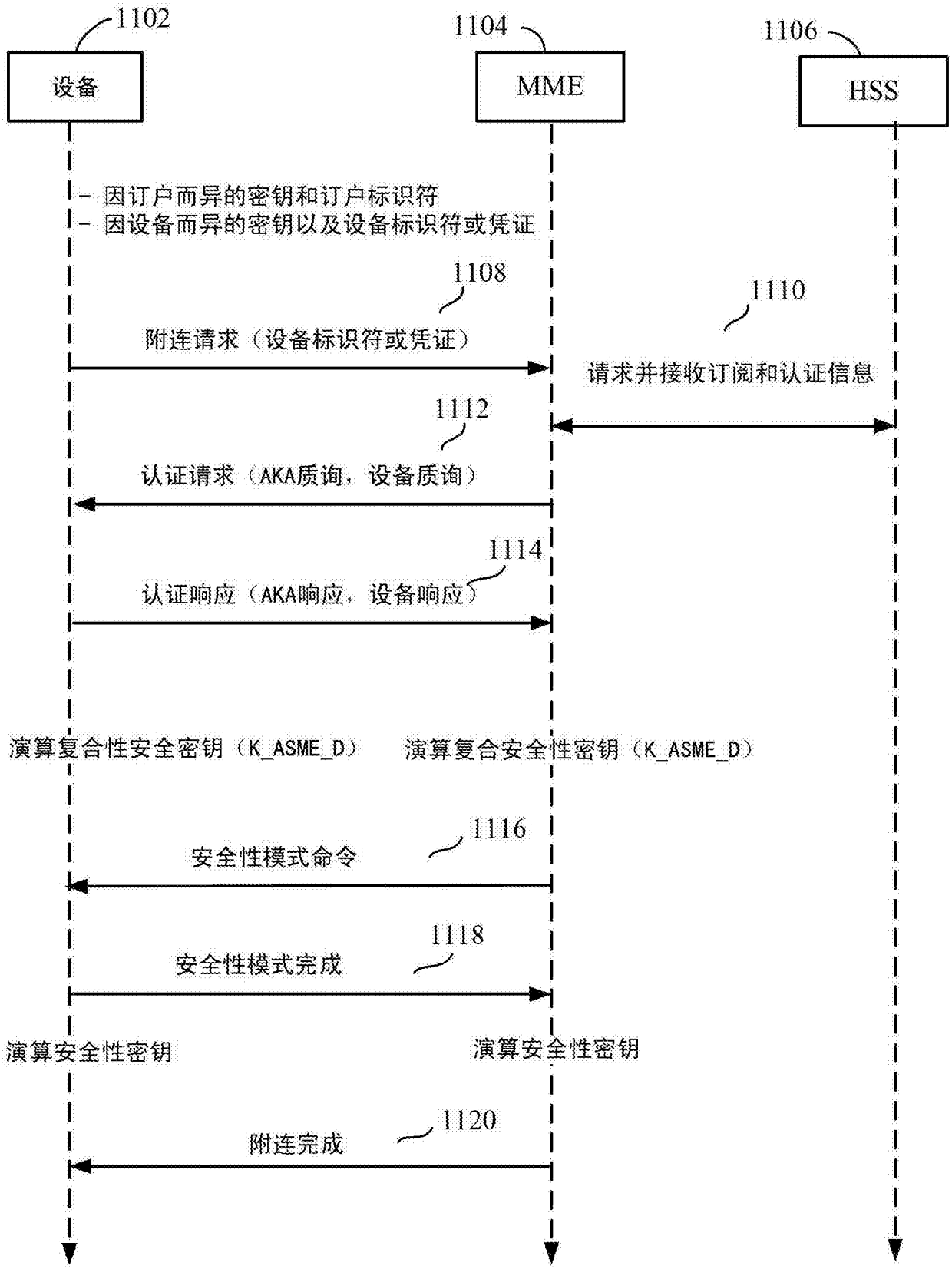

1102
设备
1104
MME
1106
HSS
- 因订户而异的密钥和订户标识符
- 因设备而异的密钥以及设备标识符或凭证
1108
附连请求（设备标识符或凭证）
1110
请求并接收订阅和认证信息
1112
认证请求（AKA质询，设备质询）
1114
认证响应（AKA响应，设备响应）
演算复合性安全密钥（K_ASME_D）
演算复合安全性密钥（K_ASME_D）
1116
安全性模式命令
1118
安全性模式完成
演算安全性密钥
演算安全性密钥
1120
附连完成

