(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 106576237 B
(45)授权公告日 2020.10.16

(21)申请号 201480080618.1
(22)申请日 2014.07.21
(65)同一申请的已公布的文献号
申请公布号 CN 106576237 A
(43)申请公布日 2017.04.19
(85)PCT国际申请进入国家阶段日
2017.01.12
(86)PCT国际申请的申请数据
PCT/CN2014/082656 2014.07.21
(87)PCT国际申请的公布数据
WO2016/011588 ZH 2016.01.28
(73)专利权人 宇龙计算机通信科技(深圳)有限公司
地址 518057 广东省深圳市南山区科技园北区梦溪道2号
(72)发明人 钟焰涛
(74)专利代理机构 北京友联知识产权代理事务所(普通合伙) 11343
代理人 尚志峰 汪海屏
(51)Int.Cl.
H04W 12/00(2006.01)
(56)对比文件
CN 102131188 A,2011.07.20
US 2008130898 A1,2008.06.05
CN 1801029 A,2006.07.12
CN 1801029 A,2006.07.12
CN 101552668 A,2009.10.07
CN 102036236 A,2011.04.27
CN 101267303 A,2008.09.17
US 2011314522 A1,2011.12.22
KR 20030015790 A,2003.02.25
WO 2011052995 A2,2011.05.05
WO 2008047195 A1,2008.04.24
审查员 缪伶娥
权利要求书3页 说明书9页 附图7页

(54)发明名称

移动管理实体、归属服务器、终端、身份认证系统和方法

(57)摘要

本发明提供了一种移动管理实体、一种归属服务器、一种终端和一种身份认证系统和身份认证方法,移动管理实体包括:发送单元,在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时,发送身份认证请求、加密密钥以及对应的数字证书至终端,以供终端根据数字证书对移动管理实体进行验证,在验证通过时使用加密密钥对国际移动用户识别码进行加密并发送至移动管理实体;接收单元,接收终端发送的加密后的国际移动用户识别码;解密单元,根据存储的与加密密钥对应的解密密钥对加密后的国际移动用户识别码进行解密。通过本发明的技术方案,可以确保只有合法的基站和合法的移动管理实体才能完成身份认证流程并获取国际移动用户识别码。

CN 106576237 B

1.一种移动管理实体,其特征在于,包括:

发送单元,在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时,发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至终端,以供所述终端根据所述数字证书对所述移动管理实体进行验证,并在验证通过时,所述终端使用所述加密密钥对国际移动用户识别码进行加密,并将加密后的国际移动用户识别码发送至所述移动管理实体;

接收单元,接收所述终端发送的所述加密后的国际移动用户识别码;

解密单元,根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密;

所述发送单元还用于:

将所述加密密钥和所述移动管理实体的实体身份信息发送至归属服务器,以供所述归属服务器对所述移动管理实体的身份进行验证,并在验证通过时,生成与所述加密密钥对应的数字证书发送至所述移动管理实体;

所述接收单元还用于:

接收所述归属服务器发送的与所述加密密钥对应的所述数字证书。

2.根据权利要求1所述的移动管理实体,其特征在于,还包括:

密钥生成单元,在所述移动管理实体首次接入网络时,生成加密密钥和与所述加密密钥对应的解密密钥;

存储单元,存储所述加密密钥和与所述加密密钥对应的解密密钥。

3.根据权利要求1或2所述的移动管理实体,其特征在于,还包括:

处理单元,在接收到所述终端发送的终止验证的信息时,停止验证。

4.一种归属服务器,其特征在于,包括:

接收单元,接收移动管理实体发送的加密密钥和所述移动管理实体的实体身份信息;

验证单元,根据所述加密密钥和所述移动管理实体的实体身份信息对所述移动管理实体的身份进行验证;

生成单元,在验证通过时,生成与所述加密密钥对应的数字证书;

发送单元,发送所述数字证书至所述移动管理实体;

其中,在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时,所述移动管理实体发送身份认证请求、所述加密密钥以及与所述加密密钥对应的所述数字证书至终端,以供所述终端根据所述数字证书对所述移动管理实体进行验证,并在验证通过时,所述终端使用所述加密密钥对国际移动用户识别码进行加密并将加密后的国际移动用户识别码发送至所述移动管理实体。

5.一种终端,其特征在于,包括:

接收单元,接收移动管理实体发送的身份认证请求、加密密钥以及数字证书;

验证单元,根据所述身份认证请求,对所述移动管理实体的数字证书进行验证;

加密单元,在所述数字证书验证通过时,通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密,以得到加密后的国际移动用户识别码;

发送单元,将所述加密后的国际移动用户识别码发送至所述移动管理实体;

所述加密单元包括:

获取单元，在所述数字证书验证通过时，获取所述终端中的国家移动用户识别码；

计算单元，根据所述加密密钥和预设的加密函数对所述国际移动用户识别码进行计算，以得到加密后的国际移动用户识别码；

其中，归属服务器为每个身份验证成功的所述移动管理实体颁发一个与所述加密密钥对应的所述数字证书；在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，所述移动管理实体发送身份认证请求、所述加密密钥以及与所述加密密钥对应的所述数字证书至终端。

6.根据权利要求5所述的终端，其特征在于，还包括：

处理单元，在所述数字证书验证未通过时，停止验证，并向所述移动管理实体发送终止验证的信息。

7.一种身份认证系统，其特征在于，包括权利要求1至3中任一项所述的移动管理实体，权利要求4所述的归属服务器和权利要求5或6所述的终端。

8.一种身份认证方法，用于身份认证系统，所述身份认证系统包括移动管理实体、终端和归属服务器，其特征在于，

所述移动管理实体在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至所述终端；

所述终端接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书，根据所述身份认证请求，对所述移动管理实体的数字证书进行验证；

在所述数字证书验证通过时，所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密，并将加密后的国际移动用户识别码发送至所述移动管理实体；

所述移动管理实体根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密；

所述移动管理实体将所述加密密钥和所述移动管理实体的实体身份信息发送至所述归属服务器；

所述归属服务器接收移动管理实体发送的加密密钥和所述移动管理实体的实体身份信息，并根据所述加密密钥和所述移动管理实体的实体身份信息对所述移动管理实体的身份进行验证；

在所述移动管理实体的身份验证通过时，所述归属服务器生成与所述加密密钥对应的数字证书，并发送所述数字证书至所述移动管理实体；

所述移动管理实体接收所述归属服务器发送的与所述加密密钥对应的所述数字证书。

9.根据权利要求8所述的身份认证方法，其特征在于，还包括：

所述移动管理实体在首次接入网络时，生成加密密钥和与所述加密密钥对应的解密密钥，并存储所述加密密钥和与所述加密密钥对应的解密密钥。

10.根据权利要求8所述的身份认证方法，其特征在于，在所述数字证书验证通过时，所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密，具体包括：

在所述数字证书验证通过时，所述终端获取国家移动用户识别码，并根据所述加密密

钥和预设的加密函数对所述国际移动用户识别码进行计算,以得到加密后的国际移动用户识别码。

11.根据权利要求8至10中任一项所述的身份认证方法,其特征在于,还包括:

