(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 111953705 A
(43)申请公布日 2020.11.17

(21)申请号 202010845406.5

(22)申请日 2020.08.20

(71)申请人 全球能源互联网研究院有限公司
地址 102209 北京市昌平区未来科技城滨河大道18号

(72)发明人 高昆仑 安宁钰 赵保华 梁潇 王志皓 任春卉

(74)专利代理机构 北京三聚阳光知识产权代理有限公司 11250
代理人 李博洋

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)
G06Q 50/06(2012.01)

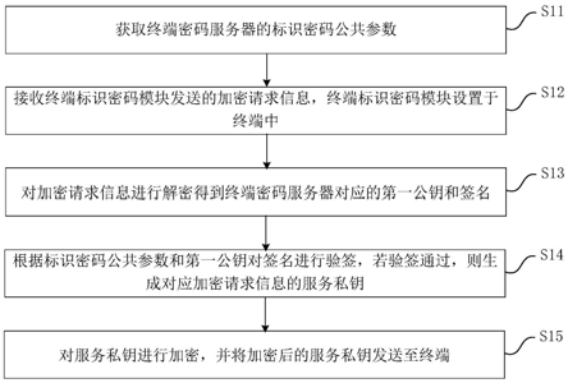
权利要求书2页 说明书15页 附图4页

(54)发明名称

物联网身份认证方法、装置及电力物联网身份认证系统

(57)摘要

本发明公开了一种物联网身份认证方法、装置及电力物联网身份认证系统，其中，该方法包括：终端从终端密码服务器获取终端身份标识和私钥，并获取服务商密码服务器对应的第二公钥；根据终端身份标识、私钥和第二公钥，生成加密请求信息并将其发送至服务商密码服务器；服务商密码服务器接收加密请求信息，并获取终端密码服务器的标识密码公共参数；对加密请求信息进行解密和验签，若验签通过，则生成对应加密请求信息的加密服务私钥并发送至终端；终端对接收到的加密服务私钥进行解密，得到服务私钥。通过实施本发明，无需进行额外的在线身份验证，在满足电力物联网系统的应用要求的基础上，降低了物联网系统互联互通的复杂度，提升了用户体验。



CN 111953705 A

1.一种物联网身份认证方法,应用于服务商密码服务器,其特征在于,包括:

获取终端密码服务器的标识密码公共参数;

接收所述终端标识密码模块发送的加密请求信息,所述终端标识密码模块设置于所述终端中;

对所述加密请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名;

根据所述标识密码公共参数和所述第一公钥对所述签名进行验签,若所述验签通过,则生成对应所述加密请求信息的服务私钥;

对所述服务私钥进行加密,并将加密后的服务私钥发送至所述终端。

2.根据权利要求1所述的方法,其特征在于,所述服务商密码服务器包括密钥管理装置;所述对所述加密请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名,包括:

通过所述密钥管理装置利用预设私钥解密所述加密请求信息,得到所述终端的第一公钥以及所述第一公钥对应的签名。

3.根据权利要求2所述的方法,其特征在于,所述服务商密码服务器还包括密钥生成装置;所述根据所述标识密码公共参数和所述第一公钥对所述签名进行验签,若所述验签通过,则生成对应所述加密请求信息的服务私钥,包括:

通过所述密钥管理装置利用所述第一公钥和所述标识密码公共参数验证所述第一公钥对应的签名;

若所述验证通过,由所述密钥管理装置将所述第一公钥发送给所述密钥生成装置,由所述密钥生成装置生成对应所述第一公钥的服务私钥。

4.根据权利要求3所述的方法,其特征在于,所述对所述服务私钥进行加密,包括:

通过所述密钥管理装置使用所述标识密码公共参数和所述第一公钥对所述服务私钥进行加密,得到加密后的服务私钥。

5.一种物联网身份认证方法,应用于终端,其特征在于,包括:

获取终端密码服务器的终端身份标识和私钥;

获取服务商密码服务器的第二公钥;

根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥,生成加密请求信息,并将所述加密请求信息发送至所述服务商密码服务器;

接收所述服务商密码服务器发送的加密服务私钥,并对所述加密服务私钥进行解密,得到所述服务商密码服务器对应的服务私钥。

6.根据权利要求5所述的方法,其特征在于,所述终端身份标识对应所述终端的第一公钥;所述根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥,生成加密请求信息,包括:

通过所述私钥对所述第一公钥进行签名,得到对应第一公钥的签名;

将所述第二公钥作为公钥对所述签名和所述第一公钥进行加密,得加密请求信息。

7.根据权利要求6所述的方法,其特征在于,所述对所述加密服务私钥进行解密,得到所述服务商密码服务器对应的服务私钥,包括:

使用所述私钥对所述加密服务私钥进行解密,得到所述加密服务私钥中包含的服务私钥。

8.一种物联网身份认证装置,应用于服务商密码服务器,其特征在于,包括:

第一获取模块,用于获取终端密码服务器的标识密码公共参数;

第一接收模块,用于接收所述终端标识密码模块发送的加密请求信息,所述终端标识密码模块设置于所述终端中;

第一解密模块,用于对所述加密请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名;

验签模块,用于根据所述标识密码公共参数和所述第一公钥对所述签名进行验签,若所述验签通过,则生成对应所述加密请求信息的服务私钥;

第一加密模块,用于对所述服务私钥进行加密,并将加密后的服务私钥发送至所述终端。

9.一种物联网身份认证装置,应用于电力物联网终端,其特征在于,包括:

第二获取模块,用于获取终端密码服务器的终端身份标识和私钥;

第三获取模块,用于获取服务商密码服务器的第二公钥;

生成模块,用于根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥,生成加密请求信息,并将所述加密请求信息发送至所述服务商密码服务器;

第二解密模块,用于接收所述服务商密码服务器发送的加密服务私钥,并对所述加密服务私钥进行解密,得到所述服务商密码服务器对应的服务私钥。

10.一种服务器,其特征在于,包括:存储器和处理器,所述存储器和所述处理器之间互相通信连接,所述存储器中存储有计算机指令,所述处理器通过执行所述计算机指令,从而执行权利要求1-4中任一项所述的物联网身份认证方法。

