(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111327583 A
(43)申请公布日 2020.06.23

(21)申请号 201910775077.9

(22)申请日 2019.08.22

(71)申请人 刘高峰
地址 518129 广东省深圳市龙岗区坂田街道吉华路635号1栋B座

(72)发明人 不公告发明人

(51)Int.Cl.
H04L 29/06(2006.01)

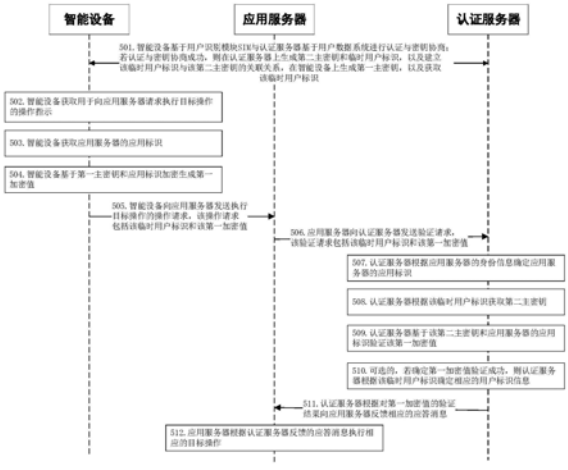
权利要求书3页 说明书35页 附图6页

(54)发明名称

一种身份认证方法、智能设备及认证服务器

(57)摘要

本发明公开了一种身份认证方法、智能设备及认证服务器。所述方法包括:若智能设备与认证服务器认证与密钥协商成功,则认证服务器建立临时用户标识与第二主密钥的关联关系,智能设备生成第一主密钥和获取所述临时用户标识;智能设备向应用服务器发送执行目标操作的操作请求和认证信息,所述认证信息包括所述临时用户标识、基于所述第一主密钥生成的第一加密值;应用服务器将所述认证信息传递给认证服务器;若认证服务器根据所述关联关系验证所述认证信息成功,则反馈表示验证成功的应答消息;应用服务器执行所述目标操作。本方法可有效解决需用户输入认证信息使得操作复杂低效的问题,以及不需在智能设备的生产过程中预先写入认证信息。



CN 111327583 A

1.一种身份认证方法,其特征在于,应用于智能设备中,所述方法包括:

基于用户识别模块SIM与认证服务器进行认证与密钥协商,若认证与密钥协商成功,则生成第一主密钥,以及获取所述认证服务器传递的临时用户标识;

获取用于向应用服务器请求执行目标操作的操作指示;

获取所述应用服务器的应用标识;

基于所述第一主密钥和所述应用标识加密生成第一加密值;

向所述应用服务器发送执行所述目标操作的操作请求,并且将所述临时用户标识和所述第一加密值传递给所述应用服务器,以使得所述应用服务器对所述临时用户标识和所述第一加密值进行认证,并且在认证成功的情况下执行所述目标操作。

2.根据权利要求1所述的方法,其特征在于,所述基于用户识别模块SIM与认证服务器进行认证与密钥协商包括:

获取所述用户识别模块SIM的移动用户标识;

向所述认证服务器发送认证与密钥协商请求,并且向所述认证服务器传递所述移动用户标识,以使得所述认证服务器根据所述移动用户标识向用户数据系统获取随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥;

接收所述认证服务器发送的认证与密钥协商挑战消息,并且获取所述认证服务器传递的所述随机数RAND和所述鉴权令牌AUTN;

向所述用户识别模块SIM发送鉴权请求,并且向所述用户识别模块SIM发送所述随机数RAND和所述鉴权令牌AUTN;

接收所述用户识别模块SIM返回的期望响应值RES、第一加密密钥CK和第一完整性密钥IK;

根据所述期望响应值RES确定第一期望响应值;

向所述认证服务器发送认证与密钥协商挑战应答消息,并且向所述认证服务器传递所述第一期望响应值,以使得所述认证服务器根据对所述第一期望响应值的验证以确定认证与密钥协商是否成功;

若接收到所述认证服务器反馈的认证与密钥协商成功应答消息,则确定所述认证与密钥协商成功,基于所述第一加密密钥CK或/和所述第一完整性密钥IK生成第一初始密钥,基于所述第一初始密钥生成第一主密钥,以及获取所述认证服务器传递的所述临时用户标识,其中,所述生成第一初始密钥的生成方式与所述用户数据系统生成所述第二初始密钥的生成方式一致,所述第一主密钥的生成方式与所述认证服务器生成第二主密钥的生成方式一致。

3.一种身份认证方法,其特征在于,应用于应用服务器中,所述方法包括:

接收智能设备发送的用于请求执行目标操作的操作请求,所述操作请求由所述智能设备在获取到用于向所述应用服务器请求执行所述目标操作的操作指示之后向所述应用服务器发送;

获取所述智能设备传递的临时用户标识和第一加密值,所述临时用户标识为所述智能设备与认证服务器在认证与密钥协商成功时获取,所述第一加密值由所述智能设备基于第一主密钥和应用标识加密生成,所述第一主密钥由所述智能设备与所述认证服务器在所述认证与密钥协商成功时生成,所述应用标识为所述应用服务器的应用标识;

向所述认证服务器发送验证请求，并且向所述认证服务器传递所述临时用户标识和所述第一加密值；

接收所述认证服务器反馈的表示验证成功的应答消息，所述表示验证成功的应答消息是在所述认证服务器对所述临时用户标识和所述第一加密值验证成功之后所反馈的；

执行所述目标操作。

4.根据权利要求3所述的方法，其特征在于，所述接收所述认证服务器反馈表示验证成功的应答消息还包括：

接收所述认证服务器反馈的用户标识信息，所述用户标识信息是所述认证服务器根据所述临时用户标识确定的。

5.一种身份认证方法，其特征在于，应用于认证服务器中，所述方法包括：

基于用户数据系统与智能设备进行认证与密钥协商，若认证与密钥协商成功，则生成第二主密钥，生成临时用户标识并传递给所述智能设备，以及建立所述临时用户标识与所述第二主密钥的关联关系；

接收应用服务器发送的验证请求，所述验证请求由所述应用服务器在接收到所述智能设备发送的用于请求执行目标操作的操作请求之后向所述认证服器发送，所述操作请求由所述智能设备在获取到用于向所述应用服务器请求执行所述目标操作的操作指示之后向所述应用服务器发送；

获取所述应用服务器传递的所述临时用户标识和第一加密值，所述应用服务器传递的所述临时用户标识和所述第一加密值由所述智能设备通过所述应用服务器传递；

根据所述应用服务器的身份信息确定所述应用服务器的应用标识；

根据所述临时用户标识在所述关联关系中获取所述第二主密钥；

基于所述第二主密钥和所述应用标识验证所述第一加密值；

若所述第一加密值验证成功，则向所述应用服务器反馈表示验证成功的应答消息，以触发所述应用服务器执行所述目标操作。

6.根据权利要求5所述的方法，其特征在于，所述基于用户数据系统与智能设备进行认证与密钥协商包括：

接收所述智能设备发送的认证与密钥协商请求，并且获取所述智能设备传递的移动用户标识；

向所述用户数据系统发送认证请求，并且向所述用户数据系统传递所述移动用户标识；

接收所述用户数据系统反馈的认证应答，并且获取所述用户数据系统反馈的随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥；

向所述智能设备发送认证与密钥协商挑战消息，并且向所述智能设备传递所述随机数RAND和所述鉴权令牌AUTN；

接收所述智能设备反馈的认证与密钥协商挑战应答消息，并且获取所述智能设备传递的第一期望响应值；

基于所述第二期望响应值验证所述第一期望响应值；

若验证所述第一期望响应值有效，则基于所述第二初始密钥生成第二主密钥，生成临时用户标识并传递给所述智能设备，以及建立所述临时用户标识与所述第二主密钥的关联

关系，向所述智能设备发送认证与密钥协商成功应答消息，其中，所述第二主密钥的生成方式与所述智能设备生成第一主密钥的生成方式一致。

7.根据权利要求30所述的方法，其特征在于，若所述第一加密值验证成功，则所述方法还包括：

根据所述临时用户标识确定相应的用户标识信息；

将所述用户标识信息传递给所述应用服务器。

8.一种智能设备，其特征在于，所述智能设备包括：存储器、处理器，所述处理器用于运行所述存储器所存储的程序，所述程序运行时执行包括权利要求1至2中任一项所述的方法；或/和，一种应用服务器，其特征在于，所述应用服务器包括：存储器、处理器，所述处理器用于运行所述存储器所存储的程序，所述程序运行时执行包括权利要求3至4中任一项所述的方法；或/和，一种认证服务器，其特征在于，所述认证服务器包括：存储器、处理器，所述处理器用于运行所述存储器所存储的程序，所述程序运行时执行包括权利要求5至7中任一项所述的方法。

9.一种认证系统，其特征在于，所述认证系统包括：认证服务器、至少一个应用服务器和至少一个智能设备；

所述智能设备包括如权利要求8所述的智能设备；

所述应用服务器包括如权利要求8所述的应用服务器；

所述认证服务器包括如权利要求8所述的认证服务器。

10.一种存储介质，其特征在于，所述存储介质中存储有程序，所述程序用于实现包括权利要求1至2中任一项所述的应用于智能设备的方法；或/和，所述程序用于实现包括权利要求3至4中任一项所述的应用于应用服务器的方法；或/和，所述程序用于实现包括权利要求5至7中任一项所述的应用于认证服务器的方法。

一种身份认证方法、智能设备及认证服务器

【技术领域】

[0001] 本发明涉及通信技术领域和互联网技术领域，尤其涉及一种身份认证方法、智能设备及认证服务器。

【背景技术】

[0002] 随着移动数据网络的快速发展，随着互联网与通信网络的融合以及通信运营商网络业务的扩展，越来越多的智能设备接入到移动数据网络，不仅包括已有的智能手机设备，还包括很多物联网智能设备，如智能手表、智能电表等。

[0003] 智能设备在使用过程中，例如智能设备在接入到应用服务器获取信息和服务时，一般都需要进行身份认证之后才能开始使用。

[0004] 现有技术中，为了便于智能设备的身份认证，通常有两种实施方式：

[0005] 一种是对于有触摸屏、键盘输入的智能设备，通过让用户在智能设备上输入认证信息(如账号密码等)以实现向应用服务器的认证，但这样会影响用户使用体验，以及降低智能设备的认证效率。

[0006] 另一种是对于不适用触摸屏、键盘输入等的智能设备，为了实现智能设备向应用服务器的认证，则会在智能设备生产时将认证信息写入智能设备，此后智能设备在接入到应用服务器时根据该写入的认证信息实现认证。但是，由于应用服务商需要将智能设备的认证信息提前告知生产商，这容易造成认证信息的泄露；此外，由于每个智能设备上写入的认证信息需是唯一的(如唯一的设备标识和密钥)，这使得认证信息的写入不仅需要专门的过程而且非常繁琐，从而大幅增加了生产成本。

[0007] 需要说明的是，上述背景信息仅用于加强对本发明背景技术的理解，因此可以包括不构成对本领域普通技术人员已知的现有技术信息。

【发明内容】

[0008] 本发明的主要目的在于提供一种身份认证方法、智能设备及认证服务器，进而至少在一定程度上解决由于相关技术的限制和缺陷而导致的一个或者多个问题，包括以下技术方案：

[0009] 第一方面，提供了一种身份认证方法，应用于智能设备中，所述方法包括：

[0010] 基于用户识别模块SIM与认证服务器进行认证与密钥协商，若认证与密钥协商成功，则生成第一主密钥，以及获取所述认证服务器传递的临时用户标识；

[0011] 获取用于向应用服务器请求执行目标操作的操作指示；

[0012] 获取所述应用服务器的应用标识；

[0013] 基于所述第一主密钥和所述应用标识加密生成第一加密值；

[0014] 向所述应用服务器发送执行所述目标操作的操作请求，并且将所述临时用户标识和所述第一加密值传递给所述应用服务器，以使得所述应用服务器对所述临时用户标识和所述第一加密值进行认证，并且在认证成功的情况下执行所述目标操作。

[0015] 优选的，所述智能设备分别与所述认证服务器、所述应用服务器通过数据网络连接。

[0016] 优选的，所述数据网络包括因特网、移动互联网。

[0017] 优选的，所述智能设备通过移动数据连接、WiFi连接或WLAN连接接入所述移动互联网。

[0018] 优选的，所述移动数据包括3G移动数据、4G移动数据、5G移动数据、6G移动数据或NB-IoT移动数据。

[0019] 优选的，所述基于用户识别模块SIM与认证服务器进行认证与密钥协商包括：

[0020] 获取所述用户识别模块SIM的移动用户标识；

[0021] 向所述认证服务器发送认证与密钥协商请求，并且向所述认证服务器传递所述移动用户标识，以使得所述认证服务器根据所述移动用户标识向用户数据系统获取随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥；

[0022] 接收所述认证服务器发送的认证与密钥协商挑战消息，并且获取所述认证服务器传递的所述随机数RAND和所述鉴权令牌AUTN；

[0023] 向所述用户识别模块SIM发送鉴权请求，并且向所述用户识别模块SIM发送所述随机数RAND和所述鉴权令牌AUTN；

[0024] 接收所述用户识别模块SIM返回的期望响应值RES、第一加密密钥CK和第一完整性密钥IK；

[0025] 根据所述期望响应值RES确定第一期望响应值；

[0026] 向所述认证服务器发送认证与密钥协商挑战应答消息，并且向所述认证服务器传递所述第一期望响应值，以使得所述认证服务器根据对所述第一期望响应值的验证以确定认证与密钥协商是否成功；

[0027] 若接收到所述认证服务器反馈的认证与密钥协商成功应答消息，则确定所述认证与密钥协商成功，基于所述第一加密密钥CK或/和所述第一完整性密钥IK生成第一初始密钥，基于所述第一初始密钥生成第一主密钥，以及获取所述认证服务器传递的所述临时用户标识，其中，所述生成第一初始密钥的生成方式与所述用户数据系统生成所述第二初始密钥的生成方式一致，所述第一主密钥的生成方式与所述认证服务器生成第二主密钥的生成方式一致。

[0028] 优选的，所述用户识别模块SIM为全球用户识别模块USIM，所述用户数据系统为归属用户服务器HSS，则：

[0029] 所述移动用户标识为国际移动用户识别码IMSI；

[0030] 所述根据所述期望响应值RES确定第一期望响应值包括：将所述期望响应值RES作为所述第一期望响应值；或者，将所述期望响应值RES哈希计算后所生成的哈希值作为所述第一期望响应值；

[0031] 所述基于所述第一加密密钥CK或/和所述第一完整性密钥IK生成第一初始密钥包括：将所述第一加密密钥CK或/和所述第一完整性密钥IK作为所述第一初始密钥；或者，基于所述第一加密密钥CK或/和所述第一完整性密钥IK生成第一密钥KASME，所述第一密钥KASME为所述第一初始密钥。

[0032] 优选的，所述用户识别模块SIM为全球用户识别模块USIM，所述用户数据系统为统

一用户管理UDM,则:

[0033] 所述移动用户标识为用户永久标识SUPI;

[0034] 所述根据所述期望响应值RES确定第一期望响应值包括:基于所述期望响应值RES生成期望响应值RES*,所述期望响应值RES*为所述第一期望响应值;或者,将所述期望响应值RES*哈希计算后所生成的哈希值作为所述第一期望响应值;

[0035] 所述基于所述第一加密密钥CK或/和所述第一完整性密钥IK生成第一初始密钥包括:基于所述第一加密密钥CK或/和所述第一完整性密钥IK生成第一密钥KAUSF,所述第一密钥KAUSF为所述第一初始密钥。

[0036] 优选的,所述向所述认证服务器发送认证与密钥协商请求还包括:

[0037] 将所述用户永久标识SUPI加密生成用户隐藏标识SUCI;

[0038] 在所述向所述认证服务器发送的认证与密钥协商请求中,将所述用户隐藏标识SUCI作为所述移动用户标识。

[0039] 优选的,所述基于所述第一初始密钥生成第一主密钥包括:

[0040] 将所述第一初始密钥作为所述第一主密钥;或者,

[0041] 基于包括所述第一初始密钥的信息生成所述第一主密钥。

[0042] 优选的,所述基于包括所述第一初始密钥的信息生成所述第一主密钥包括:

[0043] 基于包括所述第一初始密钥以及第四固定字符串或/和第四随机字符串或/和第四时间戳或/和所述移动用户标识的信息生成所述第一主密钥,所述第四固定字符串为预先配置的并且与所述认证服务器预先配置的第四固定字符串的值相同的字符串,所述第四随机字符串或/和所述第四时间戳为所述认证服务器所传递的。

[0044] 优选的,所述获取所述认证服务器传递的临时用户标识包括:

[0045] 根据所述随机数RAND生成所述临时用户标识,并且所述生成所述临时用户标识的生成方式与所述认证服务器生成临时用户标识的生成方式相同;或者,

[0046] 接收所述认证服务器传递的临时用户标识,获取所述传递的临时用户标识为所述临时用户标识。

[0047] 优选的,所述获取用于向应用服务器请求执行目标操作的操作指示包括:

[0048] 由用户或/和外部指令触发所述执行目标操作的操作指示;或/和,

[0049] 根据预先设定的判断条件自动触发所述执行目标操作的操作指示。

[0050] 优选的,所述由用户或外部指令触发所述操作指示包括:

[0051] 由用户点击执行目标操作的选项触发所述执行目标操作的操作指示;或/和,

[0052] 访问所述应用服务器,获取所述应用服务器返回的所述执行目标操作的操作指示;或/和,

[0053] 扫描图形码,从所述图形码的解码信息中获得所述执行目标操作的操作指示。

[0054] 优选的,所述获取所述应用服务器的应用标识包括:

[0055] 在所述执行目标操作的操作指示中包括所述应用标识,获取所述执行目标操作的操作指示中包括的所述应用标识;或者,

[0056] 在所述智能设备上预先配置有所述应用标识,获取所述预先配置的所述应用标识。

[0057] 优选的,所述基于所述第一主密钥和所述应用标识加密生成第一加密值包括:

[0058] 基于所述第一主密钥生成第一认证密钥，其中，所述第一认证密钥的生成方式与所述认证服务器生成第二认证密钥的生成方式一致，以使得所述第一认证密钥与所述认证服务器生成的所述第二认证密钥的值相同；

[0059] 生成第一验证信息，其中，所述第一验证信息的生成方式与所述认证服务器生成第二验证信息的生成方式一致，以使得所述第一验证信息与所述认证服务器生成的所述第二验证信息的值相同；

[0060] 基于所述第一认证密钥对所述第一验证信息加密生成第一加密值；

[0061] 其中，所述生成第一认证密钥的信息或/和所述生成第一验证信息的信息还包括所述应用标识。

[0062] 优选的，所述基于所述第一主密钥生成第一认证密钥包括：

[0063] 将所述第一主密钥作为所述第一认证密钥；或者，

[0064] 基于包括所述第一主密钥的信息生成所述第一认证密钥。

[0065] 优选的，所述基于包括所述第一主密钥的信息生成所述第一认证密钥包括：

[0066] 基于包括所述第一主密钥以及第一固定字符串或/和第一随机字符串或/和第一时间戳或/和所述临时用户标识或/和所述应用标识的信息生成所述第一认证密钥，所述第一固定字符串为预先配置的并且与所述认证服务器预先配置的第一固定字符串的值相同的字符串，所述第一随机字符串为随机生成的字符串，所述第一时间戳为通过获取当前系统时间生成；

[0067] 若生成所述第一认证密钥的信息包括所述第一随机字符串或/和所述第一时间戳，则将所述第一随机字符串或/和所述第一时间戳传递给所述应用服务器，以使得所述应用服务器将所述第一随机字符串或/和所述第一时间戳传递给所述认证服务器以生成所述第二认证密钥。

[0068] 优选的，所述生成第一验证信息包括：

[0069] 基于包括第二固定字符串或/和第二随机字符串或/和第二时间戳或/和所述临时用户标识或/和所述应用标识的信息生成所述第一验证信息，所述第二固定字符串为预先配置的并且与所述认证服务器预先配置的第二固定字符串的值相同的字符串，所述第二随机字符串为随机生成的字符串，所述第二时间戳为通过获取当前系统时间生成；

[0070] 若生成所述第一验证信息包括基于所述第二随机字符串或/和所述第二时间戳，则将所述第二随机字符串或/和所述第二时间戳传递给所述应用服务器，以使得所述应用服务器将所述第二随机字符串或/和所述第二时间戳传递给所述认证服务器以生成所述第二验证信息。

[0071] 优选的，所述基于包括第二固定字符串或/和第二随机字符串或/和第二时间戳或/和所述临时用户标识或/和所述应用标识的信息生成所述第一验证信息包括：

[0072] 将所述第二固定字符串或所述第二随机字符串或所述第二时间戳或所述临时用户标识或所述应用标识中的一种作为所述第一验证信息；或者，

[0073] 将所述第二固定字符串或所述第二随机字符串或所述第二时间戳或所述临时用户标识或所述应用标识中的一种生成的哈希值作为所述第一验证信息；或者，

[0074] 将包括所述第二固定字符串或/和所述第二随机字符串或/和所述第二时间戳或/和所述临时用户标识或/和所述应用标识的信息组合拼接后作为所述第一验证信息；或者，

[0075] 将包括所述第二固定字符串或/和所述第二随机字符串或/和所述第二时间戳或/和所述临时用户标识或/和所述应用标识的信息组合拼接后哈希计算生成的哈希值作为所述第一验证信息。

[0076] 优选的，所述基于所述第一认证密钥对所述第一验证信息加密生成第一加密值包括：

[0077] 使用签名加密算法基于所述第一认证密钥对所述第一验证信息签名加密生成所述第一加密值；或者，

[0078] 使用对称加密算法基于所述第一认证密钥对包括所述第一验证信息的信息对称加密生成所述第一加密值。

[0079] 优选的，所述方法还包括：

[0080] 将所述应用标识传递给所述应用服务器。

[0081] 第二方面，提供了一种身份认证方法，应用于应用服务器中，所述方法包括：

[0082] 接收智能设备发送的用于请求执行目标操作的操作请求，所述操作请求由所述智能设备在获取到用于向所述应用服务器请求执行所述目标操作的操作指示之后向所述应用服务器发送；

[0083] 获取所述智能设备传递的临时用户标识和第一加密值，所述临时用户标识为所述智能设备与认证服务器在认证与密钥协商成功时获取，所述第一加密值由所述智能设备基于第一主密钥和应用标识加密生成，所述第一主密钥由所述智能设备与所述认证服务器在所述认证与密钥协商成功时生成，所述应用标识为所述应用服务器的应用标识；

[0084] 向所述认证服务器发送验证请求，并且向所述认证服务器传递所述临时用户标识和所述第一加密值；

[0085] 接收所述认证服务器反馈的表示验证成功的应答消息，所述表示验证成功的应答消息是在所述认证服务器对所述临时用户标识和所述第一加密值验证成功之后所反馈的；

[0086] 执行所述目标操作。

[0087] 优选的，若接收到所述智能设备传递的应用标识，则所述方法还包括：

[0088] 判断所述传递的应用标识与所述应用服务器的应用标识是否一致；

[0089] 若是一致，则执行所述向所述认证服务器发送验证请求的步骤；

[0090] 若不一致，则不执行所述向所述认证服务器发送验证请求的步骤。

[0091] 优选的，若接收到所述智能设备传递的第一时间戳或/和第二时间戳，则所述方法还包括：

[0092] 将所述第一时间戳或/和所述第二时间戳与所述应用服务器的当前系统时间进行比较，确定两者的时间差是否在预先设定的有效范围内；

[0093] 若是在有效范围内，则执行所述向所述认证服务器发送验证请求的步骤，并且向所述认证服务器传递所述第一时间戳或/和第二时间戳；

[0094] 若不在有效范围内，则不执行所述向所述认证服务器发送验证请求的步骤。

[0095] 优选的，若接收到所述智能设备传递的第一随机字符串或/和第二随机字符串，则所述方法还包括：

[0096] 向所述认证服务器传递所述第一随机字符串或/和所述第二随机字符串。

[0097] 优选的，所述向所述认证服务器发送验证请求还包括：

[0098] 向所述认证服务器传递所述应用服务器的应用标识。

[0099] 优选的，所述接收所述认证服务器反馈表示验证成功的应答消息还包括：

[0100] 接收所述认证服务器反馈的用户标识信息，所述用户标识信息是所述认证服务器根据所述临时用户标识确定的。

[0101] 优选的，所述用户标识信息包括移动用户标识或/和MSISDN或/和第一OpenID或/和第二OpenID。

[0102] 第三方面，提供了一种身份认证方法，应用于认证服务器中，所述方法包括：

[0103] 基于用户数据系统与智能设备进行认证与密钥协商，若认证与密钥协商成功，则生成第二主密钥，生成临时用户标识并传递给所述智能设备，以及建立所述临时用户标识与所述第二主密钥的关联关系；

[0104] 接收应用服务器发送的验证请求，所述验证请求由所述应用服务器在接收到所述智能设备发送的用于请求执行目标操作的操作请求之后向所述认证服器发送，所述操作请求由所述智能设备在获取到用于向所述应用服务器请求执行所述目标操作的操作指示之后向所述应用服务器发送；

[0105] 获取所述应用服务器传递的所述临时用户标识和第一加密值，所述应用服务器传递的所述临时用户标识和所述第一加密值由所述智能设备通过所述应用服务器传递；

[0106] 根据所述应用服务器的身份信息确定所述应用服务器的应用标识；

[0107] 根据所述临时用户标识在所述关联关系中获取所述第二主密钥；

[0108] 基于所述第二主密钥和所述应用标识验证所述第一加密值；

[0109] 若所述第一加密值验证成功，则向所述应用服务器反馈表示验证成功的应答消息，以触发所述应用服务器执行所述目标操作。

[0110] 优选的，所述基于用户数据系统与智能设备进行认证与密钥协商包括：

[0111] 接收所述智能设备发送的认证与密钥协商请求，并且获取所述智能设备传递的移动用户标识；

[0112] 向所述用户数据系统发送认证请求，并且向所述用户数据系统传递所述移动用户标识；

[0113] 接收所述用户数据系统反馈的认证应答，并且获取所述用户数据系统反馈的随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥；

[0114] 向所述智能设备发送认证与密钥协商挑战消息，并且向所述智能设备传递所述随机数RAND和所述鉴权令牌AUTN；

[0115] 接收所述智能设备反馈的认证与密钥协商挑战应答消息，并且获取所述智能设备传递的第一期望响应值；

[0116] 基于所述第二期望响应值验证所述第一期望响应值；

[0117] 若验证所述第一期望响应值有效，则基于所述第二初始密钥生成第二主密钥，生成临时用户标识并传递给所述智能设备，以及建立所述临时用户标识与所述第二主密钥的关联关系，向所述智能设备发送认证与密钥协商成功应答消息，其中，所述第二主密钥的生成方式与所述智能设备生成第一主密钥的生成方式一致。

[0118] 优选的，所述基于所述第二期望响应值验证所述第一期望响应值包括：

[0119] 所述第一期望响应值为明文，比较所述第二期望响应值与所述第一期望响应值是

否一致,若一致则确定所述第一期望响应值有效;或者,

[0120] 所述第一期望响应值为哈希计算后的哈希值,则将所述第二期望响应值使用相同的哈希计算方式计算生成哈希值,并且比较两个哈希值是否一致,若一致则确定所述第一期望响应值有效。

[0121] 优选的,所述用户数据系统为归属用户服务器HSS,则:

[0122] 所述移动用户标识为国际移动用户识别码IMSI;

[0123] 所述第二期望响应值为期望响应值XRES;

[0124] 所述第二初始密钥为第二加密密钥CK或/和第二完整性密钥IK;或者,所述第二初始密钥为第二密钥KASME。

[0125] 优选的,所述用户数据系统为统一用户管理UDM,则:

[0126] 所述移动用户标识为用户永久标识SUPI;

[0127] 所述第二期望响应值为期望响应值XRES*;

[0128] 所述第二初始密钥为第二密钥KAUSF。

[0129] 优选的,所述移动用户标识为对所述用户永久标识SUPI加密后生成的用户隐藏标识SUCI,将所述用户隐藏标识SUCI作为所述向所述用户数据系统发送的认证请求中所包括的所述移动用户标识,在所述认证应答中还包括获取所述用户数据系统对所述用户隐藏标识SUCI解密后得到的所述用户永久标识SUPI,将所述解密后得到的所述用户永久标识SUPI作为后续步骤中的所述移动用户标识。

[0130] 优选的,所述基于所述第二初始密钥生成第二主密钥包括:

[0131] 将所述第二初始密钥作为所述第二主密钥;或者,

[0132] 基于包括所述第二初始密钥的信息生成所述第二主密钥。

[0133] 优选的,所述基于包括所述第二初始密钥的信息生成所述第二主密钥包括:

[0134] 基于包括所述第二初始密钥以及第四固定字符串或/和第四随机字符串或/和第四时间戳或/和所述移动用户标识的信息生成所述第二主密钥,所述第四固定字符串为预先配置的并且与所述智能设备预先配置的第四固定字符串的值相同的字符串,所述第四随机字符串为随机生成的字符串,所述第四时间戳为通过获取当前系统时间生成;

[0135] 若生成所述第二主密钥的信息包括所述第四随机字符串或/和所述第四时间戳,则将所述第四随机字符串或/和所述第四时间戳传递给所述智能设备。

[0136] 优选的,所述生成临时用户标识并传递给所述智能设备包括:

[0137] 根据所述随机数RAND生成所述临时用户标识,并且所述智能设备在接收到所述随机数RAND之后,在所述智能设备上使用相同的生成方式根据所述随机数RAND生成所述临时用户标识;或者,

[0138] 随机或按照一定规则生成所述临时用户标识,并且将所述临时用户标识传递给所述智能设备。

[0139] 优选的,所述根据所述应用服务器的身份信息确定所述应用服务器的应用标识包括:

[0140] 若以应用服务器进行身份认证的应用账号作为应用标识,则获取所述应用服务器的应用账号作为所述应用标识;或者,

[0141] 若以应用服务器的域名作为应用标识,则获取所述应用服务器的域名作为所述应

用标识;或者,

[0142] 预先保存有应用服务器的身份信息与应用标识的对应关系,获取所述应用服务器的身份信息,并根据所述身份信息在所述对应关系中获取所述应用标识。

[0143] 优选的,若接收到所述应用服务器传递的应用标识,则所述根据所述应用服务器的身份信息确定所述应用服务器的应用标识还包括:

[0144] 判断所述传递的应用标识与所述应用服务器的应用标识是否一致;

[0145] 若是一致,则执行所述根据所述临时用户标识在所述关联关系中获取所述第二主密钥;

[0146] 若不一致,则不执行所述根据所述临时用户标识在所述关联关系中获取所述第二主密钥。

[0147] 优选的,所述基于所述第二主密钥和所述应用标识验证所述第一加密值包括:

[0148] 基于所述第二主密钥生成第二认证密钥,其中,所述第二认证密钥的生成方式与所述智能设备生成第一认证密钥的生成方式一致,以使得所述第二认证密钥与所述智能设备生成的所述第一认证密钥的值相同;

[0149] 生成第二验证信息,其中,所述第二验证信息的生成方式与所述智能设备生成第一验证信息的生成方式一致,以使得所述第二验证信息与所述智能设备生成的所述第一验证信息的值相同;

[0150] 基于所述第二认证密钥和所述第二验证信息验证所述第一加密值;

[0151] 其中,所述生成第二认证密钥的信息或/和所述生成第二验证信息的信息还包括所述应用标识。

[0152] 优选的,所述基于所述第二主密钥生成第二认证密钥包括:

[0153] 将所述第二主密钥作为所述第二认证密钥;或者,

[0154] 基于包括所述第二主密钥的信息生成所述第二认证密钥。

[0155] 优选的,所述基于包括所述第二主密钥的信息生成所述第二认证密钥包括:

[0156] 基于包括所述第二主密钥以及第一固定字符串或/和第一随机字符串或/和第一时间戳或/和所述临时用户标识或/和所述应用标识的信息生成所述第二认证密钥,所述第一固定字符串为预先配置的并且与所述智能设备预先配置的第一固定字符串的值相同的字符串,所述第一随机字符串或/和所述第一时间戳为所述智能设备通过所述应用服务器所传递的。

[0157] 优选的,所述生成第二验证信息包括:

[0158] 基于包括第二固定字符串或/和第二随机字符串或/和第二时间戳或/和所述临时用户标识或/和所述应用标识的信息生成所述第二验证信息,所述第二固定字符串为预先配置的并且与所述智能设备预先配置的第二固定字符串的值相同的字符串,所述第二随机字符串或/和所述第二时间戳或/和所述应用标识为所述智能设备通过所述应用服务器所传递的。

[0159] 优选的,所述基于包括第二固定字符串或/和第二随机字符串或/和第二时间戳或/和所述临时用户标识或/和所述应用标识的信息生成所述第二验证信息包括:

[0160] 将所述第二固定字符串或所述第二随机字符串或所述第二时间戳或所述临时用户标识或所述应用标识中的一种作为所述第二验证信息;或者,

[0161] 将所述第二固定字符串或所述第二随机字符串或所述第二时间戳或所述临时用户标识或所述应用标识中的一种生成的哈希值作为所述第二验证信息;或者,

[0162] 将包括所述第二固定字符串或/和所述第二随机字符串或/和所述第二时间戳或/和所述临时用户标识或/和所述应用标识的信息组合拼接后作为所述第二验证信息;或者,

[0163] 将包括所述第二固定字符串或/和所述第二随机字符串或/和所述第二时间戳或/和所述临时用户标识或/和所述应用标识的信息组合拼接后哈希计算生成的哈希值作为所述第二验证信息。

[0164] 优选的,所述基于所述第二认证密钥和所述第二验证信息验证所述第一加密值包括:

[0165] 若所述智能设备使用签名加密算法基于所述第一认证密钥对所述第一验证信息签名加密生成所述第一加密值,则使用相同的签名加密算法基于所述第二认证密钥和所述第二验证信息验证所述第一加密值;或者,

[0166] 若所述智能设备使用对称加密算法基于所述第一认证密钥对包括所述第一验证信息的信息对称加密生成所述第一加密值,则使用相同的对称加密算法基于所述第二认证密钥和所述第二验证信息验证所述第一加密值。

[0167] 优选的,所述使用相同的签名加密算法基于所述第二认证密钥和所述第二验证信息验证所述第一加密值包括:

[0168] 使用和所述智能设备相同的签名加密算法,基于所述第二认证密钥对所述第二验证信息签名加密生成第二加密值;

[0169] 比较所述第二加密值与所述第一加密值是否一致;

[0170] 若一致,则确定所述第一加密值验证成功。

[0171] 优选的,所述使用相同的对称加密算法基于所述第二认证密钥和所述第二验证信息验证所述第一加密值包括:

[0172] 使用和所述智能设备相同的对称加密算法,基于所述第二认证密钥对所述第一加密值解密获得明文,并从所述解密获得的明文中获取第一验证信息;

[0173] 比较所述第二验证信息与所述第一验证信息是否一致;

[0174] 若一致,则确定所述第一加密值验证成功。

[0175] 优选的,若所述第一加密值验证成功,则所述方法还包括:

[0176] 根据所述临时用户标识确定相应的用户标识信息;