在所述数字证书验证未通过时,所述终端停止验证,并向所述移动管理实体发送终止验证的信息;

所述移动管理实体在接收到所述终端发送的终止验证的信息时,停止验证。

移动管理实体、归属服务器、终端、身份认证系统和方法

技术领域

[0001] 本发明涉及终端技术领域，具体而言，涉及一种移动管理实体、一种归属服务器、一种终端、一种身份认证系统和一种身份认证方法。

背景技术

[0002] 在LTE(Long Term Evolution，长期演进)网络中，演进分组系统EPS(Evolved Packet System)中的AKA(Authentication and Key Agreement，鉴权和密钥协商)是保证安全性的重要手段，而EPS-AKA的具体过程如图1所示。

[0003] 而鉴权和密钥协商后，UE(User Equipment，用户设备)和MME(Mobility Management Entity，移动管理实体)之间会产生一个中间密钥KASME，然后UE和MME会根据所述密钥KASME，进行如图2所示的鉴权流程，鉴权结束后，MME会为UE分配临时的GUTI(Globally Unique Temporary UE Identity，全球唯一临时UE标识)码，并维护GUTI码和UE的IMSI(International Mobile Subscriber Identity，国际移动用户标识)码之间的映射关系，这样，MME就可以通过用户唯一的标识GUTI码对UE进行呼叫，并通过跟踪IMSI码来实现对用户的跟踪。

[0004] 但MME可能会由于某种原因，误认为丢失GUTI码和用户UE的IMSI之间的映射关系(例如，UE返回错误的RES、UE因MME向UE发送的AUTH参数中分离出的MAC参数验证不正确而返回带有MAC failure的reject信息或UE因MME发送的AMF参数中某一位的值不正确而返回带有non-EPS authentication unacceptable的reject信息。)时，MME就要求UE以明文方式将IMSI码发给自己，以重新分配GUTI码。

[0005] 但是，如图3所示的身份认证流程就可能被攻击者利用，攻击者可以通过伪基站发射强大信号，淹没合法基站的信号，并以伪基站信号发起如图3所示的身份认证流程，以迫使UE以明文形式发送IMSI码给伪基站，从而获取用户的IMSI码，并非法利用用户的隐私信息，这对用户的隐私带来很大的威胁。

[0006] 因此，如何有效地保护UE发出的IMSI码，以确保只有合法的基站和合法的MME才能完成身份认证流程并获取IMSI码，而非法的基站和非法的MME无法完成上述身份认证流程，也无法获取UE的IMSI码，成为亟待解决的问题。

发明内容

[0007] 本发明正是基于上述问题，提出了一种新的技术方案，可以有效地提高UE发出的IMSI码的安全性，并确保只有合法的基站和合法的MME才能完成身份认证流程并获取IMSI码。

[0008] 有鉴于此，本发明的一方面提出了一种移动管理实体，包括：发送单元，在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至终端，以供所述终端根据所述数字证书对所述移动管理实体进行验证，并在验证通过时，所述终端使用所述加密密钥对国际移

动用户识别码进行加密并将加密后的国际移动用户识别码发送至所述移动管理实体;接收单元,接收所述终端发送的所述加密后的国际移动用户识别码;解密单元,根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密。

[0009] 在该技术方案中,在移动管理实体向所述终端发送身份认证请求,所述终端通过验证所述加密密钥以及与所述加密密钥对应的数字证书,可以确保所述移动管理实体的合法性,防止非法移动管理实体的入侵,同时,通过将所述国际移动用户识别码进行加密,可以保证只有拥有与所述加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别,而非法的移动管理实体即便是得到了所述国际移动用户识别,由于没有对应的解密密钥,也无法使用所述国际移动用户识别,因而,这可以有效地提高用户信息安全性,防止非法的MME盗用用户的国际移动用户识别。

[0010] 其中,加密密钥和加密密钥可以对应于公钥和私钥,即通过公钥进行加密,在解密时通过与公钥对应的私钥进行解密。当然,本领域技术人员应当理解,本申请的加密方法包括但是不限于公钥加密,还可以是采用其他现有的加密方法实现。

[0011] 在上述技术方案中,优选地,还包括:密钥生成单元,在所述移动管理实体首次接入网络时,生成加密密钥和与所述加密密钥对应的解密密钥;存储单元,存储所述加密密钥和与所述加密密钥对应的解密密钥。

[0012] 在该技术方案中,由于每个移动管理实体都对应一对加密密钥和解密密钥,且每对加密密钥与解密密钥都是相对应的,因而,可以使终端在给移动管理实体发送国际移动用户识别码时,对国际移动用户识别码进行加密,以保证只有拥有与加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别码,这有利于增强所述国际移动用户识别码的安全性。

[0013] 在上述技术方案中,优选地,所述发送单元还用于:将所述加密密钥和所述移动管理实体的实体身份信息发送至归属用户管理器,以供所述归属用户管理器对所述移动管理实体的身份进行验证,并在验证通过时,生成与所述加密密钥对应的数字证书发送至所述移动管理实体;所述接收单元还用于:接收所述归属用户管理器发送的与所述加密密钥对应的所述数字证书。

[0014] 在该技术方案中,通过为每个身份验证成功的移动管理实体颁发一个与加密密钥对应的数字证书,可以使终端根据所述数据证书来验证所述移动管理实体是否合法,以防止非法的移动管理实体盗窃终端的国际移动用户识别码。

[0015] 在上述技术方案中,优选地,还包括:处理单元,在接收到所述终端发送的终止验证的信息时,停止验证。

[0016] 在该技术方案中,在接收到终端发送的终止验证时,说明终端已判定所述移动管理实体是非法的,所述移动管理实体将无法继续身份验证。

[0017] 本发明的另一方面提出了一种归属服务器,包括:接收单元,接收移动管理实体发送的加密密钥和所述移动管理实体的实体身份信息;验证单元,根据所述加密密钥和所述移动管理实体的实体身份信息对所述移动管理实体的身份进行验证;生成单元,在验证通过时,生成与所述加密密钥对应的数字证书;发送单元,发送所述数字证书至所述移动管理实体。

[0018] 在该技术方案中,通过为每个身份验证成功的移动管理实体颁发一个与加密密钥

对应的数字证书，可以使终端根据所述数据证书来验证所述移动管理实体是否合法，以防止非法的移动管理实体盗窃终端的国际移动用户识别码。

[0019] 本发明的又一方面提出了一种终端，包括：接收单元，接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书；验证单元，根据所述身份认证请求，对所述移动管理实体的数字证书进行验证；加密单元，在所述数字证书验证通过时，通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密，以得到加密后的国际移动用户识别码；发送单元，将所述加密后的国际移动用户识别码发送至所述移动管理实体。

[0020] 在该技术方案中，通过验证所述移动管理实体的数字证书，可以确保所述移动管理实体的合法性，通过对所述国际移动用户识别码进行加密，可以进一步保证所述国际移动用户识别码的安全性，保证只有合法的移动管理实体才能使用所述国际移动用户识别码。