11.一种终端,其特征在于,包括:存储器和处理器,所述存储器和所述处理器之间互相通信连接,所述存储器中存储有计算机指令,所述处理器通过执行所述计算机指令,从而执行权利要求5-7中任一项所述的物联网身份认证方法。

12.一种电力物联网身份认证系统,其特征在于,包括:至少一服务器及至少一个终端,其中,

服务器用于获取终端密码服务器的标识密码公共参数;

所述终端用于获取终端密码服务器的终端身份标识和私钥,并获取所述服务器发送的第二公钥;

所述服务器用于接收设置于所述终端中的终端标识密码模块发送的加密请求信息;对所述加密请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名;根据所述标识密码公共参数和所述第一公钥对所述签名进行验签,若所述验签通过,则生成对应所述加密请求信息的服务私钥;对所述服务私钥进行加密,并将加密后的服务私钥发送至所述终端;

所述终端用于根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥,生成加密请求信息,并将所述加密请求信息发送至所述服务器;接收所述服务器发送的加密服务私钥,并对所述加密服务私钥进行解密,得到所述服务器对应的服务私钥。

13.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有计算机指令,所述计算机指令用于使所述计算机执行权利要求1-4中任一项所述的物联网身份认证方法或权利要求5-7中任一项所述的物联网身份认证方法。

物联网身份认证方法、装置及电力物联网身份认证系统

技术领域

[0001] 本发明涉及信息安全领域，具体涉及一种物联网身份认证方法、装置及电力物联网身份认证系统。

背景技术

[0002] 电力物联网自底向上主要包括感知层、网络层、平台层和应用层，主要实体包括感知层的电力物联网终端、网络层的电力物联网终端边缘接入设备以及平台层的各类服务实体。为保障电力物联网系统的信息安全，需为电力物联网系统构建身份认证体系。现有的身份认证体系主要以基于数字证书的公钥基础设施(Public Key Infrastructure,PKI)体系为主，然而，PKI体系使用比较复杂，在电力物联网系统中，电力物联网终端生产商、电力物联网边缘接入设备供应商和各类服务提供商(Service Provider,SP)需各自构建自身的根CA和子CA，实现互联互通较为复杂，而在实体通信身份认证时需要在线验证身份证书，复杂的互联互通过程难以满足电力物联网系统的应用要求。

发明内容

[0003] 因此，本发明要解决的技术问题在于克服现有技术中电力物联网系统的在线身份验证实现互联互通较为复杂的缺陷，从而提供一种物联网身份认证方法、装置及电力物联网身份认证系统。

[0004] 根据第一方面，本发明实施例提供一种物联网身份认证方法，应用于服务商密码服务器，包括：获取终端密码服务器的标识密码公共参数；接收所述终端标识密码模块发送的加密请求信息，所述终端标识密码模块设置于所述终端中；对所述加密请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名；根据所述标识密码公共参数和所述第一公钥对所述签名进行验签，若所述验签通过，则生成对应所述加密请求信息的服务私钥；对所述服务私钥进行加密，并将加密后的服务私钥发送至所述终端。

[0005] 结合第一方面，在第一方面的第一实施方式中，所述服务商密码服务器包括密钥管理装置；所述对所述加密请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名，包括：通过所述密钥管理装置利用预设私钥解密所述加密请求信息，得到所述终端的第一公钥以及所述第一公钥对应的签名。

[0006] 结合第一方面第一实施方式，在第一方面的第二实施方式中，所述服务商密码服务器还包括密钥生成装置；所述根据所述标识密码公共参数和所述第一公钥对所述签名进行验签，若所述验签通过，则生成对应所述加密请求信息的服务私钥，包括：通过所述密钥管理装置利用所述第一公钥和所述标识密码公共参数验证所述第一公钥对应的签名；若所述验证通过，由所述密钥管理装置将所述第一公钥发送给所述密钥生成装置，由所述密钥生成装置生成对应所述第一公钥的服务私钥。

[0007] 结合第一方面第一实施方式，在第一方面的第三实施方式中，所述对所述服务私钥进行加密，包括：通过所述密钥管理装置使用所述标识密码公共参数和所述第一公钥对

所述服务私钥进行加密，得到加密后的服务私钥。

[0008] 根据第二方面，本发明实施例提供一种物联网身份认证方法，应用于终端，包括：获取终端密码服务器的终端身份标识和私钥；获取服务商密码服务器的第二公钥；根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥，生成加密请求信息，并将所述加密请求信息发送至所述服务商密码服务器；接收所述服务商密码服务器发送的加密服务私钥，并对所述加密服务私钥进行解密，得到所述服务商密码服务器对应的服务私钥。

[0009] 结合第二方面，在第二方面的第一实施方式中，所述终端身份标识对应所述终端的第一公钥；所述根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥，生成加密请求信息，包括：通过所述私钥对所述第一公钥进行签名，得到对应第一公钥的第二签名；将所述第二公钥作为公钥对所述第二签名和所述第一公钥进行加密，得加密请求信息。

[0010] 结合第二方面第一实施方式，在第二方面的第二实施方式中，所述对所述加密服务私钥进行解密，得到所述服务商密码服务器对应的服务私钥，包括：使用所述私钥对所述加密服务私钥进行解密，得到所述加密服务私钥中包含的服务私钥。

[0011] 根据第三方面，本发明实施例提供一种物联网身份认证装置，应用于服务商密码服务器，包括：第一获取模块，用于获取终端密码服务器的标识密码公共参数；第一接收模块，用于接收所述终端标识密码模块发送的加密请求信息，所述终端标识密码模块设置于所述终端中；第一解密模块，用于对所述加密请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名；验签模块，用于根据所述标识密码公共参数和所述第一公钥对所述签名进行验签，若所述验签通过，则生成对应所述加密请求信息的服务私钥；第一加密模块，用于对所述服务私钥进行加密，并将加密后的服务私钥发送至所述终端。

