(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 109075973 B
(45)授权公告日 2022.04.05

(21)申请号 201780028149.2
(22)申请日 2017.03.28
(65)同一申请的已公布的文献号
申请公布号 CN 109075973 A
(43)申请公布日 2018.12.21
(30)优先权数据
10201606061P 2016.07.22 SG
(85)PCT国际申请进入国家阶段日
2018.11.07
(86)PCT国际申请的申请数据
PCT/SG2017/050162 2017.03.28
(87)PCT国际申请的公布数据
WO2018/017013 EN 2018.01.25
(73)专利权人 华为国际有限公司
地址 新加坡新加坡市签名大厦樟宜商务园中央2#07-08 51号
(72)发明人 康鑫 王海光 时杰 王贵林 杨艳江
(74)专利代理机构 北京龙双利达知识产权代理有限公司 11329
代理人 王君 肖鹂
(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 9/40(2022.01)
H04W 12/041(2021.01)
H04W 12/03(2021.01)
H04W 12/06(2021.01)
(56)对比文件
CN 103188080 A,2013.07.03
US 7542569 B1,2009.06.02
CN 105743646 A,2016.07.06
US 2010031042 A1,2010.02.04
CN 105790941 A,2016.07.20
CN 103532720 A,2014.01.22
CN 105530099 A,2016.04.27
审查员 许伶俐

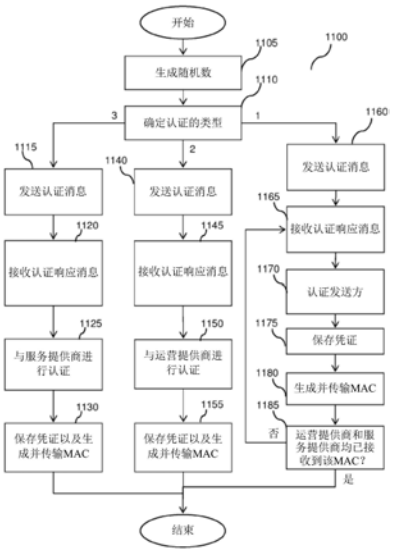
权利要求书10页 说明书26页 附图13页

(54)发明名称

一种使用基于ID的密码术进行网络和服务统一认证的方法

(57)摘要

本发明涉及一种统一认证方法,用于使设备根据基于身份的密码术来认证运营提供商网络和服务提供商网络,所述统一认证方法包括:所述设备生成认证数据包并向所述运营提供商网络传输所述认证数据包;响应于接收到所述认证数据包,所述运营提供商网络的所述单元基于所述认证类型确定认证的类型;响应于确定所述第一类型的认证,所述运营提供商网络的所述单元生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并基于所述SP_ID向所述服务提供商网络的所述单元传输所述认证数据包;以及响应于接收到所述认证数据包,所述服务提供商网络的所述单元生成第二认证响应消息并向所述设备传输所述第二认证响应消息。



CN 109075973 B

1.一种统一认证方法,其特征在于,用于使设备根据基于身份的密码术来认证第一提供商网络和第二提供商网络,所述设备、所述第一提供商网络和所述第二提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥GPK,所述统一认证方法包括:

所述设备生成认证数据包并向所述第一提供商网络传输所述认证数据包,所述认证数据包包括认证类型Auth. Type和所述第二提供商网络的ID,所述ID表示为SP_ID,其中所述Auth. Type包括:第一类型,其中认证涉及所述第一提供商网络的单元和所述第二提供商网络的单元;第二类型,其中认证涉及所述第一提供商网络的所述单元;以及第三类型,其中认证涉及所述第二提供商网络的所述单元;

响应于接收到所述认证数据包,所述第一提供商网络的所述单元基于所述认证类型确定认证的类型;

响应于确定所述第一类型的认证,所述第一提供商网络的所述单元生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并基于所述SP_ID向所述第二提供商网络的所述单元传输所述认证数据包;以及

响应于接收到所述认证数据包,所述第二提供商网络的所述单元生成第二认证响应消息并向所述设备传输所述第二认证响应消息;

所述认证数据包还包括第一随机数RAND1、所述设备的标识Device_ID和设备签名Sig_De;

其中所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第二随机数RAND2;以及

根据基于身份的加密IBE使用所述Device_ID生成包含所述RAND2的第一加密消息m1;

使用所述第一提供商网络的秘密密钥和GPK生成签名Sig_AN;以及

向所述设备传输所述第一认证响应消息,其中所述第一认证响应消息包括所述第一提供商网络的标识AN_ID、所述RAND1、所述m1和所述Sig_AN;

所述方法还包括:

响应于接收到所述第一认证响应消息,所述设备执行以下步骤:

通过使用AN_ID和所述GPK验证所述Sig_AN来认证所述第一提供商网络;

响应于认证成功,使用所述设备的秘密密钥解密m1以获得RAND2;

使用预定义的KDF导出第一会话密钥K_com,其中输入参数是所述RAND1和所述RAND2;

将所述第一会话密钥保存在所述设备的存储器中;

使用MAC生成函数生成第一消息认证码MAC1,其中所述RAND2和K_com作为输入;以及

向所述第一提供商网络的所述单元传输MAC1;

所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第三随机数RAND3;以及

根据IBE使用所述Device_ID生成包含RAND3的第二加密消息m2;

使用所述第二提供商网络的秘密密钥和所述GPK生成签名Sig_SP;以及

向所述设备传输所述第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的标识SP_ID、所述RAND1、所述m2和所述Sig_SP;

所述方法还包括:

响应于接收到所述第二认证响应消息,所述设备执行以下步骤:

通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;

响应于认证成功,使用所述设备的秘密密钥解密m2以获得RAND3;

使用预定义的KDF导出第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

将所述第二会话密钥保存在所述设备的存储器中;

使用MAC生成函数生成第二消息认证码MAC2,其中RAND3和K_ser作为输入;以及

向所述第二提供商网络的所述单元传输MAC2。

2.根据权利要求1所述的统一认证方法,其特征在于,还包括:

响应于接收到MAC1,所述第一提供商网络的所述单元执行以下步骤:

使用预定义的密钥导出函数KDF导出所述第一会话密钥K_com,其中输入参数是所述RAND1和RAND2;

使用相同所述MAC生成函数生成MAC,其中所述RAND2和K_com作为所述输入;

确定MAC1是否等于MAC;以及

响应于MAC1等于MAC,将所述第一会话密钥K_com保存在所述第一提供商网络的所述单元的存储器中。

3.根据权利要求1所述的统一认证方法,其特征在于,还包括:

响应于接收到所述MAC2,所述第二提供商网络的所述单元执行以下步骤:

使用所述预定义的密钥导出函数KDF导出所述第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

使用相同所述MAC生成函数生成MAC,其中RAND3和K_ser作为所述输入;

确定MAC2是否等于MAC;以及

响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

4.根据权利要求1所述的统一认证方法,其特征在于,还包括:

响应于确定所述第二类型的认证,所述第一提供商网络的所述单元生成第三认证响应消息并向所述设备传输所述第三认证响应消息。

5.根据权利要求4所述的统一认证方法,其特征在于,所述认证数据包还包括第一随机数RAND1、所述设备的标识Device_ID和设备签名Sig_De;

其中,所述第一提供商网络的所述单元生成所述第三认证响应消息并向所述设备传输所述第三认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第二随机数RAND2;

根据基于身份的加密IBE使用所述Device_ID生成包含所述RAND2的第一加密消息m1;

使用所述第一提供商网络的秘密密钥和GPK生成签名Sig_AN;以及

向所述设备传输所述第三认证响应消息,其中所述第三认证响应消息包括所述第一提供商网络的标识AN_ID、所述RAND1、所述m1和所述Sig_AN。

6.根据权利要求5所述的统一认证方法,其特征在于,还包括:

响应于接收到所述第三认证响应消息,所述设备执行以下步骤:

通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;

响应于认证成功,使用所述设备的秘密密钥解密m1以获得RAND2;

使用预定义的KDF导出会话密钥,其中输入参数是RAND1和RAND2;

将所述会话密钥保存在所述设备的存储器中;

使用MAC生成函数生成第一消息认证码MAC1,其中RAND2和所述会话密钥作为输入;以及

向所述第一提供商网络的所述单元传输MAC1。

7.根据权利要求6所述的统一认证方法,其特征在于,还包括:

响应于接收到所述MAC1,所述第一提供商网络的所述单元执行以下步骤:

使用预定义的密钥导出函数KDF导出所述会话密钥,其中输入参数是RAND1和RAND2;

使用相同MAC生成函数生成MAC,其中RAND2和所述会话密钥作为所述输入;

确定MAC1是否等于MAC;以及

响应于MAC1等于MAC,将所述会话密钥保存在所述第一提供商网络的所述单元的存储器中。

8.根据权利要求1所述的统一认证方法,其特征在于,还包括:

响应于确定所述第三类型的认证,所述第一提供商网络的所述单元向所述第二提供商网络的所述单元传输所述认证数据包。

9.根据权利要求8所述的统一认证方法,其特征在于,所述认证数据包还包括第一随机数RAND1、所述设备的标识Device_ID和设备签名Sig_De;

其中,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第三随机数RAND3;

根据IBE使用所述Device_ID生成包含RAND3的第二加密消息m2;

使用所述第二提供商网络的秘密密钥和所述GPK生成签名Sig_SP;以及

向所述设备传输所述第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的标识SP_ID、所述RAND1、所述m2和所述Sig_SP。

10.根据权利要求9所述的统一认证方法,其特征在于,还包括:

响应于接收到所述第二认证响应消息,所述设备执行以下步骤:

通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;

响应于认证成功,使用所述设备的所述秘密密钥解密m2以获得RAND3;

使用所述预定义的KDF导出第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

将所述第二会话密钥保存在所述设备的所述存储器中;

使用MAC生成函数生成第二消息认证码MAC2,其中RAND3和K_ser作为输入;以及

向所述第二提供商网络的所述单元传输MAC2。

11.根据权利要求10所述的统一认证方法,其特征在于,还包括:

响应于接收到所述MAC2,所述第二提供商网络的所述单元执行以下步骤:

使用所述预定义的KDF导出所述第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

使用相同MAC生成函数生成MAC,其中RAND3和K_ser作为所述输入;

确定MAC2是否等于MAC;以及

响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

12.一种使用基于身份的密码术的认证框架中的设备,其特征在于,所述认证框架涉及所述设备、第一提供商网络和第二提供商网络,所述设备、所述第一提供商网络的单元和所述第二提供商网络的单元中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥GPK,所述设备包括:

处理器、存储器,其中所述存储器上存储有指令,并且所述指令可由所述处理器执行以用于:

生成认证类型Auth. Type,其中所述Auth. Type包括:第一类型,其中认证涉及所述第一提供商网络的所述单元和所述第二提供商网络的所述单元;第二类型,其中认证涉及所述第一提供商网络的所述单元;以及第三类型,其中认证涉及所述第二提供商网络的所述单元;

生成认证数据包,其中所述认证数据包包括Auth. Type和第二提供商网络的ID,所述ID表示为SP_ID;以及

向所述第一提供商网络的所述单元传输所述认证数据包;

所述指令还包括用于以下操作的指令:

生成第一随机数RAND1;

生成设备签名Sig_De,其中所述认证数据包还包括RAND1、所述设备的标识Device_ID和Sig_De;

响应于所述Auth. Type是所述第一类型或第二类型的认证,所述指令还包括用于以下操作的指令:

从所述第一提供商网络的所述单元接收第一认证响应消息,其中所述第一认证响应消息包括所述第一提供商网络的标识AN_ID、RAND1、由所述第一提供商网络的所述单元根据基于身份的加密IBE使用所述Device_ID生成的包含第二随机数RAND2的第一加密消息m1,以及使用所述第一提供商网络的秘密密钥和所述GPK的签名Sig_AN;

通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;

响应于认证成功,使用所述设备的秘密密钥解密m1以获得RAND2;

使用预定义的KDF导出第一会话密钥K_com,其中输入参数是RAND1和RAND2;

将所述第一会话密钥保存在所述设备的所述存储器中;

使用MAC生成函数生成第一消息认证码MAC1,其中RAND2和K_com作为输入;以及

向所述第一提供商网络的所述单元传输MAC1;

响应于所述Auth. Type是所述第一类型的认证,所述指令还包括用于以下操作的指令:

从所述第二提供商网络的所述单元接收第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的ID,所述ID表示为SP_ID、RAND1、由所述第二提供商网络的所述单元根据基于身份的加密IBE使用所述Device_ID生成的包含第三随机数RAND3的第二加

密消息m2,以及使用所述第二提供商网络的所述秘密密钥和所述GPK的签名Sig_SP;

通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;

响应于认证成功,使用所述设备的秘密密钥解密m2以获得RAND3;

使用所述预定义的KDF导出第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

将所述第二会话密钥保存在所述设备的所述存储器中;

使用MAC生成函数生成第二消息认证码MAC2,其中RAND3和K_ser作为输入;以及

向所述第二提供商网络的所述单元传输MAC2。

13.根据权利要求12所述的设备,其特征在于,响应于所述Auth. Type是所述第三类型的认证,所述指令还包括用于以下操作的指令:

从所述第二提供商网络的所述单元接收认证响应消息,其中所述认证响应消息包括所述第二提供商网络的ID,所述ID表示为SP_ID、RAND1、由所述第二提供商网络的所述单元根据基于身份的加密IBE使用所述Device_ID生成的包含的第三随机数RAND3的第二加密消息m2,以及使用第二提供商网络的秘密密钥和所述GPK的签名Sig_SP;

通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;

响应于认证成功,使用所述设备的所述秘密密钥解密所述m2以获得所述RAND3;

使用所述预定义的KDF导出所述第二会话密钥K_ser,其中输入参数是RAND1和所述RAND3;

将所述第二会话密钥保存在所述设备的所述存储器中;

使用MAC生成函数生成第二消息认证码MAC2,其中RAND3和K_ser作为所述输入;以及

向所述第二提供商网络的所述单元传输所述第二消息认证码MAC2。

14.一种认证框架中的运营提供商网络,其特征在于,所述认证框架涉及设备、服务提供商网络和所述运营提供商网络,所述设备、运营提供商网络和服务提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥GPK,所述运营提供商网络包括:

认证节点,包括处理器、存储器,其中所述存储器上存储有指令,并且所述指令可由所述处理器执行以用于:

从所述设备接收认证数据包,所述认证数据包包括认证类型Auth. Type和服务提供商网络的ID,所述ID表示为SP_ID,其中所述Auth. Type包括:第一类型,其中认证涉及运营商和服务提供商网络;第二类型,其中认证涉及所述运营提供商网络;以及第三类型,其中认证涉及所述服务提供商网络;

基于所述认证类型确定认证的类型;

响应于确定所述第一类型的认证,生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并向所述服务提供商网络的单元传输所述认证数据包;

响应于确定所述第二类型的认证,生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息;以及

响应于确定所述第三类型的认证,向所述服务提供商网络的所述单元传输所述认证数据包;

所述认证数据包还包括第一随机数RAND1、所述设备的标识Device_ID和设备签名Sig_De;

其中所述指令存储在所述认证节点的所述存储器上以生成所述第一认证响应消息并

向所述设备传输所述第一认证响应消息,包括用于以下操作的指令:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第二随机数RAND2;

根据基于身份的加密IBE使用所述Device_ID生成包含RAND2的第一加密消息m1;

使用所述运营提供商网络的秘密密钥和所述GPK生成签名Sig_AN;以及

向所述设备传输所述第一认证响应消息,其中所述第一认证响应消息包括所述运营提供商网络的标识AN_ID、RAND1、m1和Sig_AN。

15.根据权利要求14所述的运营提供商网络,其特征在于,所述认证节点的所述存储器上存储有指令,所述指令可由所述处理器执行以用于:

接收所述设备通过MAC生成函数生成的第一消息认证码MAC1,其中RAND2和第一会话密钥K_com作为输入;

使用预定义的密钥导出函数KDF导出所述第一会话密钥K_com,其中输入参数是RAND1和RAND2;

使用所述MAC生成函数生成MAC,其中RAND2和K_com作为输入;

确定MAC1是否等于MAC;以及

响应于MAC1等于MAC,将所述第一会话密钥K_com保存在所述认证节点的所述存储器中。

16.一种认证框架中的服务提供商网络,其特征在于,所述认证框架涉及设备、运营提供商网络和所述服务提供商网络,所述设备、运营提供商网络和服务提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥GPK,所述服务提供商网络包括:

认证单元,包括处理器、存储器,其中所述存储器上存储有指令,并且所述指令可由所述处理器执行以用于:

从所述运营提供商网络接收认证数据包,所述认证数据包包括第一随机数RAND1、认证类型Auth. Type、服务提供商网络的ID,所述ID表示为SP_ID、所述设备的标识Device_ID和设备签名Sig_De,其中所述Auth. Type包括:第一类型,其中认证涉及所述运营提供商和服务提供商网络;第二类型,其中认证涉及所述运营提供商网络;以及第三类型,其中认证涉及所述服务提供商网络;

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第三随机数RAND3;

所述指令还包括用于以下操作的指令:

根据IBE使用所述Device_ID生成包含RAND3的第二加密消息m2;

使用所述服务提供商网络的秘密密钥和所述GPK生成签名Sig_SP;以及

向所述设备传输第二认证响应消息,其中所述第二认证响应消息包括所述服务提供商网络的标识SP_ID、RAND1、m2和Sig_SP。

17.根据权利要求16所述的服务提供商网络,其特征在于,所述指令还包括用于以下操作的指令:

接收所述设备通过MAC生成函数生成的第二消息认证码MAC2,其中RAND3和第二会话密钥K_ser作为输入;

使用预定义的KDF导出所述第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

使用所述MAC生成函数生成MAC,其中RAND3和K_ser作为输入;

确定MAC2是否等于MAC;以及

响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述认证单元的存储器中。

18.一种统一认证方法,其特征在于,用于使设备根据基于身份的密码术来认证第一提供商网络和第二提供商网络,所述设备、所述第一提供商网络和所述第二提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥GPK,所述统一认证方法包括:

所述设备生成随机数RAND1并导出第一对称密钥K_C和第二对称密钥K_S;

所述设备生成认证数据包并向第一提供商网络传输所述认证数据包,所述认证数据包包括RAND1、认证类型Auth. Type、所述第二提供商网络的ID,所述ID表示为SP_ID、所述设备的标识Device_ID和设备签名Sig_De,其中所述Auth. Type包括:第一类型,其中认证涉及所述第一提供商网络的单元和所述第二提供商网络的单元;第二类型,其中认证涉及所述第一提供商网络的所述单元;以及第三类型,其中认证涉及所述第二提供商网络的所述单元;

响应于接收到所述认证数据包,所述第一提供商网络的所述单元基于所述认证类型确定认证的类型;

响应于确定所述第一类型的认证,所述第一提供商网络的所述单元生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并基于所述SP_ID向所述第二提供商网络的所述单元传输所述认证数据包;以及

响应于接收到所述认证数据包,所述第二提供商网络的所述单元生成第二认证响应消息并向所述设备传输所述第二认证响应消息;

所述第一对称密钥K_C通过所述设备的私钥和所述第一提供商网络的所述单元的标识BS_ID导出,所述第二对称密钥K_S通过所述设备的私钥和所述第二提供商网络的所述单元的所述SP_ID导出;

所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;

响应于验证成功,生成第二随机数RAND2;

通过所述第一提供商网络的私钥和所述Device_ID导出所述第一对称密钥K_C;

使用所述K_C生成包含RAND2的第一加密消息m1,并且可使用以下方式表示:m1=En(RAND2, K_C);

使用所述第一提供商网络的秘密密钥和所述GPK生成签名Sig_AN;以及

生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,其中所述第一认证响应消息包括所述第一提供商网络的标识AN_ID、RAND1、m1和Sig_AN;