[0021] 在上述技术方案中，优选地，所述加密单元包括：获取单元，在所述数字证书验证通过时，获取所述终端中的国家移动用户识别码；计算单元，根据所述加密密钥和预设的加密函数对所述国际移动用户识别码进行计算，以得到加密后的国际移动用户识别码。

[0022] 在上述技术方案中，优选地，还包括：处理单元，在所述数字证书验证未通过时，停止验证，并向所述移动管理实体发送终止验证的信息。

[0023] 在该技术方案中，在所述数字证书验证失败时，说明终端已判定所述移动管理实体是非法的，所述终端将停止验证，同时向所述移动管理实体发送终止验证的信息，以使所述移动管理实体停止向所述终端发送数字证书验证请求。

[0024] 本发明的再一方面提出了一种身份认证方法，用于身份认证系统，所述身份认证系统包括移动管理实体、终端和归属服务器，包括：所述移动管理实体在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至所述终端；所述终端接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书，根据所述身份认证请求，对所述移动管理实体的数字证书进行验证；在所述数字证书验证通过时，所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密，并将加密后的国际移动用户识别码发送至所述移动管理实体；所述移动管理实体根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密。

[0025] 在该技术方案中，在移动管理实体向终端发送身份认证请求，终端通过验证加密密钥以及与加密密钥对应的数字证书，可以确保移动管理实体的合法性，防止非法移动管理实体的入侵，同时，通过将国际移动用户识别码进行加密，可以保证只有拥有与加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别，而非法的移动管理实体即便是得到了所述国际移动用户识别，由于没有对应的解密密钥，也无法使用所述国际移动用户识别，因而，这可以有效地提高用户信息安全性，防止非法的MME盗用用户的国际移动用户识别。

[0026] 在上述技术方案中，优选地，还包括：所述移动管理实体将所述加密密钥和所述移动管理实体的实体身份信息发送至所述归属用户管理器；所述归属用户管理器接收移动管理实体发送的加密密钥和所述移动管理实体的实体身份信息，并根据所述加密密钥和所述

移动管理实体的实体身份信息对所述移动管理实体的身份进行验证;在所述移动管理实体的身份验证通过时,所述归属用户管理器生成与所述加密密钥对应的数字证书,并发送所述数字证书至所述移动管理实体;所述移动管理实体接收所述归属用户管理器发送的与所述加密密钥对应的所述数字证书。

[0027] 在该技术方案中,通过对所述移动管理实体的实体身份信息进行验证,并为每个移动管理实体颁发一个数字证书,可以使终端根据所述数据证书验证所述移动管理实体是否合法,以防止非法的移动管理实体盗窃终端的国际移动用户识别码。

[0028] 在上述技术方案中,优选地,还包括:所述移动管理实体在首次接入网络时,生成加密密钥和与所述加密密钥对应的解密密钥,并存储所述加密密钥和与所述加密密钥对应的解密密钥。

[0029] 在该技术方案中,由于每个移动管理实体都对应一对加密密钥和解密密钥,且每对加密密钥与解密密钥都是相对应的,因而,可以使终端在给移动管理实体发送国际移动用户识别码时,对国际移动用户识别码进行加密,以保证只有拥有与加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别码,这有利于增强所述国际移动用户识别码的安全性。

[0030] 在上述技术方案中,优选地,在所述数字证书验证通过时,所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密,具体包括:在所述数字证书验证通过时,所述终端获取国家移动用户识别码,并根据所述加密密钥和预设的加密函数对所述国际移动用户识别码进行计算,以得到加密后的国际移动用户识别码。

[0031] 在上述技术方案中,优选地,还包括:在所述数字证书验证未通过时,所述终端停止验证,并向所述移动管理实体发送终止验证的信息;所述移动管理实体在接收到所述终端发送的终止验证的信息时,停止验证。

[0032] 在该技术方案中,在数字证书未通过验证时,说明所述数字证书对应的所述移动管理实体是非法的,这时,终端就会停止验证,并向所述移动管理实体发送停止验证信号,以使所述移动管理实体停止向终端发送数字证书验证请求。

[0033] 通过以上技术方案,可以有效地提高UE发出的IMSI码的安全性,并确保只有合法的基站和合法的MME才能完成身份认证流程并获取IMSI码。

附图说明

[0034] 图1示出了相关技术中鉴权和密钥协商的流程示意截图;

[0035] 图2示出了相关技术中利用K_{ASME}进行鉴权和密钥协商的流程示意截图;

[0036] 图3示出了相关技术中为移动管理实体颁发数字证书的流程示意截图;

[0037] 图4示出了根据本发明的实施例的移动管理实体的结构示意图;

[0038] 图5示出了根据本发明的实施例的归属服务器的结构示意图;

[0039] 图6示出了根据本发明的实施例的终端的结构示意图;

[0040] 图7示出了根据本发明的实施例的身份认证系统的结构示意图;

[0041] 图8示出了根据本发明的实施例的身份认证方法的流程示意图;

[0042] 图9示出了根据本发明的另一个实施例的身份认证方法的流程示意图;

[0043] 图10示出了根据本发明的实施例的为移动管理实体颁发数字证书的流程示意图。

具体实施方式

[0044] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

[0045] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

[0046] 图4示出了根据本发明的实施例的移动管理实体的结构示意图。

[0047] 如图4所示，根据本发明的实施例的移动管理实体400，包括：发送单元402，在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至终端，以供所述终端根据所述数字证书对所述移动管理实体进行验证，并在验证通过时，所述终端使用所述加密密钥对国际移动用户识别码进行加密并将加密后的国际移动用户识别码发送至所述移动管理实体；接收单元404，接收所述终端发送的所述加密后的国际移动用户识别码；解密单元406，根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密。

[0048] 在该技术方案中，在移动管理实体向终端发送身份认证请求，终端通过验证加密密钥以及与加密密钥对应的数字证书，可以确保移动管理实体的合法性，防止非法移动管理实体的入侵，同时，通过将国际移动用户识别码进行加密，可以保证只有拥有与加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别，而非法的移动管理实体即便是得到了国际移动用户识别，由于没有对应的解密密钥，也无法使用国际移动用户识别，因而，这可以有效地提高用户信息安全性，防止非法的MME盗用用户的国际移动用户识别。

[0049] 其中，加密密钥和加密密钥可以对应于公钥和私钥，即通过公钥进行加密，在解密时通过与公钥对应的私钥进行解密。当然，本领域技术人员应当理解，本申请的加密方法包括但是不限于公钥加密，还可以是采用其他现有的加密方法实现。

[0050] 在上述技术方案中，优选地，还包括：密钥生成单元408，在所述移动管理实体首次接入网络时，生成加密密钥和与所述加密密钥对应的解密密钥；存储单元，存储所述加密密钥和与所述加密密钥对应的解密密钥。

[0051] 在该技术方案中，由于每个移动管理实体都对应一对加密密钥和解密密钥，且每对加密密钥与解密密钥都是相对应的，因而，可以使终端在给移动管理实体发送国际移动用户识别码时，对国际移动用户识别码进行加密，以保证只有拥有与加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别码，这有利于增强所述国际移动用户识别码的安全性。