[0012] 根据第四方面，本发明实施例提供一种物联网身份认证装置，应用于电力物联网终端，包括：第二获取模块，用于获取终端密码服务器的终端身份标识和私钥；第三获取模块，用于获取服务商密码服务器的第二公钥；生成模块，用于根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥，生成加密请求信息，并将所述加密请求信息发送至所述服务商密码服务器；第二解密模块，用于接收所述服务商密码服务器发送的加密服务私钥，并对所述加密服务私钥进行解密，得到所述服务商密码服务器对应的服务私钥。

[0013] 根据第五方面，本发明实施例提供一种服务器，包括：存储器和处理器，所述存储器和所述处理器之间互相通信连接，所述存储器中存储有计算机指令，所述处理器通过执行所述计算机指令，从而执行第一方面或第一方面任一实施方式所述的物联网身份认证方法。

[0014] 根据第六方面，本发明实施例提供一种终端，包括：存储器和处理器，所述存储器和所述处理器之间互相通信连接，所述存储器中存储有计算机指令，所述处理器通过执行所述计算机指令，从而执行第二方面或第二方面任一实施方式所述的物联网身份认证方法。

[0015] 根据第七方面，本发明实施例提供一种电力物联网身份认证系统，包括：至少一服务器及至少一个终端，其中，服务器用于获取终端密码服务器的标识密码公共参数；所述终端用于获取终端密码服务器的终端身份标识和私钥，并获取所述服务器的第二公钥；所述服务器用于接收设置于所述终端中的终端标识密码模块发送的加密请求信息；对所述加密

请求信息进行解密得到所述终端密码服务器对应的第一公钥和签名;根据所述标识密码公共参数和所述第一公钥对所述签名进行验签,若所述验签通过,则生成对应所述加密请求信息的服务私钥;对所述服务私钥进行加密,并将加密后的服务私钥发送至所述终端;所述终端用于根据所述终端身份标识、所述终端身份标识对应的私钥和所述第二公钥,生成加密请求信息,并将所述加密请求信息发送至所述服务器;接收所述服务器发送的加密服务私钥,并对所述加密服务私钥进行解密,得到所述服务器对应的服务私钥。

[0016] 根据第八方面,本发明实施例提供一种计算机可读存储介质,所述计算机可读存储介质存储有计算机指令,所述计算机指令用于使所述计算机执行第一方面或第一方面任一实施方式所述的物联网身份认证方法或执行第二方面或第二方面任一实施方式所述的物联网身份认证方法。

[0017] 本发明技术方案,具有如下优点:

[0018] 1.本发明提供的物联网身份认证方法、装置和服务器,通过获取终端密码服务器的标识密码公共参数,接收设置于终端的终端标识密码模块发送的加密请求信息,对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名,根据标识密码公共参数和第一公钥对签名进行验签,若验签通过,则生成对应加密请求信息的服务私钥,对服务私钥进行加密,并将加密后的服务私钥发送至终端。由于第一公钥为终端的身份标识号,即第一公钥可以由终端的身份标识号进行唯一确定,而终端的身份标识号是不变的,进而保证了第一公钥的真实性,无需通过第三方来保证其真实性,同时,服务私钥可以根据第一公钥生成,进而保证了服务私钥的真实性,由此降低了物联网系统互联互通的复杂度。相较于在线身份验证,该方法在服务端和终端通过获取的服务私钥进行身份认证以实现终端与服务之间的安全通信,无需进行额外的在线身份验证,降低了物联网系统复杂度,满足了电力物联网系统的应用要求,确保了电力物联网系统安全高效运行,提升了用户体验。

[0019] 2.本发明提供的物联网身份认证方法、装置和终端,通过获取终端密码服务器的终端身份标识和私钥并获取服务商密码服务器的第二公钥,根据终端身份标识、终端身份标识对应的私钥和第二公钥,生成加密请求信息,并将加密请求信息发送至服务商密码服务器,接收服务商密码服务器发送的加密请求信息对应的加密服务私钥,并对加密服务私钥进行解密,得到服务商密码服务器对应的服务私钥。由于第二公钥为服务商密码服务器的身份标识号,即第二公钥可以由服务商密码服务器的身份标识号唯一确定,而服务商密码服务器的身份标识号是不变的,进而保证了第二公钥的真实性,无需通过第三方来保证其真实性,而终端解密的服务私钥是根据第一公钥生成,其具有真实性和安全性,由此保证了终端与服务商密码服务器端的安全运行。同时,通过在服务商密码服务器端和终端通过获取的服务私钥进行身份验证以实现终端与服务商密码服务器端之间的安全通信,由此降低了物联网系统互联互通的复杂度,提升了用户体验。

[0020] 3.本发明提供的电力物联网身份认证系统,通过服务器获取终端密码服务器的标识密码公共参数;终端获取服务器的第二公钥并获取终端密码服务器的终端身份标识和私钥,根据终端身份标识、终端身份标识对应的私钥和第二公钥,生成加密请求信息,并将加密请求信息发送至服务器;服务器接收终端发送的加密请求信息,对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名,根据标识密码公共参数和第一公钥对所述签名进行验签,若验签通过,则生成对应加密请求信息的服务私钥,对服务私钥进行加密,

并将加密后的服务私钥发送至终端;终端接收服务器发送的加密服务私钥,并对加密服务私钥进行解密,得到服务器对应的服务私钥。由于第一公钥和第二公钥分别由终端的身份标识号和服务商密码服务器的身份标识号唯一确定,而终端的身份标识号和服务商密码服务器的身份标识号是不变的,进而保证了第一公钥和第二公钥的真实性和固定性,无需通过第三方来保证其真实性,同时,服务私钥可以根据第一公钥生成,进而保证了服务私钥的真实性,确保了电力物联网系统安全高效运行。通过获取的服务私钥进行身份认证以实现终端与服务之间的安全通信,无需进行额外的在线身份验证,在满足了电力物联网系统的应用要求的基础上,降低了物联网系统互联互通的复杂度,提升了用户体验。