[0177] 将所述用户标识信息传递给所述应用服务器。

[0178] 优选的,所述根据所述临时用户标识确定相应的用户标识信息包括:

[0179] 根据所述临时用户标识获取用户身份标识;

[0180] 根据所述用户身份标识确定所述用户标识信息。

[0181] 优选的,所述根据所述临时用户标识获取用户身份标识包括:

[0182] 根据所述临时用户标识在临时用户标识与移动用户标识的关联关系中获取移动用户标识,将所述移动用户标识确定为所述用户身份标识,所述临时用户标识与移动用户标识的关联关系是在生成所述临时用户标识时建立的;或者,

[0183] 根据所述移动用户标识获取对应的MSISDN,将所述对应的MSISDN确定为所述用户身份标识;或者,

[0184] 预先建立有临时用户标识与用户身份标识的关联关系，根据所述临时用户标识在所述临时用户标识与用户身份标识的关联关系中获取所述用户身份标识，所述临时用户标识与用户身份标识的关联关系是在生成所述临时用户标识时建立的。

[0185] 优选的，所述根据所述用户身份标识确定所述用户标识信息包括：

[0186] 将所述用户身份标识作为所述用户标识信息；或/和，

[0187] 获取所述用户身份标识和所述应用标识对应的第一OpenID，确定所述第一OpenID为所述用户标识信息；或/和，

[0188] 基于所述用户身份标识和所述应用标识加密生成第二OpenID，确定所述第二OpenID为所述用户标识信息。

[0189] 优选的，所述根据所述用户身份标识和所述应用标识确定对应的第一OpenID包括：

[0190] 根据所述用户身份标识和所述应用标识获取对应的第一OpenID；

[0191] 若获取到对应的第一OpenID，则确定所述获取到的对应的第一OpenID为所述第一OpenID；

[0192] 若未获取到对应的第一OpenID，则生成一个唯一的第一OpenID，确定所述唯一的第一OpenID为所述第一OpenID，并且建立所述用户身份标识和所述应用标识与所述唯一的第一OpenID的对应关系。

[0193] 第四方面，提供一种智能设备，所述智能设备包括：存储器、处理器，所述处理器用于运行所述存储器所存储的程序，所述程序运行时实现上述第一方面应用于智能设备中的一种身份认证方法。

[0194] 提供一种应用服务器，所述应用服务器包括：存储器、处理器，所述处理器用于运行所述存储器所存储的程序，所述程序运行时实现上述第二方面应用于应用服务器中的一种身份认证方法。

[0195] 提供一种认证服务器，所述认证服务器包括：存储器、处理器，所述处理器用于运行所述存储器所存储的程序，所述程序运行时实现上述第三方面应用于认证服务器中的一种身份认证方法。

[0196] 提供一种存储介质，其特征在于，所述存储介质中存储有程序，所述程序用于实现包括上述第一方面应用于智能设备中的一种身份认证方法。

[0197] 提供一种存储介质，其特征在于，所述存储介质中存储有程序，所述程序用于实现包括上述第二方面应用于应用服务器中的一种身份认证方法。

[0198] 提供一种存储介质，其特征在于，所述存储介质中存储有程序，所述程序用于实现包括上述第三方面应用于认证服务器中的一种身份认证方法。

[0199] 第五方面，提供一种认证系统，所述认证系统包括：认证服务器、至少一个应用服务器和至少一个智能设备；所述认证服务器包括上述第四方面所述的认证服务器；所述应用服务器包括上述第四方面所述的应用服务器；所述智能设备包括上述第四方面所述的智能设备。

[0200] 其中，所述认证服务器与每一个所述智能设备相连接，用于分别与所述智能设备进行认证与密钥协商，以生成第二主密钥和生成临时用户标识，以及建立所述临时用户标识与所述第二主密钥的关联关系，以及将所述临时用户标识传递给所述智能设备。

[0201] 其中，每一个所述智能设备分别与所述认证服务器相连接，用于分别与所述认证服务器进行所述认证与密钥协商，以生成第一主密钥和获取所述临时用户标识。

[0202] 其中，每一个所述智能设备分别与一个或多个所述应用服务器相连接，用于分别获取对应连接的所述应用服务器的应用标识，基于所述第一主密钥和所述应用标识加密生成第一加密值，向所述对应连接的应用服务器发送执行目标操作的操作请求、所述临时用户标识和所述第一加密值，以使得所述对应连接的应用服务器对所述临时用户标识和所述第一加密值进行认证，并且在认证成功的情况下执行所述目标操作。

[0203] 其中，每一个所述应用服务器分别与一个或多个所述智能设备相连接，用于分别接收所述智能设备发送的所述执行目标操作的操作请求、所述临时用户标识和所述第一加密值。

[0204] 其中，每一个所述应用服务器分别与所述认证服务器相连接，用于分别将所述临时用户标识和所述第一加密值传递给所述认证服务器以进行验证，若接收到所述认证服务器反馈的表示验证成功的应答消息，则执行所述目标操作。

[0205] 其中，所述认证服务器与每一个所述应用服务器相连接，用于分别接收所述应用服务器传递的所述临时用户标识和所述第一加密值，根据所述临时用户标识在所述关联关系中获取第二主密钥，根据所述应用服务器的身份信息确定所述应用服务器的应用标识，基于所述第二主密钥和所述应用标识验证所述第一加密值，若验证成功，则反馈表示验证成功的应答消息，从而触发所述应用服务器执行所述目标操作。

[0206] 综上所述，本发明提供的技术方案带来的有益效果至少包括：第一方面，解决了现有的智能设备身份认证方式需要用户输入认证信息而导致的操作较为复杂低效的问题，提高了用户使用体验；第二方面，不需要在智能设备的生产过程中预先写入认证信息，由此可以提高智能设备的生产效率和节省生产成本；第三方面，即使是更换了智能设备，只要使用的是同一用户识别模块SIM，应用服务器还是可以辨识其身份，避免了更换智能设备后需要重新绑定用户账号等问题。

【附图说明】

[0207] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0208] 图1是本发明各实施例所涉及的一种实施环境结构示意图；

[0209] 图2是一种身份认证方法实施例一的流程示意图；

[0210] 图3是一种身份认证方法实施例二的流程示意图；

[0211] 图4是一种身份认证方法实施例三的流程示意图；

[0212] 图5是一种身份认证方法实施例四的流程示意图；

[0213] 图6是认证与密钥协商过程实施例的流程示意图；

[0214] 图7是一种认证系统实施例一的结构示意图；

[0215] 图8是一种认证系统实施例二的结构示意图；

[0216] 图9是一种认证系统实施例三的结构示意图。

[0217] 本发明目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

【具体实施方式】

[0218] 为使本发明的目的、技术方案和优点更加清楚,下面将结合附图对本发明实施方式作进一步地详细描述。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0219] 一、相关名词术语

[0220] 为了便于理解,对本文中涉及的一些名词作介绍和说明。

[0221] 移动用户标识:用于唯一地识别用户识别模块SIM的标识,移动用户标识包括国际移动用户识别码(International Mobile Subscriber Identification Number,IMSI),或者IP多媒体私有标识(IP Multimedia Private Identity,IMPI),或者用户永久标识(5G Subscription Permanent Identifier,SUPI),或者对用户永久标识加密后的结果即用户隐藏标识(Subscription Concealed Identifier,SUCI)。

[0222] MSISDN:移动用户ISDN号码(Mobile Subscriber ISDN Number),为呼叫一个移动用户所需拨打的号码,以及为向一个移动用户发送短信消息的接收号码,也就是通常所说的移动电话号码。

[0223] 临时用户标识:用于临时标识用户身份的标识。

[0224] 用户身份标识:用于长期标识用户身份的标识,包括移动用户标识、MSISDN或其他可以用于长期标识用户身份的标识。

[0225] 应用标识:用于唯一地识别应用服务器的标识。应用标识可以是应用服务器的域名或URI(Uniform Resource Identifie,统一资源标识符),也可以是一个字符串。

[0226] OpenID:在应用服务器中用于识别用户或智能设备身份的唯一标识,是认证服务器为了不把用户身份标识(如移动用户标识、MSISDN等)直接提供给应用服务器,而根据应用标识和用户标识生成的、用于在应用服务器中代替用户身份标识的标识。换言之,用户或智能设备的身份在应用服务器中使用OpenID来标识。

[0227] 认证与密钥协商机制:英文简称为AKA(Authentication and Key Agreement,AKA),基于挑战应答机制,完成用户与移动通信网络之间的身份认证,同时基于身份认证对通信加密密钥进行协商。

[0228] 用户识别模块SIM:用于为用户存储包括移动用户标识、移动用户密钥(K)、归属网络、AKA相关算法等的应用,用户基于用户识别模块SIM实现向移动通信网络的身份认证,具体包括全球用户识别模块(Universal Subscriber Identity Module,USIM)和IP多媒体服务识别模块(IP Multimedia Services Identity Module,ISIM)。

[0229] 签名加密算法:指用于加密地核实信息真实性的加密算法,只有信息的发送者才能产生的别人无法伪造的一段数字串,这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明,例如消息认证码(诸如基于哈希的消息认证码HMAC、密码分组链接消息认证码CBC-MAC、伽罗瓦消息认证码GMAC等)、含密钥加密的哈希函数、基于RSA的数字方案(诸如RSA-PSS)、数字签名算法(DSA)和椭圆曲线数字签名算法等。

[0230] 对称加密算法:指加密和解密使用相同密钥的加密算法,例如三重数据加密标准(Triple Data Encryption Standard,DES)、高级加密标准(Advanced Encryption

Standard,AES)等。

[0231] 二、实施环境结构示意图

[0232] 请参考图1,其示出了本发明各个实施例所涉及的一种实施环境的结构示意图。该实施环境包括智能设备、应用服务器、认证服务器和用户数据系统。

[0233] 智能设备:智能设备通过移动数据(包括3G移动数据、4G移动数据、5G移动数据、6G移动数据或NB-IoT移动数据)、WLAN、WiFi、LAN、固定宽带等有线或无线方式接入网络,与认证服务器通过网络相连接以进行认证与密钥协商,与应用服务器通过网络相连接以进行身份认证,该网络包括因特网、移动互联网等数据网络。智能设备是可插入、内嵌或者外部连接有用户识别模块SIM并且支持对用户识别模块SIM读取的智能设备,不仅可以是智能手表、智能手环等可穿戴式的物联网智能设备,也可以是智能电表、智能水表、智能家居、智能车载终端、物联网网关等物联网智能设备,还可以是智能手机、平板电脑等用户智能设备。

[0234] 应用服务器:用于向智能设备提供应用服务的服务器,与智能设备通过网络相连接,以获取智能设备的身份认证并向智能设备提供应用服务;与认证服务器通过网络相连接,以用于向认证服务器发送验证请求。

[0235] 认证服务器:与智能设备通过网络相连接,用于接收并执行智能设备的认证与密钥协商请求;与用户数据系统通过网络相连接,以用于基于用户数据系统与智能设备进行认证与密钥协商;与应用服务器通过网络相连接,用于接收应用服务器发送的验证请求,并向应用服务器返回验证结果。认证服务器通常由通信运营商提供。可以理解,在实际应用环境中,可以有多个甚至大量由不同应用服务商提供的应用服务器,认证服务器与这些应用服务器分别通过网络相连接,并且接收这些应用服务器发送的验证请求。

[0236] 用户数据系统:在移动通信网络中用于存储移动用户标识、移动用户密钥(K)、AKA相关算法并对用户进行身份认证等的系统,也被称为用户签约服务器,具体包括归属用户服务器(home subscriber server,HSS)或/和统一数据管理(unified data management,UDM)。

[0237] 本领域技术人员可以理解,图1中示出的实施环境结构并不构成对实施环境的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0238] 三、一种身份认证方法实施例一

[0239] 请参考图2,其示出了本发明提供的一种身份认证方法实施例一的流程图。本实施例以该方法应用于图1所示实施环境中的智能设备来举例说明,该方法可以包括:

[0240] 步骤201.基于用户识别模块SIM与认证服务器进行认证与密钥协商,若认证与密钥协商成功,则生成第一主密钥,以及获取所述认证服务器传递的临时用户标识。

[0241] 智能设备基于用户识别模块SIM与认证服务器基于用户数据系统进行认证与密钥协商;若认证与密钥协商成功,则认证服务器生成第二主密钥和生成临时用户标识,以及建立所述临时用户标识与所述第二主密钥的关联关系,以及将所述临时用户标识传递给智能设备;智能设备则生成第一主密钥,以及获取认证服务器传递的所述临时用户标识。

[0242] 步骤202.获取用于向应用服务器请求执行目标操作的操作指示。

[0243] 步骤203.获取所述应用服务器的应用标识。

[0244] 步骤204.基于所述第一主密钥和所述应用标识加密生成第一加密值。

[0245] 步骤205.向所述应用服务器发送执行所述目标操作的操作请求,并且将所述临时

用户标识和所述第一加密值传递给所述应用服务器，以使得所述应用服务器对所述临时用户标识和所述第一加密值进行认证，并且在认证成功的情况下执行所述目标操作。

[0246] 智能设备向所述应用服务器发送执行所述目标操作的操作请求，并且在将所述临时用户标识和所述第一加密值传递给所述应用服务器之后，应用服务器将所述临时用户标识和所述第一加密值传递给所述认证服务器，从而使得所述认证服务器根据所述临时用户标识在所述关联关系中获取所述第二主密钥，并且根据所述第二主密钥验证所述第一加密值，若验证成功，则向所述应用服务器反馈表示验证成功的应答消息，从而触发所述应用服务器执行所述目标操作。

[0247] 上述向所述应用服务器发送执行所述目标操作的操作请求，并且将所述临时用户标识和所述第一加密值传递给所述应用服务器的实施方式，既可以在一个步骤中同时进行，例如在所述操作请求中包括所述临时用户标识和所述第一加密值；也可以分成二个步骤进行，例如在发送所述操作请求之后发送所述临时用户标识和所述第一加密值；还可以分成更多的步骤进行，例如将所述临时用户标识和所述第一加密值分成两个步骤分别发送等。

[0248] 综上所述，本实施例提供的方法，智能设备通过与认证服务器进行认证与密钥协商以生成第一主密钥和获取临时用户标识，基于所述第一主密钥和应用服务器的应用标识加密生成第一加密值，向所述应用服务器发送执行目标操作的操作请求、所述临时用户标识和所述第一加密值，以使得所述应用服务器对所述临时用户标识和所述第一加密值进行认证，并且在认证成功的情况下执行所述目标操作。本实施例提供的方法，可以有效解决现有智能设备的身份认证需要用户输入认证信息而导致的操作较为复杂低效的问题，提高了用户使用体验，或者不需要在智能设备的生产过程中预先写入认证信息，由此可以提高智能设备的生产效率和节省生产成本。

[0249] 四、一种身份认证方法实施例二

[0250] 请参考图3，其示出了本发明提供的一种身份认证方法实施例二的流程图。本实施例以该方法应用于图1所示实施环境中的应用服务器来举例说明，该方法可以包括：

[0251] 步骤301.接收智能设备发送的用于请求执行目标操作的操作请求。

[0252] 所述操作请求由所述智能设备在获取到用于向所述应用服务器请求执行所述目标操作的操作指示之后向所述应用服务器发送。

[0253] 步骤302.获取所述智能设备传递的临时用户标识和第一加密值。

[0254] 所述临时用户标识为所述智能设备与认证服务器在认证与密钥协商成功之时获取，所述第一加密值由所述智能设备基于第一主密钥和应用标识加密生成，所述第一主密钥由所述智能设备与所述认证服务器在所述认证与密钥协商成功之时生成，所述应用标识为所述应用服务器的应用标识。

[0255] 需要说明的是，步骤302通常和步骤301同时进行，即接收智能设备发送的用于请求执行目标操作的操作请求、获取所述智能设备传递的临时用户标识和第一加密值在一个步骤中同时进行，例如，智能设备在发送的所述操作请求中包括所述临时用户标识和所述第一加密值，则应用服务器在接收到所述操作请求时，同时获取所述操作请求中包括的所述临时用户标识和所述第一加密值。但是在本实施例中，仅以步骤302和步骤301分成二个步骤进行举例说明，对此不作具体限定。

[0256] 步骤303.向所述认证服务器发送验证请求，并且向所述认证服务器传递所述临时用户标识和所述第一加密值。

[0257] 向所述认证服务器发送验证请求，并且向所述认证服务器传递所述临时用户标识和所述第一加密值的实施方式，既可以在一个步骤中同时进行，例如在所述验证请求中包括所述临时用户标识和所述第一加密值；也可以分成二个步骤进行，例如在发送所述验证请求之后发送所述临时用户标识和所述第一加密值；还可以分成更多的步骤进行，例如将所述临时用户标识和所述第一加密值分成两个步骤分别发送等。

[0258] 步骤304.接收所述认证服务器反馈的表示验证成功的应答消息。

[0259] 所述表示验证成功的应答消息是在所述认证服务器对所述临时用户标识和所述第一加密值验证成功之后所反馈的。

[0260] 步骤305.执行所述目标操作。

[0261] 应用服务器在接收到认证服务器反馈的表示验证成功的应答消息之后，则确定智能设备的身份认证成功，从而执行所述目标操作。

[0262] 综上所述，本实施例提供的方法，应用服务器通过接收智能设备发送的执行目标操作的操作请求、临时用户标识和第一加密值，将所述临时用户标识和所述第一加密值传递给认证服务器以进行验证；若接收到所述认证服务器在验证成功之后反馈的表示验证成功的应答消息，则执行所述目标操作。本实施例提供的方法，应用服务器可以对智能设备提供一种安全、便捷的身份认证方式，提高了应用服务器对用户的使用体验和节省了智能设备的生产成本。