[0052] 在上述技术方案中，优选地，所述发送单元402还用于：将所述加密密钥和所述移动管理实体的实体身份信息发送至归属用户管理器，以供所述归属用户管理器对所述移动管理实体的身份进行验证，并在验证通过时，生成与所述加密密钥对应的数字证书发送至所述移动管理实体；所述接收单元404还用于：接收所述归属用户管理器发送的与所述加密

密钥对应的所述数字证书。

[0053] 在该技术方案中，通过为每个身份验证成功的移动管理实体颁发一个与加密密钥对应的数字证书，可以使终端根据所述数据证书来验证所述移动管理实体是否合法，以防止非法的移动管理实体盗窃终端的国际移动用户识别码。

[0054] 在上述技术方案中，优选地，还包括：处理单元412，在接收到所述终端发送的终止验证的信息时，停止验证。

[0055] 在该技术方案中，在接收到终端发送的终止验证时，说明终端已判定所述移动管理实体是非法的，所述移动管理实体将无法继续身份验证。

[0056] 图5示出了根据本发明的实施例的归属服务器的结构示意图。

[0057] 如图5所示，根据本发明的实施例的归属服务器500，包括：接收单元502，接收移动管理实体发送的加密密钥和所述移动管理实体的实体身份信息；验证单元504，根据所述加密密钥和所述移动管理实体的实体身份信息对所述移动管理实体的身份进行验证；生成单元506，在验证通过时，生成与所述加密密钥对应的数字证书；发送单元508，发送所述数字证书至所述移动管理实体。

[0058] 在该技术方案中，通过为每个身份验证成功的移动管理实体颁发一个与加密密钥对应的数字证书，可以使终端根据所述数据证书来验证所述移动管理实体是否合法，以防止非法的移动管理实体盗窃终端的国际移动用户识别码。

[0059] 图6示出了根据本发明的实施例的终端的结构示意图。

[0060] 如图6所示，根据本发明的实施例的终端600，包括：接收单元602，接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书；验证单元604，根据所述身份认证请求，对所述移动管理实体的数字证书进行验证；加密单元606，在所述数字证书验证通过时，通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密，以得到加密后的国际移动用户识别码；发送单元608，将所述加密后的国际移动用户识别码发送至所述移动管理实体。

[0061] 在该技术方案中，通过验证所述移动管理实体的数字证书，可以确保所述移动管理实体的合法性，通过对所述国际移动用户识别码进行加密，可以进一步保证所述国际移动用户识别码的安全性，保证只有合法的移动管理实体才能使用所述国际移动用户识别码。

[0062] 在上述技术方案中，优选地，所述加密单元606包括：获取单元6062，在所述数字证书验证通过时，获取所述终端中的国家移动用户识别码；计算单元6064，根据所述加密密钥和预设的加密函数对所述国际移动用户识别码进行计算，以得到加密后的国际移动用户识别码。

[0063] 在上述技术方案中，优选地，还包括：处理单元610，在所述数字证书验证未通过时，停止验证，并向所述移动管理实体发送终止验证的信息。

[0064] 在该技术方案中，在所述数字证书验证失败时，说明终端已判定所述移动管理实体是非法的，所述终端将停止验证，同时向所述移动管理实体发送终止验证的信息，以使所述移动管理实体停止向所述终端发送数字证书验证请求。

[0065] 图7示出了根据本发明的实施例的身份认证系统的结构示意图。

[0066] 如图7所示，根据本发明的实施例的身份认证系统包括：移动管理实体400、归属服

务器500和终端600。

[0067] 其中，归属服务器500用于对移动管理实体400的身份进行验证，并在移动管理实体400的身份验证成功时，为移动管理实体400颁发数字证书；

[0068] 移动管理实体400用于在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，则向终端600发送身份认证请求、加密密钥以及归属服务器500颁发的数字证书；

[0069] 所述终端600用于根据所述数字证书对所述移动管理实体400进行验证，并在验证通过时，所述终端600使用所述加密密钥对国际移动用户识别码进行加密并将加密后的国际移动用户识别码发送至所述移动管理实体400。

[0070] 图8示出了根据本发明的实施例的身份认证方法的流程示意图。

[0071] 如图8所示，根据本发明的实施例的身份认证方法的流程，包括：步骤802，所述移动管理实体在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至所述终端；步骤804，所述终端接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书，根据所述身份认证请求，对所述移动管理实体的数字证书进行验证；步骤806，在所述数字证书验证通过时，所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密，并将加密后的国际移动用户识别码发送至所述移动管理实体；步骤808，所述移动管理实体根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密。

[0072] 在该技术方案中，在该技术方案中，在移动管理实体向所述终端发送身份认证请求，所述终端通过验证所述加密密钥以及与所述加密密钥对应的数字证书，可以确保所述移动管理实体的合法性，防止非法移动管理实体的入侵，同时，通过将所述国际移动用户识别码进行加密，可以保证只有拥有与所述加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别，而非法的移动管理实体即便是得到了所述国际移动用户识别，由于没有对应的解密密钥，也无法使用所述国际移动用户识别，因而，这可以有效地提高用户信息安全性，防止非法的MME盗用用户的国际移动用户识别。

[0073] 在上述技术方案中，优选地，还包括：所述移动管理实体将所述加密密钥和所述移动管理实体的实体身份信息发送至所述归属用户管理器；所述归属用户管理器接收移动管理实体发送的加密密钥和所述移动管理实体的实体身份信息，并根据所述加密密钥和所述移动管理实体的实体身份信息对所述移动管理实体的身份进行验证；在所述移动管理实体的身份验证通过时，所述归属用户管理器生成与所述加密密钥对应的数字证书，并发送所述数字证书至所述移动管理实体；所述移动管理实体接收所述归属用户管理器发送的与所述加密密钥对应的所述数字证书。

[0074] 在该技术方案中，通过对所述移动管理实体的实体身份信息进行验证，并为每个移动管理实体颁发一个数字证书，可以使终端根据所述数据证书验证所述移动管理实体是否合法，以防止非法的移动管理实体盗窃终端的国际移动用户识别码。

[0075] 在上述技术方案中，优选地，还包括：所述移动管理实体在首次接入网络时，生成加密密钥和与所述加密密钥对应的解密密钥，并存储所述加密密钥和与所述加密密钥对应的解密密钥。

[0076] 在该技术方案中，由于每个移动管理实体都对应一对加密密钥和解密密钥，且每对加密密钥与解密密钥都是相对应的，因而，可以使终端在给移动管理实体发送国际移动用户识别码时，对国际移动用户识别码进行加密，以保证只有拥有与加密密钥对应的解密密钥的合法移动管理实体才能使用所述国际移动用户识别码，这有利于增强所述国际移动用户识别码的安全性。

[0077] 在上述技术方案中，优选地，在所述数字证书验证通过时，所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密，具体包括：在所述数字证书验证通过时，所述终端获取国家移动用户识别码，并根据所述加密密钥和预设的加密函数对所述国际移动用户识别码进行计算，以得到加密后的国际移动用户识别码。