所述方法还包括:

响应于接收到所述第一认证响应消息,所述设备执行以下步骤:

通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;

响应于认证成功,使用所述第一对称密钥K_C解密m1以获得RAND2;

使用预定义的KDF导出第一会话密钥K_com,其中输入参数是RAND1和RAND2;

将所述第一会话密钥保存在所述设备的存储器中;

使用MAC生成函数生成第一消息认证码MAC1,其中RAND2和K_com作为输入;以及

向所述第一提供商网络的所述单元传输MAC1;

所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第三随机数RAND3;

通过所述第二提供商网络的私钥和所述Device_ID导出所述第二对称密钥K_S;

使用所述K_S生成包含RAND3的第二加密消息m2;

使用所述第二提供商网络的所述秘密密钥和所述GPK生成签名Sig_SP;以及

生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的标识SP_ID、RAND1、m2和Sig_SP;

所述方法还包括:

响应于接收到所述第二认证响应消息,所述设备执行以下步骤:

通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;

响应于认证成功,使用所述第二对称密钥K_S解密m2以获得RAND3;

使用所述预定义的KDF导出第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

将所述第二会话密钥保存在所述设备的所述存储器中;

使用MAC生成函数生成第二消息认证码MAC2,其中RAND3和K_ser作为输入;以及

向所述第二提供商网络的所述单元传输MAC2。

19.根据权利要求18所述的统一认证方法,其特征在于,还包括:

响应于接收到所述MAC1,所述第一提供商网络的所述单元执行以下步骤:

使用所述预定义的密钥导出函数KDF导出所述第一会话密钥K_com,其中输入参数是RAND1和RAND2;

使用相同MAC生成函数生成MAC,其中RAND2和K_com作为所述输入;

确定MAC1是否等于MAC;以及

响应于MAC1等于MAC,将所述第一会话密钥K_com保存在所述第一提供商网络的所述单元的存储器中。

20.根据权利要求19所述的统一认证方法,其特征在于,还包括:

响应于接收到所述MAC2,所述第二提供商网络的所述单元执行以下步骤:

使用所述预定义的KDF导出第二会话密钥K_ser,其中输入参数是RAND1和RAND3;

使用相同所述MAC生成函数生成MAC,其中RAND3和K_ser作为所述输入;

确定MAC2是否等于MAC;

响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

21.一种统一认证方法,其特征在于,用于使设备根据基于身份的密码术来认证第一提供商网络和第二提供商网络,所述设备、所述第一提供商网络和所述第二提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥GPK,所述统一认证方法包括:

所述设备生成随机数RAND1并导出Diffie-Hellman公钥A,所述Diffie-Hellman公钥A由$A=g^{RAND1} \bmod p$导出,其中mod表示取模运算;

所述设备生成认证数据包并向第一提供商网络传输所述认证数据包,所述认证数据包包括Diffie-Hellman公钥A、认证类型Auth. Type、所述第二提供商网络的ID,所述ID表示为SP_ID、所述设备的标识Device_ID以及设备签名Sig_De,其中所述Auth. Type包括:第一类型,其中认证涉及所述第一提供商网络的单元和所述第二提供商网络的单元;第二类型,其中认证涉及所述第一提供商网络的所述单元;以及第三类型,其中认证涉及所述第二提供商网络的所述单元;

响应于接收到所述认证数据包,所述第一提供商网络的所述单元基于所述认证类型确定认证的类型;

响应于确定所述第一类型的认证,所述第一提供商网络的所述单元生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并基于所述SP_ID向所述第二提供商网络的所述单元传输所述认证数据包;以及

响应于接收到所述认证数据包,所述第二提供商网络的所述单元生成第二认证响应消息并向所述设备传输所述第二认证响应消息;

所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第二随机数RAND2;

所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤还包括:

导出Diffie-Hellman公钥B,其中$B=g^{RAND2} \bmod p$;以及

导出第一会话密钥K_com,其中$K_com=A^{RAND2} \bmod p$;

所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤还包括:

使用所述第一提供商网络的秘密密钥和所述GPK生成签名Sig_AN;以及

生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,其中所述第一认证响应消息包括所述第一提供商网络的标识AN_ID、Diffie-Hellman公钥A、Diffie-Hellman公钥B和Sig_AN;

所述统一认证方法包括:

响应于接收到所述第一认证响应消息,所述设备执行以下步骤:

通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;

响应于认证成功,使用所述Diffie-Hellman公钥B导出所述第一会话密钥K_com,其中$K_com=B^{RAND2} \bmod p$;

将所述第一会话密钥保存在所述设备的存储器中;

使用MAC生成函数生成第一消息认证码MAC1,其中所述Diffie-Hellman公钥B和K_com作为输入;以及

向所述第一提供商网络的所述单元传输MAC1。

22.根据权利要求21所述的统一认证方法,其特征在于,还包括:

响应于接收到所述MAC1,所述第一提供商网络的所述单元执行以下步骤:

使用相同MAC生成函数生成MAC,其中Diffie-Hellman公钥B和K_com作为所述输入;

确定MAC1是否等于MAC;以及

响应于MAC1等于MAC,将所述第一会话密钥K_com保存在所述第一提供商网络的所述单元的存储器中。

23.根据权利要求22所述的统一认证方法,其特征在于,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:

使用所述Device_ID和所述GPK验证所述Sig_De;以及

响应于验证成功,生成第三随机数RAND3。

24.根据权利要求23所述的统一认证方法,其特征在于,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:

导出Diffie-Hellman公钥C,其中$C=g^{RAND3} \bmod p$;以及

导出第二会话密钥K_ser,其中$K_ser=A^{RAND3} \bmod p$。

25.根据权利要求24所述的统一认证方法,其特征在于,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤还包括:

使用所述第二提供商网络的秘密密钥和所述GPK生成签名Sig_SP;以及

生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的ID,所述ID表示为SP_ID、Diffie-Hellman公钥A、Diffie-Hellman公钥C和Sig_SP。

26.根据权利要求25所述的统一认证方法,其特征在于,还包括:

响应于接收到所述第二认证响应消息,所述设备执行以下步骤:

通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;

响应于认证成功,使用所述Diffie-Hellman公钥C导出所述第二会话密钥K_ser,其中$K_ser=C^{RAND3} \bmod p$;

将所述第二会话密钥保存在所述设备的所述存储器中;

使用MAC生成函数生成第二消息认证码MAC2,其中所述Diffie-Hellman公钥C和K_ser作为输入;以及

向所述第二提供商网络的所述单元传输MAC2。

27.根据权利要求26所述的统一认证方法,其特征在于,还包括:

响应于接收到所述MAC2,所述第二提供商网络的所述单元执行以下步骤:

使用相同MAC生成函数生成MAC,其中Diffie-Hellman公钥C和K_ser作为所述输入;

确定MAC2是否等于MAC;以及

响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

一种使用基于ID的密码术进行网络和服务统一认证的方法

技术领域

[0001] 本发明涉及一种运营提供商和服务提供商之间的认证框架的方法和系统。具体地,本发明涉及一种根据基于ID的密码术的运营提供商和服务提供商之间的统一认证框架的方法和系统。

背景技术

[0002] 在当前的3G/4G蜂窝网络中,在用户设备(User Equipment,UE)和网络之间采用相互认证,以保护移动设备和网络在数据通信期间不被窃听或操纵。3G/4G采用的当前相互认证协议是认证和密钥协商(Authentication and Key Agreement,AKA)。为了执行AKA,UE和核心网(Core Network,CN)需要在两侧都保存一些预共享的机密信息。

[0003] 在3G/4G网络中,在网络侧,凭证保存在名为归属用户服务器(Home Subscriber Server,HSS)的服务器中;而在UE侧,凭证保存在名为全球用户身份模块(Universal Subscriber Identity Module,USIM)卡的独立设备中。USIM卡是内嵌在UE内USIM槽中的计算设备。USIM和UE可以通过特殊接口交换信息。目前,3G/4G网络在相互认证中使用对称密钥。因此,对于给定的国际移动用户识别码(International Mobile Subscriber Identification,IMSI),保存在相应USIM和HSS中的凭证是相同的。

[0004] 当UE想要接入网络并传输和接收数据时,UE必须基于AKA执行与CN的相互认证。图1所示的AKA过程称为网络接入认证。在AKA过程中,UE首先向移动性管理实体(Mobility Management Entity,MME)发送附着请求。响应于接收到附着请求,MME将附着请求转发到HSS,HSS随后基于与UE共享的凭证生成认证向量。将认证向量发送到MME,MME随后向UE发送包含认证材料的认证数据响应。UE对网络进行认证,然后将包含认证码的用户认证发送给MME。进而,MME对认证码进行验证并对UE进行认证。在认证之后,UE与MME和eNB交换密钥材料以进一步生成用于控制和数据面的会话密钥。

[0005] 在传统的通信系统中,当用户想要使用任何第三方服务时,必须进行服务认证。通常,服务认证基于“用户名+密码”,其安全级别远低于网络接入认证。用户必须首先进行网络接入认证,然后进行服务认证才能使用该服务。因此,必须维护两个认证系统以提供这种类型的认证服务。

[0006] 因此,本领域技术人员正努力为用户提供更好的认证系统和方法,以便与运营提供商和服务提供商进行认证。

发明内容

[0007] 本发明实施例提供的系统和方法解决了上述和其它问题,并且在本领域中取得了进步。根据本发明的系统和方法实施例的第一个优点是仅需要一个认证消息来认证蜂窝网络和服务提供商,这极大地方便了用户并减少了网络开销。根据本发明的系统和方法实施例的第二个优点是网络和服务统一认证框架实现了与网络认证相同的安全级别,该安全级别远高于服务认证的级别。

[0008] 根据本发明的一方面，通过以下方式提供了一种统一认证方法，用于使设备根据基于身份的密码术来认证第一提供商网络和第二提供商网络，其中所述设备、第一提供商网络和第二提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥(Global Public Key，GPK)。所述统一认证方法包括：所述设备生成认证数据包并向所述第一提供商网络传输所述认证数据包，所述认证数据包包括认证类型(Auth. Type)和所述第二提供商网络的ID(SP_ID)，其中所述Auth. Type包括：第一类型，其中认证涉及所述第一提供商网络的单元和所述第二提供商网络的单元；第二类型，其中认证涉及所述第一提供商网络的所述单元；以及第三类型，其中认证涉及所述第二提供商网络的所述单元；响应于接收到所述认证数据包，所述第一提供商网络的所述单元基于所述认证类型确定认证的类型；响应于确定所述第一类型的认证，所述第一提供商网络的所述单元生成第一认证响应消息并向所述设备传输所述第一认证响应消息，并基于所述SP_ID向所述第二提供商网络的所述单元传输所述认证数据包；以及响应于接收到所述认证数据包，所述第二提供商网络的所述单元生成第二认证响应消息并向所述设备传输所述第二认证响应消息。根据本发明的实施例，所述Sig_De由所述设备使用所述设备的所述秘密密钥和所述全局公钥(Global Public Key，GPK)生成。根据本实施例的实施例，所述认证数据包还包括第一随机数(RAND1)、所述设备的标识(Device_ID)和设备签名(Sig_De)。

[0009] 根据本发明实施例，所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤包括：使用所述Device_ID和所述GPK验证所述Sig_De；以及响应于验证成功，生成第二随机数(RAND2)。随后，所述方法根据基于身份的加密(Identity Based Encryption，IBE)使用所述Device_ID生成包含RAND2的第一加密消息m1；使用所述第一提供商网络的所述秘密密钥和GPK生成签名(Sig_AN)；以及向所述设备传输所述第一认证响应消息，其中所述第一认证响应消息包括所述第一提供商网络的标识(AN_ID)、RAND1、m1和Sig_AN。

[0010] 根据本发明实施例，所述方法还包括：响应于接收到所述第一认证响应消息，所述设备执行以下步骤：通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络；响应于认证成功，使用所述设备的所述秘密密钥解密m1以获得RAND2；使用所述预定义的KDF导出第一会话密钥(K_com)，其中输入参数是RAND1和RAND2；将所述第一会话密钥保存在所述设备的所述存储器中；使用MAC生成函数生成第一消息认证码(MAC1)，其中RAND2和K_com作为所述输入；以及向所述第一提供商网络的所述单元传输MAC1。

[0011] 根据本发明实施例，所述方法还包括：响应于接收到所述MAC1，所述第一提供商网络的所述单元执行以下步骤：使用预定义的密钥导出函数(Key Derivation Function，KDF)导出所述第一会话密钥(K_com)，其中输入参数是RAND1和RAND2；使用所述相同MAC生成函数生成MAC，其中RAND2和K_com作为所述输入；确定MAC1是否等于MAC；以及响应于MAC1等于MAC，将所述第一会话密钥K_com保存在所述第一提供商网络的所述单元的存储器中。

[0012] 根据本发明实施例，所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括：使用所述Device_ID和所述GPK验证所述Sig_De；以及响应于验证成功，生成第三随机数(RAND3)；根据IBE使用所述Device_ID生成包含RAND3的第二加密消息(m2)；使用所述第二提供商网络的所述秘密密钥和所述GPK生成签名(Sig_SP)；以及生成所述第二认证响应消息并向所述设备传输所述第二认证响应

消息,其中所述第二认证响应消息包括所述第二提供商网络的标识(SP_ID)、RAND1、m2和Sig_SP。

[0013] 根据本发明实施例,所述方法还包括:响应于接收到所述第二认证响应消息,所述设备执行以下步骤:通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;响应于认证成功,使用所述设备的所述秘密密钥解密m2以获得RAND3;使用所述预定义的KDF导出第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;将所述第二会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第二消息认证码(MAC1),其中RAND3和K_ser作为所述输入;以及向所述第二提供商网络的所述单元传输MAC2。

[0014] 根据本发明实施例,所述方法还包括:响应于接收到所述MAC2,所述第二提供商网络的所述单元执行以下步骤:使用所述预定义的KDF导出所述第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;使用所述相同MAC生成函数生成MAC,其中RAND3和K_ser作为所述输入;确定MAC2是否等于MAC;以及响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

[0015] 根据本发明实施例,所述方法还包括:响应于确定所述第二类型的认证,所述第一提供商网络的所述单元生成第三认证响应消息并向所述设备传输所述第三认证响应消息。

[0016] 根据本发明实施例,所述第一提供商网络的所述单元生成所述第三认证响应消息并向所述设备传输所述第三认证响应消息的步骤包括:使用所述Device_ID和所述GPK验证所述Sig_De;响应于验证成功,生成第二随机数(RAND2)。

[0017] 根据本发明实施例,所述第一提供商网络的所述单元生成所述第三认证响应消息并向所述设备传输所述第三认证响应消息的步骤还包括:根据基于身份的加密(Identity Based Encryption,IBE)使用所述Device_ID生成包含所述RAND2的第一加密消息(m1);使用所述第一提供商网络的所述秘密密钥和GPK生成签名(Sig_AN);生成所述第三认证响应消息并向所述设备传输所述第三认证响应消息,其中所述第三认证响应消息包括所述第一提供商网络的标识(AN_ID)、RAND1、m1和Sig_AN。

[0018] 根据本发明实施例,所述方法还包括:响应于接收到所述第三认证响应消息,所述设备执行以下步骤:通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;响应于认证成功,使用所述设备的所述秘密密钥解密m1以获得RAND2;使用所述预定义的KDF导出第一会话密钥(K_com),其中输入参数是RAND1和RAND2;将所述会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第一消息认证码(MAC1),其中RAND2和K_com作为所述输入;以及向所述第一提供商网络的所述单元传输MAC1。

[0019] 根据本发明实施例,所述方法还包括:响应于接收到所述MAC1,所述第一提供商网络的所述单元执行以下步骤:使用预定义的密钥导出函数(Key Derivation Function,KDF)导出所述会话密钥(K_com),其中输入参数是RAND1和RAND2;使用所述相同MAC生成函数生成MAC,其中RAND2和K_com作为所述输入;确定MAC1是否等于MAC;以及响应于MAC1等于MAC,将所述会话密钥K_com保存在所述第一提供商网络的所述单元的存储器中。

[0020] 根据本发明实施例,所述方法还包括:响应于确定所述第三类型的认证,所述第一提供商网络的所述单元向所述第二提供商网络的所述单元传输所述认证数据包。

[0021] 根据本发明实施例,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:使用所述Device_ID和所述GPK验证

所述Sig_De;响应于验证成功,生成第三随机数(RAND3)。

[0022] 根据本发明实施例,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤还包括:根据IBE使用所述Device_ID生成包含RAND3的第二加密消息(m2);使用所述第二提供商网络的所述秘密密钥和所述GPK生成签名(Sig_SP);生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的标识(SP_ID)、RAND1、m2和Sig_SP。

[0023] 根据本发明实施例,所述方法还包括:响应于接收到所述第二认证响应消息,所述设备执行以下步骤:通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;响应于认证成功,使用所述设备的所述秘密密钥解密m2以获得RAND3;使用所述预定义的KDF导出第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;将所述第二会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第二消息认证码(MAC1),其中RAND3和K_ser作为所述输入;以及向所述第二提供商网络的所述单元传输MAC2。

[0024] 根据本发明实施例,所述方法还包括:响应于接收到所述MAC2,所述第二提供商网络的所述单元执行以下步骤:使用所述预定义的KDF导出所述第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;使用所述相同MAC生成函数生成MAC,其中RAND3和K_ser作为所述输入;确定MAC2是否等于MAC;以及响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

[0025] 根据本发明的另一方面,提供了一种使用基于身份的密码术的认证框架中的设备,所述认证框架涉及所述设备、第一提供商网络和第二提供商网络,其中所述设备、所述第一提供商网络的单元和所述第二提供商网络的单元中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥(Global Public Key,GPK),所述设备包括:处理器、存储器和指令,其中所述指令存储在所述存储器上并且可由所述处理器执行以用于:生成认证类型(Auth. Type),其中所述Auth. Type包括:第一类型,其中认证涉及所述第一提供商网络的所述单元和所述第二提供商网络的所述单元;第二类型,其中认证涉及所述第一提供商网络的所述单元;以及第三类型,其中认证涉及所述第二提供商网络的所述单元;生成认证数据包,其中所述认证数据包包括Auth. Type和服务提供商网络的ID(SP_ID);以及向所述第一提供商网络的所述单元传输所述认证数据包。所述Sig_De通过所述设备的所述秘密密钥和所述GPK生成。

[0026] 根据本发明实施例,所述指令还包括用于以下操作的指令:生成第一随机数(RAND1);以及生成设备签名(Sig_De),其中所述认证数据包还包括RAND1、所述设备的标识(Device_ID)和Sig_De。

[0027] 根据本发明实施例,响应于所述Auth. Type是所述第一类型或第二类型的认证,所述指令还包括用于以下操作的指令:从所述第一提供商网络的所述单元接收第一认证响应消息,其中所述第一认证响应消息包括所述第一提供商网络的标识(AN_ID)、RAND1、由所述第一提供商网络的所述单元根据基于身份的加密(Identity Based Encryption,IBE)使用所述Device_ID生成的包含第二随机数(RAND2)的第一加密消息m1,以及使用所述第一提供商网络的所述秘密密钥和所述GPK的签名(Sig_AN);通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;响应于认证成功,使用所述设备的所述秘密密钥解密m1以获得RAND2;使用所述预定义的KDF导出所述第一会话密钥(K_com),其中输入参数是RAND1

和RAND2;将所述第一会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第一消息认证码(MAC1),其中RAND2和K_com作为所述输入;以及向所述第一提供商网络的所述单元传输MAC1。