[0263] 五、一种身份认证方法实施例三

[0264] 请参考图4，其示出了本发明提供的一种身份认证方法实施例三的流程图。本实施例以该方法应用于图1所示实施环境中的认证服务器来举例说明，该方法可以包括：

[0265] 步骤401.基于用户数据系统与智能设备进行认证与密钥协商，若认证与密钥协商成功，则生成第二主密钥，生成临时用户标识并传递给所述智能设备，以及建立所述临时用户标识与所述第二主密钥的关联关系。

[0266] 认证服务器基于用户数据系统与智能设备基于用户识别模块SIM进行认证与密钥协商；若认证与密钥协商成功，则认证服务器生成第二主密钥和生成临时用户标识，以及建立所述临时用户标识与所述第二主密钥的关联关系，以及将所述临时用户标识传递给智能设备；智能设备则生成第一主密钥，以及获取认证服务器传递的所述临时用户标识。

[0267] 步骤402.接收应用服务器发送的验证请求。

[0268] 所述验证请求由所述应用服务器在接收到所述智能设备发送的用于请求执行目标操作的操作请求之后向所述认证服器发送，所述操作请求由所述智能设备在获取到用于向所述应用服务器请求执行所述目标操作的操作指示之后向所述应用服务器发送。

[0269] 步骤403.获取所述应用服务器传递的所述临时用户标识和第一加密值。

[0270] 所述临时用户标识和所述第一加密值由所述智能设备通过所述应用服务器传递，所述第一加密值由所述智能设备基于所述第一主密钥和应用标识加密生成，所述应用标识为所述应用服务器的应用标识。

[0271] 需要说明的是，步骤403通常和步骤402同时进行，即接收应用服务器发送的验证请求、获取所述应用服务器传递的所述临时用户标识和第一加密值在一个步骤中同时进

行，例如，应用服务器在发送的所述验证请求中包括所述临时用户标识和所述第一加密值，则认证服务器在接收到所述验证请求时，同时获取所述验证请求中包括的所述临时用户标识和所述第一加密值。但是在本实施例中，仅以步骤403和步骤402分成二个步骤进行举例说明，对此不作具体限定。

[0272] 步骤404.根据所述应用服务器的身份信息确定所述应用服务器的应用标识。

[0273] 步骤405.根据所述临时用户标识在所述关联关系中获取所述第二主密钥。

[0274] 由于在步骤401中建立了所述临时用户标识与所述第二主密钥的关联关系，则可以根据所述临时用户标识在所述关联关系中获取所述第二主密钥。

[0275] 步骤406.基于所述第二主密钥和所述应用标识验证所述第一加密值。

[0276] 由于在步骤401中生成的所述第二主密钥与所述智能设备生成的第一主密钥的值是相同的，而所述第一加密值是由所述智能设备基于所述第一主密钥和应用标识加密生成的，则认证服务器可以基于所述第二主密钥和所述应用标识验证所述第一加密值。

[0277] 步骤407.若所述第一加密值验证成功，则向所述应用服务器反馈表示验证成功的应答消息。

[0278] 若所述第一加密值验证成功，则所述认证服务器向所述应用服务器反馈表示验证成功的应答消息，以触发所述应用服务器执行所述目标操作。

[0279] 综上所述，本实施例提供的方法，认证服务器通过与智能设备进行认证与密钥协商以建立临时用户标识与第二主密钥的关联关系，若接收到应用服务器传递的所述临时用户标识和第一加密值，则根据所述关联关系验证所述临时用户标识和所述第一加密值；若验证成功，则反馈表示验证成功的应答消息，从而触发所述应用服务器执行所述目标操作。本实施例提供的方法，认证服务器可以向应用服务器提供一种集中的、平台化的验证服务，该验证服务使得应用服务器能对智能设备提供一种安全、便携的身份认证方式，提高了应用服务器对用户的使用体验，以及有效节省智能设备需预先写入认证信息而产生的生产成本；以及为通信运营商提供了一种集中的、平台化的面向互联网业务和物联网业务的基础服务能力，促进了通信网络与互联网、物联网的业务融合。

[0280] 六、一种身份认证方法实施例四

[0281] 请参考图5，其示出了本发明提供的一种身份认证方法实施例四的流程示意图。本实施例是结合了上述一种身份认证方法实施例一、实施例二和实施例三所形成的实施例。本实施例以该方法应用于图1所示的实施环境来举例说明，该方法可以包括：

[0282] 步骤501.智能设备基于用户识别模块SIM与认证服务器基于用户数据系统进行认证与密钥协商；若认证与密钥协商成功，则在认证服务器上生成第二主密钥和临时用户标识，以及建立该临时用户标识与该第二主密钥的关联关系，在智能设备上生成第一主密钥，以及获取该临时用户标识。

[0283] 智能设备连接的用户识别模块SIM中存储有移动用户标识、移动用户密钥(K)和AKA相关算法，相应的，在认证服务器连接的用户数据系统中存储有该移动用户标识、该移动用户标识对应的移动用户密钥(K)和AKA相关算法。

[0284] 因此，智能设备基于用户识别模块SIM与认证服务器基于用户数据系统可以通过认证与密钥协商机制进行认证与密钥协商，若认证与密钥协商成功，则智能设备与认证服务器可以协商生成值相同的主密钥，为了区分，在这里将智能设备上生成的密钥称为第一

主密钥，将认证服务器上生成的密钥称为第二主密钥。

[0285] 同时，认证服务器生成临时用户标识，以及将该临时用户标识传递给智能设备；并且建立该临时用户标识与协商生成的第二主密钥的关联关系，以使得认证服务器在接收到该临时用户标识时，可以根据该临时用户标识在该关联关系中获取到该第二主密钥。相对应的，智能设备获取认证服务器传递的该临时用户标识。

[0286] 具体的，智能设备与认证服务器进行认证与密钥协商可以包括多种实施方式，在认证与密钥协商过程实施例中，提供了一种用以实现智能设备与认证服务器进行认证与密钥协商的实施方式。

[0287] 步骤502.智能设备获取用于向应用服务器请求执行目标操作的操作指示。

[0288] 目标操作是指需要对智能设备进行身份认证的网络操作。例如，目标操作为登录操作、入网操作、上报状态操作或各种业务应用操作等，其中，登录操作是指智能设备登录到应用服务器的操作；入网操作是指智能设备初次接入到应用服务器时需要通过身份认证才能进行账号绑定、设备配置等的操作；上报状态操作是指智能设备将当前获取到的状态信息上报给应用服务器的操作，上报的状态消息可以是智能设备的当前状态，也可以是智能设备检测到的环境属性(如温度、湿度等)。

[0289] 上述用于请求执行目标操作的操作指示既可以由用户或外部指令触发；也可以由智能设备自动触发，具体包括：

[0290] 例如，由用户点击执行目标操作的选项触发执行目标操作的操作指示。

[0291] 又例如，智能设备访问应用服务器，若应用服务器判断该访问操作需要对智能设备进行身份认证，则向智能设备返回需要该智能设备提供身份认证的操作指示。

[0292] 再例如，应用服务器生成用于指示智能设备执行目标操作的图形码，智能设备扫描该图形码，通过对该图形码解码后获得用于执行目标操作的操作指示。图形码可以为二维码或条形码，也可以是其它可以通过扫描解码方式获取其信息的图形。由于二维码的编码范围广、信息容量大，因此，图形码可优选采用二维码。

[0293] 还例如，由智能设备根据预先设定的判断条件自动触发，如根据预先设定的时间周期自动触发，或者在检测到的状态达到某个条件时自动触发等；例如智能设备检测是否已经入网，若检测结果为未入网，则触发执行入网操作等。

[0294] 步骤503.智能设备获取应用服务器的应用标识。

[0295] 智能设备获取应用服务器的应用标识可以包括多种实施方式：

[0296] 例如，在用于执行目标操作的操作指示中包括应用标识，智能设备获取该操作指示中包括的应用标识。可以理解，如果采用此种实施方式，则此种实施方式应该在步骤502之后执行。

[0297] 又例如，在智能设备上预先配置了应用标识，智能设备获取该预先配置的应用标识。可以理解，如果采用此种实施方式，则此种实施方式也可以在步骤502之前执行。

[0298] 步骤504.智能设备基于第一主密钥和应用标识加密生成第一加密值。

[0299] 在智能设备获取到第一主密钥和应用标识之后，则智能设备可以基于第一主密钥和应用标识加密以生成第一加密值。具体地，可以包括如下多个子步骤：

[0300] 子步骤504-1.智能设备基于第一主密钥生成第一认证密钥。

[0301] 智能设备基于第一主密钥生成第一认证密钥，生成方式可以包括多种实施方式，

至少可以包括：

[0302] 例如，将该第一主密钥作为第一认证密钥。

[0303] 又例如，基于包括该第一主密钥的信息生成第一认证密钥。具体地，以密钥派生算法公式为例，可以表示为：DK＝PBKDF2(passphrase,Salt,c,dkLen)，其中：DK是生成的第一认证密钥，PBKDF2是密钥派生算法，passphrase是该第一主密钥，或该第一主密钥和其他信息组合拼接的字符串，例如，passphrase是该第一主密钥和第一固定字符串(1)或/和第一随机字符串或/和第一时间戳或/和该临时用户标识或/和该应用标识组合拼接的字符串，其中，该第一固定字符串(1)为预先配置的并且与认证服务器预先配置的第一固定字符串(2)的值相同的字符串，第一随机字符串为本地随机生成的字符串，第一时间戳为通过获取智能设备的当前系统时间生成；Salt是盐值，在本例中是一个固定字符串；c是迭代次数；dkLen是密钥输出长度，可以根据使用的加密算法生成符合要求的密钥长度。

[0304] 子步骤504-2.智能设备生成第一验证信息。

[0305] 智能设备生成第一验证信息，以使得该第一验证信息用于加密，并且要使得该第一验证信息与认证服务器生成的第二验证信息的值相同。

[0306] 智能设备可以将第二固定字符串(1)或第二随机字符串或第二时间戳或该临时用户标识或该应用标识中的一种作为第一验证信息；或者，智能设备可以将第二固定字符串(1)或第二随机字符串或第二时间戳或该临时用户标识或该应用标识中的一种使用哈希算法进行哈希计算，将生成的哈希值作为第一验证信息；或者，智能设备将包括第二固定字符串(1)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识的信息组合拼接后生成第一验证信息；或者，智能设备将包括第二固定字符串(1)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识的信息组合拼接后生成的信息，再使用哈希算法进行哈希计算，将生成的哈希值作为第一验证信息。

[0307] 其中，该第二固定字符串(1)为预先配置的与认证服务器上预先配置的第二固定字符串(2)的值相同的字符串，该第二随机字符串为本地随机生成的字符串，该第二时间戳为通过获取智能设备的当前系统时间生成。

[0308] 上述子步骤504-1和504-2中，生成第一认证密钥的信息和生成第一验证信息的信息中至少有一个需包括该应用标识，即，生成第一认证密钥的信息或/和生成第一验证信息的信息还包括该应用标识。

[0309] 子步骤504-3.智能设备基于第一认证密钥对第一验证信息加密生成第一加密值。

[0310] 根据上述子步骤504-1、504-2中生成的第一认证密钥和第一验证信息，智能设备基于该第一认证密钥对该第一验证信息加密生成第一加密值。根据所使用的加密算法的不同，可以包括多种实施方式，至少可以包括：

[0311] 第一种实施方式，智能设备使用签名加密算法基于第一认证密钥对第一验证信息签名加密生成第一加密值。

[0312] 智能设备使用签名加密算法基于该第一认证密钥对该第一验证信息签名加密生成签名值，该签名值即为第一加密值。签名值可以唯一地识别第一验证信息，只有使用相同的签名加密算法、相同值的签名密钥、相同值的待签名信息才可以生成相同的签名值。

[0313] 例如，以签名加密算法使用哈希消息认证码为例，签名方式可以表示为：Signature＝HMAC_SHA256(k,m)，其中m是待签名信息即该第一验证信息，k是签名密钥即该

第一认证密钥,HMAC_SHA256是签名加密算法,Signature是签名值即第一加密值。

[0314] 又例如,以签名加密算法使用含密钥加密的哈希函数为例,签名方式可以表示为:Signature＝SHA256(k||m),其中m是待签名信息即该第一验证信息,k是签名密钥即该第一认证密钥,“k||m”表示将k和m组合拼接,SHA256是哈希函数,Signature是签名值即第一加密值。

[0315] 第二种实施方式,智能设备使用对称加密算法基于第一认证密钥对第一验证信息或包括第一验证信息的信息对称加密生成第一加密值。

[0316] 智能设备使用对称加密算法基于该第一认证密钥对第一验证信息或包括该第一验证信息的信息对称加密生成密文,该密文即为第一加密值,只有使用相同的对称加密算法、相同值的密钥才可以将该密文解密后得到原来的明文。

[0317] 例如,以对称加密算法使用AES为例,加密方式可以表示为:s＝AES_ENCRYPT(m,k),其中m是明文,该明文是第一验证信息,或者是包括该第一验证信息的信息,k是加密密钥即该第一认证密钥,AES_ENCRYPT是加密算法,s是加密结果即第一加密值。

[0318] 上述的包括该第一验证信息的信息,是指用于加密的明文中包括该第一验证信息和其他信息,例如将该第一验证信息和其他信息组合拼接后生成的信息,对于该其他信息,如非特别说明,在本实施例中并不进行限定。

[0319] 步骤505.智能设备向应用服务器发送执行目标操作的操作请求,该操作请求包括该临时用户标识和该第一加密值。

[0320] 智能设备根据上述步骤中获取到的执行目标操作的操作指示,以及根据获取的临时用户标识和生成的第一加密值,向应用服务器发送执行目标操作的操作请求,该操作请求包括临时用户标识和第一加密值。

[0321] 智能设备向应用服务器发送临时用户标识和第一加密值的目的,是为了使得应用服务器将该临时用户标识和第一加密值发送给认证服务器以进行验证,从而使得应用服务器能够根据认证服务器反馈的验证结果确定智能设备的身份认证是否成功。

[0322] 进一步的,在该操作请求中还可以包括应用标识。

[0323] 可以理解,为了使得认证服务器生成与第一认证密钥的值相同的第二认证密钥,则如果生成第一认证密钥的信息还包括第一随机字符串或/和第一时间戳,则在该操作请求中还包括该第一随机字符串或/和第一时间戳,以使得应用服务器将该第一随机字符串或/和第一时间戳发送给认证服务器以生成第二认证密钥。

[0324] 可以理解,为了使得认证服务器生成与第一验证信息的值相同的第二验证信息,则如果生成的第一验证信息还包括第二随机字符串或/和第二时间戳,则在该操作请求中还包括该第二随机字符串或/和该第二时间戳,以使得应用服务器将该第二随机字符串或/和该第二时间戳发送给认证服务器以生成第二验证信息。

[0325] 可以理解,如果生成的第一验证信息还包括临时用户标识,如上所述,在操作请求中已经包括了该临时用户标识。

[0326] 相应地,应用服务器接收智能设备发送的操作请求,并且获取操作请求中包括的临时用户标识和第一加密值。进一步的,如果在操作请求中还包括了应用标识、第一随机字符串、第二随机字符串、第一时间戳或/和第二时间戳,则应用服务器获取这些值。

[0327] 进一步的,如果从操作请求中获取了应用标识,则应用服务器判断该应用标识是

否是应用服务器自身的应用标识。具体地，将该应用标识与自身的应用标识进行比对，判断二者是否一致；若是一致，则执行下述步骤506及其后续步骤；若是不一致，则不执行下述步骤506及其后续步骤。

[0328] 进一步的，如果从操作请求中获取了第一时间戳或/和第二时间戳，则应用服务器判断该第一时间戳或/和第二时间戳是否有效。具体地，将该第一时间戳或/和第二时间戳与应用服务器的当前系统时间分别进行比较，确定两者的时间差是否在预先设定的有效范围内：如果是在有效的范围内，则执行下述步骤506及其后续步骤；如果不是在有效的范围内，则不执行下述步骤506及其后续步骤。

[0329] 步骤506.应用服务器向认证服务器发送验证请求，该验证请求包括该临时用户标识和该第一加密值。

[0330] 应用服务器在接收到智能设备发送的执行目标操作的操作请求之后，为了确认是否要执行该目标操作，需要对智能设备进行身份认证。

[0331] 应用服务器向认证服务器发送验证请求，该验证请求包括该临时用户标识和该第一加密值。

[0332] 进一步的，如果在上述步骤505的操作请求中还包括了第一随机字符串、第二随机字符串、第一时间戳或/和第二时间戳，则在发送的验证请求中还包括该第一随机字符串、该第二随机字符串、该第一时间戳或/和该第二时间戳。

[0333] 进一步的，在发送的验证请求中还可以包括应用标识。

[0334] 相应地，认证服务器接收应用服务器发送的验证请求，并且获取该验证请求中包括的临时用户标识和第一加密值，以及获取该第一随机字符串、该第二随机字符串、该第一时间戳或/和该第二时间戳、该应用标识。

[0335] 步骤507.认证服务器根据应用服务器的身份信息确定应用服务器的应用标识。

[0336] 认证服务器获取应用服务器的应用标识，为了确保获取的应用标识确实是该应用服务器的应用标识，则根据应用服务器的身份信息确定应用服务器的应用标识。

[0337] 例如，若以应用服务器向认证服务器进行身份认证的应用账号作为应用标识，则认证服务器在应用服务器的身份认证通过之后获取的应用账号，即为应用服务器的应用标识。需要注意的是，这里的身份认证是指应用服务器向认证服务器的身份认证，例如，在上述步骤506应用服务器向认证服务器发送的验证请求中，携带有应用服务器的身份认证信息，例如应用账号和密码、应用账号和经过密钥加密的加密值、令牌或会话状态等身份认证信息，认证服务器根据身份认证信息对应用服务器进行认证，在身份认证信息认证通过之后，获取该身份认证信息中的应用账号，或者获取令牌或会话状态关联的应用账号，该获取的应用账号即为应用服务器的应用标识。