[0078] 在上述技术方案中，优选地，还包括：在所述数字证书验证未通过时，所述终端停止验证，并向所述移动管理实体发送终止验证的信息；所述移动管理实体在接收到所述终端发送的终止验证的信息时，停止验证。

[0079] 在该技术方案中，在数字证书未通过验证时，说明所述数字证书对应的所述移动管理实体是非法的，这时，终端就会停止验证，并向所述移动管理实体发送停止验证信号，以使所述移动管理实体停止向终端发送数字证书验证请求。

[0080] 图9示出了根据本发明的另一个实施例的身份认证方法的流程示意图。

[0081] 如图9所示，根据本发明的另一个实施例的身份认证方法的流程，包括：

[0082] 步骤902，MME(移动管理实体)向UE(终端)发起身份认证请求。

[0083] 步骤904，在UE响应MME的身份认证请求之后，MME将加密密钥和证书cert发送给UE。

[0084] 步骤906，UE开始验证MME的加密密钥和证书cert的正确性。

[0085] 步骤908，判断MME的证书是否成功cert通过验证，并在证书未通过验证时，执行步骤910；反之，执行步骤912。

[0086] 步骤910，在MME的证书未通过验证时，UE终止验证并向MME返回终止信息。

[0087] 步骤912，在MME的证书通过验证时，UE将IMSI码通过加密密钥加密。

[0088] 步骤914，UE将加密后的IMSI码发送给MME。

[0089] 步骤916，MME利用解密密钥对加密后的IMSI码进行解密，以得到UE的IMSI码。

[0090] 图10示出了根据本发明的实施例的为移动管理实体颁发数字证书的流程示意图。

[0091] 下面以加密密钥为公钥，解密密钥为私钥为例，详细说明归属服务器为移动管理实体颁发数字证书的流程。

[0092] 如图10所示，根据本发明的实施例的归属服务器为移动管理实体颁发数字证书的流程，包括：

[0093] 步骤1002，在MME首次接入网络时，生成公钥与公钥对应的私钥，组成公私密钥对(pk，sk)。

[0094] 步骤1004，MME将公钥pk和实体身份信息发送给HSS/CA。

[0095] 步骤1006，HSS/CA(归属服务器)开始验证MME的身份。

[0096] 步骤1008，HSS/CA根据MME的实体身份信息来判断MME是否可以通过身份验证，并在MME未通过身份验证时，执行步骤1010；反之，执行步骤1012。

[0097] 步骤1010,在MME未通过身份验证时,HSS/CA终止验证并向MME返回终止信息。

[0098] 步骤1012,在MME通过身份验证时,HSS/CA根据MME的公钥pk生成MME一个与公钥pk对应的数字证书cert。

[0099] 步骤1014,HSS/CA将cert发送给MME。

[0100] 以上结合附图详细说明了本发明的技术方案,通过本发明的技术方案,可以有效地提高UE发出的IMSI码的安全性,并确保只有合法的基站和合法的MME才能完成身份认证流程并获取IMSI码。

[0101] 根据本发明的实施方式,还提供了一种存储在非易失性机器可读介质上的程序产品,用于身份认证,所述程序产品包括用于使计算机系统执行以下步骤的机器可执行指令:移动管理实体在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时,发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至终端;所述终端接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书,根据所述身份认证请求,对所述移动管理实体的数字证书进行验证;在所述数字证书验证通过时,所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密,并将加密后的国际移动用户识别码发送至所述移动管理实体;所述移动管理实体根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密。

[0102] 根据本发明的实施方式,还提供了一种非易失机器可读介质,存储有用于身份认证的程序产品,所述程序产品包括用于使计算机系统执行以下步骤的机器可执行指令:所述移动管理实体在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时,发送身份认证请求、加密密钥以及与所述加密密钥对应的数字证书至所述终端;所述终端接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书,根据所述身份认证请求,对所述移动管理实体的数字证书进行验证;在所述数字证书验证通过时,所述终端通过所述移动管理实体发送的所述加密密钥对所述终端中的国际移动用户识别码进行加密,并将加密后的国际移动用户识别码发送至所述移动管理实体;所述移动管理实体根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密。

[0103] 根据本发明的实施方式,还提供了一种机器可读程序,所述程序使机器执行如上所述技术方案中任一所述的身份认证方法。

[0104] 根据本发明的实施方式,还提供了一种存储有机器可读程序的存储介质,其中,所述机器可读程序使得机器执行如上所述技术方案中任一所述的身份认证方法。

[0105] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

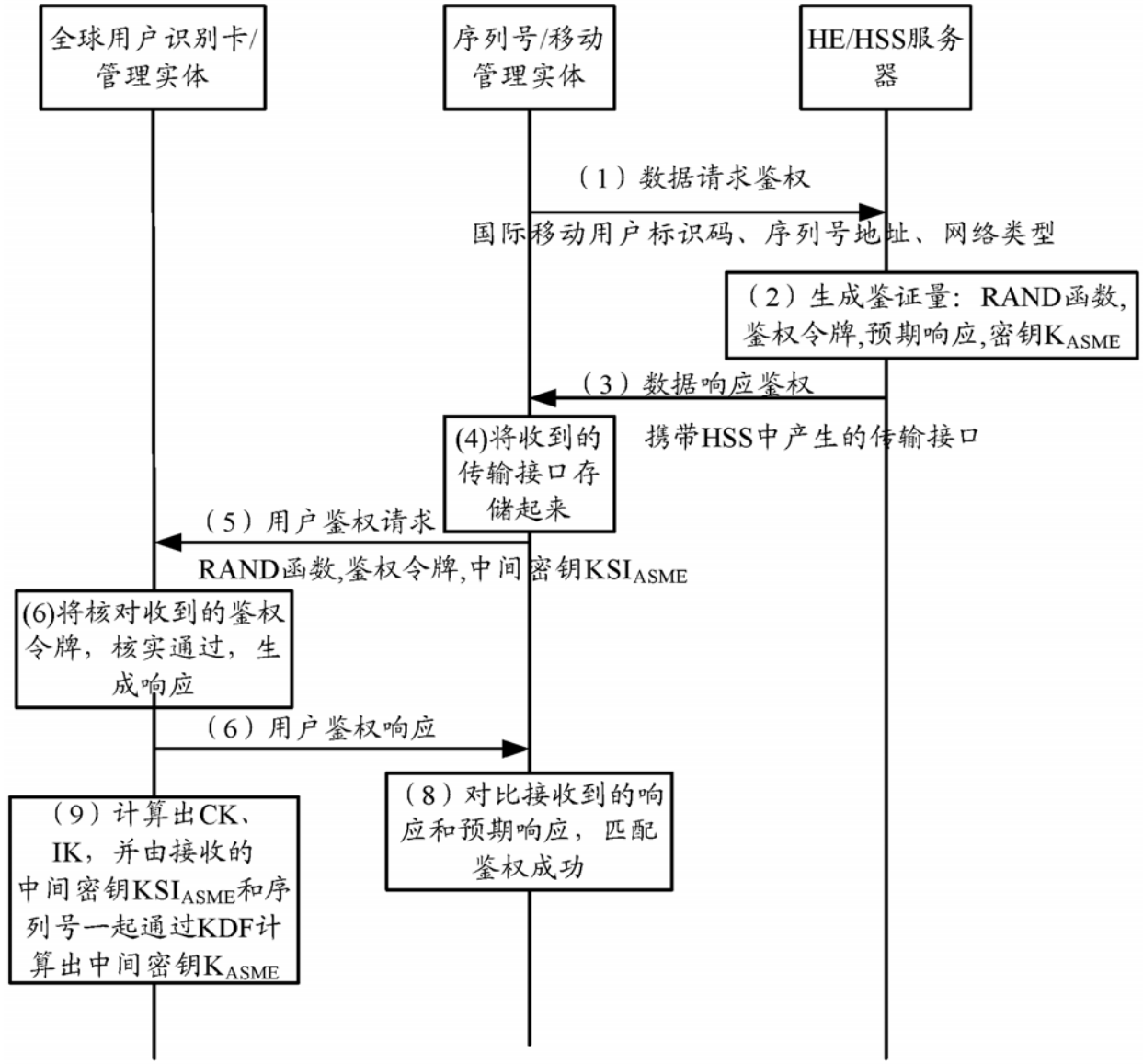
全球用户识别卡/管理实体
序列号/移动管理实体
HE/HSS服务器
（1）数据请求鉴权
国际移动用户标识码、序列号地址、网络类型
（2）生成鉴证量：RAND函数,鉴权令牌,预期响应,密钥K_{ASME}
（3）数据响应鉴权
携带HSS中产生的传输接口
(4)将收到的传输接口存储起来
（5）用户鉴权请求
RAND函数,鉴权令牌,中间密钥KSI_{ASME}
(6)将核对收到的鉴权令牌，核实通过，生成响应
（6）用户鉴权响应
（8）对比接收到的响应和预期响应，匹配鉴权成功
（9）计算出CK、IK，并由接收的中间密钥KSI_{ASME}和序列号一起通过KDF计算出中间密钥K_{ASME}