附图说明

[0021] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案,下面将对具体实施方式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,下面描述中的附图是本发明的一些实施方式,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,还可以根据这些附图获得其他的附图。

[0022] 图1为本发明实施例中物联网身份认证方法的流程图;

[0023] 图2为本发明实施例中物联网身份认证方法的流程图;

[0024] 图3为本发明实施例中物联网身份认证装置的原理框图;

[0025] 图4为本发明实施例中物联网身份认证装置的原理框图;

[0026] 图5为本发明实施例中服务器的结构示意图;

[0027] 图6为本发明实施例中终端的结构示意图;

[0028] 图7为本发明实施例中电力物联网身份认证系统的原理框图;

[0029] 图8为本发明实施例中电力物联网身份认证系统的工作流程图;

[0030] 图9为本发明实施例中物联网终端与服务商密码服务器进行身份认证和获取服务私钥的流程图。

具体实施方式

[0031] 下面将结合附图对本发明的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0032] 在本发明的描述中,需要说明的是,术语“中心”、“上”、“下”、“左”、“右”、“竖直”、“水平”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作,因此不能理解为对本发明的限制。此外,术语“第一”、“第二”、“第三”仅用于描述目的,而不能理解为指示或暗示相对重要性。

[0033] 在本发明的描述中,需要说明的是,除非另有明确的规定和限定,术语“安装”、“相连”、“连接”应做广义理解,例如,可以是固定连接,也可以是可拆卸连接,或一体地连接;可以是机械连接,也可以是电连接;可以是直接相连,也可以通过中间媒介间接相连,还可以是两个元件内部的连通,可以是无线连接,也可以是有线连接。对于本领域的普通技术人员而言,可以具体情况理解上述术语在本发明中的具体含义。

[0034] 此外，下面所描述的本发明不同实施方式中所涉及的技术特征只要彼此之间未构成冲突就可以相互结合。

[0035] 实施例1

[0036] 本实施例提供一种物联网身份认证方法，应用于电力物联网系统中的服务商密码服务器上，以实现服务商密码服务器与物联网终端之间的互联互通，如图1所示，该物联网身份认证方法包括如下步骤：

[0037] S11，获取终端密码服务器的标识密码公共参数。

[0038] 示例性地，终端密码服务器为电力物联网终端生产商密码服务器。标识密码公共参数为终端密码服务器的系统参数，可以根据系统参数生成算法steup进行生成。终端密码服务器可以为电力物联网终端提供身份标识TPID以及对应的出厂私钥$TO\text{-}RK_{TPID}$。

[0039] S12，接收终端标识密码模块发送的加密请求信息，终端标识密码模块设置于终端中。

[0040] 示例性地，终端标识密码模块(Identity-Based Cryptographic Module，IBCM)可以根据标准化的标识密码算法进行加密、解密、签名和验签等密码运算，此处的标识密码模块可以为内置在电力物联网终端中的硬件模块，也可以为内置在电力物联网终端中的软件模块，本申请对此不作限定。加密请求信息为电力物联网终端向服务商密码服务器发送的服务请求。

[0041] S13，对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名。

[0042] 示例性地，服务商密码服务器在接收到电力物联网终端发送的加密请求信息之后，可以根据其自身私钥对接收到的加密请求信息进行解密，获取加密请求信息中包含的第一公钥和签名。其中，第一公钥为电力物联网终端对应的身份标识TPID，签名为电力物联网终端根据其身份标识TPID和出厂私钥$TO\text{-}RK_{TPID}$生成的。

[0043] S14，根据标识密码公共参数和第一公钥对签名进行验签，若验签通过，则生成对应加密请求信息的服务私钥。

[0044] 示例性地，根据标识密码公共参数和第一公钥(身份标识TPID)对签名进行验证，若签名验证通过，则根据第一公钥(身份标识TPID)生成加密请求信息对应的服务私钥。

[0045] S15，对服务私钥进行加密，并将加密后的服务私钥发送至终端。

[0046] 示例性地，服务商加密服务器对生成的服务私钥进行加密处理。具体地，服务商加密服务器可以采用标识密码公共参数和第一公钥(身份标识TPID)对服务私钥进行加密，得到加密服务私钥，并将得到的加密服务私钥发送至电力物联网终端。

[0047] 本实施例提供的物联网身份认证方法，服务商密码服务器通过获取终端密码服务器的标识密码公共参数，接收设置于终端的终端标识密码模块发送的加密请求信息，对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名，根据标识密码公共参数和第一公钥对签名进行验签，若验签通过，则生成对应加密请求信息的服务私钥，对服务私钥进行加密，并将加密后的服务私钥发送至终端。由于第一公钥为终端的身份标识号，即第一公钥可以由终端的身份标识号进行唯一确定，而终端的身份标识号是不变的，进而保证了第一公钥的真实性，无需通过第三方来保证其真实性，同时，服务私钥可以根据第一公钥生成，进而保证了服务私钥的真实性，由此降低了物联网系统互联互通的复杂度。相较于在线身份验证，该方法在服务端和终端通过获取的服务私钥进行身份认证以实现终端与服务

之间的安全通信,无需进行额外的在线身份验证,降低了物联网系统复杂度,满足了电力物联网系统的应用要求,确保了电力物联网系统安全高效运行,提升了用户体验。

[0048] 作为一个可选的实施方式,服务商密码服务器包括密钥管理装置,上述步骤S13,包括:通过密钥管理装置利用预设私钥解密加密请求信息,得到终端的第一公钥以及第一公钥对应的签名。

[0049] 示例性地,加密请求信息为电力物联网终端发送的服务请求信息,加密请求信息包括身份标识TPID和签名信息。若该加密请求信息为$ENC_{SPID}(SIGN_{TO-RKTPID}(TPID)|TPID)$,密钥管理装置(Key Management Center,KMC)可以利用自身的私钥RK_{SPID}解密该加密请求信息,得到身份标识TPID及其签名$SIGN_{TO-RKTPID}$,其中,身份标识TPID即为电力物联网终端的第一公钥,签名$SIGN_{TO-RKTPID}$为对应第一公钥的签名。