[0338] 又例如，域名作为应用服务器的一种身份信息，如果以域名作为应用标识，则认证服务器根据应用服务器的IP地址进行域名反向解析获得域名，然后以该获得的域名作为应用服务器的应用标识。

[0339] 还例如，在认证服务器上预先保存有应用服务器的身份信息与应用标识的对应关系，认证服务器获取应用服务器的身份信息(如获取该应用服务器的应用账号、IP或域名等身份信息)，然后根据获取的身份信息在该对应关系中查找和获取应用服务器的应用标识。

[0340] 进一步的，认证服务器在获取到应用服务器的应用标识之后，如果在应用服务器

发送的验证请求中还包括有应用标识，则认证服务器判断该获取的应用服务器的应用标识与验证请求中包括的应用标识是否一致；若是一致，则执行下述步骤508及其后续步骤；若是不一致，则不执行下述步骤508及其后续步骤。

[0341] 步骤508.认证服务器根据该临时用户标识获取第二主密钥。

[0342] 在步骤501中，智能设备与认证服务器成功执行认证与密钥协商过程之后，在认证服务器上存储有临时用户标识与第二主密钥的关联关系，则认证服务器根据该临时用户标识在该关联关系中获取关联的第二主密钥。可以理解，该获取的关联的第二主密钥，即认证服务器在步骤501中所生成的第二主密钥。

[0343] 步骤509.认证服务器基于该第二主密钥和应用服务器的应用标识验证该第一加密值。

[0344] 由于在认证与密钥协商成功之后，在智能设备上生成的第一主密钥与认证服务器上生成的第二主密钥的值是相同的，因此，认证服务器可以使用与智能设备基于第一主密钥和应用标识加密生成第一加密值时相对应的实施方式，基于该第二主密钥和在步骤508中确定的应用标识验证该第一加密值。

[0345] 具体地，可以包括如下子步骤：

[0346] 子步骤509-1.认证服务器使用和智能设备相同的认证密钥生成方式基于该第二主密钥生成第二认证密钥。

[0347] 认证服务器使用和智能设备生成第一认证密钥时相同的认证密钥生成方式基于第二主密钥生成第二认证密钥，其中，相同的认证密钥生成方式包括密钥派生算法、输入信息、选择的参数都保持相同。由于智能设备上的第一主密钥和认证服务器上的第二主密钥的值是相同的，从而使得生成的第二认证密钥和智能设备上生成的第一认证密钥的值相同。

[0348] 具体地，第二认证密钥生成方式可以包括：

[0349] 例如，以使用和步骤504-1中智能设备相同的认证密钥生成方式为例，如果智能设备使用第一主密钥作为第一认证密钥，则认证服务器使用该第二主密钥作为第二认证密钥。

[0350] 又例如，以使用和步骤504-1中智能设备相同的认证密钥生成方式为例，如果智能设备基于包括该第一主密钥的信息生成第一认证密钥，则认证服务器基于包括该第二主密钥的信息生成第二认证密钥，并且该第二认证密钥的生成方式与智能设备生成第一认证密钥的生成方式一致。可以理解，如果智能设备生成第一认证密钥还包括其他的输入信息或输入参数，则认证服务器生成第二认证密钥也需包括使用相同的输入信息或输入参数，以使得生成的第二认证密钥和智能设备生成的第一认证密钥的值相同。

[0351] 具体地，以步骤504-1相对应的示例为例，密钥派生算法公式为：DK＝PBKDF2(passphrase,Salt,c,dkLen)，其中：DK是生成的第二认证密钥，PBKDF2是与智能设备相同的密钥派生算法，passphrase是该第二主密钥，或该第二主密钥和其他信息组合拼接的字符串，该其他信息的值与智能设备生成第一认证密钥的相同，并且组合拼接方式与认证服务器一致，例如，passphrase是该第二主密钥和第一固定字符串(2)或/和第一随机字符串或/和第一时间戳或/和该临时用户标识或/和该应用标识组合拼接的字符串，其中，该第一固定字符串(2)为预先配置的并且与智能设备预先配置的第一固定字符串(1)的值相同的

字符串，该第一随机字符串或/和该第一时间戳为从应用服务器发送的验证请求中所获取的；Salt是盐值，是一个与智能设备相同的固定字符串；c是与智能设备中相同的迭代次数；dkLen是与智能设备中相同的密钥输出长度。

[0352] 至此，由于在智能设备上的第一主密钥和在认证服务器上根据临时用户标识获取的第二主密钥的值是相同的，而由于第一认证密钥和第二认证密钥是使用相同的密钥生成方式、基于值相同的主密钥生成的，因此，第一认证密钥和第二认证密钥的值也是相同的。

[0353] 子步骤509-2.认证服务器生成第二验证信息。

[0354] 认证服务器生成第二验证信息，并且第二验证信息的生成方式与智能设备生成第一验证信息的生成方式一致，以使得该生成的第二验证信息的值与智能设备生成的第一验证信息的值相同。

[0355] 以使用和子步骤504-2生成第一验证信息相同的验证信息生成方式为例，如果智能设备将第二固定字符串(1)或第二随机字符串或第二时间戳或该临时用户标识或该应用标识中的一种作为第一验证信息，则认证服务器将第二固定字符串(2)或第二随机字符串或第二时间戳或该临时用户标识或该应用标识中相同的一种作为第二验证信息。

[0356] 以使用和子步骤504-2生成第一验证信息相同的验证信息生成方式为例，如果智能设备将第二固定字符串(1)或第二随机字符串或第二时间戳或该临时用户标识或该应用标识中的一种的哈希值作为第一验证信息，则认证服务器将第二固定字符串(2)或第二随机字符串或第二时间戳或该临时用户标识或该应用标识中相同的一种使用相同的哈希算法进行哈希计算，并将生成的哈希值作为第二验证信息。

[0357] 以使用和子步骤504-2生成第一验证信息相同的验证信息生成方式为例，如果智能设备将包括第二固定字符串(1)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识的信息生成第一验证信息，则认证服务器将包括第二固定字符串(2)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识的信息生成第二验证信息。例如，如果智能设备将第二固定字符串(1)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识组合拼接后作为第一验证信息，则认证服务器将第二固定字符串(2)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识使用相同的方式组合拼接后作为第二验证信息。

[0358] 以使用和子步骤504-2生成第一验证信息相同的验证信息生成方式为例，如果智能设备将包括第二固定字符串(1)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识的信息组合拼接后哈希计算生成的哈希值作为第一验证信息，则认证服务器将包括第二固定字符串(2)或/和第二随机字符串或/和第二时间戳或/和该临时用户标识或/和该应用标识的信息使用相同的方式组合拼接后生成的信息，再使用相同的哈希算法对该组合拼接后的信息进行哈希计算，并将生成的哈希值作为第二验证信息。

[0359] 其中，该第二固定字符串(2)为预先配置的并且与智能设备上预先配置的第二固定字符串(1)的值相同的字符串，该第二随机字符串或/和该第二时间戳为智能设备所发送的，该应用标识为步骤507所确定的应用服务器的应用标识。

[0360] 可以理解，如果智能设备生成第一验证信息还包括其他的输入信息，则认证服务器生成第二验证信息也需包括使用相同的输入信息，以使得生成的第二验证信息和智能设备生成的第一验证信息的值相同。

[0361] 至此，由于第一验证信息和第二验证信息是使用相同的验证信息生成方式、基于相同值的信息生成的，因此，第一验证信息和第二验证信息的值也是相同的。

[0362] 可以理解，由于智能设备在生成第一认证密钥的信息或/和生成第一验证信息的信息还包括有应用标识，则认证服务器在生成第二认证密钥的信息或/和生成第二验证信息的信息中也包括有该应用标识。

[0363] 子步骤509-3.认证服务器基于该第二认证密钥和该第二验证信息验证该第一加密值。

[0364] 与智能设备中生成第一加密值包括的多种实施方式相对应的，认证服务器基于该第二认证密钥和该第二验证信息验证该第一加密值需使用相对应的实施方式，具体实施方式包括：

[0365] 第一种实施方式，与智能设备使用签名加密算法生成第一加密值的实施方式相对应的，认证服务器使用和智能设备相同的签名加密算法，基于该第二认证密钥和该第二验证信息验证该第一加密值。具体可以包括如下子步骤：

[0366] 子步骤a.认证服务器使用和智能设备相同的签名加密算法，基于该第二认证密钥对该第二验证信息签名加密生成第二加密值。

[0367] 认证服务器使用和智能设备相同的签名加密算法基于该第二认证密钥对该第二验证信息签名加密生成签名值，该签名值即为第二加密值。

[0368] 例如，以签名加密算法使用和子步骤504-3智能设备中相同的哈希消息认证码为例，签名方式可以表示为:Signature＝HMAC_SHA256(k,m)，其中m是待签名信息即第二验证信息，k是签名密钥即第二认证密钥，HMAC_SHA256是与智能设备相同的哈希消息认证码，Signature是签名值即第二加密值。

[0369] 又例如，以签名算法使用和子步骤504-3智能设备中相同的含密钥加密的哈希函数为例，签名方式可以表示为:Signature＝SHA256(k||m)，其中m是待签名信息即该第二验证信息，k是签名密钥即该第二认证密钥，“k||m”表示将k和m组合拼接，SHA256是与智能设备相同的哈希函数，Signature是签名值即第二加密值。

[0370] 至此，由于认证服务器使用的是和智能设备相同的签名算法，第二验证信息和第一验证信息是值相同的待签名信息，第二认证密钥和第一认证密钥是值相同的签名密钥，则生成的第二加密值和第一加密值应当相同。

[0371] 子步骤b.认证服务器比较第二加密值与第一加密值是否一致；若一致，则确定第一加密值验证成功。

[0372] 认证服务器比较该第二加密值和该第一加密值是否一致，包括：

[0373] 如果比较结果是一致的，则确定该第一加密值验证成功。

[0374] 如果比较结果是不一致的，则确定该第一加密值验证失败。

[0375] 第二种实施方式，与智能设备使用对称加密算法生成第一加密值相对应的，认证服务器使用和智能设备相同的对称加密算法，基于该第二认证密钥和该第二验证信息验证该第二加密值。具体可以包括：

[0376] 子步骤i.认证服务器使用和智能设备相同的对称加密算法，基于该第二认证密钥对该第一加密值解密获得明文，并从该明文中获取第一验证信息。

[0377] 认证服务器使用和智能设备相同的对称加密算法基于该第二认证密钥对该第一

加密值解密,从而获得解密后的明文。

[0378] 例如,以使用与智能设备在子步骤504-3中使用的相同的AES对称加密算法为例,解密方式可以表示为:m＝AES_DENCRYPT(s,k),其中m是解密后的结果值,即解密后的明文,k是解密密钥即该第二认证密钥,AES_DENCRYPT是解密算法,s是密文即第一加密值。

[0379] 由于该明文是第一验证信息或者是包括该第一验证信息的信息,因此,可以从该明文中获取到解密后的第一验证信息。

[0380] 子步骤ii.认证服务器比较该第二验证信息与该解密后的第一验证信息是否一致;若一致,则确定第一加密值验证成功。

[0381] 认证服务器比较该第二验证信息和该解密后的第一验证信息是否一致,包括:

[0382] 如果比较结果是一致的,则确定该第一加密值验证成功。

[0383] 如果比较结果是不一致的,则确定该第一加密值验证失败。

[0384] 步骤510.可选的,若确定第一加密值验证成功,则认证服务器根据该临时用户标识确定相应的用户标识信息。

[0385] 若确定第一加密值验证成功,则认证服务器根据该临时用户标识确定相应的用户标识信息,具体可以包括:

[0386] 步骤510a.根据该临时用户标识确定用户身份标识。

[0387] 临时用户标识可以用于唯一地识别用户,根据临时用户标识确定的用户身份标识,也用于唯一地识别用户。

[0388] 例如,根据该临时用户标识在临时用户标识与移动用户标识的关联关系中获取移动用户标识,将移动用户标识确定为用户身份标识。临时用户标识与移动用户标识的关联关系是在智能设备与认证服务器进行认证与密钥协商的过程中建立的。

[0389] 又例如,根据该临时用户标识在临时用户标识与移动用户标识的关联关系中获取移动用户标识,然后再根据该移动用户标识获取对应的MSISDN,将该对应的MSISDN确定为用户身份标识。具体地,在用户数据系统中(例如归属用户服务器HSS或统一数据管理UDM),存储了移动用户标识与MSISDN的映射关系,根据移动用户标识可以在该映射关系中获取到对应的MSISDN。因此,认证服务器向用户数据系统发送包括该移动用户标识的MSISDN查询请求,用户数据系统向认证服务器反馈该移动用户标识对应的MSISDN,则认证服务器获取到对应的MSISDN。

[0390] 再例如,预先建立有临时用户标识与用户身份标识的关联关系,根据临时用户标识在该关联关系中获取用户身份标识。具体地,在认证服务器上预先建立有与移动用户标识相对应的用户身份标识,在智能设备与认证服务器进行认证与密钥协商的过程中,根据移动用户标识获取对应的用户身份标识,再建立该临时用户标识与该用户身份标识的关联关系,以使得根据该临时用户标识在该关联关系中能查找和获取到该用户身份标识。

[0391] 步骤510b.根据该用户身份标识确定用户标识信息。

[0392] 认证服务器根据用户身份标识确定相应的用户标识信息,可以包括多种实施方式,具体可以包括:

[0393] 实施方式一,将该用户身份标识作为用户标识信息。

[0394] 实施方式二,获取该用户身份标识和应用标识对应的第一OpenID,将该第一OpenID作为用户标识信息。

[0395] 具体地，在认证服务器上存储有用户身份标识和应用标识与第一OpenID的对应关系，即根据该用户身份标识和应用标识在该对应关系中能够查找到对应的第一OpenID。

[0396] 认证服务器根据该用户身份标识和应用标识在该对应关系中查找对应的第一OpenID。

[0397] 如果查找到对应的第一OpenID，则说明认证服务器已经为该用户创建了在该应用中对应用户身份的唯一标识，即为该用户身份标识创建了用于该应用标识的第一OpenID，则认证服务器获取该对应的第一OpenID。

[0398] 如果没有查找到对应的第一OpenID，则说明认证服务器没有为该用户创建在该应用中对应用户身份的唯一标识，即没有为该用户身份标识创建用于该应用标识的第一OpenID，则认证服务器生成一个唯一的OpenID，即生成一个唯一的字符串作为第一OpenID，并且建立该用户身份标识和应用标识与该第一OpenID的对应关系，以使得根据该用户身份标识和应用标识在该对应关系中能获取到该第一OpenID。

[0399] 实施方式三，基于该用户身份标识和应用标识加密生成第二OpenID，将该第二OpenID作为用户标识信息。

[0400] 认证服务器基于该用户身份标识和应用标识加密后生成的加密值作为第二OpenID，例如将该用户身份标识和应用标识组合之后，使用哈希算法加密生成哈希值，将该哈希值作为第二OpenID。当下次将该用户身份标识和应用标识使用相同的组合方式组合之后，再使用相同的哈希算法加密，生成的还是相同值的第二OpenID。

[0401] 步骤511.认证服务器根据对第一加密值的验证结果向应用服务器反馈相应的应答消息。

[0402] 认证服务器根据对第一加密值的验证结果向应用服务器反馈相应的应答消息，具体包括：

[0403] 若确定第一加密值验证成功，则向应用服务器反馈表示验证成功的应答消息；

[0404] 进一步地，如果实施了上述步骤510，则认证服务器在该表示验证成功的应答消息中还包括该用户标识信息，即包括该用户身份标识、该第一OpenID或/和该第二OpenID。

[0405] 若确定第一加密值验证失败，则向应用服务器反馈表示验证失败的应答消息。

[0406] 相应地，应用服务器接收认证服务器反馈的应答消息。

[0407] 步骤512.应用服务器根据认证服务器反馈的应答消息执行相应的目标操作。

[0408] 应用服务器根据接收到的认证服务器反馈的应答消息，确定智能设备的身份认证是否成功并执行相应的目标操作，包括：

[0409] 如果应答消息是表示验证成功的应答消息，则应用服务器确定智能设备的身份认证成功，并执行目标操作；例如，如果目标操作是登录操作、入网操作或上报状态操作，则执行相应的操作。

[0410] 进一步的，如果实施了上述步骤510，并且在表示验证成功的应答消息中还包括用户标识信息，则应用服务器可以将获取到的用户身份标识、第一OpenID或/和第二OpenID作为辨识用户或智能设备身份的标识，例如进行存储以用于智能设备下次操作时辨识其身份，或者与用户或智能设备在应用服务器中的用户账号进行绑定等。这样，即使是更换了智能设备，只要是使用同一用户识别模块SIM，应用服务器获取的还是相同的用户标识信息，从而可以保持其提供的信息和服务的一致性。

[0411] 如果应答消息是表示验证失败的应答消息，则应用服务器确定智能设备的身份认证失败，不执行目标操作。

[0412] 需要说明的是，在实施一次上述步骤501之后，智能设备、应用服务器和认证服务器可以多次实施步骤502至步骤512，即智能设备、应用服务器和认证服务器可以基于步骤501中协商生成的主密钥和临时用户标识等信息，然后多次实施步骤502至步骤512所述的身份认证过程，从而可以多次实现智能设备向应用服务器的身份认证和执行目标操作。