图1

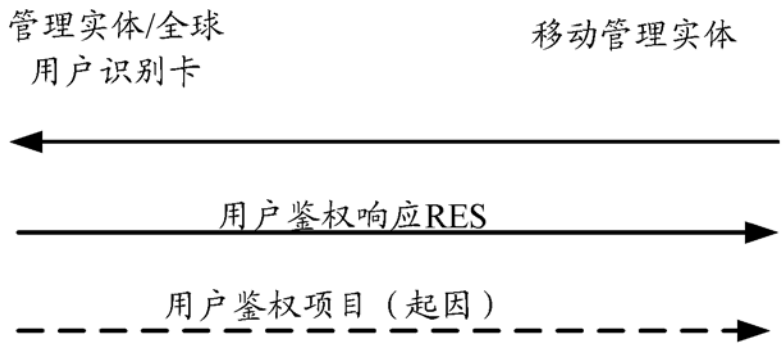
管理实体/全球用户识别卡
移动管理实体
用户鉴权响应RES
用户鉴权项目（起因）

图2

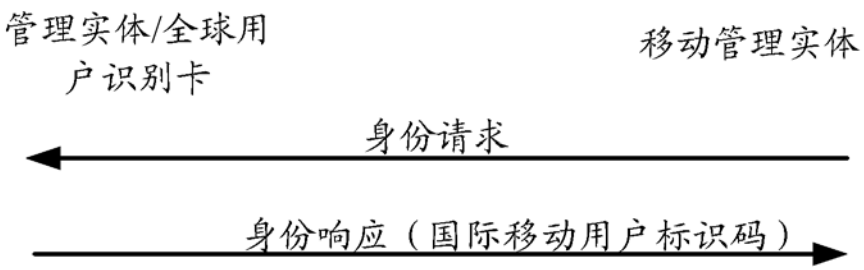
管理实体/全球用户识别卡
移动管理实体
身份请求
身份响应（国际移动用户标识码）

图3


发送单元402
密钥生成单元408
接收单元404
存储单元410
解密单元406
第一处理单元412
移动管理实体400

图4


接收单元502
验证单元504
生成单元506
发送单元508
归属服务器500

图5

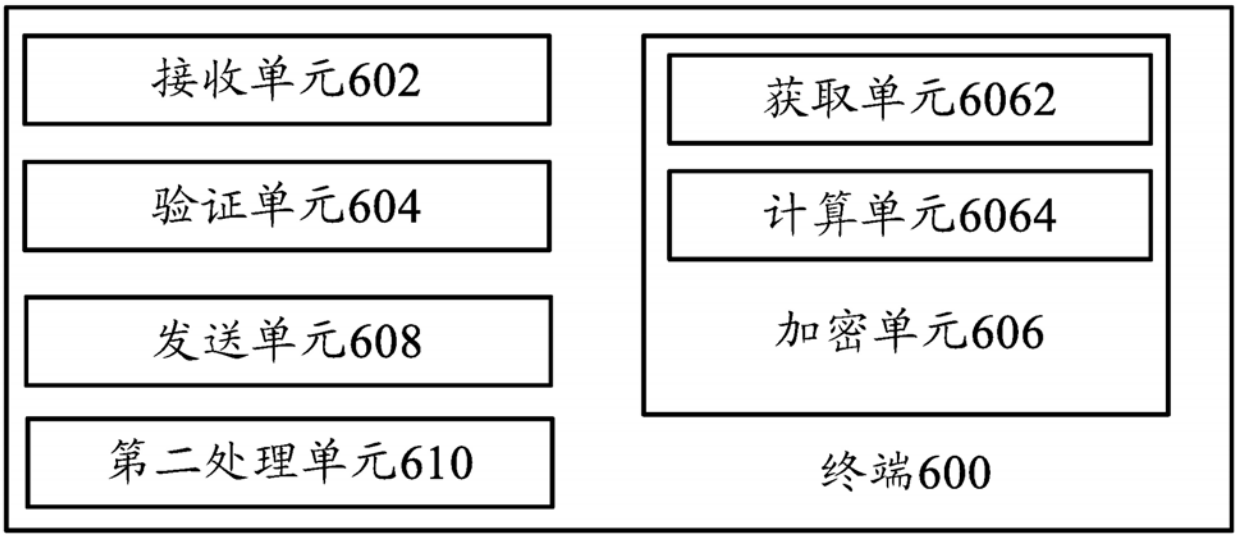
接收单元602
验证单元604
发送单元608
第二处理单元610
获取单元6062
计算单元6064
加密单元606
终端600