[0028] 根据本发明实施例,响应于所述Auth. Type是所述第一类型或第二类型的认证,所述指令还包括用于以下操作的指令:从所述第二提供商网络的所述单元接收第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的标识(SP_ID)、RAND1、由所述第二提供商网络的所述单元根据基于身份的加密(Identity Based Encryption,IBE)使用所述Device_ID生成的包含第三随机数(RAND3)的第二加密消息m2,以及使用所述第二提供商网络的所述秘密密钥和所述GPK的签名(Sig_SP);通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;响应于认证成功,使用所述设备的所述秘密密钥解密m2以获得RAND3;使用所述预定义的KDF导出所述第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;将所述第二会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第二消息认证码(MAC1),其中RAND3和K_ser作为所述输入;以及向所述第二提供商网络的所述单元传输MAC2。

[0029] 根据本发明实施例,响应于所述Auth. Type是所述第三类型的认证,所述指令还包括用于以下操作的指令:从所述第二提供商网络的所述单元接收认证响应消息,其中所述认证响应消息包括所述第二提供商网络的标识(SP_ID)、RAND1、由所述第二提供商网络的所述单元根据基于身份的加密(Identity Based Encryption,IBE)使用所述Device_ID生成的包含第二随机数(RAND2)的加密消息m,以及使用所述服务提供商网络的所述秘密密钥和所述GPK的签名(Sig_SP);通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;响应于认证成功,使用所述设备的所述秘密密钥解密m2以获得RAND2;使用所述预定义的KDF导出所述第二会话密钥(K_ser),其中输入参数是RAND1和RAND2;将所述第二会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成消息认证码(Message Authentication Code,MAC),其中RAND2和K_ser作为所述输入;以及向所述第二提供商网络的所述单元传输MAC。

[0030] 根据本发明的另一方面,提供了一种使用基于身份的密码术的认证框架中的运营提供商网络,所述认证框架涉及设备、服务提供商网络和所述运营提供商网络,其中所述设备、运营提供商网络和服务提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥(Global Public Key,GPK),所述运营提供商网络包括:认证节点,包括处理器、存储器和指令,其中所述指令存储在所述存储器上并且可由所述处理器执行以用于:从所述设备接收认证数据包,所述认证数据包包括第一随机数(RAND1)、认证类型(Auth. Type)、服务提供商网络的ID(SP_ID)、所述设备的标识(Device_ID)和设备签名(Sig_De),其中所述Auth. Type包括:第一类型,其中认证涉及所述运营商和服务提供商网络;第二类型,其中认证涉及所述运营提供商网络;以及第三类型,其中认证涉及所述服务提供商网络;基于所述认证类型确定认证的类型;响应于确定所述第一类型的认证,生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并基于所述SP_ID向所述第二提供商网络的单元传输所述认证数据包;响应于确定所述第二类型的认证,生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息;以及响应于确定所述第三类型的认证,向所述第二提供商网络的所述单元传输所述认证数据包。Sig_De由所述设备使用所述设备的

所述秘密密钥以及所述公钥(Global Public Key,GPK)生成。所述认证数据包还包括第一随机数(RAND1)、所述设备的标识(Device_ID)和设备签名(Sig_De)。

[0031] 根据本发明实施例,所述指令存储在所述认证节点的所述存储器上以生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,包括用于以下操作的指令:使用所述Device_ID和所述GPK验证所述Sig_De;以及响应于验证成功,生成第二随机数(RAND2)。

[0032] 根据本发明实施例,所述指令存储在所述认证节点的所述存储器上以生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,还包括用于以下操作的指令:根据基于身份的加密(Identity Based Encryption,IBE)使用所述Device_ID生成包含RAND2的第一加密消息(m1);使用所述运营提供商网络的所述秘密密钥和所述GPK生成签名(Sig_AN);以及生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,其中所述第一认证响应消息包括所述运营提供商网络的标识(AN_ID)、RAND1、m1和Sig_AN。

[0033] 根据本发明实施例,所述指令存储在所述认证节点的所述存储器上以生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,还包括用于以下操作的指令:接收所述设备通过MAC生成函数生成的第一消息认证码(MAC1),其中RAND2和第一会话密钥(K_com)作为所述输入;使用预定义的密钥导出函数(Key Derivation Function,KDF)导出所述第一会话密钥(K_com),其中输入参数是RAND1和RAND2;使用MAC生成函数生成MAC,其中RAND2和K_com作为所述输入;确定MAC1是否等于MAC;响应于MAC1等于MAC,将所述第一会话密钥K_com保存在所述认证节点的所述存储器中。

[0034] 根据本发明的另一方面,提供了一种使用基于身份的密码术的认证框架中的服务提供商网络,所述认证框架涉及设备、运营提供商网络和所述服务提供商网络,其中所述设备、运营提供商网络和服务提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥(Global Public Key,GPK),所述服务提供商网络包括:认证单元,包括处理器、存储器和指令,其中所述指令存储在所述存储器上并且可由所述处理器执行以用于:从所述运营提供商网络接收认证数据包,所述认证数据包包括第一随机数(RAND1)、认证类型(Auth. Type)、服务提供商网络的ID(SP_ID)、所述设备的标识(Device_ID)和设备签名(Sig_De),其中所述Auth. Type包括:第一类型,其中认证涉及所述运营商和服务提供商网络;第二类型,其中认证涉及所述运营提供商网络;以及第三类型,其中认证涉及所述服务提供商网络;使用所述Device_ID和所述GPK验证所述Sig_De;响应于验证成功,生成第三随机数(RAND3)。

[0035] 根据本发明实施例,所述指令还包括用于以下操作的指令:根据IBE使用所述Device_ID生成包含RAND3的第二加密消息(m2);使用所述服务提供商网络的所述秘密密钥和所述GPK生成签名(Sig_SP);生成所述第二认证响应消息并向所述设备传输第二认证响应消息,其中所述第二认证响应消息包括所述服务提供商网络的标识(SP_ID)、RAND1、m2和Sig_SP。

[0036] 根据本发明实施例,所述指令还包括用于以下操作的指令:接收所述设备通过MAC生成函数生成的第二消息认证码(MAC2),其中RAND3和第二会话密钥(K_ser)作为所述输入;使用预定义的KDF导出所述第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;使用所述MAC生成函数生成MAC,其中RAND3和K_ser作为所述输入;确定MAC2是否等于MAC;以及

响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述认证单元的所述存储器中。

[0037] 根据本发明的另一方面,提供了一种统一认证方法,用于使设备根据基于身份的密码术来认证第一提供商网络和第二提供商网络,其中所述设备、第一提供商网络和第二提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥(Global Public Key,GPK),所述统一认证方法包括:所述设备生成随机数(RAND1)并导出第一对称密钥(K_C)和第二对称密钥(K_S);所述设备生成认证数据包并向所述运营提供商网络传输所述认证数据包,所述认证数据包包括RAND1、认证类型(Auth. Type)、所述第二提供商网络的ID(SP_ID)、所述设备的标识(Device_ID)和设备签名(Sig_De),其中所述Auth. Type包括:第一类型,其中认证涉及所述第一提供商网络的单元和所述第二提供商网络的单元;第二类型,其中认证涉及所述第一提供商网络的所述单元;以及第三类型,其中认证涉及所述第二提供商网络的所述单元;响应于接收到所述认证数据包,所述第一提供商网络的所述单元基于所述认证类型确定认证的类型;响应于确定所述第一类型的认证,所述第一提供商网络的所述单元生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并基于所述SP_ID向所述第二提供商网络的所述单元传输所述认证数据包;以及响应于接收到所述认证数据包,所述第二提供商网络的所述单元生成第二认证响应消息并向所述设备传输所述第二认证响应消息。所述Sig_De由所述设备使用所述设备的所述秘密密钥和所述全局公钥(Global Public Key,GPK)生成。

[0038] 根据本发明实施例,所述第一对称密钥(K_C)通过所述设备的所述私钥(xH(Device_ID))和所述第一提供商网络的所述单元的标识(BS_ID)导出,所述第二对称密钥(K_S)通过所述xH(Device_ID)和所述第二提供商网络的所述单元的所述标识(SP_ID)导出。

[0039] 根据本发明实施例,所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤包括:使用所述Device_ID和所述GPK验证所述Sig_De;以及响应于验证成功,生成第二随机数(RAND2)。

[0040] 根据本发明实施例,所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤还包括:通过所述第一提供商网络的所述私钥(xH(BS_ID))和所述Device_ID导出所述第一对称密钥(K_C);使用所述K_C生成包含RAND2的第一加密消息(m1),并且可使用以下方式表示:m1=En(RAND2,K_C);使用所述第一提供商网络的所述秘密密钥和所述GPK生成签名(Sig_AN);以及生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,其中所述第一认证响应消息包括所述第一提供商网络的标识(AN_ID)、RAND1、m1和Sig_AN。

[0041] 根据本发明实施例,所述方法还包括:响应于接收到所述第一认证响应消息,所述设备执行以下步骤:通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;响应于认证成功,使用所述第一对称密钥K_C解密m1以获得RAND2;使用预定义的KDF导出第一会话密钥(K_com),其中输入参数是RAND1和RAND2;将所述第一会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第一消息认证码(MAC1),其中RAND2和K_com作为所述输入;以及向所述第一提供商网络的所述单元传输MAC1。

[0042] 根据本发明实施例,所述方法还包括:响应于接收到所述MAC1,所述第一提供商网络的所述单元执行以下步骤:使用所述预定义的密钥导出函数(Key Derivation

Function,KDF)导出所述第一会话密钥(K_com),其中输入参数是RAND1和RAND2;使用所述相同MAC生成函数生成MAC,其中RAND2和K_com作为所述输入;确定MAC1是否等于MAC;以及响应于MAC1等于MAC,将所述第一会话密钥K_com保存在所述第一提供商网络的所述单元的存储器中。

[0043] 根据本发明实施例,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:使用所述Device_ID和所述GPK验证所述Sig_De;以及响应于验证成功,生成第三随机数(RAND3)。

[0044] 根据本发明实施例,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤还包括:通过所述第二提供商网络的所述私钥(xH(SP_ID))和所述Device_ID导出所述第二对称密钥(K_S);使用所述K_S生成包含RAND3的第二加密消息(m2);使用所述第二提供商网络的所述秘密密钥和所述GPK生成签名(Sig_SP);生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的标识(SP_ID)、RAND1、m2和Sig_SP。

[0045] 根据本发明实施例,所述方法还包括:响应于接收到所述第二认证响应消息,所述设备执行以下步骤:通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;响应于认证成功,使用所述第二对称密钥K_S解密m2以获得RAND3;使用所述预定义的KDF导出所述第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;将所述第二会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第二消息认证码(MAC1),其中RAND3和K_ser作为所述输入;以及向所述第二提供商网络的所述单元传输MAC2。

[0046] 根据本发明实施例,所述方法还包括:响应于接收到所述MAC2,所述第二提供商网络的所述单元执行以下步骤:使用所述预定义的KDF导出第二会话密钥(K_ser),其中输入参数是RAND1和RAND3;使用所述相同MAC生成函数生成MAC,其中RAND3和K_ser作为所述输入;确定MAC2是否等于MAC;响应于MAC2等于MAC,将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

[0047] 根据本发明的另一方面,提供了一种统一认证方法,用于使设备根据基于身份的密码术来认证第一提供商网络和第二提供商网络,其中所述设备、第一提供商网络和第二提供商网络中的每一个具有公钥生成器发布的不同私钥以及相同全局公钥(Global Public Key,GPK)。所述统一认证方法包括:所述设备生成随机数(RAND1)并导出DH公钥(A),所述DH公钥(A)由$A=g^{RAND1} \bmod p$导出,其中mod表示所述取模运算;所述设备生成认证数据包并向所述运营提供商网络传输所述认证数据包,所述认证数据包包括DH公钥(A)、认证类型(Auth. Type)、所述第二提供商网络的ID(SP_ID)、所述设备的标识(Device_ID)以及设备签名(Sig_De),其中所述Auth. Type包括:第一类型,其中认证涉及所述第一提供商网络的单元和所述第二提供商网络的单元;第二类型,其中认证涉及所述第一提供商网络的所述单元;以及第三类型,其中认证涉及所述第二提供商网络的所述单元;响应于接收所述认证数据包,所述第一提供商网络的所述单元基于所述认证类型确定认证的类型;响应于确定所述第一类型的认证,所述第一提供商网络的所述单元生成第一认证响应消息并向所述设备传输所述第一认证响应消息,并基于所述SP_ID向所述第二提供商网络的所述单元传输所述认证数据包;以及响应于接收到所述认证数据包,所述第二提供商网络的所述单元生成第二认证响应消息并向所述设备传输所述第二认证响应消息。所述Sig_De由所述

设备使用所述设备的所述秘密密钥和所述全局公钥(Global Public Key,GPK)生成。

[0048] 根据本发明实施例,所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤包括:使用所述Device_ID和所述GPK验证所述Sig_De;以及响应于验证成功,生成第二随机数(RAND2)。

[0049] 根据本发明实施例,所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤还包括:导出DH公钥(B),其中$B=g^{RAND2} \bmod p$;以及导出第一会话密钥(K_com),其中$K_com=A^{RAND2} \bmod p$。

[0050] 根据本发明实施例,所述第一提供商网络的所述单元生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息的步骤还包括:使用所述第一提供商网络的所述秘密密钥和所述GPK生成签名(Sig_AN);以及生成所述第一认证响应消息并向所述设备传输所述第一认证响应消息,其中所述第一认证响应消息包括所述第一提供商网络的标识(AN_ID)、DH公钥(A)、DH公钥(B)和Sig_AN。

[0051] 根据本发明实施例,所述方法还包括:响应于接收到所述第一认证响应消息,所述设备执行以下步骤:通过使用AN_ID和所述GPK验证Sig_AN来认证所述第一提供商网络;响应于认证成功,使用所述DH公钥(B)导出所述第一会话密钥K_com,其中$K_com=B^{RAND2} \bmod p$;将所述第一会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第一消息认证码(MAC1),其中所述DH公钥(B)和K_com作为所述输入;以及向所述第一提供商网络的所述单元传输MAC1。

[0052] 根据本发明实施例,所述方法还包括:响应于接收到所述MAC1,所述第一提供商网络的所述单元执行以下步骤:使用所述相同MAC生成函数生成MAC,其中DH公钥(B)和K_com作为所述输入;确定MAC1是否等于MAC;以及响应于MAC1等于MAC,将所述第一会话密钥K_com保存在所述第一提供商网络的所述单元的存储器中。

[0053] 根据本发明实施例,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤包括:使用所述Device_ID和所述GPK验证所述Sig_De;以及响应于验证成功,生成第三随机数(RAND3)。

[0054] 根据本发明实施例,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤还包括:导出DH公钥(C),其中$C=g^{RAND3} \bmod p$;以及导出第二会话密钥(K_ser),其中$K_ser=A^{RAND3} \bmod p$。

[0055] 根据本发明实施例,所述第二提供商网络的所述单元生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息的步骤还包括:使用所述第二提供商网络的所述秘密密钥和所述GPK生成签名(Sig_SP);以及生成所述第二认证响应消息并向所述设备传输所述第二认证响应消息,其中所述第二认证响应消息包括所述第二提供商网络的标识(SP_ID)、DH公钥(A)、DH公钥(C)和Sig_SP。

[0056] 根据本发明实施例,所述方法还包括:响应于接收到所述第二认证响应消息,所述设备执行以下步骤:通过使用SP_ID和所述GPK验证Sig_SP来认证所述第二提供商网络;响应于认证成功,使用所述DH公钥(C)导出所述第二会话密钥K_ser,其中$K_ser=C^{RAND3} \bmod p$;将所述第二会话密钥保存在所述设备的所述存储器中;使用MAC生成函数生成第二消息认证码(MAC2),其中所述DH公钥(C)和K_ser作为所述输入;以及向所述第二提供商网络的所述单元传输MAC2。

[0057] 根据本发明实施例，所述方法还包括：响应于接收到所述MAC2，所述第二提供商网络的所述单元执行以下步骤：使用所述相同MAC生成函数生成MAC，其中DH公钥(C)和K_ser作为所述输入；确定MAC2是否等于MAC；以及响应于MAC2等于MAC，将所述第二会话密钥K_ser保存在所述第二提供商网络的所述单元的存储器中。

附图说明

[0058] 在以下详细描述中描述并在以下附图中示出根据本发明的以上优点和特征：

[0059] 图1示出了AKA过程；

[0060] 图2示出了根据本发明的使用认证类型来指示认证的类型以进行该认证；

[0061] 图3示出了根据本发明的一种对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的过程300；

[0062] 图4示出了根据本发明的一种使用对称密钥方法对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的过程400；

[0063] 图5示出了根据本发明实施例的一种使用Diffie-Hellman对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的替代过程500；

[0064] 图6示出了双方之间的标准Diffie-Hellman密钥协商过程；

[0065] 图7示出了根据本发明实施例的一种对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的替代过程700；

[0066] 图8示出了根据本发明实施例的一种对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的替代过程800；

[0067] 图9示出了根据本发明实施例的一种对用于导出密钥的随机数进行加密的服务提供商认证过程的过程900；

[0068] 图10示出了根据本发明实施例的一种对用于导出密钥的随机数进行加密的运营提供商认证过程的过程1000；

[0069] 图11示出了根据本发明的由设备210执行的过程1100；

[0070] 图12示出了根据本发明实施例的由运营提供商220的认证节点执行的过程1200；以及

[0071] 图13示出了根据本发明实施例的由服务提供商230的认证单元执行的过程1300。

具体实施方式

[0072] 本发明涉及一种运营提供商和服务提供商之间的认证框架的方法和系统。具体地，本发明涉及一种根据基于ID的密码术的运营提供商和服务提供商之间的统一认证框架的方法和系统。

[0073] 通过根据本发明的系统和方法主要可以解决三个问题。首先，当前的运营提供商网络接入认证与服务提供商网络认证是分开的。因此，终端设备必须经过两个认证过程才能访问运营提供商网络和服务提供商网络。

[0074] 其次，当前的服务提供商网络认证通常基于“用户名+密码”。换句话说，用户需要记住多组“用户名+密码”才能访问多个服务。这带来了不便和麻烦。通过所提出的统一认证，服务提供商网络认证可以与运营提供商网络认证一起完成，或者通过运营提供商网络

认证方法完成。这意味着用户不需要记住任何密码,这给用户带来了极大便利。

[0075] 最后,可以克服的另一个问题是在采用统一认证时保证用户隐私。具体地,用户和服务提供商之间的消息不应暴露给移动网络运营商(Mobile Network Operator,MNO),并且用户和MNO之间的消息不应暴露给服务提供商。

[0076] 在本发明中,提出了一种使用基于ID的密码术的第一提供商网络和第二提供商网络统一认证方案。本质上,本概念是使用一个认证消息来成功实现第一提供商网络接入认证和第二提供商网络认证。出于本发明的目的,第一网络是运营提供商网络,第二网络是服务提供商网络。此外,引入了称为认证类型的新参数。认证类型用作指示符以识别用户希望继续进行哪些类型的认证(例如,仅运营提供商网络访问、仅服务提供商网络访问或统一认证)。此外,提出了几种不同的方法来保护用于生成会话密钥的随机数。

[0077] 基于身份的密码术(identity-based cryptography,IBC)是一种公钥密码术,其中公钥是已知字符串,例如电子邮件地址、电话号码、域名或物理IP地址。对于基于IBC的系统,公钥生成器可以基于给定的全局公钥(Global Public Key,GPK)和全局秘密密钥(Global Secret Key,GSK)为任何给定ID生成私钥(SKID)。所生成的私钥SKID与GPK和ID一起分发给实体(Alice或Bob)。