[0413] 需要说明的是，上述步骤504中智能设备基于第一主密钥和应用标识加密生成第一加密值的目的，是为了使得生成的第一加密值和应用标识相绑定，确保该第一加密值确实是用于向该应用标识对应的应用服务器进行身份认证的第一加密值，而不是用于向其他应用服务器进行身份认证的第一加密值，防止应用服务器仿冒该智能设备向其他应用服务器发送操作请求和进行身份认证。例如，如果生成第一加密值的信息中没有包括应用标识，则应用服务器在接收到智能设备发送的临时用户标识和第一加密值之后，有可能会仿冒智能设备向其他应用服务器发送该临时用户标识和该第一加密值，其他应用服务器将该临时用户标识和该第一加密值传递给认证服务器以进行验证时，由于认证服务器不能实现对该第一加密值和其他应用服务器身份是否绑定的鉴别，即认证服务器不能鉴别出该第一加密值是否是用于向该其他应用服务器进行身份认证的第一加密值，因此也会通过验证。

[0414] 综上所述，本实施例提供的方法，智能设备基于与认证服务器在认证与密钥协商成功之后生成的临时用户标识和第一主密钥，以及根据应用服务器的应用标识向应用服务器发起执行目标操作的操作请求，应用服务器向认证服务器发送包括相关认证信息的验证请求，认证服务器基于与智能设备在认证与密钥协商成功之后生成和存储的临时用户标识与第二主密钥的关联关系验证该验证请求，应用服务器根据认证服务器反馈的验证结果确定智能设备身份认证是否成功以及是否执行目标操作。本实施例带来的技术效果至少包括：第一方面，解决了现有的智能设备身份认证方式需要用户输入认证信息而导致的操作较为复杂低效的问题，提高了用户使用体验；第二方面，不需要在智能设备的生产过程中预先写入认证信息，由此可以提高智能设备的生产效率和节省生产成本；第三方面，即使是更换了智能设备，只要是同一用户识别模块SIM，应用服务器还是可以根据用户标识信息辨识其身份，避免了更换智能设备后需要重新绑定用户账号等问题；第四方面，使得认证服务器可以向应用服务器提供一种集中的、平台化的验证服务，该验证服务使得应用服务器能对智能设备提供一种安全、便携的身份认证方式；第五方面，用户识别模块SIM作为用户在移动通信网络中的必备组件，将其应用在互联网、物联网等应用服务的身份认证领域，提高了应用服务商的用户获取效率和减少了用户投入；第六方面，为通信运营商提供了一种集中的、平台化的面向互联网业务和物联网业务的基础服务能力，促进了通信网络与互联网、物联网的业务融合。

[0415] 七、认证与密钥协商过程实施例

[0416] 请参考图6，其示出了本发明提供的一种认证与密钥协商过程实施例的流程图。本实施例以该过程应用于图1所示实施环境来举例说明，该过程可以包括：

[0417] 步骤601.智能设备获取用户识别模块SIM的移动用户标识。

[0418] 本实施例以用户识别模块SIM是USIM，用户数据系统是归属用户服务器HSS或/和统一数据管理UDM为例进行说明。

[0419] 例如,以使用的用户数据系统是归属用户服务器HSS为例,则通过USIM上获取的移动用户标识是IMSI,智能设备通过操作系统上的API获取IMSI(例如Android系统上使用getSubscriberId方法),或者智能设备通过APDU命令读取USIM的EFimsi值来获取IMSI。

[0420] 又例如,以使用的用户数据系统是统一用户管理UDM为例,则通过USIM获取的移动用户标识是SUPI,SUPI由IMSI和网络标识等组成。

[0421] 需要说明的是,实际应用中,统一用户管理UDM主要作为5G网络的用户数据系统,归属用户服务器HSS主要作为3G/4G网络的用户数据系统,但若统一用户管理UDM保持了对归属用户服务器HSS的向前兼容,则本实施例各步骤中应用在归属用户服务器HSS的示例,也可以应用在统一用户管理UDM。

[0422] 步骤602.智能设备向认证服务器发送认证与密钥协商请求,该认证与密钥协商请求包括移动用户标识。

[0423] 进一步地,如上述步骤601中的示例,如果移动用户标识为SUPI,则还可以将该SUPI加密生成SUCI,并将该SUCI作为该认证与密钥协商请求中的移动用户标识,即,智能设备向认证服务器发送认证与密钥协商请求,在该认证与密钥协商请求中包括该SUCI。

[0424] 相应地,认证服务器接收智能设备发送的认证与密钥协商请求,并且获取该认证与密钥协商请求包括的移动用户标识。

[0425] 步骤603.认证服务器向用户数据系统发送认证请求,该认证请求包括移动用户标识。

[0426] 例如,以使用的用户数据系统是归属用户服务器HSS、移动用户标识是IMSI为例,可以通过向归属用户服务器HSS的SWx接口发送Multimedia-Auth-Request认证请求,在该认证请求中包括移动用户标识(即IMSI)。

[0427] 又例如,再以使用的用户数据系统是归属用户服务器HSS、移动用户标识是IMSI为例,可以通过向归属用户服务器HSS的S6a接口发送Authentication-Information-Request_S6认证请求,在该认证请求中包括移动用户标识(即IMSI)、服务网络标识以及网络类型,例如,服务网络标识是MCC(Mobile Country Code,移动国家码)+MNC(Mobile Network Code,移动网络码),网络类型是E-UTRAN。

[0428] 再例如,以使用的用户数据系统是统一用户管理UDM、移动用户标识是SUPI或SUCI为例,认证服务器向统一数据管理UDM发送Nudm_Authentication_Get认证请求,该认证请求中包括移动用户标识(即SUPI或SUCI),以及服务网络名(SN name),该服务网络名是认证服务器的服务网络名。

[0429] 需要说明的是,如果认证服务器同时连接有归属用户服务器HSS和统一数据管理UDM,则认证服务器需将认证请求发送给移动用户标识所属的归属用户服务器HSS或统一数据管理UDM,例如根据移动用户标识的类型或范围确定认证请求是要发送给归属用户服务器HSS还是统一数据管理UDM。

[0430] 步骤604.认证服务器接收用户数据系统反馈的认证应答,该认证应答包括随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥。

[0431] 在用户数据系统接收到认证服务器发送的认证请求之后,用户数据系统根据该认证请求反馈相应的认证应答,该认证应答包括随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥。

[0432] 相应地，认证服务器从该认证应答中获取随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥。

[0433] 例如，以使用的用户数据系统是归属用户服务器HSS为例，在归属用户服务器HSS接收到认证服务器发送的Multimedia-Auth-Request认证请求之后，归属用户服务器HSS向认证服务器返回Multimedia-Auth-Answer认证应答，该认证应答中包括随机数RAND、鉴权令牌AUTN、期望响应值XRES、第二加密密钥CK和第二完整性密钥IK，其中，第二期望响应值为期望响应值XRES，第二初始密钥为第二加密密钥CK或/和第二完整性密钥IK。可以理解，第二初始密钥为第二加密密钥CK或/和第二完整性密钥IK，是指在生成或使用第二初始密钥时包括第二加密密钥CK或/和第二完整性密钥IK。

[0434] 又例如，再以使用的用户数据系统是归属用户服务器HSS为例，在归属用户服务器HSS接收到认证服务器发送的Authentication-Information-Request_S6认证请求之后，归属用户服务器HSS向认证服务器返回Authentication-Information-Answer_S6认证应答，该认证应答中包括随机数RAND、鉴权令牌AUTN、期望响应值XRES、第二密钥K_{ASME}，其中，第二期望响应值为期望响应值XRES，第二初始密钥为第二密钥K_{ASME}。

[0435] 再例如，以使用的用户数据系统是统一用户管理UDM为例，在统一数据管理UDM接收到认证服务器发送的Nudm_Authentication_Get认证请求之后，统一数据管理UDM向认证服务器返回Nudm_Authentication_Get认证应答，该认证应答中包括随机数RAND、鉴权令牌AUTN、期望响应值XRES*和第二密钥K_{AUSF}，其中，第二期望响应值为期望响应值XRES*，第二初始密钥为第二密钥K_{AUSF}。进一步的，如果认证服务器向统一数据管理UDM发送的Nudm_Authentication_Get认证请求中包括的移动用户标识为SUCI，则统一用户管理UDM返回的Nudm_Authenticate_Get认证应答中还包括对该SUCI解密后得到的SUPI，并且认证服务器将该解密后的SUPI作为后续步骤中的移动用户标识。

[0436] 步骤605.认证服务器向智能设备发送认证与密钥协商挑战消息，该认证与密钥协商挑战消息包括随机数RAND和鉴权令牌AUTN。

[0437] 认证服务器保留第二期望响应值和第二初始密钥，并向智能设备发送认证与密钥协商挑战消息，该认证与密钥协商挑战消息包括该随机数RAND和该鉴权令牌AUTN。

[0438] 相应地，智能设备接收认证服务器发送的认证与密钥协商挑战消息，并从中获取该随机数RAND和该鉴权令牌AUTN。

[0439] 步骤606.智能设备向用户识别模块SIM发送鉴权请求，该鉴权请求包括该随机数RAND和该鉴权令牌AUTN。

[0440] 智能设备向用户识别模块SIM发送鉴权请求(例如通过发送APDU命令AUTHENTICATE)，该鉴权请求包括该随机数RAND和该鉴权令牌AUTN。

[0441] 步骤607.智能设备接收用户识别模块SIM的返回值，且根据该返回值获得第一期望响应值，该返回值包括期望响应值RES、第一加密密钥CK和第一完整性密钥IK。

[0442] 在用户识别模块SIM接收到智能设备发送的鉴权请求之后，用户识别模块SIM经过鉴权计算后向智能设备发送返回值，该返回值包括期望响应值RES、第一加密密钥CK和第一完整性密钥IK，智能设备接收该返回值。

[0443] 以使用的用户数据系统是归属用户服务器HSS为例，即与认证服务器保留的第二期望响应值为期望响应值XRES相对应的，智能设备从返回值中获取的期望响应值RES即为

第一期望响应值。

[0444] 以使用的用户数据系统是统一用户管理UDM为例,即与认证服务器保留的第二期望响应值为期望响应值XRES*相对应的,智能设备参照TS33.501 Annex A.4中“RES*和XRES*派生函数”中使用的方式,即使用和统一数据管理UDM生成期望响应值XRES*相同的方式,根据期望响应值RES生成期望响应值RES*,该期望响应值RES*即为第一期望响应值。

[0445] 进一步地,为了保护期望响应值RES或期望响应值RES*的安全,避免在传输过程中被泄露,还可以使用哈希算法(例如SHA256)对期望响应值RES或期望响应值RES*进行哈希计算,将经过哈希计算后生成的哈希值作为第一期望响应值,而不发送期望响应值RES或期望响应值RES*的明文。

[0446] 步骤608.智能设备向认证服务器发送认证与密钥协商挑战应答消息,该认证与密钥协商挑战应答消息包括第一期望响应值。

[0447] 智能设备向认证服务器发送认证与密钥协商挑战应答消息,该认证与密钥协商挑战应答消息包括该第一期望响应值。

[0448] 相应地,认证服务器接收智能设备发送的认证与密钥协商挑战应答消息,并获取该第一期望响应值。

[0449] 步骤609.认证服务器基于第二期望响应值验证第一期望响应值;若验证第一期望响应值有效,则执行步骤610。

[0450] 认证服务器在接收的认证与密钥挑战应答消息中获取到第一期望响应值之后,认证服务器将本地保留的第二期望响应值对其进行验证。

[0451] 如果第一期望响应值为期望响应值RES或期望响应值RES*的明文,则比较第二期望响应值与第一期望响应值是否一致;若一致,则确定验证第一期望响应值有效;若不一致,则确定验证第一期望响应值无效;或者,

[0452] 如果第一期望响应值为期望响应值RES或期望响应值RES*经过哈希计算后的哈希值,则将第二期望响应值使用相同的哈希计算方式计算生成哈希值,并且比较两个哈希值是否一致;若一致,则确定验证第一期望响应值有效;若不一致,则确定验证第一期望响应值无效。

[0453] 若确定验证第一期望响应值有效,则执行下述步骤610;若确定验证无效,则向智能设备发送认证与密钥协商应答消息,该认证与密钥协商应答消息是认证与密钥协商失败应答消息,并跳转执行下述步骤613。

[0454] 步骤610.认证服务器基于第二初始密钥生成第二主密钥。

[0455] 在上述步骤605中,认证服务器保留了第二初始密钥,认证服务器基于该第二初始密钥生成第二主密钥。

[0456] 例如,以该第二初始密钥作为第二主密钥。

[0457] 又例如,基于包括该第二初始密钥的信息生成第二主密钥。具体地,以密钥派生算法公式为例,可以表示为:DK＝PBKDF2(passphrase,Salt,c,dkLen),其中:DK是生成的第二主密钥,PBKDF2是密钥派生算法,passphrase是该第二初始密钥和其他信息组合拼接的字符串,例如,passphrase是该第二初始密钥,或该第二初始密钥和第四固定字符串(2)或/和第四随机字符串或/和第四时间戳或/和该移动用户标识组合拼接的字符串,该第四固定字符串(2)为预先配置的并且与智能设备上预先配置的第四固定字符串(1)的值相同的字符

串，该第四随机字符串为本地随机生成的字符串，该第四时间戳为通过获取认证服务器的当前系统时间生成；Salt是盐值，在本例中是一个固定字符串；c是迭代次数；dkLen是密钥输出长度，可以根据需要生成符合要求的密钥长度。

[0458] 步骤611.认证服务器生成临时用户标识，并且建立该临时用户标识与该第二主密钥的关联关系。

[0459] 认证服务器生成临时用户标识，并且建立该临时用户标识与第二主密钥的关联关系，以使得认证服务器在接收到该临时用户标识时，能够根据该临时用户标识获取到该第二主密钥。

[0460] 认证服务器生成临时用户标识可以包括多种实施方式，具体可以包括：

[0461] 第一种实施方式，根据随机数RAND生成临时用户标识。

[0462] 由于上述随机数RAND是临时生成的随机数，则认证服务器可以根据该随机数RAND生成临时用户标识，例如将该随机数RAND作为临时用户标识，又例如根据该随机数RAND基于一定的规则生成临时用户标识等(如在随机数RAND前加上前缀组合生成临时用户标识)。

[0463] 第二种实施方式，随机或按照一定规则生成临时用户标识。

[0464] 随机生成临时用户标识，或者按照一定的规则生成临时用户标识，例如生成一个唯一的随机数并加上固定的前缀组合生成临时用户标识等。

[0465] 进一步的，认证服务器建立该临时用户标识与该移动用户标识的关联关系，以使得根据该临时用户标识在该关联关系中能获取到该移动用户标识。

[0466] 再进一步的，在认证服务器上预先为用户创建有一个唯一的用户身份标识，并且预先建立有移动用户标识与用户身份标识的对应关系，因此，根据该移动用户标识获取对应的用户身份标识，然后再建立该临时用户标识与该用户身份标识的关联关系，以使得根据该临时用户标识在该关联关系中能获取到该用户身份标识。

[0467] 步骤612.认证服务器向智能设备发送认证与密钥协商应答消息，该认证与密钥协商应答消息是认证与密钥协商成功应答消息。

[0468] 如果在生成第二主密钥的信息中还包括第三随机字符串，则在该认证与密钥协商成功应答消息中还包括该第三随机字符串。

[0469] 需要说明的是，步骤610和步骤611还可以在步骤612即认证服务器向智能设备发送认证与密钥协商成功应答消息之后执行。当然，如果生成第二主密钥的信息在实施方式上还包括第三随机字符串，则步骤610需在步骤612之前执行。

[0470] 步骤613.智能设备接收认证服务器发送的认证与密钥协商应答消息并执行相应的操作。

[0471] 智能设备接收认证服务器发送的认证与密钥协商应答消息，该认证与密钥协商应答消息包括认证与密钥协商成功应答消息或认证与密钥协商失败应答消息。

[0472] 智能设备根据该认证与密钥协商应答消息执行相应的操作，包括：

[0473] 如果该认证与密钥协商应答消息是认证与密钥协商成功应答消息，则智能设备执行下述步骤614。

[0474] 如果该认证与密钥协商应答消息是认证与密钥协商失败应答消息，则不执行下述步骤，结束本次认证与密钥协商过程。

[0475] 步骤614.智能设备基于第一初始密钥生成第一主密钥，该第一初始密钥是基于第

一加密密钥CK或/和第一完整性密钥IK生成的。

[0476] 在步骤607用户识别模块SIM向智能设备发送的返回值中，智能设备获取第一加密密钥CK或/和第一完整性密钥IK，智能设备根据该第一加密密钥CK或/和该第一完整性密钥IK生成第一初始密钥。

[0477] 与认证服务器上的第二初始密钥为第二加密密钥CK或/和第二完整性密钥IK相对应的，智能设备以该第一加密密钥CK或/和该第一完整性密钥IK作为第一初始密钥。可以理解，第一初始密钥为第一加密密钥CK或/和第一完整性密钥IK，是指在生成或使用第一初始密钥时包括第一加密密钥CK或/和第一完整性密钥IK，并且与第二初始密钥为第二加密密钥CK或/和第二完整性密钥IK时的生成或使用方式相一致，以使得第一初始密钥与第二初始密钥的值相同。

[0478] 与认证服务器上的第二初始密钥为第二密钥K_{ASME}相对应的，智能设备参照TS33.401 Annex A.2中“K_{ASME}派生函数”中使用的方式，即使用和归属用户服务器HSS生成第二密钥K_{ASME}相同的方式，根据第一加密密钥CK或/和第一完整性密钥IK生成第一密钥K_{ASME}，该第一密钥K_{ASME}即为第一初始密钥。

[0479] 与认证服务器上的第二初始密钥为第二密钥K_{AUSF}相对应的，智能设备参照TS33.501 Annex A.2中“K_{AUSF}派生函数”中使用的方式，即使用和统一数据管理UDM生成第二密钥K_{AUSF}相同的方式，根据第一加密密钥CK或/和第一完整性密钥IK生成第一密钥K_{AUSF}，该第一密钥K_{AUSF}即为第一初始密钥。