[0050] 作为一个可选的实施方式,服务商密码服务器还包括密钥生成装置,上述步骤S14,包括:

[0051] 首先,通过密钥管理装置利用第一公钥和标识密码公共参数验证第一公钥对应的签名。

[0052] 示例性地,由于签名是根据电力物联网终端的出厂私钥$TO-RK_{TPID}$对电力物联网终端的第一公钥TPID进行签名得到的,密钥管理装置KMC则可以利用第一公钥TPID和电力物联网终端密码服务器的标识密码公共参数$Pram_{TO}$对第一公钥对应的签名$SIGN_{TO-RKTPID}(TPID)$进行验证。

[0053] 其次,若验证通过,由密钥管理装置将第一公钥发送给密钥生成装置,由密钥生成装置生成对应第一公钥的服务私钥。

[0054] 示例性地,若签名通过验证,则服务商密码服务器的密钥管理装置KMC将第一公钥TPID发送至密钥生成装置(Key Generate Center,KGC),由密钥生成装置KGC生成第一公钥对应的服务私钥$SP-RK_{TPID}$。

[0055] 作为一个可选的实施方式,上述步骤S15,包括:通过密钥管理装置使用标识密码公共参数和第一公钥对服务私钥进行加密,得到加密后的服务私钥。

[0056] 示例性地,服务商密钥服务器的密钥管理装置KMC使用电力物联网终端密码服务器的标识密码公共参数$Pram_{TO}$和电力物联网终端的第一公钥(身份标识TPID)对服务私钥$SP-RK_{TPID}$进行加密,得到加密的服务私钥$ENC_{TPID}(SP-RK_{TPID})$。

[0057] 实施例2

[0058] 本实施例提供一种物联网身份认证方法,应用于电力物联网系统中的物联网终端上,以实现服务商密码服务器与物联网终端之间的互联互通,如图2所示,该物联网身份认证方法包括如下步骤:

[0059] S21,获取终端密码服务器的终端身份标识和私钥。

[0060] 示例性地,终端密码服务器为电力物联网终端生产商密码服务器。终端身份标识为终端密码服务器为电力物联网终端提供的身份标识TPID。私钥为终端密码服务器内置到电力物联网终端的出厂私钥$TO-RK_{TPID}$。其中,终端身份标识即为电力物联网终端的第一公钥。

[0061] S22,获取服务商密码服务器的第二公钥。

[0062] 示例性地,第二公钥为服务商密码服务器的身份标识SPID。服务商密码服务器用

于为电力物联网终端提供服务，当电力物联网终端请求服务商提供的某项服务时，需要向服务商密码服务器发送服务请求。为保证服务商密码服务器与电力物联网终端之间的安全通信，电力物联网终端可以通过可信公开渠道获取服务商密码服务器的身份标识SPID(第二公钥)，以供电力物联网终端根据第二公钥获取服务商密码服务器提供的服务私钥。

[0063] S23，根据终端身份标识、终端身份标识对应的私钥和第二公钥，生成加密请求信息，并将加密请求信息发送至服务商密码服务器。

[0064] 示例性地，加密请求信息为服务请求消息，具体的可以为服务私钥请求信息。电力物联网终端可以根据终端身份标识TPID、第二公钥SPID和终端身份标识对应的私钥(出厂私钥$TO\text{-}RK_{TPID}$)生成该加密请求信息，并将该加密请求信息发送至服务商密码服务器。

[0065] S24，接收服务商密码服务器发送的加密服务私钥，并对加密服务私钥进行解密，得到服务商密码服务器对应的服务私钥。

[0066] 示例性地，服务商密码服务器根据加密请求信息生成对应的服务私钥，将该服务私钥加密后发送至电力物联网终端。电力物联网终端接收该加密服务私钥，并对该加密服务私钥进行解密，获取服务商密码服务器根据加密请求信息生成的服务私钥。

[0067] 本实施例提供的物联网身份认证方法，终端通过获取终端密码服务器的终端身份标识和私钥并获取服务商密码服务器对应的第二公钥，根据终端身份标识、终端身份标识对应的私钥和第二公钥，生成加密请求信息，并将加密请求信息发送至服务商密码服务器，接收服务商密码服务器发送的加密请求信息对应的加密服务私钥，并对加密服务私钥进行解密，得到服务商密码服务器对应的服务私钥。由于第二公钥为服务商密码服务器的身份标识号，即第二公钥可以由服务商密码服务器的身份标识号唯一确定，而服务商密码服务器的身份标识号是不变的，进而保证了第二公钥的真实性，无需通过第三方来保证其真实性，而终端解密的服务私钥是根据第一公钥生成，其具有真实性和安全性，由此保证了终端与服务商密码服务器端的安全运行。同时，通过在服务商密码服务器端和终端通过获取的服务私钥进行身份验证以实现终端与服务商密码服务器端之间的安全通信，由此降低了物联网系统互联互通的复杂度，提升了用户体验。

[0068] 作为一个可选的实施方式，终端身份标识对应终端的第一公钥，上述步骤S23，包括：

[0069] 首先，通过私钥对第一公钥进行签名，得到对应第一公钥的签名。

[0070] 示例性地，电力物联网终端使用其出厂私钥$TO\text{-}RK_{TPID}$对身份标识TPID进行签名，即使用出厂私钥$TO\text{-}RK_{TPID}$对第一公钥进行签名得到对应的签名$SIGN_{TO\text{-}RKTPID}(TPID)$。

[0071] 其次，将第二公钥作为公钥对签名和第一公钥进行加密，得加密请求信息。

[0072] 示例性地，电力物联网终端使用服务商密码服务器的身份标识SPID(第二公钥)作为公钥，采用加密算法对该签名$SIGN_{TO\text{-}RKTPID}(TPID)$和第一公钥(身份标识TPID)进行加密处理，得到加密请求信息$ENC_{SPID}(SIGN_{TO\text{-}RKTPID}(TPID)|TPID)$。