[0078] IBC包括基于身份的加密(identity-based encryption,IBE)和基于身份的签名(identity-based signature,IBS)。IBE主要用于加密,而IBS主要用于签名消息。例如,当想要向Bob发送秘密消息时,Alice加密具有Bob的ID的消息。当Bob收到消息时,Bob用其私钥解密该消息。当Alice希望Bob对其自身进行认证时,Alice首先生成随机数,并进一步基于已知算法使用SKID和GPK生成随机数的签名。然后,Alice将带有随机数、签名及其ID的消息发送给另一个实体Bob。在接收到该消息之后,Bob基于已知算法使用所接收的随机数、签名,ID和GPK对Alice进行认证。如果验证成功,Bob随后会与Alice进行认证。同样,Alice也可以使用Bob的签名和ID对实体Bob进行认证。通过上面的示例,可以看出基于IBC的认证的优势在于在认证中不需要集中式服务器来保留设备凭证。

[0079] 图2示出了使用认证类型250来指示认证的类型以进行该认证。如上所述,本发明公开了一种使用基于ID的密码术的运营提供商网络和服务提供商网络统一认证方案。虽然UE 210可以与运营提供商220和服务提供商230进行认证,但是本发明中提出的认证过程还允许用户单独地与运营商和服务提供商进行认证。因此,认证类型250用于识别要进行的认证的类型。出于本发明的目的,如果认证类型250是第一类型1,则UE与运营提供商220和服务提供商230两者进行认证。如果认证类型250是第二类型2,则UE与运营提供商220进行认证以进行运营商网络访问。如果认证类型250是第三类型3,则UE与服务提供商230进行认证以进行服务级访问。

[0080] 首先讨论认证类型250的第一类型1,然后是第二类型2和第三类型3。

[0081] 图3示出了一种对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的过程300。具体地,IBE用于加密随机数。

[0082] 过程300开始于步骤305,即设备210生成随机数(RAND1)。然后,设备210在步骤310中向运营提供商220的认证节点(Authentication Node,AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下:(Auth.Type,SP_ID,Device_ID,RAND1,Sig_

De,……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。由于过程300是运营提供商和服务提供商的统一认证过程,因此过程300的认证类型250是第一类型的认证1。

[0083] 在步骤315中,响应于接收到认证消息,认证节点首先识别认证类型。如果认证类型是统一认证,则认证节点基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地,认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功,则AN生成随机数(RAND2)。此后,AN使用预定义的密钥导出函数(key derivation function,KDF)导出密钥(表示为K_com)。KDF的输入参数包括RAND1和RAND2,并且可使用以下方式表示:K_com=KDF(RAND1,RAND2,……)。

[0084] 在步骤320中,AN将认证消息转发给服务提供商的认证单元。

[0085] 在步骤325中,认证节点生成加密消息m1,并向设备210发送认证响应消息。加密消息m1根据IBE使用Device_ID加密RAND2而获得,并且可使用以下方式表示:m1=En(RAND2,Device_ID)。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0086] 在步骤330中,响应于从AN接收到认证响应消息,设备210通过验证AN签名(Sig_AN)来认证AN。具体地,设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果验证成功,则设备使用其私钥和设备的SKID解密消息m1以获得RAND2。然后,设备使用预定义的KDF导出密钥(K_com)。KDF的输入参数应包括RAND1和RAND2,并且可使用以下方式表示:K_com=KDF(RAND1,RAND2,……)。然后,设备210将密钥K_com保存在其存储器中。RAND1也包含在认证响应消息中以防止重放攻击。

[0087] 在步骤335中,设备210使用MAC生成函数生成消息认证码(MAC1),其中RAND2和K_com作为输入。设备向AN发送MAC1。

[0088] 在步骤340中,响应于从设备210接收MAC1,AN对MAC1进行验证。为了对MAC1进行验证,AN使用相同MAC生成函数生成MAC,其中RAND2和K_com作为输入,并查看MAC1是否等于MAC。如果验证成功,则AN将密钥K_com保存在其存储器中。本领域技术人员将认识到,AN可以在该步骤中而不是在步骤315中导出密钥(表示为K_com)。具体地,在接收到MAC1时,AN在对MAC1进行验证之前导出密钥(表示为K_com)。

[0089] 在步骤345中,响应于从AN接收到认证消息,服务提供商230的认证单元首先基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地,认证单元使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功,则认证单元生成随机数(RAND3)。然后,认证单元使用预定义的密钥导出函数(key derivation function,KDF)导出密钥(表示为K_ser)。KDF的输入参数应包括RAND1和RAND3,并且可使用以下方式表示:K_ser=KDF(RAND1,RAND3,……)。

[0090] 在步骤350中,认证单元生成加密消息m2,并向设备210发送认证响应消息。加密消息m2根据IBE使用Device_ID加密RAND3而获得,并且可使用以下方式表示:m2=En(RAND3,Device_ID)。认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m2和认证单元签名(表示为Sig_SP)。认证单元签名由认证单元通过IBS使用认证单元的秘密密钥(SKID)和GPK生成。

[0091] 在步骤355中，响应于从服务提供商230接收到认证响应消息，设备210通过验证认证单元的签名(Sig_SP)来对其进行认证。然后，设备使用其私钥解密消息m2以获得RAND3。然后，设备210使用预定义的KDF导出密钥(K_ser)。KDF的输入参数应包括RAND1和RAND3，并且可使用以下方式表示：K_ser=KDF(RAND1,RAND3,……)。然后，设备将密钥K_ser保存在其存储器中。

[0092] 在步骤360中，设备使用MAC生成函数生成消息认证码(MAC2)，其中RAND3和K_ser作为输入。设备210将MAC2发送到服务提供商230的认证单元。

[0093] 在步骤365中，响应于接收MAC2，认证单元对MAC2进行验证。为了对MAC2进行验证，认证单元使用相同MAC生成函数生成MAC，其中RAND3和K_ser作为输入，并查看MAC2是否等于MAC。如果验证成功，则认证单元将密钥K_ser保存在其存储器中。本领域技术人员将认识到，认证单元可以在该步骤中而不是在步骤345中导出密钥(表示为K-ser)。具体地，在接收到MAC2时，认证单元在对MAC2进行验证之前导出密钥(表示为K-ser)。

[0094] 过程300在步骤365之后结束。重要的是要注意，过程300中示出的步骤可以按所示顺序执行，或以不同顺序执行。例如，可以将步骤310中的认证数据包，即认证消息发送给服务提供商而不是运营提供商。或者，可以将步骤310中的认证数据包，即认证消息发送给服务提供商以及运营提供商。此外，两个或多个步骤可以并行执行而不是顺序执行。例如，步骤315、325至340可以与步骤345至365并行执行而不脱离本发明。

[0095] 出于本发明的目的，假设设备210配备有多个公钥和私钥集，并且至少一个密钥集用于IBS，并且至少一个密钥集用于IBE。如果使用多组公钥和私钥，则在发送给运营提供商和服务提供商的认证消息中也会指示用于指示所使用的公钥和私钥集的索引，以便运营提供商和服务提供商知悉用于认证的公钥和私钥集。

[0096] 出于本发明的目的，仅考虑三方，即设备、MNO等运营提供商和服务提供商。这里描述了MNO的一个网络单元，即认证节点。MNO可以提供另一个网络单元，称之为黑名单服务器。认证节点的功能是在授予设备访问权限之前对设备进行认证。黑名单服务器用于存储被侵设备ID。在认证设备之前，认证节点应首先确保设备ID不在黑名单服务器中。这里还描述了服务提供商的一个网络单元，即认证单元。服务提供商还可以提供称之为身份管理服务器的另一网络单元。认证单元的功能是在授予设备访问其服务之前对设备进行认证。身份管理服务器用于生成和管理设备的身份。

[0097] 图4示出了一种使用对称密钥方法对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的过程400。除了随机数的加密之外，过程400类似于过程300。具体地，还使用对称密钥加密随机数。

[0098] 过程400开始于步骤405，即设备210生成随机数(RAND1)并导出第一对称密钥(K_C)和第二对称密钥(K_S)。第一对称密钥(K_C)利用设备的私钥(xH(Device_ID))和AN的ID(BS_ID)导出，并且可使用以下方式表示：K_C=e(xH(Device_ID),H(BS_ID))。第二对称密钥(K_S)利用设备的私钥(xH(Device_ID))和认证单元的ID(SP_ID)导出，并且可使用以下方式表示：K_S=e(xH(Device_ID),H(SP_ID))。

[0099] 然后，设备210在步骤410中向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type，

SP_ID,Device_ID,RAND1,Sig_De,……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。这类似于过程300的步骤310。

[0100] 在步骤415中,响应于接收到认证消息,认证节点首先识别认证类型。如果认证类型是统一认证,则认证节点基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地,认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功,则AN生成随机数(RAND2)。此后,AN使用预定义的密钥导出函数(key derivation function,KDF)导出密钥(表示为K_com)。KDF的输入参数包括RAND1和RAND2,并且可使用以下方式表示:K_com=KDF(RAND1,RAND2,……)。此后,AN利用其私钥(xH(BS_ID))和设备ID(Device_ID)导出另一对称密钥(K_C),并且可使用以下方式表示:K_C=e(xH(BS_ID),H(Device_ID))。

[0101] 在步骤420中,AN将认证消息转发给服务提供商的认证单元。

[0102] 在步骤425中,认证节点生成加密消息m1,并向设备210发送认证响应消息。加密消息m1通过使用K_C加密RAND2而获得,并且可使用以下方式表示:m1=En(RAND2,K_C)。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0103] 在步骤430中,响应于从AN接收到认证响应消息,设备210通过验证AN签名(Sig_AN)来认证AN。具体地,设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果认证成功,则使用K_C解密消息m1以获得RAND2。然后,使用预定义的KDF导出密钥(K_com)。KDF的输入参数应包括RAND1和RAND2,并且可使用以下方式表示:K_com=KDF(RAND1,RAND2,.....)。设备将密钥K_com保存在其存储器中。在步骤435中,设备210使用MAC生成函数生成消息认证码(MAC1),其中RAND2和K_com作为输入。设备向AN发送MAC1。

[0104] 在步骤440中,响应于从设备210接收MAC1,AN对MAC1进行验证。为了对MAC1进行验证,AN使用相同MAC生成函数生成MAC,其中RAND2和K_com作为输入,并查看MAC1是否等于MAC。如果验证成功,则AN将密钥K_com保存在其存储器中。

[0105] 在步骤445中,响应于从AN接收到认证消息,服务提供商230的认证单元首先基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地,认证单元使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功,则认证单元生成随机数(RAND3)。然后,认证单元使用预定义的密钥导出函数(key derivation function,KDF)导出密钥(表示为K_ser)。KDF的输入参数应包括RAND1和RAND3,并且可使用以下方式表示:K_ser=KDF(RAND1,RAND3,……)。此后,认证单元利用其私钥(xH(SP_ID))和设备ID(Device_ID)导出另一对称密钥(K_S),并且可使用以下方式表示:K_S=e(xH(SP_ID),H(Device_ID))。

[0106] 在步骤450中,认证单元生成加密消息m2,并向设备210发送认证响应消息。加密消息m2通过使用K_S加密RAND3而获得,并且可使用以下方式表示:m2=En(RAND3,K_S)。认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m2和认证单元签名(表示为Sig_SP)。认证单元签名由认证单元通过IBS使用认证单元的秘密密钥(SKID)和GPK生成。

[0107] 在步骤455中,响应于从服务提供商230接收到认证响应消息,设备210通过验证认证单元的签名(Sig_SP)来对其进行认证。然后,设备使用K_S解密消息m2以获得RAND3。然

后，设备210使用预定义的KDF导出密钥(K_ser)。KDF的输入参数应包括RAND1和RAND3，并且可使用以下方式表示：K_ser=KDF(RAND1,RAND3,……)。然后，设备210将密钥K_ser保存在其存储器中。

[0108] 在步骤460中，使用MAC生成函数生成消息认证码(MAC2)，其中RAND3和K_ser作为输入。设备210将MAC2发送到服务提供商230的认证单元。

[0109] 在步骤465中，响应于接收到MAC2，认证单元对MAC2进行验证。为了对MAC2进行验证，认证单元使用相同MAC生成函数生成MAC，其中RAND3和K_ser作为输入，并查看MAC2是否等于MAC。如果验证成功，则认证单元将密钥K_ser保存在其存储器中。

[0110] 过程400在步骤465之后结束。在过程400中，对称密钥K_C和K_S的使用基于IBS方案的重要特征，其为：对于ID1_SK=xH(ID1)和ID2_SK=xH(ID2)，对称密钥K=e(xH(ID1),H(ID2))等于K=e(H(ID1),xH(ID2))。图5示出了一种使用Diffie-Hellman对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的过程500。除了随机数的加密之外，过程500类似于过程300。具体地，使用Diffie-Hellman加密随机数。

[0111] 过程500开始于步骤505，即设备210生成随机数(RAND1)和导出DH公钥(A)。DH公钥(A)由$A=g^{RAND1} \bmod p$导出，其中mod表示取模运算。

[0112] 然后，设备210在步骤510中向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、设备的DH公钥(A)和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type,SP_ID,Device_ID,A,Sig_De,……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。

[0113] 在步骤515中，响应于接收到认证消息，认证节点首先识别认证类型。如果认证类型是统一认证，则认证节点基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地，认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则AN生成随机数(RAND2)。此后，AN计算其DH公钥(B)并导出密钥(表示为K_com)。DH公钥(B)通过$B=g^{RAND2} \bmod p$计算得出，而密钥通过$K_com=A^{RAND2} \bmod p$导出。

[0114] 在步骤520中，AN将认证消息转发给服务提供商的认证单元。

[0115] 在步骤525中，认证节点向设备210发送认证响应消息。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的设备的DH公钥(A)、认证节点的DH公钥(B)和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0116] 在步骤530中，响应于从AN接收到认证响应消息，设备210通过验证AN签名(Sig_AN)来认证AN。具体地，设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果认证成功，则使用所接收的DH公钥来导出密钥(K_com)，即$K_com=B^{RAND2} \bmod p$。然后，设备210将密钥K_com保存在其存储器中。

[0117] 在步骤535中，设备210使用MAC生成函数生成消息认证码(MAC1)，其中B和K_com作为输入。设备向AN发送MAC1。

[0118] 在步骤540中，响应于从设备210接收到MAC1，AN对MAC1进行验证。为了对MAC1进行验证，AN使用相同MAC生成函数生成MAC，其中B和K_com作为输入，并查看MAC1是否等于MAC。如果验证成功，则AN将密钥K_com保存在其存储器中。

[0119] 在步骤545中，响应于从AN接收到认证消息，服务提供商230的认证单元首先基于

IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地,认证单元使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功,则认证单元生成随机数(RAND3)。然后,认证单元通过$C=g^{RAND3}$ mod p计算其DH公钥(C),并通过$K_ser=A^{RAND3}$ mod p导出密钥。

[0120] 在步骤550中,认证单元向设备210发送认证响应消息。认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的设备的DH公钥(A)、认证单元的DH公钥(C)和认证单元签名(表示为Sig_SP)。认证单元签名由认证单元通过IBS使用认证单元的秘密密钥(SKID)和GPK生成。

[0121] 在步骤555中,响应于从服务提供商230接收到认证响应消息,设备210通过验证认证单元的签名(Sig_SP)来对其进行认证。然后,设备使用所接收的DH公钥导出密钥(K_ser),即$K_ser=C^{RAND1}$ mod p。然后,设备210将密钥K_ser保存在其存储器中。

[0122] 在步骤560中,设备使用MAC生成函数生成消息认证码(MAC2),其中C和K_ser作为输入。设备210将MAC2发送到服务提供商230的认证单元。

[0123] 在步骤565中,响应于接收到MAC2,认证单元对MAC2进行验证。为了对MAC2进行验证,认证单元使用相同MAC生成函数生成MAC,其中C和K_ser作为输入,并查看MAC2是否等于MAC。如果验证成功,则认证单元将密钥K_ser保存在其存储器中。

[0124] 过程500在步骤565之后结束。图6示出了两方,即Alice和Bob之间的标准Diffie-Hellman密钥协商过程。首先,双方必须同意不需要保密的任意数字。在本示例中,“g”和“p”是已知的,而“a”和“b”是未知的,$K=A^b$ mod $p=(g^b$ mod $p)^b=g^{ab}$ mod $p=(g^b$ mod $p)^a=B^a$ mod p。Alice为了与Bob交换密钥,Alice首先为“a”选择一个随机数并确定“A”。然后Alice向Bob发送“g”、“p”和“A”。响应于从Alice接收信息,Bob选择“b”并确定“B”。然后,Bob向Alice发送“B”。对于Alice,通过“B”能够确定K,因为$K=B^a$ mod p。对于Bob,通过“A”能够确定K,因为$K=A^b$ mod p。K是共享秘密密钥,只为Alice和Bob所知。

[0125] 图7示出了一种对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的过程700。具体地,过程700示出了认证节点代表设备210与服务提供商进行认证。

[0126] 过程700开始于步骤705,即设备210生成随机数(RAND1)。然后,设备210在步骤710中向运营提供商220的认证节点(Authentication Node,AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下:(Auth.Type,SP_ID,Device_ID,RAND1,Sig_De,……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。

[0127] 在步骤715中,响应于接收到认证消息,认证节点首先识别认证类型。如果认证类型是统一认证,则认证节点基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地,认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功,则AN生成随机数(RAND2)。此后,AN使用预定义的密钥导出函数(key derivation function,KDF)导出密钥(表示为K_com)。KDF的输入参数包括RAND1和RAND2,并且可使用以下方式表示:K_com=KDF(RAND1,RAND2,……)。

[0128] 在步骤720中,AN将认证消息转发给服务提供商的认证单元。

[0129] 在步骤725中,响应于从AN接收到认证消息,服务提供商230的认证单元首先基于

IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地,认证单元使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功,则认证单元生成随机数(RAND3)。然后,认证单元使用预定义的密钥导出函数(key derivation function,KDF)导出密钥(表示为K_ser)。KDF的输入参数应包括RAND1和RAND3,并且可使用以下方式表示:K_ser=KDF(RAND1,RAND3,……)。

[0130] 在步骤730中,认证单元生成认证响应消息(m2)并将其发送到AN。认证响应消息(m2)包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m1和认证单元签名(表示为Sig_SP)。认证单元签名由认证单元通过IBS使用认证单元的秘密密钥(SKID)和GPK生成。加密消息m1根据IBE使用Device_ID加密RAND3而获得,并且可使用以下方式表示:m1=En(RAND3,Device_ID)。

[0131] 在步骤735中,响应于接收到m2,认证节点生成加密消息m3,并向设备210发送认证响应消息。加密消息m3根据IBE使用Device_ID加密RAND2而获得,并且可使用以下方式表示:m3=En(RAND2,Device_ID)。认证响应消息包括m1、AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m3和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0132] 在步骤740中,响应于从AN接收到认证响应消息,设备210通过验证AN签名(Sig_AN)来认证AN。具体地,设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果验证成功,则设备使用其私钥和设备的SKID解密消息m3以获得RAND2。然后,设备使用预定义的KDF导出密钥(K_com)。KDF的输入参数应包括RAND1和RAND2,并且可使用以下方式表示:K_com=KDF(RAND1,RAND2,.....)。然后,设备210将密钥K_com保存在其存储器中。然后,设备210使用从服务提供商获得的认证响应消息来对认证单元进行认证。设备210然后对服务提供商签名(Sig_SP)进行验证。然后,设备使用其私钥解密消息m1以获得RAND3。然后,设备210使用预定义的KDF导出密钥(K_ser)。KDF的输入参数应包括RAND1和RAND3,并且可使用以下方式表示:K_ser=KDF(RAND1,RAND3,……)。然后,设备210将密钥K_ser保存在其存储器中。

[0133] 在步骤745,设备210使用MAC生成函数生成第一消息认证码(MAC1),其中RAND2和K_com作为输入,并使用MAC生成函数生成第二消息认证码(MAC2),其中RAND3和K_ser作为输入。设备向AN发送MAC1和MAC2。