[0480] 在生成第一初始密钥之后，智能设备使用和认证服务器相同的主密钥生成方式，基于该第一初始密钥生成第一主密钥。

[0481] 例如，如果在步骤610中认证服务器以该第二初始密钥作为第二主密钥，则智能设备以该第一初始密钥作为第一主密钥。

[0482] 又例如，如果在步骤610中认证服务器基于包括第二初始密钥的信息生成第二主密钥，则智能设备基于包括该第一初始密钥的信息生成第一主密钥。具体地，以使用和步骤610认证服务器相同的密钥派生算法为例，密钥派生算法公式可以表示为DK＝PBKDF2(passphrase,Salt,c,dkLen)，其中：DK是生成的第一主密钥；PBKDF2是与认证服务器相同的密钥派生算法；passphrase是该第一初始密钥和其他信息组合拼接的字符串，该其他信息的值与认证服务器生成第二主密钥的相同，并且组合拼接方式与认证服务器一致，例如，passphrase是该第一初始密钥和第四固定字符串(1)或/和第四随机字符串或/和第四时间戳或/和该移动用户标识组合拼接的字符串，其中，该第四固定字符串(1)是在智能设备上预先配置的并且与认证服务器上生成第二主密钥时所使用的第四固定字符串(2)的值相同的字符串，该第四随机字符串或/和第四时间戳是从认证服务器发送的认证与密钥协商成功应答消息中所获取的；Salt是盐值，是一个与认证服务器相同的固定字符串；c是与认证服务器相同的迭代次数；dkLen是与认证服务器相同的密钥输出长度。

[0483] 由于智能设备上生成的第一初始密钥与认证服务器上获取的第二初始密钥的值相同，又由于主密钥的生成方式一致，因此，在智能设备上生成的第一主密钥与认证服务器上生成的第二主密钥的值相同。

[0484] 步骤615.智能设备获得该临时用户标识。

[0485] 根据步骤611中认证服务器生成临时用户标识的实施方式，智能设备使用相对应

的实施方式获取该临时用户标识。具体包括：

[0486] 第一种实施方式，若认证服务器根据随机数RAND生成临时用户标识，则智能设备根据该随机数RAND生成临时用户标识。

[0487] 若认证服务器根据随机数RAND生成临时用户标识，由于在步骤605中智能设备接收到认证服务器发送的认证与密钥协商挑战消息，并从中获取到该随机数RAND，则智能设备根据该获取到的随机数RAND生成临时用户标识。

[0488] 如果认证服务器将该随机数RAND作为临时用户标识，则智能设备将该随机数RAND作为临时用户标识；如果认证服务器根据该随机数RAND基于一定的规则生成临时用户标识等(如在随机数RAND前加上前缀组合生成临时用户标识)，则智能设备根据该随机数RAND基于同样的规则生成临时用户标识。

[0489] 第二种实施方式，若认证服务器随机或按照一定规则生成临时用户标识，则由认证服务器将该临时用户标识传递给智能设备，智能设备获取该临时用户标识。

[0490] 如果认证服务器随机或按照一定规则生成临时用户标识，则由认证服务器将该临时用户标识传递给智能设备，例如在步骤612中认证服务器向智能设备发送的认证与密钥协商成功应答消息还包括该临时用户标识，智能设备在接收到认证与密钥协商成功应答消息之后，从中获取该临时用户标识；又例如智能设备在接收到认证服务器发送的认证与密钥协商成功应答消息之后，通过与认证服务器保持的连接状态或会话状态发送临时用户标识的获取请求，并获取认证服务器反馈的该临时用户标识。

[0491] 通过本实施例提供的方法，智能设备基于用户识别模块SIM中存储的移动用户标识、移动用户密钥(K)和相关AKA算法，以及认证服务器基于用户数据系统中存储的移动用户标识、移动用户密钥(K)和相关AKA算法，经过智能设备和认证服务器间的认证与密钥协商过程，在认证与密钥协商成功之后，在认证服务器上生成了第二主密钥和临时用户标识，以及建立该临时用户标识与该第二主密钥的关联关系，在智能设备上生成第一主密钥，以及获取该临时用户标识，从而智能设备可以使用生成的第一主密钥和获取的临时用户标识生成认证信息后实现向应用服务器的身份认证，而应用服务器则向认证服务器转发该认证信息以请求获得认证服务器的验证，认证服务器则基于生成的第二主密钥和临时用户标识及其关联关系实现对应用服务器转发的认证信息的验证。

[0492] 八、一种认证系统实施例一

[0493] 请参考图7，其示出了本发明提供的一种认证系统实施例一的结构示意图。该认证系统包括：第一智能设备、第一应用服务器、第二智能设备和认证服务器。

[0494] 其中，所述第一智能设备是一个智能设备(如一个智能手表)，所述第二智能设备是另一个智能设备(如另一个智能手表)，所述第一应用服务器是用于向智能设备提供应用服务的服务器(如一种智能手表类应用服务)。

[0495] 其中，在所述第一智能设备向所述第一应用服务器进行身份认证和执行目标操作时，将所述第一智能设备作为所述一种身份认证方法实施例四中的智能设备，将所述第一应用服务器作为所述一种身份认证方法实施例四中的应用服务器，将所述认证服务器作为所述一种身份认证方法实施例四中的认证服务器，实施如所述一种身份认证方法实施例四中所述的过程；其中，所述第一智能设备与所述认证服务器实施如所述一种身份认证方法实施例四中所述的步骤501时，还可以参照所述认证与密钥协商过程实施例进行实施，即将

所述第一智能设备作为所述认证与密钥协商过程实施例中的智能设备，将所述认证服务器作为所述认证与密钥协商过程实施例中的认证服务器，实施如所述认证与密钥协商过程实施例中所述的过程。

[0496] 其中，在所述第二智能设备向所述第一应用服务器进行身份认证和执行目标操作时，将所述第二智能设备作为所述一种身份认证方法实施例四中的智能设备，将所述第一应用服务器作为所述一种身份认证方法实施例四中的应用服务器，将所述认证服务器作为所述一种身份认证方法实施例四中的认证服务器，实施如所述一种身份认证方法实施例四中所述的过程；其中，所述第二智能设备与所述认证服务器实施如所述一种身份认证方法实施例四中所述的步骤501时，还可以参照所述认证与密钥协商过程实施例进行实施，即将所述第二智能设备作为所述认证与密钥协商过程实施例中的智能设备，将所述认证服务器作为所述认证与密钥协商过程实施例中的认证服务器，实施如所述认证与密钥协商过程实施例中所述的过程。

[0497] 本实施例提供的认证系统，该认证系统内包括两个智能设备，每个智能设备分别与应用服务器相连接，并且每个智能设备分别向应用服务器进行身份认证和执行相应的目标操作。实际应用中，认证系统内还可以包括多个智能设备，每个智能设备分别与应用服务器相连接，并且每个智能设备分别向应用服务器进行身份认证和执行相应的目标操作，具体的实施方式不再赘述。

[0498] 九、一种认证系统实施例二

[0499] 请参考图8，其示出了本发明提供的一种认证系统实施例二的结构示意图。该认证系统包括：第三智能设备、第三应用服务器、第四应用服务器和认证服务器。

[0500] 其中，所述第三智能设备是一种类型的智能设备(如一种智能手表)，所述第三应用服务器是用于向所述第三智能设备提供一种应用服务的服务器(如向智能手表提供一种应用服务)，所述第四应用服务器是用于向所述第三智能设备提供另一种应用服务的服务器(如向智能手表提供另一种应用服务)。

[0501] 其中，将所述第三智能设备作为所述一种身份认证方法实施例四中的智能设备，将所述认证服务器作为所述一种身份认证方法实施例四中的认证服务器，实施如所述一种身份认证方法实施例四中所述的步骤501；进一步的，实施该步骤501还可以参照所述认证与密钥协商过程实施例，即将所述第三智能设备作为所述认证与密钥协商过程实施例中的智能设备，将所述认证服务器作为所述认证与密钥协商过程实施例中的认证服务器，实施如所述认证与密钥协商过程实施例中所述的过程。

[0502] 其中，在实施如上所述一种身份认证方法实施例四中所述的步骤501之后，在所述第三智能设备向所述第三应用服务器进行身份认证和执行目标操作时，将所述第三智能设备作为所述一种身份认证方法实施例四中的智能设备，将所述认证服务器作为所述一种身份认证方法实施例四中的认证服务器，将所述第三应用服务器作为所述一种身份认证方法实施例四中的应用服务器，实施如所述一种身份认证方法实施例四中所述的步骤502至步骤512。需要说明的是，在实施步骤503时为了让所述第三智能设备获取的应用标识是所述第三应用服务器的应用标识，在实施步骤505时为了让所述第三智能设备将所述执行目标操作的操作请求发送到所述第三应用服务器，则，在实施步骤503时，可以在执行目标操作的操作指示中包括所述第三应用服务器的应用标识和请求地址，所述第三智能设备在执行

目标操作的操作指示中获取所述第三应用服务器的应用标识和请求地址;或者,在所述第三智能设备上预先配置有所述第三应用服务器的应用标识和请求地址,所述第三智能设备根据执行目标操作的操作指示获取所述第三应用服务器的应用标识和请求地址,例如,如果是执行一种目标操作的操作指示,则获取所述第三应用服务器的应用标识和请求地址。

[0503] 其中,在实施如上所述一种身份认证方法实施例四中所述的步骤501之后,在所述第三智能设备向所述第四应用服务器进行身份认证和执行目标操作时,将所述第三智能设备作为所述一种身份认证方法实施例四中的智能设备,将所述认证服务器作为所述一种身份认证方法实施例四中的认证服务器,将所述第四应用服务器作为所述一种身份认证方法实施例四中的应用服务器,实施如所述一种身份认证方法实施例四中所述的步骤502至步骤512,从而实现所述第三智能设备向所述第四应用服务器的身份认证。需要说明的是,在实施步骤503时为了让所述第三智能设备获取的应用标识是所述第四应用服务器的应用标识,在实施步骤505时为了让所述第三智能设备将所述执行目标操作的操作请求发送到所述第四应用服务器,则,在实施步骤503时,可以在执行目标操作的操作指示中包括所述第四应用服务器的应用标识和请求地址,所述第三智能设备在执行目标操作的操作指示中获取所述第四应用服务器的应用标识和请求地址;或者,在所述第三智能设备上预先配置有所述第四应用服务器的应用标识和请求地址,所述第三智能设备根据执行目标操作的操作指示获取所述第四应用服务器的应用标识和请求地址,例如,如果是执行另一种目标操作的操作指示,则获取所述第四应用服务器的应用标识和请求地址。

[0504] 还需要说明的是,在所述第三智能设备与所述认证服务器实施一次如上所述一种身份认证方法实施例四中所述的步骤501之后,所述第三智能设备与所述第三应用服务器、所述第四应用服务器可以分别多次实施如上所述一种身份认证方法实施例四中所述的步骤502至步骤512,从而可以多次实现所述第三智能设备分别向所述第三应用服务器、所述第四应用服务器的身份认证和执行目标操作。

[0505] 本实施例提供的认证系统,该认证系统内的智能设备与两个应用服务器分别相连接,并且智能设备分别向该两个应用服务器进行身份认证和执行相应的目标操作。实际应用中,认证系统内还可以包括多个应用服务器,智能设备与该多个应用服务器分别相连接,并且智能设备分别向该多个应用服务器进行身份认证和执行相应的目标操作,具体的实施方式不再赘述。

[0506] 十、一种认证系统实施例三

[0507] 请参考图9,其示出了本发明提供的一种认证系统实施例三的结构示意图。该认证系统包括:第一智能设备、第一应用服务器、第三智能设备、第三应用服务器、第四应用服务器和认证服务器;

[0508] 所述第一智能设备向所述第一应用服务器进行身份认证的实施方式,可以参照一种认证系统实施例一中的第一智能设备向第一应用服务器进行身份认证的实施方式,具体的实施方式不再赘述。

[0509] 所述第三智能设备分别向所述第三应用服务器和所述第四应用服务器进行身份认证的实施方式,可以参照一种认证系统实施例二中的第三智能设备分别向第三应用服务器和第四应用服务器进行身份认证的实施方式,具体的实施方式不再赘述。

[0510] 需要说明的是,在本文中,术语“包括”、“包含”、“传递”、“发送”或者任何其他变体

意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、产品或者系统不仅包括那些要素，而且还可以包括没有明确列出的其他要素，或者是还可以包括为这种过程、方法、产品或者系统所固有的要素。

[0511] 术语“第一”、“第二”、“第三”等(如果存在)仅用于区别类似的对象，而不用于描述特定的顺序或先后次序。应该理解，这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。

[0512] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0513] 可以以许多方式来实现本发明的方法、装置和系统。例如，可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本发明的方法、装置和系统。用于方法的步骤的上述顺序仅是为了进行说明，本发明的方法的步骤不限于以上具体描述的顺序，除非以其它方式特别说明。此外，在一些实施例中，还可将本发明实施为记录在记录介质中的程序，这些程序包括用于实现根据本发明的方法的机器可读指令。因而，本发明还覆盖存储用于执行根据本发明的方法的程序的记录介质。

[0514] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

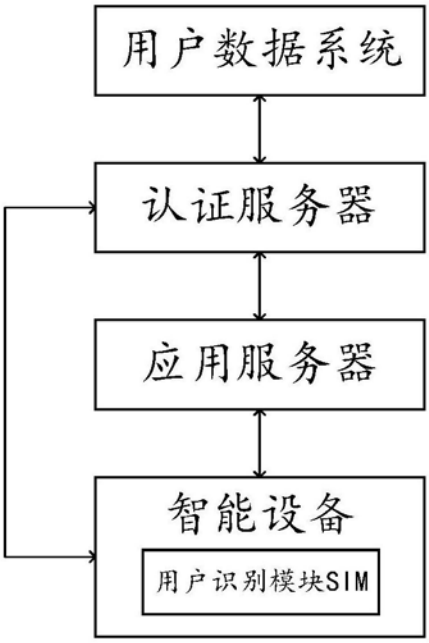

用户数据系统
认证服务器
应用服务器
智能设备
用户识别模块SIM

图1

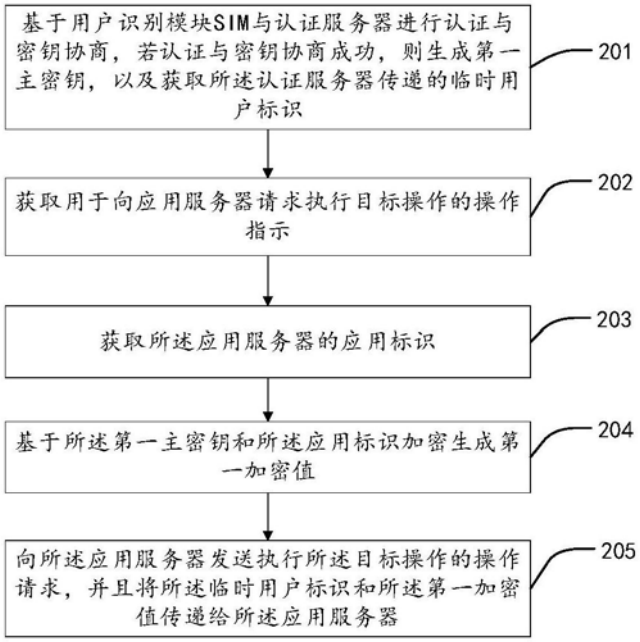

基于用户识别模块SIM与认证服务器进行认证与密钥协商，若认证与密钥协商成功，则生成第一主密钥，以及获取所述认证服务器传递的临时用户标识
201
获取用于向应用服务器请求执行目标操作的操作指示
202
获取所述应用服务器的应用标识
203
基于所述第一主密钥和所述应用标识加密生成第一加密值
204
向所述应用服务器发送执行所述目标操作的操作请求，并且将所述临时用户标识和所述第一加密值传递给所述应用服务器
205

图2

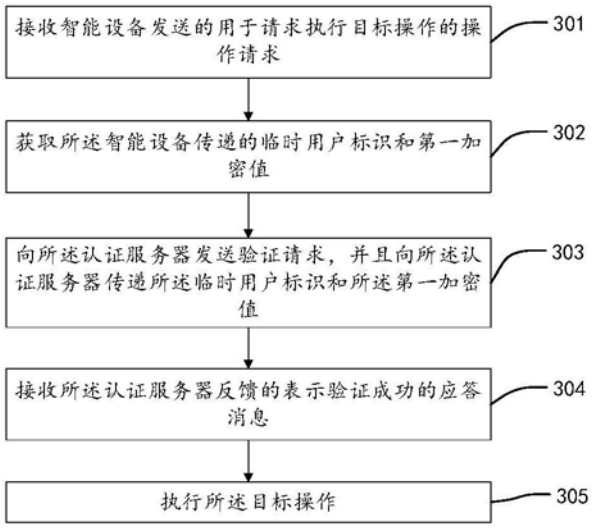

接收智能设备发送的用于请求执行目标操作的操作请求
301
获取所述智能设备传递的临时用户标识和第一加密值
302
向所述认证服务器发送验证请求，并且向所述认证服务器传递所述临时用户标识和所述第一加密值
303
接收所述认证服务器反馈的表示验证成功的应答消息
304
执行所述目标操作
305