[0073] 作为一个可选的实施方式，上述步骤S24，包括：使用私钥对加密服务私钥进行解密，得到加密服务私钥中包含的服务私钥。

[0074] 示例性地，电力物联网终端采用解密算法以及终端密码服务器下发的出厂私钥$TO\text{-}RK_{TPID}$对服务商密码服务器发送的加密服务私钥$ENC_{TPID}(SP\text{-}RK_{TPID})$进行解密，得到服务商密码服务器根据加密请求信息生成的服务私钥$SP\text{-}RK_{TPID}$。

[0075] 电力物联网终端通过与服务商密码服务器之间进行安全通信获取加密请求信息对应的服务私钥,并完成身份注册。在电力物联网终端通过与服务商密码服务器之间进行安全通信的过程中,无需进行在线身份验证,仅是通过电力物联网终端根据接收的服务商密码服务器的第二公钥和出厂私钥生成加密请求信息,服务商密码服务器则根据该加密请求信息生成服务私钥发送至电力物联网终端,电力物联网终端成功获取该服务私钥则表征电力物联网终端与服务商密码服务器之间完成身份注册。

[0076] 实施例3

[0077] 本实施例提供一种物联网身份认证装置,应用于电力物联网系统中的服务商密码服务器上,以实现服务商密码服务器与物联网终端之间的互联互通,如图3所示,该物联网身份认证装置包括:

[0078] 第一获取模块31,用于获取终端密码服务器的标识密码公共参数。详细内容参见上述方法实施例对应步骤S11的相关描述,此处不再赘述。

[0079] 第一接收模块32,用于接收终端标识密码模块发送的加密请求信息,终端标识密码模块设置于终端中。详细内容参见上述方法实施例对应步骤S12的相关描述,此处不再赘述。

[0080] 第一解密模块33,用于对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名。详细内容参见上述方法实施例对应步骤S13的相关描述,此处不再赘述。

[0081] 验签模块34,用于根据标识密码公共参数和第一公钥对签名进行验签,若验签通过,则生成对应加密请求信息的服务私钥。详细内容参见上述方法实施例对应步骤S14的相关描述,此处不再赘述。

[0082] 第一加密模块35,用于对服务私钥进行加密,并将加密后的服务私钥发送至终端。详细内容参见上述方法实施例对应步骤S15的相关描述,此处不再赘述。

[0083] 本实施例提供的物联网身份认证装置,应用于服务商密码服务器,服务商密码服务器通过获取终端密码服务器的标识密码公共参数,接收设置于终端的终端标识密码模块发送的加密请求信息,对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名,根据标识密码公共参数和第一公钥对签名进行验签,若验签通过,则生成对应加密请求信息的服务私钥,对服务私钥进行加密,并将加密后的服务私钥发送至终端。由于第一公钥为终端的身份标识号,即第一公钥可以由终端的身份标识号进行唯一确定,而终端的身份标识号是不变的,进而保证了第一公钥的真实性,无需通过第三方来保证其真实性,同时,服务私钥可以根据第一公钥生成,进而保证了服务私钥的真实性,由此降低了物联网系统互联互通的复杂度。该装置通过在服务端和终端通过获取的服务私钥进行身份认证以实现终端与服务之间的安全通信,无需进行额外的在线身份验证,降低了物联网系统复杂度,满足了电力物联网系统的应用要求,确保了电力物联网系统安全高效运行,提升了用户体验。

[0084] 作为一个可选的实施方式,服务商密码服务器包括密钥管理装置,密钥管理装置用于利用预设私钥解密加密请求信息,得到终端的第一公钥以及第一公钥对应的签名。详细内容参见上述方法实施例对应的相关描述,此处不再赘述。

[0085] 作为一个可选的实施方式,服务商密码服务器还包括密钥生成装置,密钥生成装置用于利用第一公钥和标识密码公共参数验证第一公钥对应的签名;若验证通过,由密钥管理装置将第一公钥发送给密钥生成装置,由密钥生成装置生成对应第一公钥的服务私

钥。详细内容参见上述方法实施例对应的相关描述，此处不再赘述。

[0086] 作为一个可选的实施方式，密钥管理装置还用于使用标识密码公共参数和第一公钥对服务私钥进行加密，得到加密后的服务私钥。详细内容参见上述方法实施例对应的相关描述，此处不再赘述。

[0087] 实施例4

[0088] 本实施例提供一种物联网身份认证装置，应用于电力物联网系统中的物联网终端上，以实现服务商密码服务器与物联网终端之间的互联互通，如图4所示，该物联网身份认证装置包括：

[0089] 第二获取模块41，用于获取终端密码服务器的终端身份标识和私钥。详细内容参见上述方法实施例对应步骤S21的相关描述，此处不再赘述。

[0090] 第三获取模块42，用于获取服务商密码服务器的第二公钥。详细内容参见上述方法实施例对应步骤S22的相关描述，此处不再赘述。

[0091] 生成模块43，用于根据终端身份标识、终端身份标识对应的私钥和第二公钥，生成加密请求信息，并将加密请求信息发送至服务商密码服务器。详细内容参见上述方法实施例对应步骤S23的相关描述，此处不再赘述。

[0092] 第二解密模块44，用于接收服务商密码服务器发送的加密服务私钥，并对加密服务私钥进行解密，得到服务商密码服务器对应的服务私钥。详细内容参见上述方法实施例对应步骤S24的相关描述，此处不再赘述。

[0093] 本实施例提供的物联网身份认证装置，应用于终端，终端通过获取终端密码服务器的终端身份标识和私钥并获取服务商密码服务器对应的第二公钥，根据终端身份标识、终端身份标识对应的私钥和第二公钥，生成加密请求信息，并将加密请求信息发送至服务商密码服务器，接收服务商密码服务器发送的加密请求信息对应的加密服务私钥，并对加密服务私钥进行解密，得到服务商密码服务器对应的服务私钥。由于第二公钥为服务商密码服务器的身份标识号，即第二公钥可以由服务商密码服务器的身份标识号唯一确定，而服务商密码服务器的身份标识号是不变的，进而保证了第二公钥的真实性，无需通过第三方来保证其真实性，而终端解密的服务私钥是根据第一公钥生成，其具有真实性和安全性，由此保证了终端与服务商密码服务器端的安全运行。同时，通过在服务商密码服务器端和终端通过获取的服务私钥进行身份验证以实现终端与服务商密码服务器端之间的安全通信，由此降低了物联网系统互联互通的复杂度，提升了用户体验。