[0134] 在步骤750中,响应于从设备210接收到MAC1和MAC2,AN对MAC1进行验证。为了对MAC1进行验证,AN使用相同MAC生成函数生成MAC,其中RAND2和K_com作为输入,并查看MAC1是否等于MAC。如果验证成功,则AN将密钥K_com保存在其存储器中。本领域技术人员将认识到,AN可以在该步骤中而不是在步骤715中导出密钥(表示为K-com)。具体地,在接收到MAC1时,AN在对MAC1进行验证之前导出密钥(表示为K-com)。

[0135] 在步骤755中,AN将MAC2转发给服务提供商。

[0136] 在步骤760中,响应于从AN接收到MAC2,认证单元对MAC2进行验证。为了对MAC2进行验证,认证单元使用相同MAC生成函数生成MAC,其中RAND3和K_ser作为输入,并查看MAC2是否等于MAC。如果验证成功,则认证单元将密钥K_ser保存在其存储器中。本领域技术人员将认识到,认证单元可以在该步骤中而不是在步骤725中导出密钥(表示为K-ser)。具体地,在接收到MAC2时,认证单元在对MAC2进行验证之前导出密钥(表示为K-ser)。

[0137] 过程700在步骤760之后结束。

[0138] 图8示出了一种对用于导出密钥的随机数进行加密的运营提供商和服务提供商统一认证过程的过程800。具体地，过程800示出了在与服务提供商进行认证之前首先与运营提供商220进行认证的顺序过程。

[0139] 过程800开始于步骤805，即设备210生成随机数(RAND1)。然后，设备210在步骤810中向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type，SP_ID，Device_ID，RAND1，Sig_De，……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。

[0140] 在步骤815中，响应于接收到认证消息，认证节点首先识别认证类型。如果认证类型是统一认证，则认证节点基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地，认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则AN生成随机数(RAND2)。此后，AN使用预定义的密钥导出函数(key derivation function，KDF)导出密钥(表示为K_com)。KDF的输入参数包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1，RAND2，……)。

[0141] 在步骤820中，认证节点生成加密消息m1，并向设备210发送认证响应消息。加密消息m1根据IBE使用Device_ID加密RAND2而获得，并且可使用以下方式表示：m1=En(RAND2，Device_ID)。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0142] 在步骤825中，响应于从AN接收到认证响应消息，设备210通过验证AN签名(Sig_AN)来认证AN。具体地，设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果验证成功，则设备使用其私钥和设备的SKID解密消息m1以获得RAND2。然后，设备使用预定义的KDF导出密钥(K_com)。KDF的输入参数应包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1，RAND2，.....)。然后，设备210将密钥K_com保存在其存储器中。

[0143] 在步骤830中，设备210使用MAC生成函数生成消息认证码(MAC1)，其中RAND2和K_com作为输入。设备向AN发送MAC1。

[0144] 在步骤835中，响应于从设备210接收到MAC1，AN对MAC1进行验证。为了对MAC1进行验证，AN使用相同MAC生成函数生成MAC，其中RAND2和K_com作为输入，并查看MAC1是否等于MAC。如果验证成功，则AN将密钥K_com保存在其存储器中。本领域技术人员将认识到，AN可以在该步骤中而不是在步骤815中导出密钥(表示为K-com)。具体地，在接收到MAC1时，AN在对MAC1进行验证之前导出密钥(表示为K-com)。

[0145] 在步骤840中，AN将认证消息转发给服务提供商的认证单元。认证消息包括设备ID(Device_ID)、指示设备已成功与运营提供商进行认证的指示符(Auth_Succ)、从设备接收的随机数(RAND 1)、认证节点的签名(Sig_AN)。

[0146] 在步骤845中，响应于从AN接收到认证消息，服务提供商230的认证单元首先验证AN签名(Sig_De)。具体地，认证单元使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则认证单元生成随机数(RAND3)。然后，认证单元使用预定义的密钥导出函数(key derivation function，KDF)导出密钥(表示为K_ser)。KDF的输入参数应包括RAND1和RAND3，并且可使用以下方式表示：K_ser=KDF(RAND1，RAND3，……)。然后，认证单元

将密钥K_ser保存在其存储器中。

[0147] 在步骤850中，认证单元生成加密消息m2，并向AN发送认证响应消息。加密消息m2根据IBE使用Device_ID加密RAND3而获得，并且可使用以下方式表示：m2=En(RAND3，Device_ID)。认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m2和认证单元签名(表示为Sig_SP)。认证单元签名由认证单元通过IBS使用认证单元的秘密密钥(SKID)和GPK生成。

[0148] 在步骤855中，响应于从服务提供商230接收到认证响应消息，AN通过验证认证单元的签名(Sig_SP)来对其进行认证。如果认证成功，则AN生成消息认证码MAC2并向设备发送消息。该消息包括加密消息m2、指示服务提供商被成功认证的指示符(SP_Auth)和MAC2。MAC2由AN使用m2、SP_Auth、K_com生成，并且可使用以下方式表示：MAC2=MAC(m2，SP_Auth，K_com)。

[0149] 在步骤865中，响应于从AN接收到消息，设备对MAC2进行验证。为了对MAC2进行验证，设备使用相同MAC生成函数生成MAC，并查看MAC2是否等于MAC。如果验证成功，则设备使用其私钥解密消息m2以获得RAND3。然后，设备210使用预定义的KDF导出密钥(K_ser)。KDF的输入参数应包括RAND1和RAND3，并且可使用以下方式表示：K_ser=KDF(RAND1，RAND3，……)。然后，设备210将密钥K_ser保存在其存储器中。

[0150] 过程800在步骤865之后结束。

[0151] 图9示出了一种对用于导出密钥的随机数进行加密的服务提供商认证过程的过程900。仅当设备已与运营提供商建立网络连接时，此过程才适用。

[0152] 过程900开始于步骤905，即设备210生成随机数(RAND1)。然后，设备210在步骤910中向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type，SP_ID，Device_ID，RAND1，Sig_De，……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。由于过程900是服务提供商认证过程，因此过程900的认证类型250是第三类型的认证3。

[0153] 在步骤915中，响应于接收到认证消息，认证节点首先识别认证类型。如果认证类型是第三类型的认证3，则认证节点在步骤920中将认证消息转发到服务提供商的认证单元。

[0154] 在步骤925中，响应于从AN接收到认证消息，服务提供商230的认证单元首先基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地，认证单元使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则认证单元生成随机数(RAND2)。然后，认证单元使用预定义的密钥导出函数(key derivation function，KDF)导出密钥(表示为K_ser)。KDF的输入参数应包括RAND1和RAND2，并且可使用以下方式表示：K_ser=KDF(RAND1，RAND2，……)。

[0155] 在步骤930中，认证单元生成加密消息(m)，并向设备210发送认证响应消息。加密消息m根据IBE使用Device_ID加密RAND2而获得，并且可使用以下方式表示：m=En(RAND2，Device_ID)。认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m和认证单元签名(表示为Sig_SP)。认证单元签名由认证单元通过IBS使用认证单元的秘密密钥(SKID)和GPK生成。

[0156] 在步骤935中，响应于从服务提供商230接收到认证响应消息，设备210通过验证认证单元的签名(Sig_SP)来对其进行认证。然后，设备使用其私钥解密消息m以获得RAND2。然后，设备210使用预定义的KDF导出密钥(K_ser)。KDF的输入参数应包括RAND1和RAND2，并且可使用以下方式表示：K_ser=KDF(RAND1,RAND2,……)。然后，设备210将密钥K_ser保存在其存储器中。

[0157] 在步骤940中，设备使用MAC生成函数生成消息认证码(MAC1)，其中RAND2和K_ser作为输入。设备210将MAC1发送到服务提供商230的认证单元。

[0158] 在步骤945中，响应于接收到MAC1，认证单元对MAC1进行验证。为了对MAC1进行验证，认证单元使用相同MAC生成函数生成MAC，其中RAND2和K_ser作为输入，并查看MAC1是否等于MAC。如果验证成功，则认证单元将密钥K_ser保存在其存储器中。本领域技术人员将认识到，认证单元可以在该步骤中而不是在步骤925中导出密钥(表示为K-ser)。具体地，在接收到MAC1时，认证单元在对MAC1进行验证之前导出密钥(表示为K-ser)。

[0159] 过程900在步骤945之后结束。

[0160] 图10示出了一种对用于导出密钥的随机数进行加密的运营提供商认证过程的过程1000。当设备希望访问运营提供商的网络时，此过程适用。

[0161] 过程1000开始于步骤1005，即设备210生成随机数(RAND1)。然后，设备210在步骤1010中向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type,Device_ID,RAND1,Sig_De,……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。由于过程1000是运营提供商和服务提供商统一认证过程，因此过程1000的认证类型250是第二类型的认证2。

[0162] 在步骤1015中，响应于接收到认证消息，认证节点首先识别认证类型。如果认证类型是第二类型的认证，则认证节点基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地，认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则AN生成随机数(RAND2)。此后，AN使用预定义的密钥导出函数(key derivation function，KDF)导出密钥(表示为K_com)。KDF的输入参数包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1,RAND2,……)。

[0163] 在步骤1025中，认证节点生成加密消息m1，并向设备210发送认证响应消息。加密消息m1根据IBE使用Device_ID加密RAND2而获得，并且可使用以下方式表示：m1=En(RAND2,Device_ID)。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0164] 在步骤1030中，响应于从AN接收到认证响应消息，设备210通过验证AN签名(Sig_AN)来认证AN。具体地，设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果验证成功，则设备使用其私钥和设备的SKID解密消息m1以获得RAND2。然后，设备使用预定义的KDF导出密钥(K_com)。KDF的输入参数应包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1,RAND2,.....)。然后，设备210将密钥K_com保存在其存储器中。

[0165] 在步骤1035中，设备210使用MAC生成函数生成消息认证码(MAC1)，其中RAND2和K_com作为输入。设备向AN发送MAC1。

[0166] 在步骤1040中，响应于从设备210接收到MAC1，AN对MAC1进行验证。为了对MAC1进行验证，AN使用相同MAC生成函数生成MAC，其中RAND2和K_com作为输入，并查看MAC1是否等于MAC。如果验证成功，则AN将密钥K_com保存在其存储器中。本领域技术人员将认识到，AN可以在该步骤中而不是在步骤1015中导出密钥(表示为K-com)。具体地，在接收到MAC1时，认证节点在对MAC1进行验证之前导出密钥(表示为K-com)。

[0167] 过程1000在步骤1040之后结束。

[0168] 图11示出了根据本发明的由设备210执行的过程1100。过程1100开始于步骤1105，即生成随机数(RAND1)。

[0169] 在如过程400所述的另一实施例中，可以修改步骤1105以进一步导出第一对称密钥(K_C)和第二对称密钥(K_S)。第一对称密钥(K_C)利用设备的私钥(xH(Device_ID))和AN的ID(BS_ID)导出，并且可使用以下方式表示：K_C=e(xH(Device_ID)，H(BS_ID))。第二对称密钥(K_S)利用设备的私钥(xH(Device_ID))和认证单元的ID(SP_ID)导出，并且可使用以下方式表示：K_S=e(xH(Device_ID)，H(SP_ID))。

[0170] 在如过程500所述的另一实施例中，可以修改步骤1105以进一步导出DH公钥(A)。DH公钥(A)由$A=g^{RAND1} \bmod p$导出，其中mod表示取模运算。

[0171] 在步骤1110中，过程1100确定认证的类型。如果认证是针对涉及运营提供商和服务提供商的统一认证，则过程1100指示1以进行第一类型的认证，并且此后继续执行步骤1160。如果认证是针对仅涉及运营提供商的认证，则过程1100指示2以进行第二类型的认证，并且此后继续执行步骤1140。如果认证是针对仅涉及服务提供商的认证，则过程1100指示3以进行第三类型的认证，并且此后继续执行步骤1115。

[0172] 在步骤1115中，过程1100向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type，SP_ID，Device_ID，RAND1，Sig_De，……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。

[0173] 在如过程500所述的另一实施例中，可以修改步骤1115，使得认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、设备的DH公钥(A)和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type，SP_ID，Device_ID，A，Sig_De，……)。

[0174] 在步骤1120中，过程1100从服务提供商230接收认证响应消息。认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m和认证单元签名(表示为Sig_SP)。加密消息m通过服务提供商230的认证单元根据IBE使用Device_ID加密RAND2而导出，并且可使用以下方式表示：m=En(RAND2，Device_ID)。

[0175] 在步骤1125中，过程1100通过认证其签名(Sig_SP)来认证服务提供商230。如果认证成功，则过程1100使用设备的私钥解密消息m以获得RAND2，并使用预定义的KDF导出密钥(K_ser)。KDF的输入参数包括RAND1和RAND2，并且可使用以下方式表示：K_ser=KDF(RAND1，RAND2，……)。

[0176] 在步骤1130中，过程1100将密钥(K-ser)、RAND1和RAND2保存在存储器中。然后，过程1100生成消息认证码(Message Authentication Code，MAC)并向服务提供商230传输该

消息认证码。该MAC通过MAC生成函数而生成，其中RAND2和K_ser作为输入。

[0177] 步骤1115至1130涉及第三类型的认证，其中设备与服务提供商230进行认证。

[0178] 在步骤1140中，过程1100向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type,Device_ID,RAND1,Sig_De,……)。设备签名由设备通过IBS使用设备的秘密密钥(SKID)和GPK生成。

[0179] 在步骤1145中，过程1100从运营提供商220接收认证响应消息。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m和AN签名(表示为Sig_AN)。加密消息m通过运营提供商根据IBE使用Device_ID加密RAND2而导出，并且可使用以下方式表示：m=En(RAND2,Device_ID)。

[0180] 在步骤1150中，响应于从AN接收到认证响应消息，过程1100通过验证AN签名(Sig_AN)来认证AN。具体地，设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果认证成功，则过程1100使用设备的私钥解密消息m以获得RAND2，并使用预定义的KDF导出密钥(K_com)。KDF的输入参数应包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1，RAND2,.....)。

[0181] 在步骤1155中，过程1100将密钥(K-com)、RAND1和RAND2保存在存储器中。然后，过程1100生成消息认证码(Message Authentication Code,MAC)并向服务提供商230传输该消息认证码。该MAC通过MAC生成函数而生成，其中RAND2和K_com作为输入。

[0182] 步骤1140至1155涉及第二类型的认证，其中设备与运营提供商220进行认证。

[0183] 在步骤1160中，过程1100向运营提供商220的认证节点(Authentication Node，AN)发送认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type，SP_ID,Device_ID,RAND1,Sig_De,……)。

[0184] 在步骤1165中，过程1100从运营提供商220或服务提供商230接收第一认证响应消息或第二认证响应消息。出于讨论目的，将假设第一认证响应消息来自运营提供商220，第二认证响应消息来自服务提供商230。

[0185] 第一认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。加密消息m1通过运营提供商220根据IBE使用Device_ID加密RAND2而导出，并且可使用以下方式表示：m1=En(RAND2,Device_ID)。

[0186] 在如过程400所述的另一实施例中，可以修改步骤1165，使得第一认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。加密消息m1通过使用K_C对RAND2进行加密而获得，并且可使用以下方式表示：m1=En(RAND2,K_C)。

[0187] 在如过程500所述的另一实施例中，可以修改步骤1165，使得第一认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的设备的DH公钥(A)、认证节点的DH公钥(B)和AN签名(表示为Sig_AN)。

[0188] 第二认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m2和认证单元签名(表示为Sig_SP)。加密消息m2通过认证单元根据IBE使用Device_ID加密RAND3而导出，并且可使用以下方式表示：m2=En(RAND3,Device_ID)。

[0189] 在如过程400所述的另一实施例中，可以修改步骤1165，使得第二认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m2和认证单元签名(表示为Sig_SP)。加密消息m2通过使用K_S对RAND3进行加密而获得，并且可使用以下方式表示：m2=En(RAND3,K_S)。

[0190] 在如过程500所述的另一实施例中，可以修改步骤1165，使得第二认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的设备的DH公钥(A)、认证单元的DH公钥(C)和认证单元签名(表示为Sig_SP)。

[0191] 在步骤1170中，响应于从运营提供商220接收到第一认证响应消息，过程1100通过验证AN签名(Sig_AN)来认证运营提供商220。具体地，设备使用AN的ID(AN_ID)和GPK来验证AN签名(Sig_AN)。如果认证成功，则过程1100使用设备的私钥解密消息m1以获得RAND2，并使用预定义的KDF导出密钥(K_com)。KDF的输入参数应包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1,RAND2,.....)。

[0192] 在如过程400所述的另一实施例中，可以修改步骤1170，使得在过程1100通过验证AN签名(Sig_AN)成功认证AN之后，过程1100使用K_C解密消息m1以获得RAND2。然后，过程1100使用预定义的KDF导出密钥(K_com)。KDF的输入参数包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1,RAND2,……)。

[0193] 在如过程500所述的另一实施例中，可以修改步骤1170，使得在过程1100通过验证AN签名(Sig_AN)成功认证AN之后，过程1100使用所接收的DH公钥导出密钥(K_com)，即$K_com=B^{RAND2} \bmod p$。

[0194] 在步骤1170中，响应于从运营提供商220或直接从服务提供商230接收到第二认证响应消息，过程1100通过验证其签名(Sig_SP)来认证服务提供商230。如果认证成功，则过程1100使用其私钥解密消息m2以获得RAND3，并使用预定义的KDF导出密钥(K_ser)。KDF的输入参数应包括RAND1和RAND3，并且可使用以下方式表示：K_ser=KDF(RAND1,RAND3,……)。

[0195] 在如过程400所述的另一实施例中，可以修改步骤1170，使得在过程1100通过验证服务提供商230的签名(Sig_SP)成功认证服务提供商230之后，过程1100使用其私钥解密消息m2以获得RAND3，使用预定义的KDF导出密钥(K_ser)。KDF的输入参数应包括RAND1和RAND3，并且可使用以下方式表示：K_ser=KDF(RAND1,RAND3,……)。

[0196] 在如过程500所述的另一实施例中，可以修改步骤1170，使得在过程1100通过验证服务提供商230的签名(Sig_SP)成功认证服务提供商230之后，过程1100使用所接收的DH公钥导出密钥(K_ser)，即$K_ser=C^{RAND1} \bmod p$。

[0197] 在步骤1175中，过程1100根据在步骤1165中设备接收到的是第一认证响应消息还是第二认证响应消息，将用于运营提供商220的第一凭证或用于服务提供商230的第二凭证保存在存储器中。第一凭证包括密钥(K_com)。第二凭证包括密钥(K_ser)。

[0198] 在步骤1180中，过程1100根据在步骤1165中设备接收到的是第一认证响应消息还是第二认证响应消息，生成第一消息认证码(MAC1)并向运营提供商220传输第一消息认证码，生成第二消息认证码MAC2并向服务提供商230传输第二消息认证码。使用MAC生成函数生成MAC1，其中RAND2和K_com作为输入。使用MAC生成函数生成MAC2，其中RAND3和K_ser作为输入。

[0199] 在步骤1185中，过程1100确定是否已接收到两个认证响应消息。如果已经接收到两个认证响应消息，则过程1100结束。否则，过程1100从步骤1165重复并等待第二认证响应。

[0200] 图12示出了由运营提供商220的认证节点执行的过程1200。过程1200开始于步骤1205，即从设备210接收认证消息。

[0201] 在步骤1210中，过程1200基于认证类型(Auth. Type)250确定认证的类型。如果Auth. Type指示1，则过程1200确定第一类型的认证，并且此后继续执行步骤1260。如果Auth. Type指示2，则过程1200确定第二类型的认证，并且此后继续执行步骤1240。如果Auth. Type指示3，则过程1200确定第三类型的认证，并且此后继续执行步骤1215。