图6

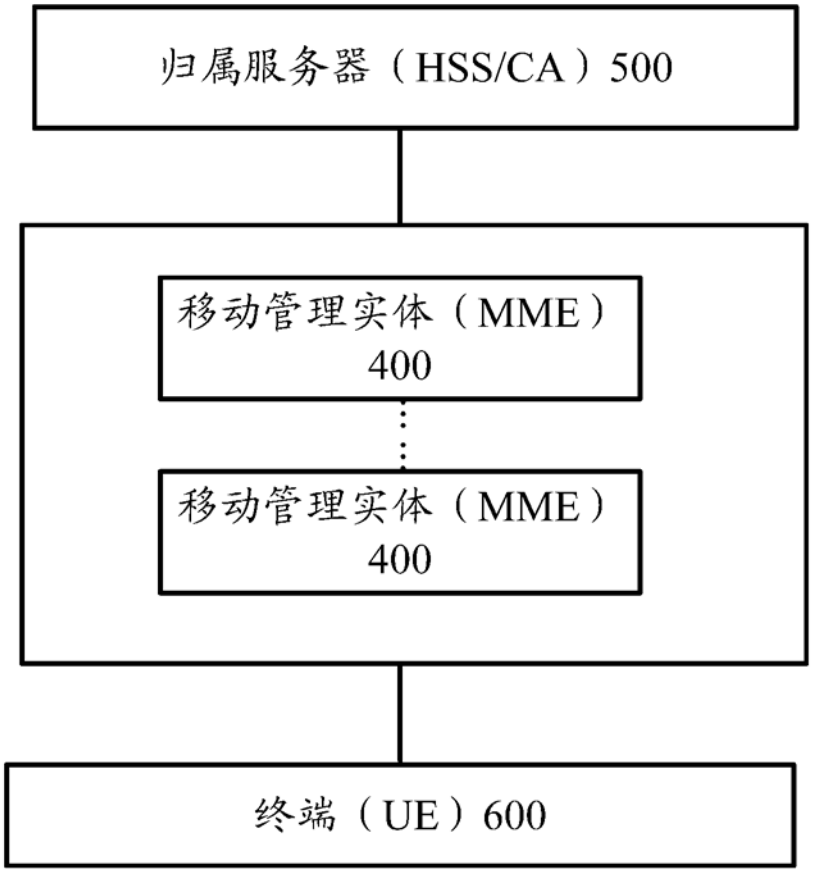

图7

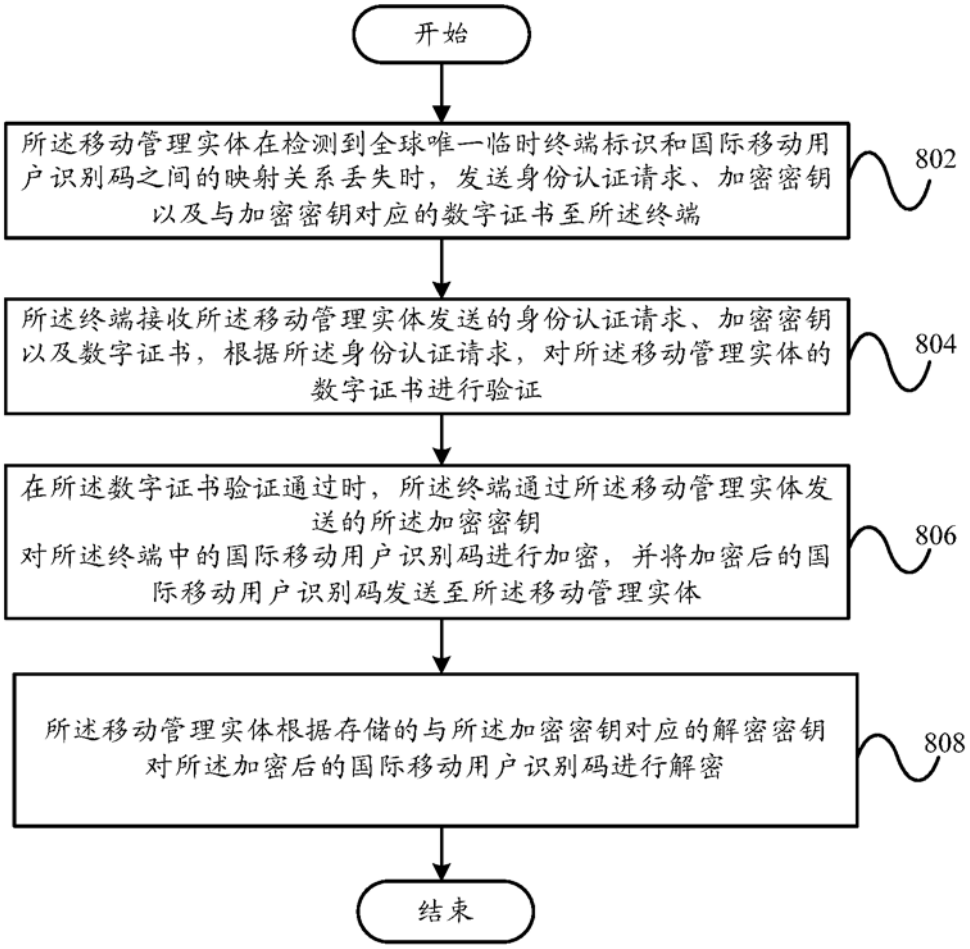
开始
所述移动管理实体在检测到全球唯一临时终端标识和国际移动用户识别码之间的映射关系丢失时，发送身份认证请求、加密密钥以及与加密密钥对应的数字证书至所述终端
802
所述终端接收所述移动管理实体发送的身份认证请求、加密密钥以及数字证书，根据所述身份认证请求，对所述移动管理实体的数字证书进行验证
804
在所述数字证书验证通过时，所述终端通过所述移动管理实体发送的所述加密密钥
对所述终端中的国际移动用户识别码进行加密，并将加密后的国际移动用户识别码发送至所述移动管理实体
806
所述移动管理实体根据存储的与所述加密密钥对应的解密密钥对所述加密后的国际移动用户识别码进行解密
808
结束