图11

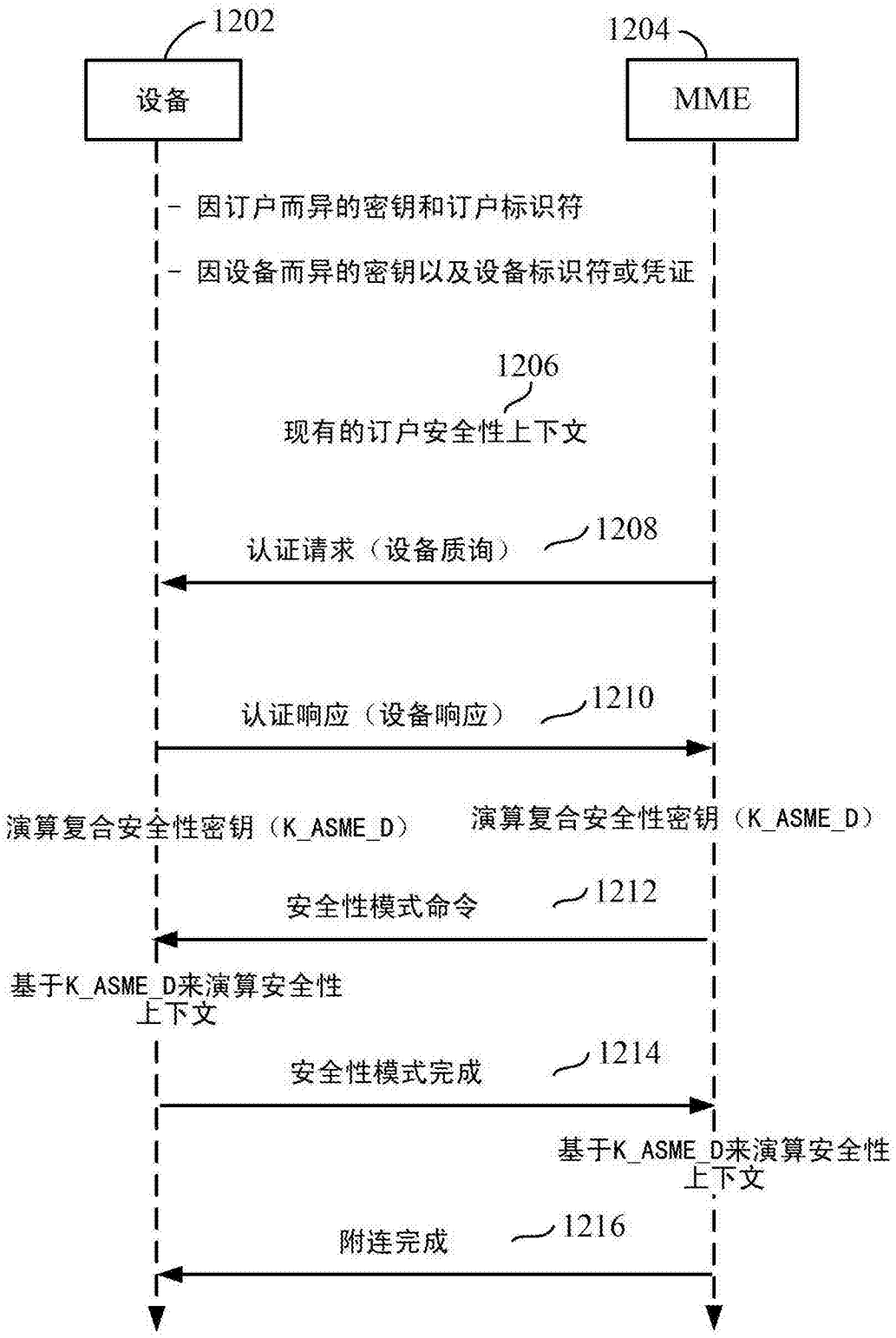

1202
设备
1204
MME
- 因订户而异的密钥和订户标识符
- 因设备而异的密钥以及设备标识符或凭证
1206
现有的订户安全性上下文
认证请求（设备质询）
1208
认证响应（设备响应）
1210
演算复合安全性密钥（K_ASME_D）
演算复合安全性密钥（K_ASME_D）
安全性模式命令
1212
基于K_ASME_D来演算安全性上下文
安全性模式完成
1214
基于K_ASME_D来演算安全性上下文
附连完成
1216

图12