[0202] 在步骤1215中，过程1200将认证消息转发给服务提供商230的认证单元。

[0203] 在步骤1240中，过程1200基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地，认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则过程1200在步骤1245中生成随机数(RAND2)并使用预定义的密钥导出函数(key derivation function，KDF)导出密钥(表示为K_com)。KDF的输入参数包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1，RAND2，……)。

[0204] 在步骤1250中，过程1200生成加密消息m1，并向设备210发送认证响应消息。加密消息m1根据IBE使用Device_ID加密RAND2而获得，并且可使用以下方式表示：m1=En(RAND2，Device_ID)。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0205] 在步骤1255中，过程1200从设备210接收MAC1。作为响应，过程1200通过使用相同MAC生成函数生成MAC来验证MAC1，其中RAND2和K_com作为输入，并且查看MAC1是否等于MAC。如果MAC等于MAC1，则过程1200在步骤1258中将K_com、RAND1和RAND2保存在存储器中。本领域技术人员将认识到，认证节点可以在该步骤中而不是在步骤1245中导出密钥(表示为K-com)。具体地，在接收到MAC1时，认证节点在对MAC1进行验证之前导出密钥(表示为K-com)。

[0206] 在步骤1260中，过程1200基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地，认证节点使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则过程1200生成随机数(RAND2)并使用预定义的密钥导出函数(key derivation function，KDF)导出密钥(表示为K_com)。KDF的输入参数包括RAND1和RAND2，并且可使用以下方式表示：K_com=KDF(RAND1，RAND2，……)。

[0207] 在步骤1265中，过程1200将认证消息转发给服务提供商的认证单元。本领域技术人员将认识到，步骤1265可以在步骤1260之前发生而不脱离本发明。

[0208] 在步骤1270中，过程1200生成加密消息m1，并向设备210发送认证响应消息。加密消息m1根据IBE使用Device_ID加密RAND2而获得，并且可使用以下方式表示：m1=En(RAND2，Device_ID)。认证响应消息包括AN的ID(表示为AN_ID)、从设备接收的随机数(RAND1)、加密消息m1和AN签名(表示为Sig_AN)。AN签名由AN通过IBS使用AN的秘密密钥(SKID)和GPK生成。

[0209] 在步骤1275中，过程1200从设备210接收MAC1。作为响应，过程1200对MAC1进行验

证。为了对MAC1进行验证，AN使用相同MAC生成函数生成MAC，其中RAND2和K_com作为输入，并查看MAC1是否等于MAC。如果MAC1等于MAC，则过程1200在步骤1280中将K-com保存在存储器中。本领域技术人员将认识到，认证节点可以在该步骤中而不是在步骤1260中导出密钥(表示为K-com)。具体地，在接收到MAC1时，认证节点在对MAC1进行验证之前导出密钥(表示为K-com)。

[0210] 过程1200在步骤1280之后结束。

[0211] 图13示出了由服务提供商230的认证单元执行的过程1300。过程1300开始于步骤1305，即从AN接收认证消息。认证消息包括认证类型(Auth. Type)250、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。可能的消息格式如下：(Auth.Type,SP_ID,Device_ID,RAND1,Sig_De,……)。

[0212] 在步骤1310中，过程1300基于IBS使用设备ID(Device_ID)来验证设备签名(Sig_De)。具体地，认证单元使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则过程1300在步骤1315中生成随机数(RAND2)并使用预定义的密钥导出函数(key derivation function,KDF)导出密钥(表示为K_ser)。KDF的输入参数应包括RAND1和RAND2，并且可使用以下方式表示:K_ser=KDF(RAND1,RAND2,……)。

[0213] 在步骤1320中，过程1300生成加密消息(m)，并向设备210发送认证响应消息。加密消息m根据IBE使用Device_ID加密RAND2而获得，并且可使用以下方式表示:m=En(RAND2,Device_ID)。认证响应消息包括认证单元的ID(表示为SP_ID)、从设备接收的随机数(RAND1)、加密消息m和认证单元签名(表示为Sig_SP)。认证单元签名由认证单元通过IBS使用认证单元的秘密密钥(SKID)和GPK生成。

[0214] 在步骤1325中，过程1300从设备210接收MAC1。作为响应，过程1300对MAC1进行验证。为了对MAC1进行验证，过程1300使用相同MAC生成函数生成MAC，其中RAND2和K_ser作为输入，并查看MAC1是否等于MAC。如果MAC1等于MAC，则过程1300在步骤1330中将包括K_ser的凭证保存在存储器中。本领域技术人员将认识到，认证单元可以在该步骤中而不是在步骤1315中导出密钥(表示为K-ser)。具体地，在接收到MAC1时，认证单元在对MAC1进行验证之前导出密钥(表示为K-ser)。

[0215] 过程1300在步骤1330之后结束。

[0216] 总而言之，如果设备210想要与运营和/或服务提供商网络进行认证，则该设备生成认证数据包并向运营提供商网络传输该认证数据包。认证数据包包括认证消息，包括认证类型(Auth. Type)、服务提供商网络的ID(SP_ID)、设备ID(Device_ID)、RAND1和设备签名(Sig_De)。

[0217] 响应于接收到认证数据包，运营提供商网络确定认证的类型。如果认证是第一类型或第三类型，则运营提供商网络将认证数据包转发到服务提供商网络。运营提供商网络和服务提供商网络都会相应地处理认证数据包，即首先通过验证设备签名(Sig_De)来认证设备。具体地，运营提供商网络和服务提供商网络使用设备ID(Device_ID)和GPK来验证设备签名(Sig_De)。如果验证成功，则运营提供商网络和服务提供商网络分别生成RAND2和RAND3。此后，运营提供商网络和服务提供商网络分别生成K_com(使用具有RAND1和RAND2的KDF)和K-ser(使用具有RAND1和RAND3的KDF)。随机数(RAND2和RAND3)通过IBE使用设备ID进行加密，然后和各自对应的签名(Sig_AN和Sig_SP)一起传输给设备。或者，可以在运营商

和服务提供商接收到MAC1和MAC2之后生成会话密钥K-com和K-ser。

[0218] 响应于从运营提供商网络和服务提供商网络接收到加密的随机数，设备使用相应的身份(Sig_ID和SP_ID)来认证签名。如果验证成功，则设备解密随机数(RAND2和RAND3)并使用RAND2和RAND1导出用于运营提供商网络的第一会话密钥，并使用RAND3和RAND1导出用于服务提供商网络的第二会话密钥。然后，设备使用MAC生成函数为运营提供商网络生成第一消息认证码(MAC1)，其中RAND2和K_com作为输入，并使用MAC生成函数为服务提供商网络生成第二消息认证码(MAC2)，其中RAND3和K_ser作为输入。然后向运营提供商网络传输MAC1和MAC2。

[0219] 响应于接收到MAC1和MAC2，运营提供商网络首先认证MAC1。在可选实施例中，运营提供商网络和网络提供商网络分别在认证MAC1和MAC2之前生成K_com和K-ser。如果验证成功，则运营提供商网络保存第一会话密钥并将MAC2转发到服务提供商网络。响应于接收到MAC2，服务提供商网络验证MAC2。如果验证成功，则运营提供商网络保存第二会话密钥。

[0220] 第一会话密钥K-com和第二会话密钥K-ser分别由设备用于与运营提供商网络和服务提供商网络进行通信。

[0221] 所提出的方法可以应用于需要网络接入认证和服务认证的所有通信系统，包括5G通信系统的所有三个主要应用场景：增强型移动宽带(enhanced Mobile BroadBand，eMBB)、大规模物联网(massive Internet of Things，mIoT)、高可靠低延迟通信(Ultra Reliable Low Latency Communication，uRLLC)。

[0222] 所提出的网络和服务统一认证使用一个认证数据包来生成两组会话密钥(一组用于网络，另一组用于服务)，可以有效地分离网络运营商和服务提供商之间的信息。

[0223] 注意，UE、设备、运营提供商网络的各种单元以及服务提供商网络的各种单元是众所周知的。因此，为简洁起见，省略了UE、设备、运营提供商网络的单元和服务提供商网络的单元中的每一个的操作系统、配置、结构、组件等。重要的是，根据本发明实施例的方法和系统以存储在存储介质上的指令形式提供，并且可由相应UE、设备、认证节点等运营提供商网络的单元和认证单元等服务提供商网络的单元的处理器执行。

[0224] 以上是对用于与运营提供商和/或服务提供商进行认证的统一认证框架的方法和系统的实施例的描述。

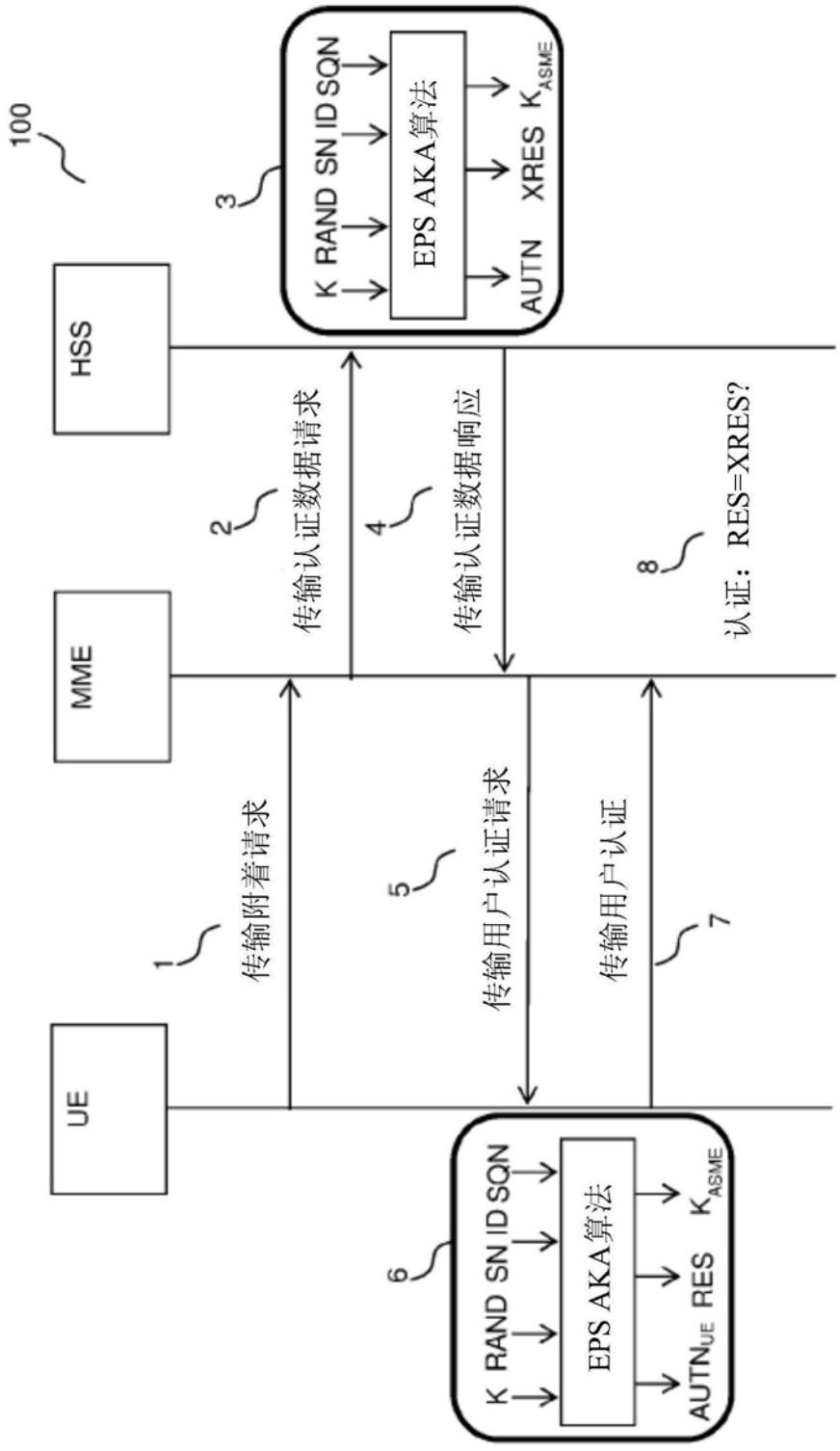

100
HSS
MME
UE
3
K RAND SN ID SQN
EPS AKA算法
AUTN XRES K_{ASME}
2
传输认证数据请求
4
传输认证数据响应
8
认证：RES=XRES?
1
传输附着请求
5
传输用户认证请求
传输用户认证
7
6
K RAND SN ID SQN
EPS AKA算法
$AUTN_{UE}$ RES K_{ASME}

图1

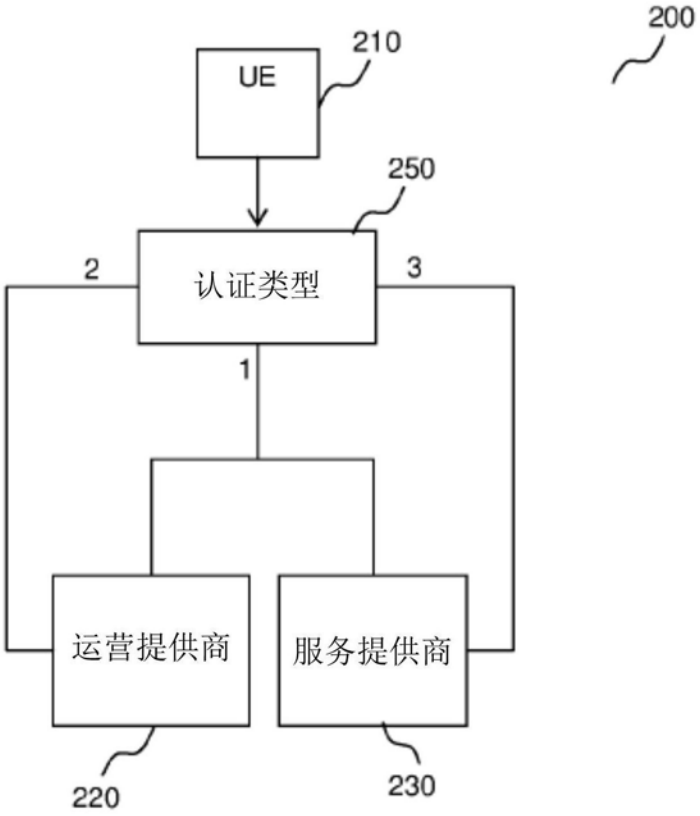


图2

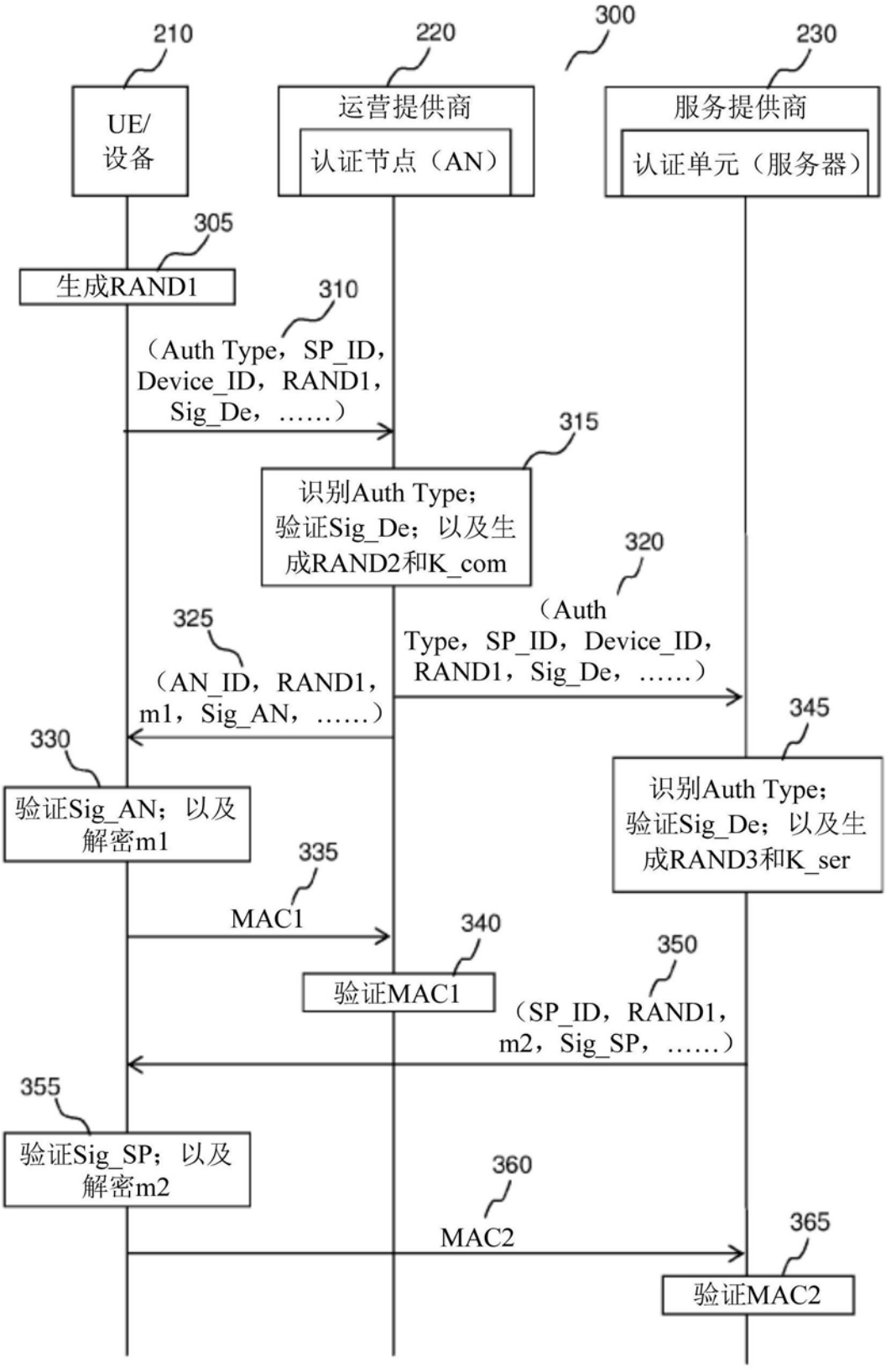

210
220
300
230
UE/
设备
运营提供商
认证节点（AN）
服务提供商
认证单元（服务器）
305
生成RAND1
310
（Auth Type，SP_ID，
Device_ID，RAND1，
Sig_De，……）
315
识别Auth Type；
验证Sig_De；以及生
成RAND2和K_com
320
（Auth
Type，SP_ID，Device_ID，
RAND1，Sig_De，……）
325
（AN_ID，RAND1，
m1，Sig_AN，……）
345
识别Auth Type；
验证Sig_De；以及生
成RAND3和K_ser
330
验证Sig_AN；以及
解密m1
335
MAC1
340
验证MAC1
350
（SP_ID，RAND1，
m2，Sig_SP，……）
355
验证Sig_SP；以及
解密m2
360
MAC2
365
验证MAC2