[0094] 作为一个可选的实施方式，终端身份标识对应终端的第一公钥，上述生成模块43，包括：

[0095] 签名子模块，用于通过私钥对第一公钥进行签名，得到对应第一公钥的第二签名。详细内容参见上述方法实施例对应的相关描述，此处不再赘述。

[0096] 加密子模块，用于将第二公钥作为公钥对第二签名和第一公钥进行加密，得加密请求信息。详细内容参见上述方法实施例对应的相关描述，此处不再赘述。

[0097] 作为一个可选的实施方式，上述第二解密模块44，包括：

[0098] 解密子模块，用于使用私钥对加密服务私钥进行解密，得到加密服务私钥中包含的服务私钥。详细内容参见上述方法实施例对应的相关描述，此处不再赘述。

[0099] 实施例5

[0100] 本实施例提供一种服务器，如图5所示，该设备包括处理器51和存储器52，其中处理器51和存储器52可以通过总线或者其他方式连接，图5中以通过总线连接为例。

[0101] 处理器51可以为中央处理器(Central Processing Unit，CPU)。处理器51还可以为其他通用处理器、数字信号处理器(Digital Signal Processor，DSP)、图形处理器(Graphics Processing Unit，GPU)、嵌入式神经网络处理器(Neural-network Processing Unit，NPU)或者其他专用的深度学习协处理器、专用集成电路(Application Specific Integrated Circuit，ASIC)、现场可编程门阵列(Field-Programmable Gate Array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等芯片，或者上述各类芯片的组合。

[0102] 存储器52作为一种非暂态计算机可读存储介质，可用于存储非暂态软件程序、非暂态计算机可执行程序以及模块，如本发明实施例中的物联网身份认证方法对应的程序指令/模块(如图3所示的第一获取模块31、第一接收模块32、第一解密模块33、验签模块34和第一加密模块35)。处理器51通过运行存储在存储器52中的非暂态软件程序、指令以及模块，从而执行处理器的各种功能应用以及数据处理，即实现上述方法实施例中的物联网身份认证方法。

[0103] 存储器52可以包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需要的应用程序；存储数据区可存储处理器51所创建的数据等。此外，存储器52可以包括高速随机存取存储器，还可以包括非暂态存储器，例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施例中，存储器52可选包括相对于处理器51远程设置的存储器，这些远程存储器可以通过网络连接至处理器51。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0104] 所述一个或者多个模块存储在所述存储器52中，当被所述处理器51执行时，执行如图1所示实施例中的物联网身份认证方法。

[0105] 通过获取终端密码服务器的标识密码公共参数，接收设置于终端的终端标识密码模块发送的加密请求信息，对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名，根据标识密码公共参数和第一公钥对签名进行验签，若验签通过，则生成对应加密请求信息的服务私钥，对服务私钥进行加密，并将加密后的服务私钥发送至终端。由于第一公钥为终端的身份标识号，即第一公钥可以由终端的身份标识号进行唯一确定，而终端的身份标识号是不变的，进而保证了第一公钥的真实性，无需通过第三方来保证其真实性，同时，服务私钥可以根据第一公钥生成，进而保证了服务私钥的真实性，由此降低了物联网系统互联互通的复杂度。相较于在线身份验证，该物联网验证方法在服务端和终端通过获取的服务私钥进行身份认证以实现终端与服务之间的安全通信，无需进行额外的在线身份验证，降低了物联网系统复杂度，满足了电力物联网系统的应用要求，确保了电力物联网系统安全高效运行，提升了用户体验。

[0106] 上述服务器的具体细节可以对应参阅图1至图4所示的实施例中对应的相关描述和效果进行理解，此处不再赘述。未在本实施例中详尽描述的技术细节，具体可参见如图1至图4所示的实施例中的相关描述。

[0107] 实施例6

[0108] 本实施例提供一种终端，如图6所示，该设备包括处理器61和存储器62，其中处理

器61和存储器62可以通过总线或者其他方式连接,图6中以通过总线连接为例。

[0109] 处理器61可以为中央处理器(Central Processing Unit,CPU)。处理器61还可以为其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、图形处理器(Graphics Processing Unit,GPU)、嵌入式神经网络处理器(Neural-network Processing Unit,NPU)或者其他专用的深度学习协处理器、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等芯片,或者上述各类芯片的组合。

[0110] 存储器62作为一种非暂态计算机可读存储介质,可用于存储非暂态软件程序、非暂态计算机可执行程序以及模块,如本发明实施例中的物联网身份认证方法对应的程序指令/模块(如图4所示的第二获取模块41、第三获取模块42、生成模块43和第二解密模块44)。处理器61通过运行存储在存储器62中的非暂态软件程序、指令以及模块,从而执行处理器的各种功能应用以及数据处理,即实现上述方法实施例中的物联网身份认证方法。

[0111] 存储器62可以包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需要的应用程序;存储数据区可存储处理器61所创建的数据等。此外,存储器62可以包括高速随机存取存储器,还可以包括非暂态存储器,例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施例中,存储器62可选包括相对于处理器61远程设置的存储器,这些远程存储器可以通过网络连接至处理器61。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0112] 所述一个或者多个模块存储在所述存储器62中,当被所述处理器61执行时,执行如图2所示实施例中的物联网身份认证方法。