图3

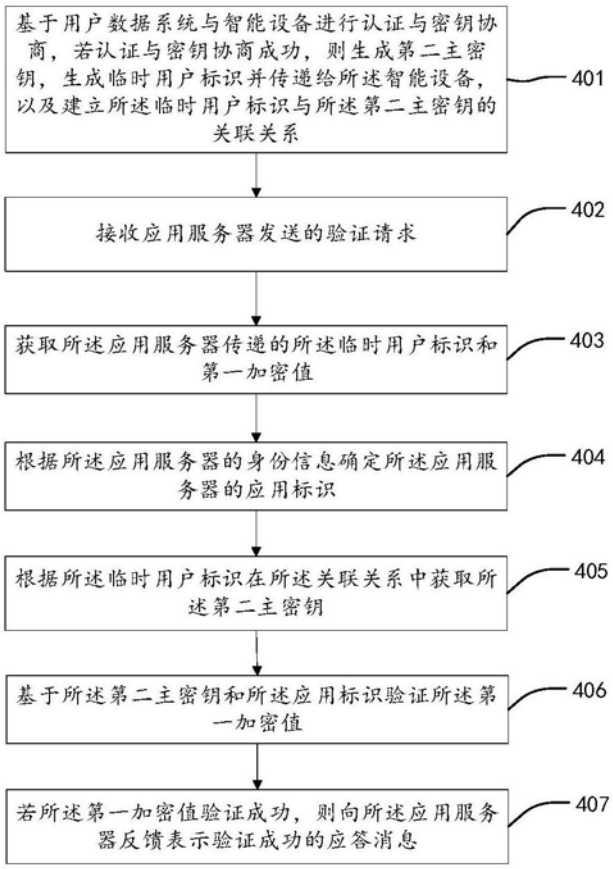

基于用户数据系统与智能设备进行认证与密钥协商，若认证与密钥协商成功，则生成第二主密钥，生成临时用户标识并传递给所述智能设备，以及建立所述临时用户标识与所述第二主密钥的关联关系
401
接收应用服务器发送的验证请求
402
获取所述应用服务器传递的所述临时用户标识和第一加密值
403
根据所述应用服务器的身份信息确定所述应用服务器的应用标识
404
根据所述临时用户标识在所述关联关系中获取所述第二主密钥
405
基于所述第二主密钥和所述应用标识验证所述第一加密值
406
若所述第一加密值验证成功，则向所述应用服务器反馈表示验证成功的应答消息
407

图4

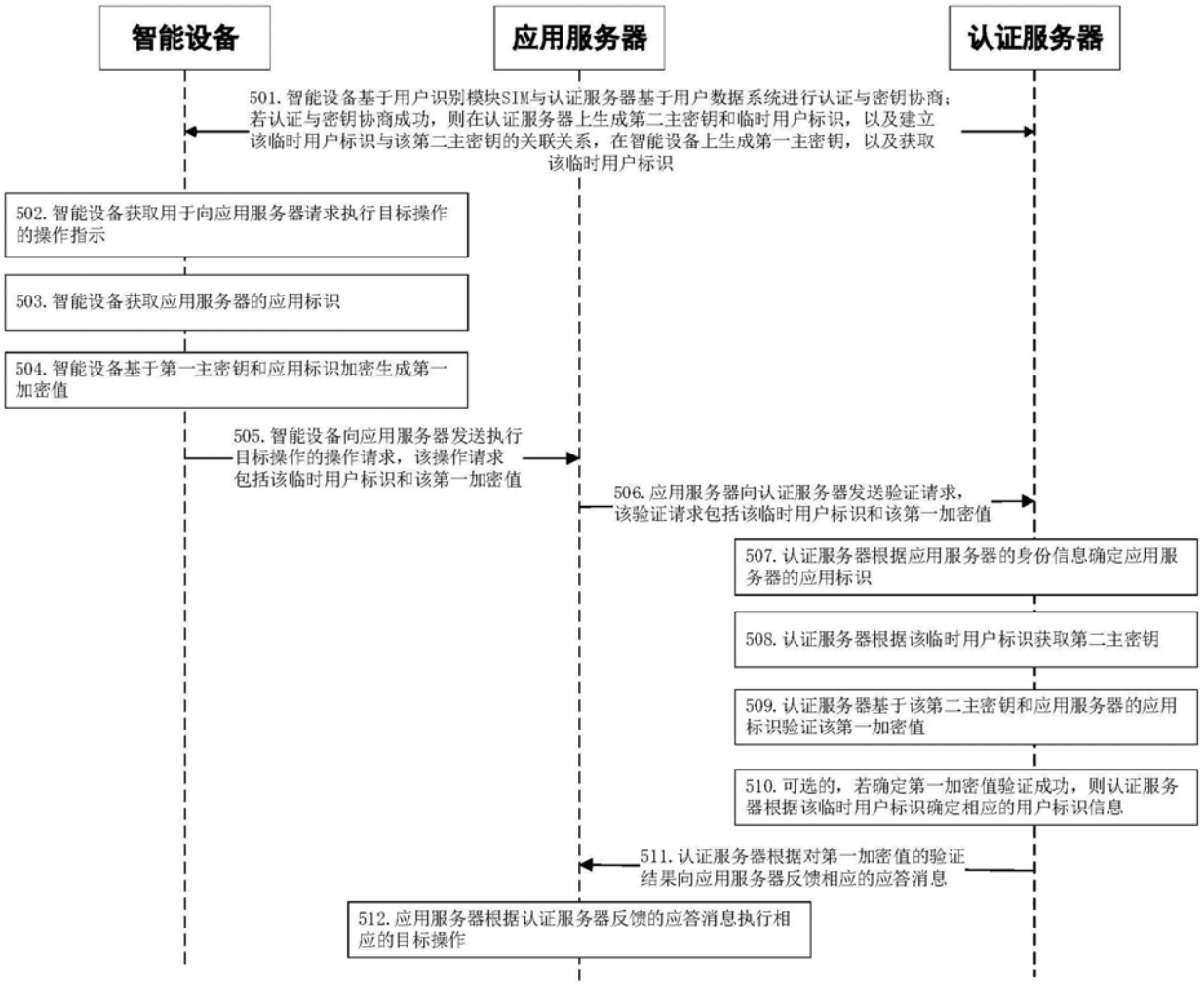

智能设备
应用服务器
认证服务器
501.智能设备基于用户识别模块SIM与认证服务器基于用户数据系统进行认证与密钥协商；若认证与密钥协商成功，则在认证服务器上生成第二主密钥和临时用户标识，以及建立该临时用户标识与该第二主密钥的关联关系，在智能设备上生成第一主密钥，以及获取该临时用户标识
502.智能设备获取用于向应用服务器请求执行目标操作的操作指示
503.智能设备获取应用服务器的应用标识
504.智能设备基于第一主密钥和应用标识加密生成第一加密值
505.智能设备向应用服务器发送执行目标操作的操作请求，该操作请求包括该临时用户标识和该第一加密值
506.应用服务器向认证服务器发送验证请求，该验证请求包括该临时用户标识和该第一加密值
507.认证服务器根据应用服务器的身份信息确定应用服务器的应用标识
508.认证服务器根据该临时用户标识获取第二主密钥
509.认证服务器基于该第二主密钥和应用服务器的应用标识验证该第一加密值
510.可选的，若确定第一加密值验证成功，则认证服务器根据该临时用户标识确定相应的用户标识信息
511.认证服务器根据对第一加密值的验证结果向应用服务器反馈相应的应答消息
512.应用服务器根据认证服务器反馈的应答消息执行相应的目标操作

图5

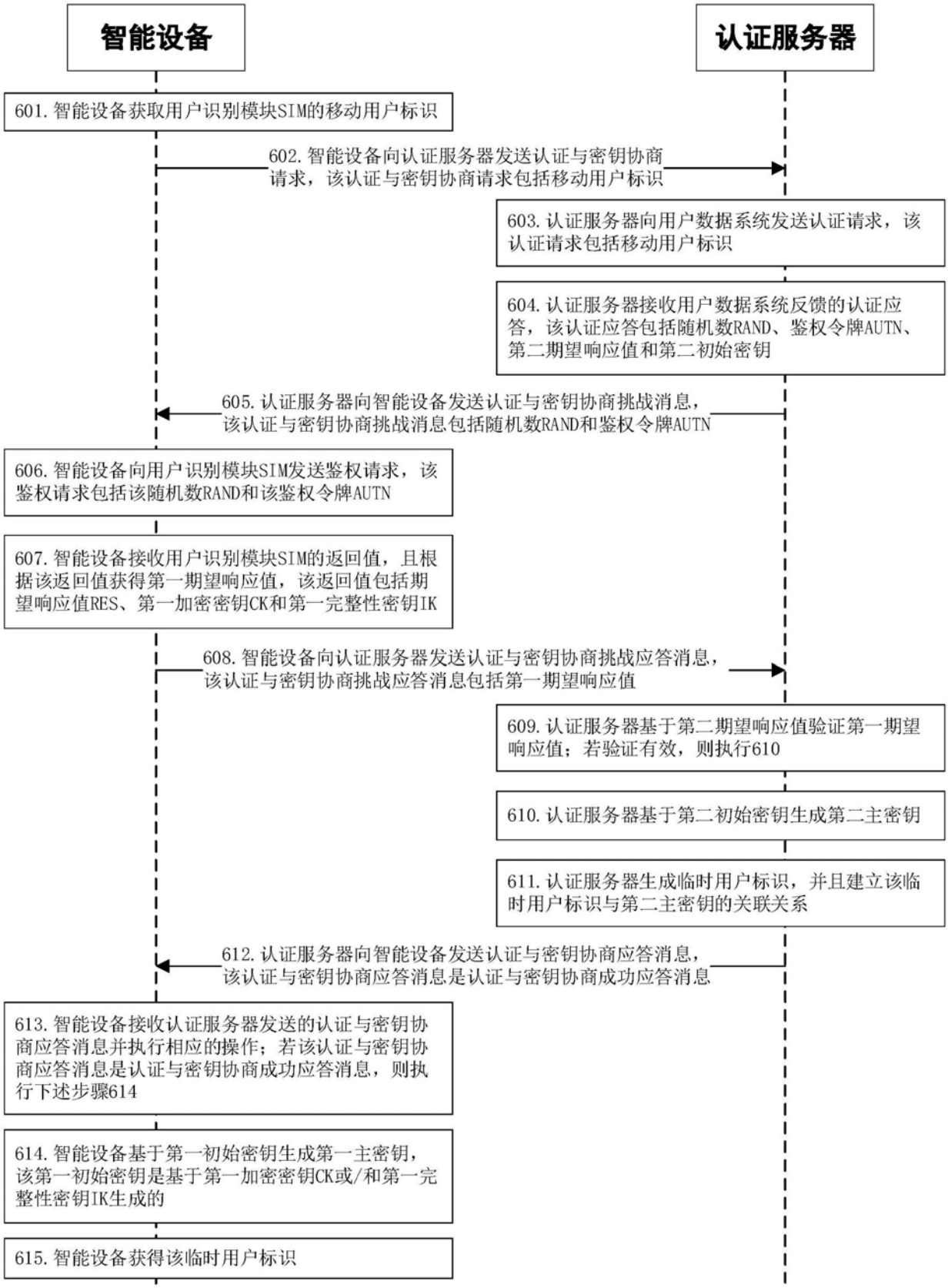

智能设备
认证服务器
601. 智能设备获取用户识别模块SIM的移动用户标识
602. 智能设备向认证服务器发送认证与密钥协商请求，该认证与密钥协商请求包括移动用户标识
603. 认证服务器向用户数据系统发送认证请求，该认证请求包括移动用户标识
604. 认证服务器接收用户数据系统反馈的认证应答，该认证应答包括随机数RAND、鉴权令牌AUTN、第二期望响应值和第二初始密钥
605. 认证服务器向智能设备发送认证与密钥协商挑战消息，该认证与密钥协商挑战消息包括随机数RAND和鉴权令牌AUTN
606. 智能设备向用户识别模块SIM发送鉴权请求，该鉴权请求包括该随机数RAND和该鉴权令牌AUTN
607. 智能设备接收用户识别模块SIM的返回值，且根据该返回值获得第一期望响应值，该返回值包括期望响应值RES、第一加密密钥CK和第一完整性密钥IK
608. 智能设备向认证服务器发送认证与密钥协商挑战应答消息，该认证与密钥协商挑战应答消息包括第一期望响应值
609. 认证服务器基于第二期望响应值验证第一期望响应值；若验证有效，则执行610
610. 认证服务器基于第二初始密钥生成第二主密钥
611. 认证服务器生成临时用户标识，并且建立该临时用户标识与第二主密钥的关联关系
612. 认证服务器向智能设备发送认证与密钥协商应答消息，该认证与密钥协商应答消息是认证与密钥协商成功应答消息
613. 智能设备接收认证服务器发送的认证与密钥协商应答消息并执行相应的操作；若该认证与密钥协商应答消息是认证与密钥协商成功应答消息，则执行下述步骤614
614. 智能设备基于第一初始密钥生成第一主密钥，该第一初始密钥是基于第一加密密钥CK或/和第一完整性密钥IK生成的
615. 智能设备获得该临时用户标识

图6

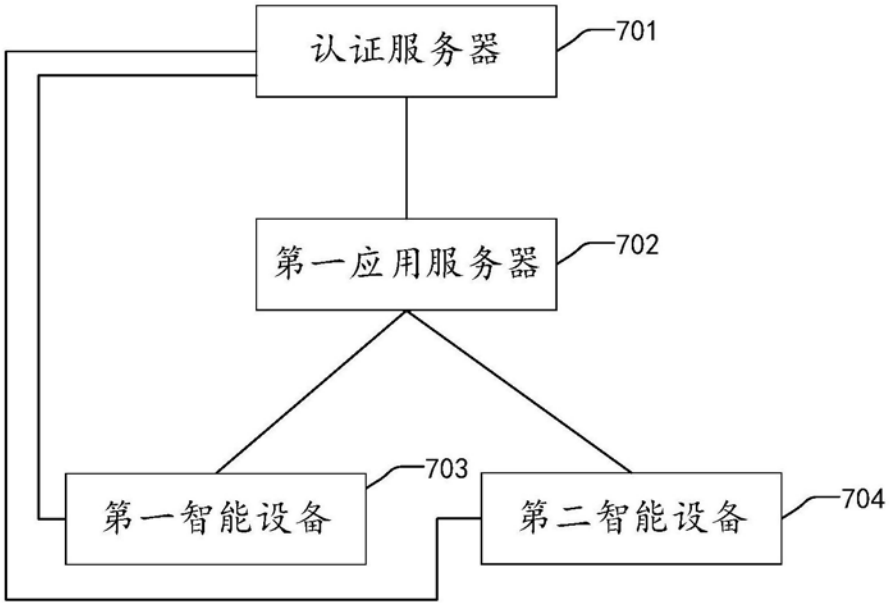

认证服务器
701
第一应用服务器
702
第一智能设备
703
第二智能设备
704

图7

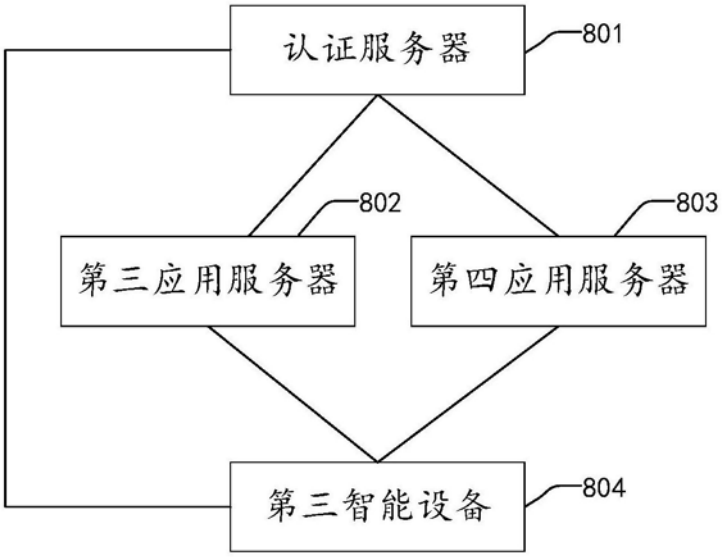

认证服务器
801
第三应用服务器
802
第四应用服务器
803
第三智能设备
804

图8

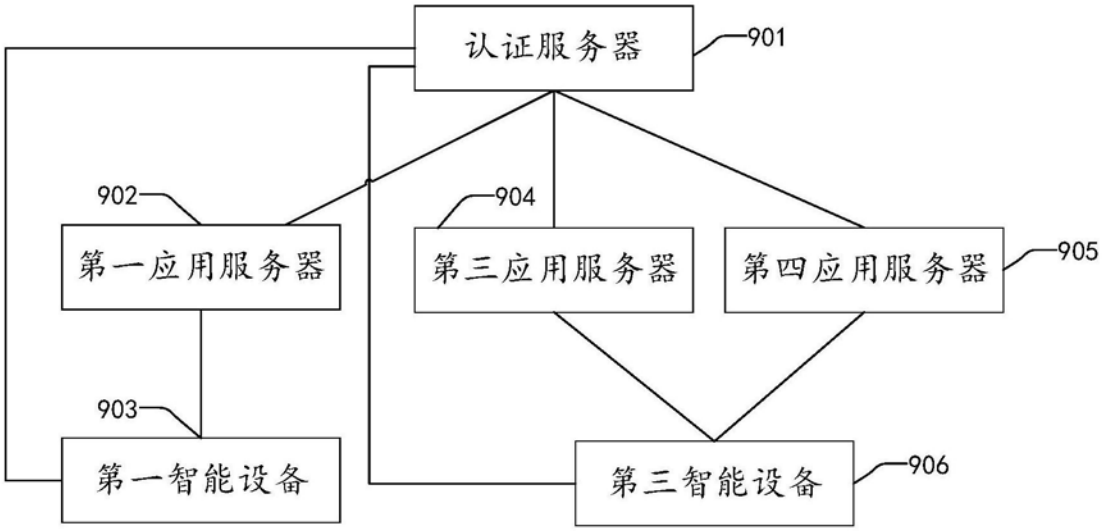

认证服务器
901
902
第一应用服务器
904
第三应用服务器
第四应用服务器
905
903
第一智能设备
第三智能设备
906

图9