图8

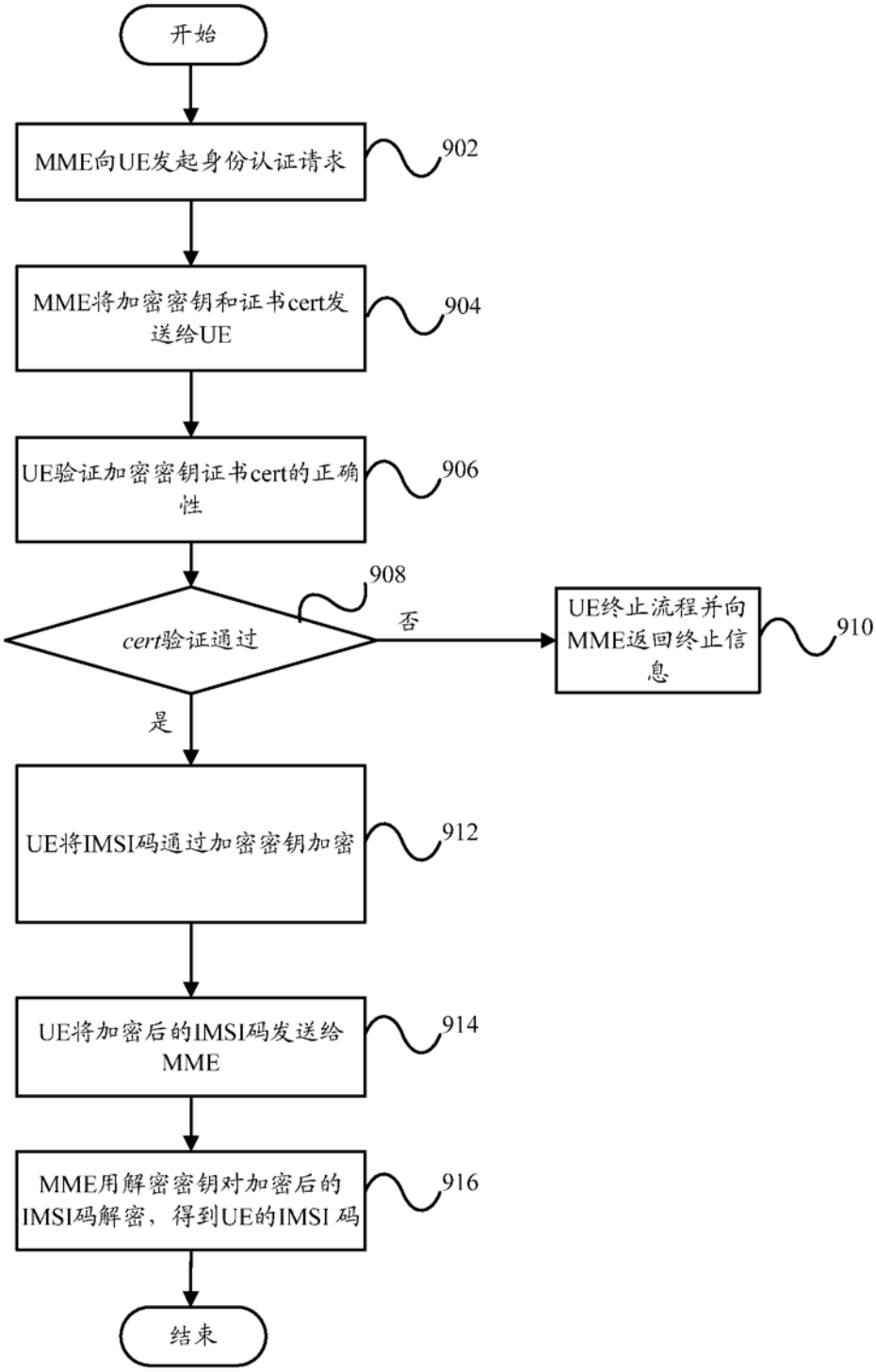
开始
MME向UE发起身份认证请求
902
MME将加密密钥和证书cert发送给UE
904
UE验证加密密钥证书cert的正确性
906
908
cert验证通过
否
UE终止流程并向MME返回终止信息
910
是
UE将IMSI码通过加密密钥加密
912
UE将加密后的IMSI码发送给MME
914
MME用解密密钥对加密后的IMSI码解密，得到UE的IMSI码
916
结束

图9

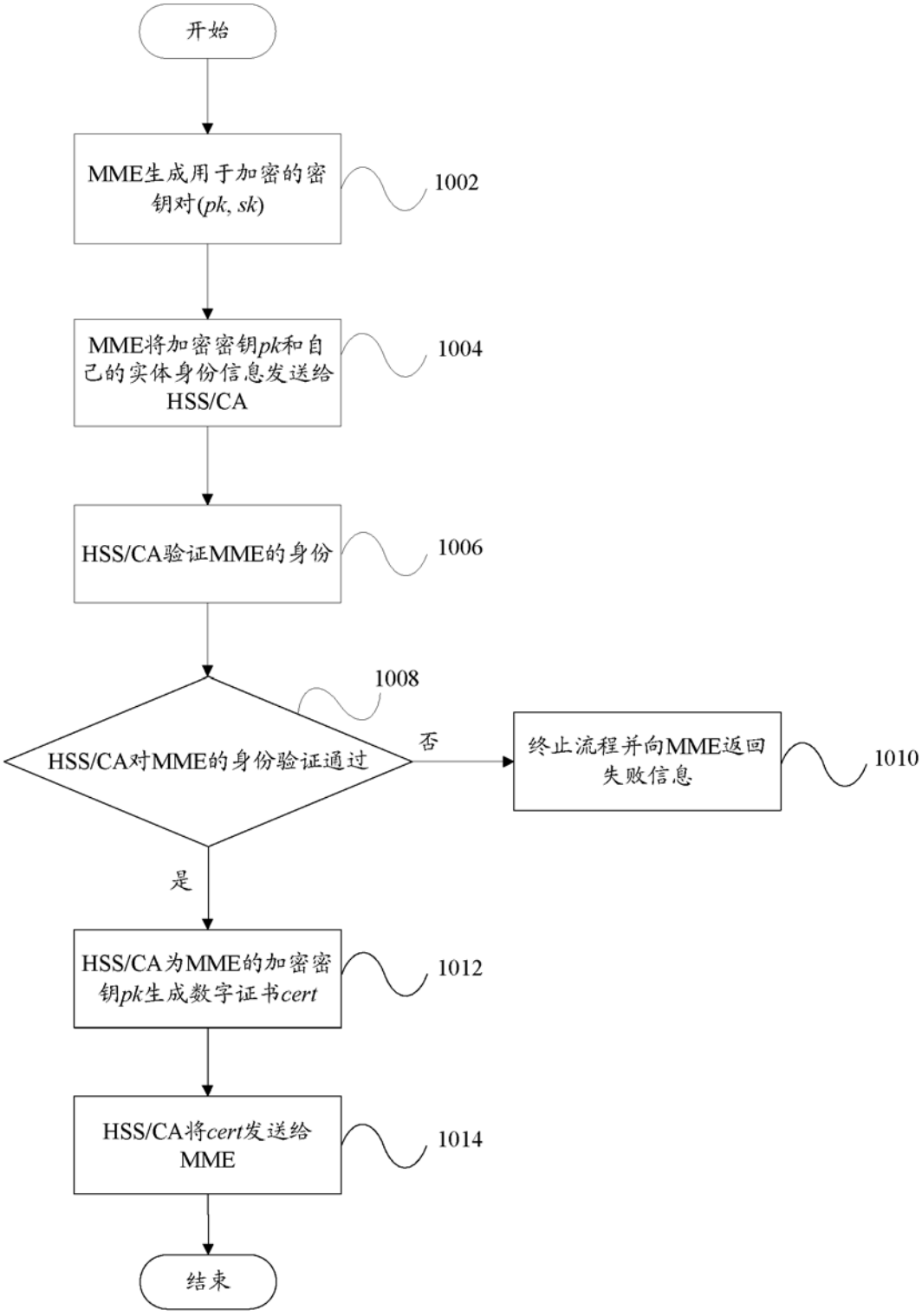
开始
MME生成用于加密的密钥对(pk, sk)
1002
MME将加密密钥pk和自己的实体身份信息发送给HSS/CA
1004
HSS/CA验证MME的身份
1006
1008
HSS/CA对MME的身份验证通过
否
终止流程并向MME返回失败信息
1010
是
HSS/CA为MME的加密密钥pk生成数字证书cert
1012
HSS/CA将cert发送给MME
1014
结束

图10