图3

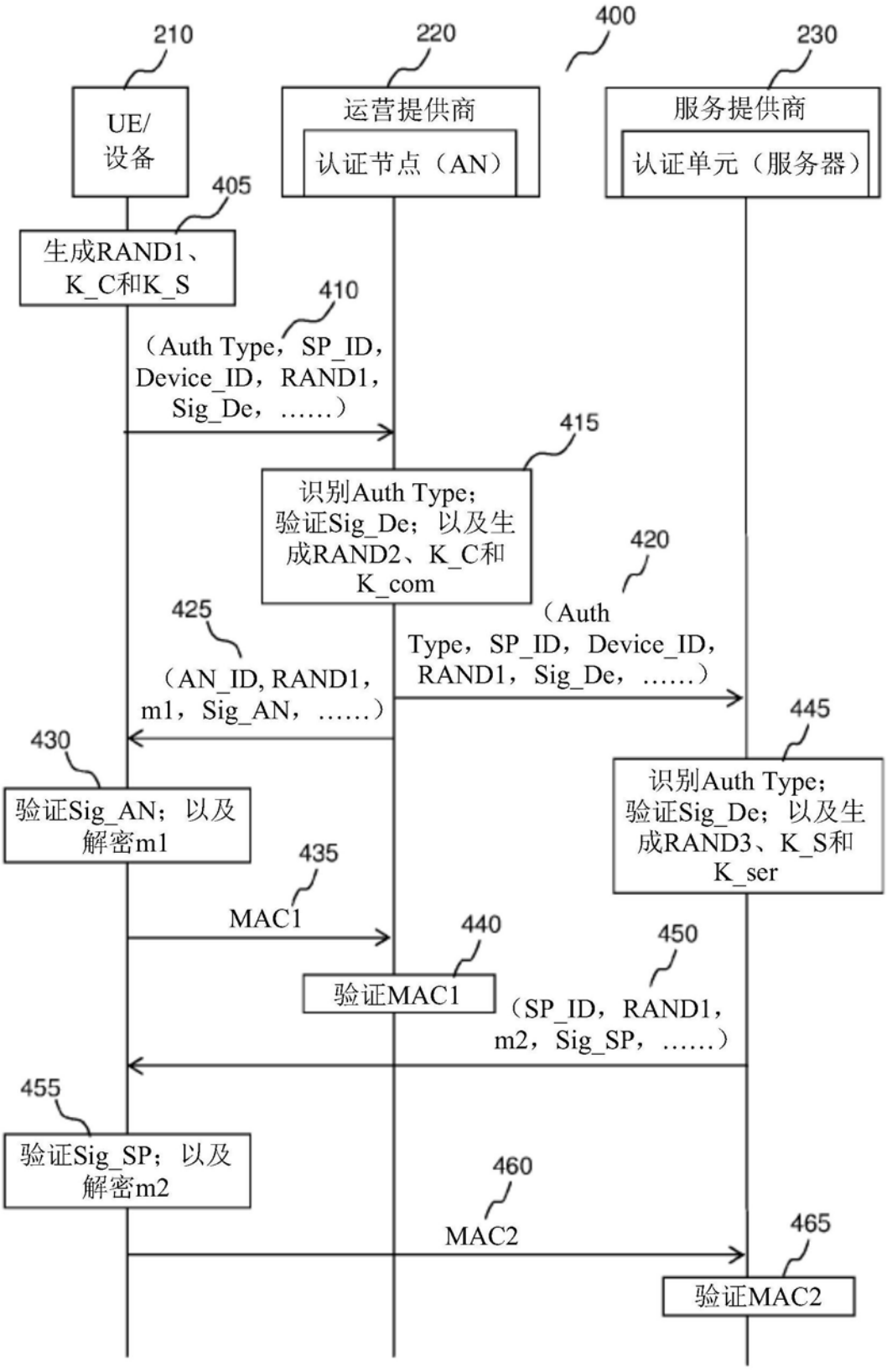

210
220
400
230
UE/
设备
运营提供商
认证节点（AN）
服务提供商
认证单元（服务器）
405
生成RAND1、
K_C和K_S
410
（Auth Type，SP_ID，
Device_ID，RAND1，
Sig_De，……）
415
识别Auth Type；
验证Sig_De；以及生
成RAND2、K_C和
K_com
420
（Auth
Type，SP_ID，Device_ID，
RAND1，Sig_De，……）
425
（AN_ID, RAND1，
m1，Sig_AN，……）
430
验证Sig_AN；以及
解密m1
445
识别Auth Type；
验证Sig_De；以及生
成RAND3、K_S和
K_ser
435
MAC1
440
验证MAC1
450
（SP_ID，RAND1，
m2，Sig_SP，……）
455
验证Sig_SP；以及
解密m2
460
MAC2
465
验证MAC2

图4

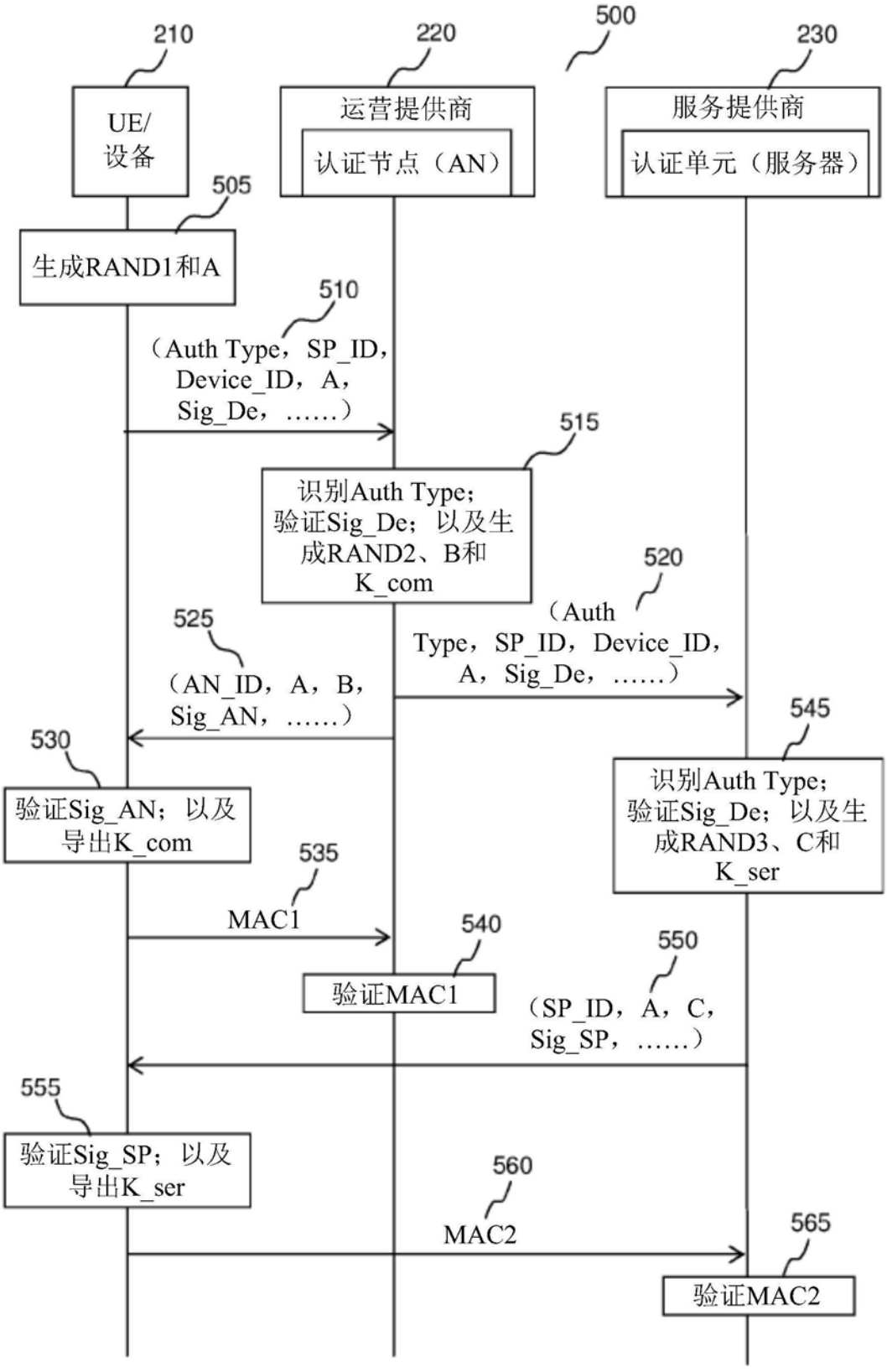

500
210
220
230
UE/
设备
运营提供商
认证节点（AN）
服务提供商
认证单元（服务器）
505
生成RAND1和A
510
（Auth Type，SP_ID，
Device_ID，A，
Sig_De，……）
515
识别Auth Type；
验证Sig_De；以及生
成RAND2、B和
K_com
520
（Auth
Type，SP_ID，Device_ID，
A，Sig_De，……）
525
（AN_ID，A，B，
Sig_AN，……）
530
验证Sig_AN；以及
导出K_com
545
识别Auth Type；
验证Sig_De；以及生
成RAND3、C和
K_ser
535
MAC1
540
验证MAC1
550
（SP_ID，A，C，
Sig_SP，……）
555
验证Sig_SP；以及
导出K_ser
560
MAC2
565
验证MAC2

图5

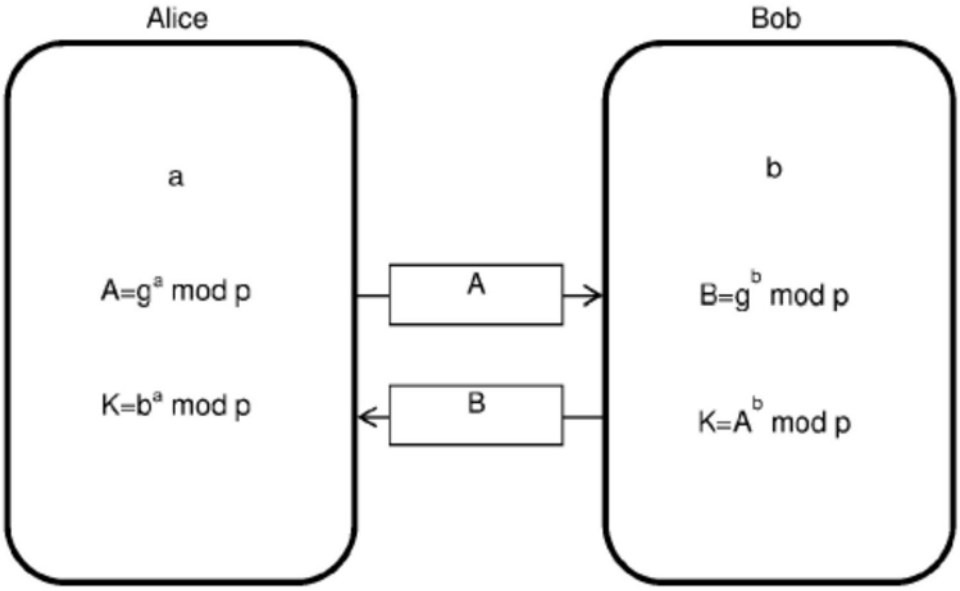


图6

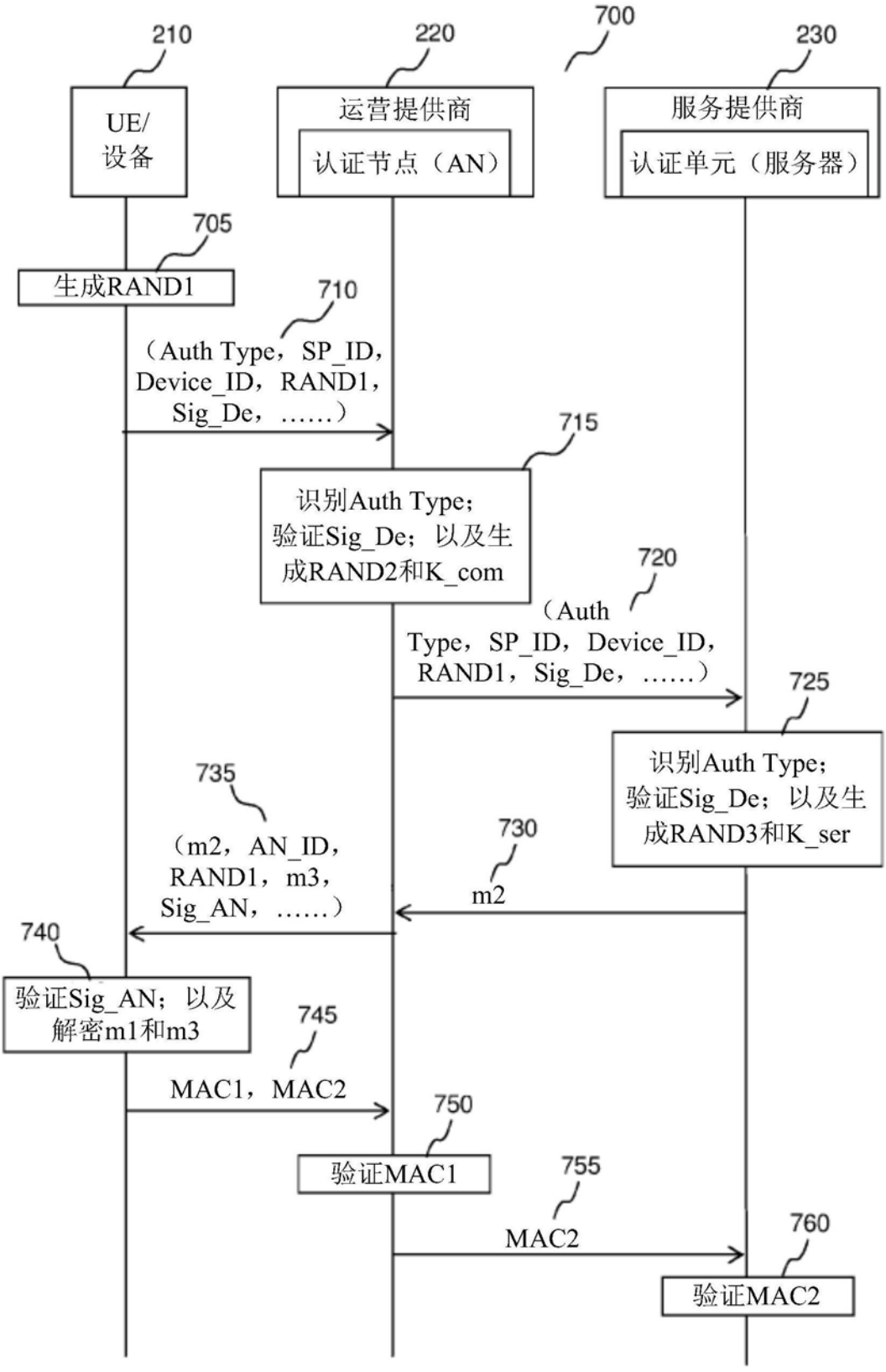

700
210
220
230
UE/
设备
运营提供商
认证节点（AN）
服务提供商
认证单元（服务器）
705
生成RAND1
710
（Auth Type，SP_ID，
Device_ID，RAND1，
Sig_De，……）
715
识别Auth Type；
验证Sig_De；以及生
成RAND2和K_com
720
（Auth
Type，SP_ID，Device_ID，
RAND1，Sig_De，……）
725
识别Auth Type；
验证Sig_De；以及生
成RAND3和K_ser
735
（m2，AN_ID，
RAND1，m3，
Sig_AN，……）
730
m2
740
验证Sig_AN；以及
解密m1和m3
745
MAC1，MAC2
750
验证MAC1
755
MAC2
760
验证MAC2

图7

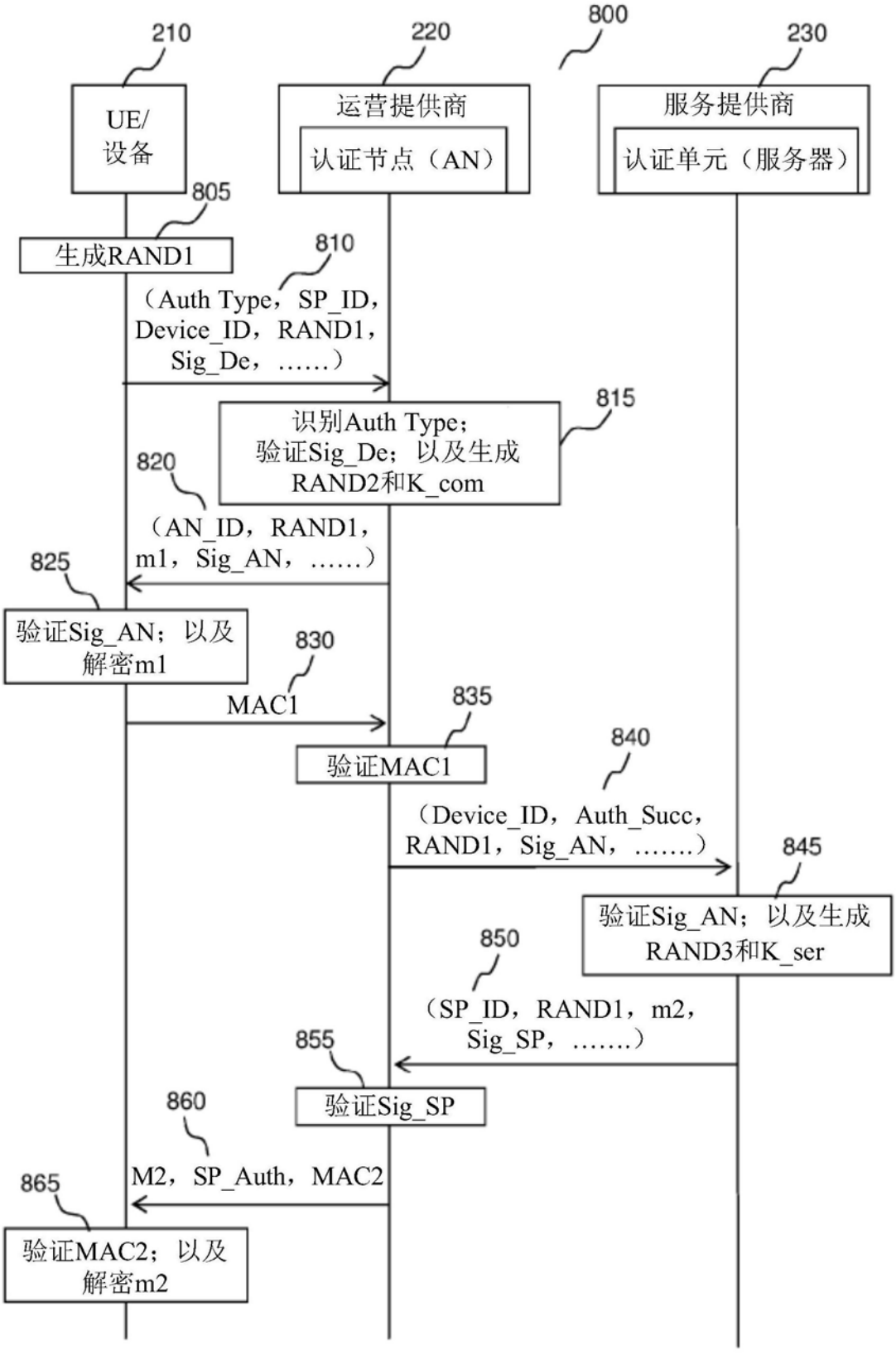

210
220
800
230
UE/
设备
运营提供商
认证节点（AN）
服务提供商
认证单元（服务器）
805
生成RAND1
810
（Auth Type，SP_ID，
Device_ID，RAND1，
Sig_De，……）
815
识别Auth Type；
验证Sig_De；以及生成
RAND2和K_com
820
（AN_ID，RAND1，
m1，Sig_AN，……）
825
验证Sig_AN；以及
解密m1
830
MAC1
835
验证MAC1
840
（Device_ID，Auth_Succ，
RAND1，Sig_AN，……）
845
验证Sig_AN；以及生成
RAND3和K_ser
850
（SP_ID，RAND1，m2，
Sig_SP，……）
855
验证Sig_SP
860
M2，SP_Auth，MAC2
865
验证MAC2；以及
解密m2

图8

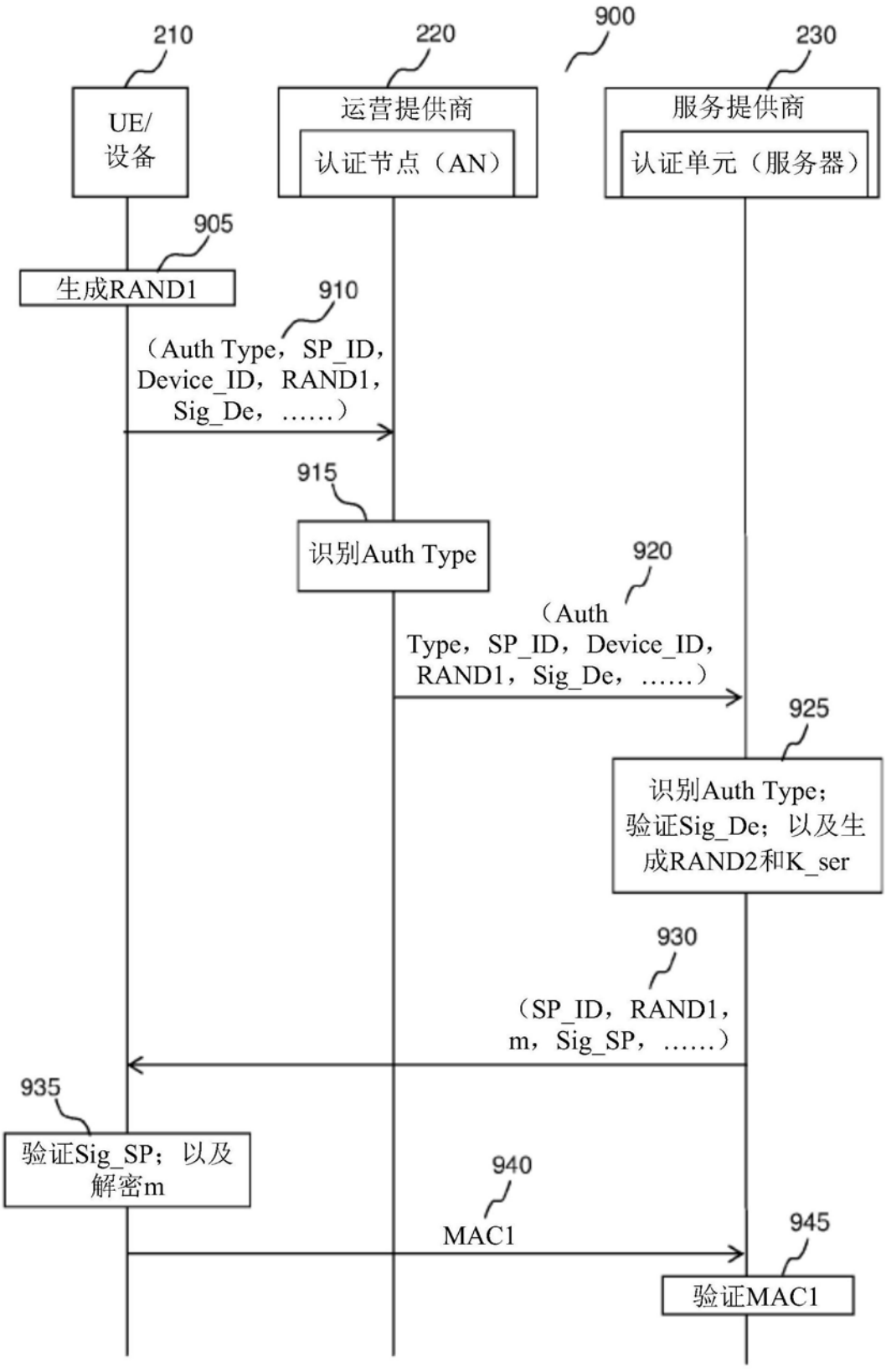

900
210
220
230
UE/
设备
运营提供商
认证节点（AN）
服务提供商
认证单元（服务器）
905
生成RAND1
910
（Auth Type，SP_ID，
Device_ID，RAND1，
Sig_De，……）
915
识别Auth Type
920
（Auth
Type，SP_ID，Device_ID，
RAND1，Sig_De，……）
925
识别Auth Type；
验证Sig_De；以及生
成RAND2和K_ser
930
（SP_ID，RAND1，
m，Sig_SP，……）
935
验证Sig_SP；以及
解密m
940
MAC1
945
验证MAC1

图9

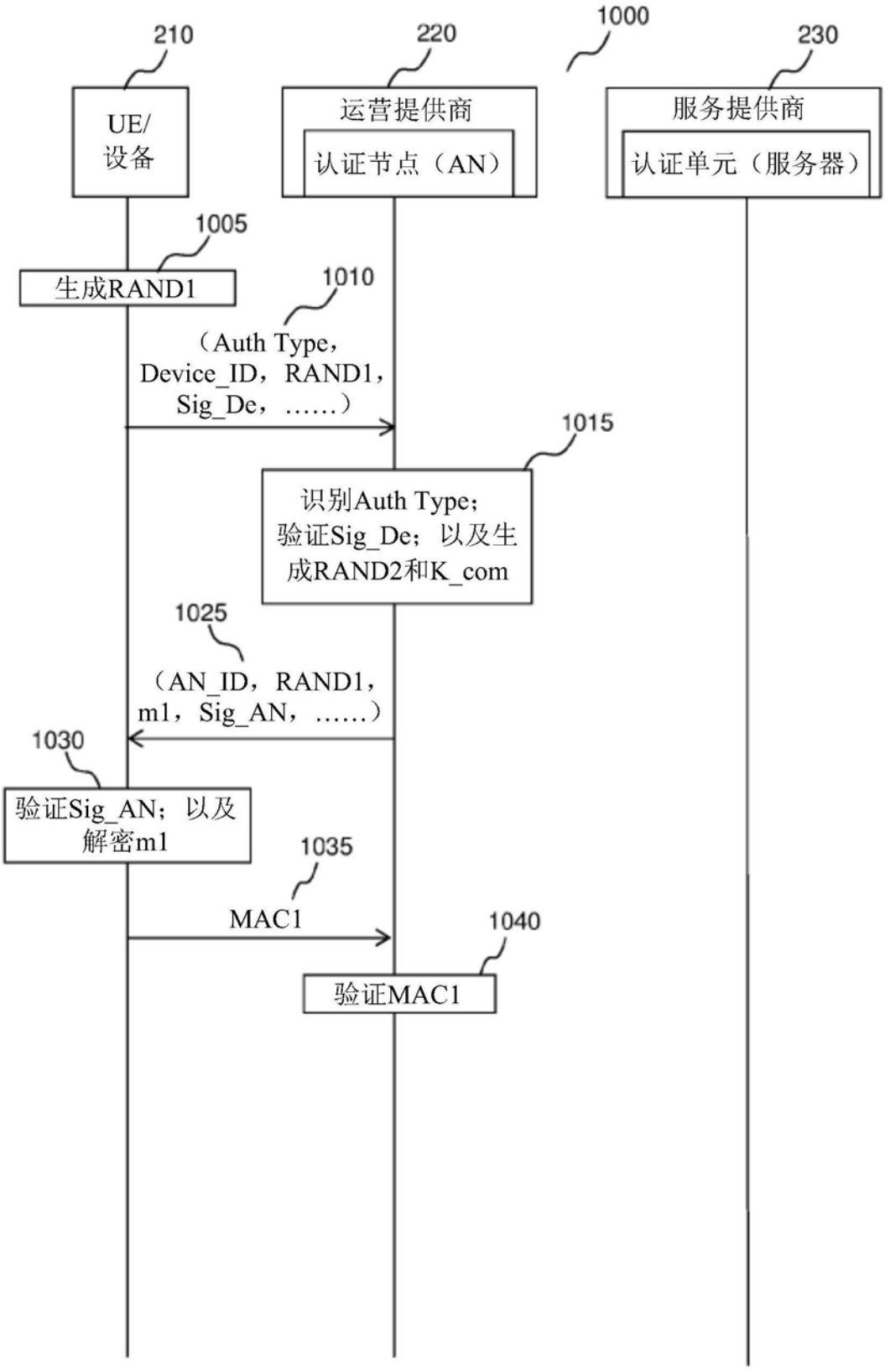

210
220
1000
230
UE/
设备
运营提供商
认证节点（AN）
服务提供商
认证单元（服务器）
1005
生成RAND1
1010
（Auth Type，
Device_ID，RAND1，
Sig_De，……）
1015
识别Auth Type；
验证Sig_De；以及生
成RAND2和K_com
1025
（AN_ID，RAND1，
m1，Sig_AN，……）
1030
验证Sig_AN；以及
解密m1
1035
MAC1
1040
验证MAC1

图10

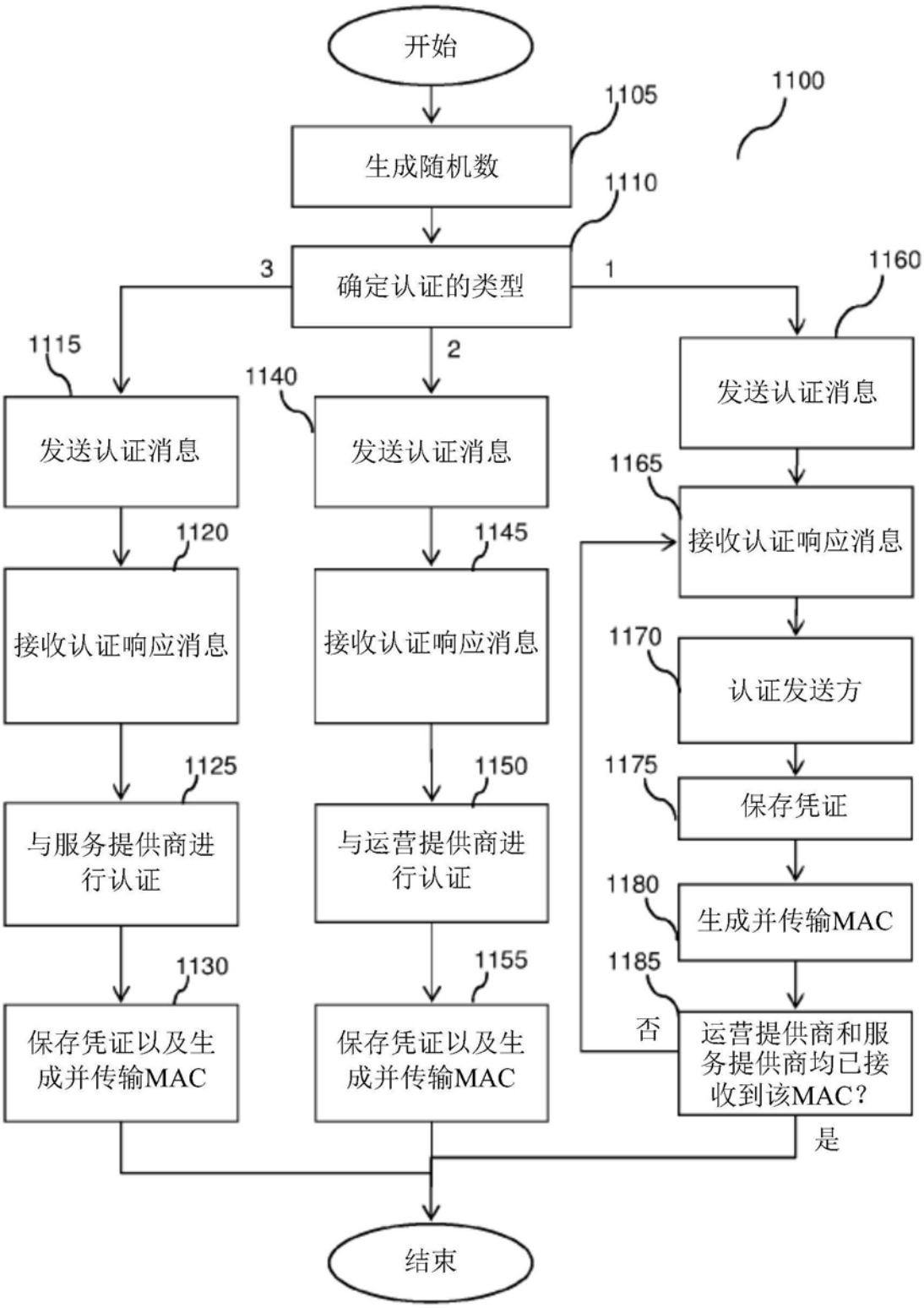

开始
1100
1105
生成随机数
1110
确定认证的类型
3
1
2
1160
发送认证消息
1115
发送认证消息
1140
发送认证消息
1165
接收认证响应消息
1120
接收认证响应消息
1145
接收认证响应消息
1170
认证发送方
1125
与服务提供商进行认证
1150
与运营提供商进行认证
1175
保存凭证
1180
生成并传输MAC
1130
保存凭证以及生成并传输MAC
1155
保存凭证以及生成并传输MAC
1185
否
运营提供商和服务提供商均已接收到该MAC?
是
结束

图11

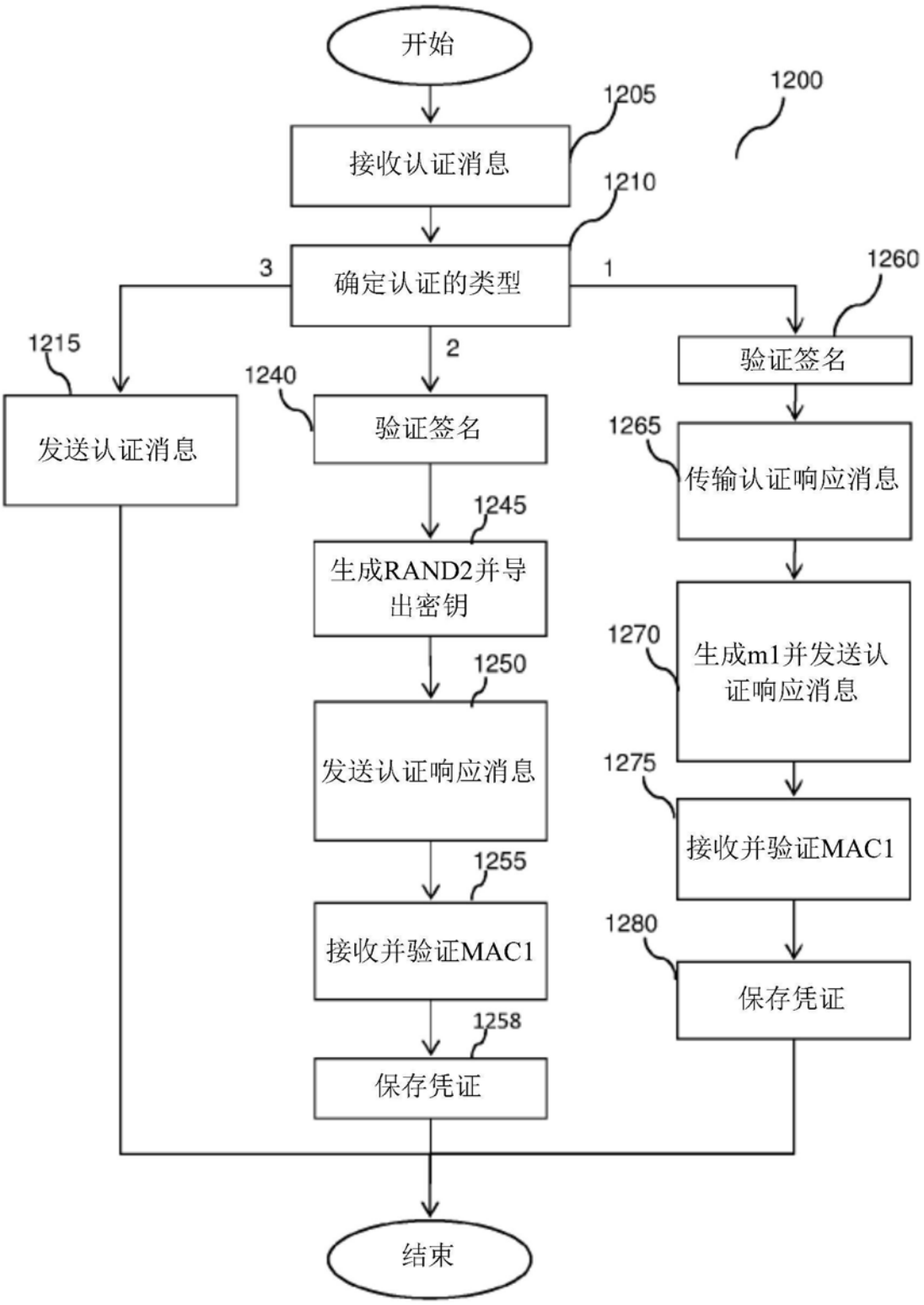

开始
1200
1205
接收认证消息
1210
确定认证的类型
3
1
2
1260
验证签名
1215
发送认证消息
1240
验证签名
1265
传输认证响应消息
1245
生成RAND2并导出密钥
1270
生成m1并发送认证响应消息
1250
发送认证响应消息
1275
接收并验证MAC1
1255
接收并验证MAC1
1280
保存凭证
1258
保存凭证
结束

图12

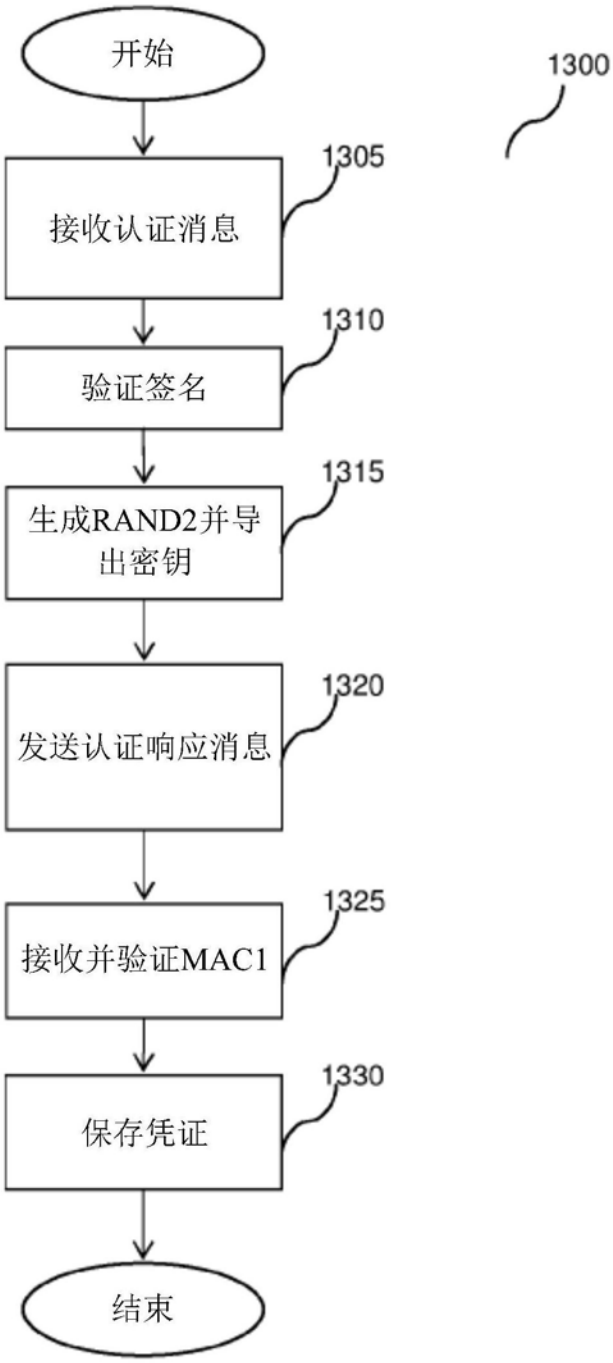

开始
1300
1305
接收认证消息
1310
验证签名
1315
生成RAND2并导出密钥
1320
发送认证响应消息
1325
接收并验证MAC1
1330
保存凭证
结束

图13