[0113] 通过获取终端密码服务器的终端身份标识和私钥并获取服务商密码服务器的第二公钥,根据终端身份标识、终端身份标识对应的私钥和第二公钥,生成加密请求信息,并将加密请求信息发送至服务商密码服务器,接收服务商密码服务器发送的加密请求信息对应的加密服务私钥,并对加密服务私钥进行解密,得到服务商密码服务器对应的服务私钥。由于第二公钥为服务商密码服务器的身份标识号,即第二公钥可以由服务商密码服务器的身份标识号唯一确定,而服务商密码服务器的身份标识号是不变的,进而保证了第二公钥的真实性,无需通过第三方来保证其真实性,而终端解密的服务私钥是根据第一公钥生成,其具有真实性和安全性,由此保证了终端与服务商密码服务器端的安全运行。同时,通过在服务商密码服务器端和终端通过获取的服务私钥进行身份验证以实现终端与服务商密码服务器端之间的安全通信,由此降低了物联网系统互联互通的复杂度,提升了用户体验。

[0114] 上述终端的具体细节可以对应参阅图1至图5所示的实施例中对应的相关描述和效果进行理解,此处不再赘述。未在本实施例中详尽描述的技术细节,具体可参见如图1至图5所示的实施例中的相关描述。

[0115] 实施例7

[0116] 本实施例提供一种电力物联网身份认证系统,用于实现服务商密码服务器、物联网终端和边缘接入设备服务器之间的互联互通,如图7所示,该电力物联网身份认证系统包括:至少一服务器71及至少一个终端72,其中,服务器71用于获取终端密码服务器的标识密码公共参数;终端72用于获取终端密码服务器71的终端身份标识和私钥,并获取服务器71

的第二公钥。详细内容参见上述方法实施例对应部分的相关描述，此处不再赘述。

[0117] 终端72用于根据终端身份标识、终端身份标识对应的私钥和第二公钥，生成加密请求信息，并将加密请求信息发送至服务器71。服务器71用于接收设置于终端72中的终端标识密码模块发送的加密请求信息；对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名。详细内容参见上述方法实施例对应部分的相关描述，此处不再赘述。

[0118] 服务器71还用于根据标识密码公共参数和第一公钥对签名进行验签，若验签通过，则生成对应加密请求信息的服务私钥；对服务私钥进行加密，并将加密后的服务私钥发送至终端72。终端72还用于接收服务器71发送的加密服务私钥，并对加密服务私钥进行解密，得到服务器对应的服务私钥。详细内容参见上述方法实施例对应部分的相关描述，此处不再赘述。

[0119] 具体地，如图8所示，电力物联网系统主要实体包括：感知层的电力物联网终端(Terminal of Power IOT,TP)、网络层的电力物联网终端边缘接入设备(Gateway of Power IOT,GP)以及平台层的各类服务实体。在电力物联网系统中，按照电力物联网系统业务的参与角色，密码服务器可分为电力物联网终端密码服务器、电力物联网边缘接入设备密码服务器和服务商密码服务器。密码服务器内部主要包含密钥生成装置KGC和密钥管理装置KMC，其中，KGC的主要功能是根据标识密码系统参数生成系统主密钥，并根据申请方的身份标识ID生成相应私钥；KMC的主要功能是管理和存储标识密码系统参数，并根据实际需求进行实体身份管理和密钥管理等操作。密码服务器之间可以通过交换标识密码公共参数实现跨域身份认证，密码服务器和电力物联网系统中包含的终端通过相关安全通信协议进行通信。其中，安全通信协议是指利用标识密码算法构建的安全通信协议，用于服务与服务间、终端与服务间以及终端与终端间的安全通信。

[0120] 如图8所示，电力物联网身份认证系统的工作流程如下：

[0121] 步骤一：密码服务器初始化。对物联网终端密码服务器、服务商密码服务器和边缘接入设备密码服务器分别进行初始化处理，生成各自密码系统参数和主密钥。

[0122] 步骤二：交换密码公共参数。物联网终端密码服务器、服务商密码服务器和边缘接入设备密码服务器分别通过安全可信的公开渠道向其他服务器公布各自的标识密码系统参数和主公钥。

[0123] 步骤三：下发初始身份标识ID和私钥。物联网终端密码服务器向其对应的物联网终端发送物联网终端身份标识和出厂私钥；服务商密码服务器向其对应的服务终端发送服务终端身份标识和服务私钥；边缘接入设备密码服务器向其对应的边缘接入设备发送边缘接入设备身份标识和出厂私钥。其中，物联网终端密码服务器将物联网终端身份标识和出厂私钥内置在物联网终端标识密码模块中；服务商密码服务器将服务终端身份标识和服务私钥内置在服务终端标识密码模块中；边缘接入设备密码服务器将边缘接入设备身份标识和出厂私钥内置在边缘接入设备终端标识密码模块中。

[0124] 步骤四：身份认证和服务私钥下发。当一终端(物联网终端或物联网边缘接入设备终端)首次接入服务终端时，需要完成身份认证并安全获取服务终端相应的服务私钥。例如，电力物联网终端首次接入服务终端，如图9所示，其身份认证和获取服务私钥的具体过程如下：

[0125] (1)当电力物联网终端出厂时，电力物联网终端密码服务器TP-OEM向电力物联网

终端标识密码模块中内置电力物联网终端身份标识TPID(第一公钥)及其对应的出厂私钥$TO\text{-}RK_{TPID}$。

[0126] (2)服务商密码服务器SP通过可信公开渠获取电力物联网终端密码服务器TP-OEM的标识密码公共参数$Pram_{TO}$;当然,电力物联网终端也可以通过可信公开渠道获取服务商密码服务器的身份标识SPID(第二公钥)及其标识密码公共参数$Pram_{SP}$,当存在多个服务商密码服务器需要相互进行身份验证时,电力物联网终端则需要获取服务商密码服务器的身份标识SPID(第二公钥)及其标识密码公共参数$Pram_{SP}$,此处不涉及多个服务商密码服务器,电力物联网终端无需获取服务商密码服务器的身份标识SPID(第二公钥)及其标识密码公共参数$Pram_{SP}$。

[0127] (3)电力物联网终端TP向服务商密码服务器SP发送身份验证和服务私钥请求信息。电力物联网终端TP使用其出厂私钥$TO\text{-}RK_{TPID}$对其身份标识TPID进行签名$SIGN_{TO\text{-}RKTPID}(TPID)$,并使用服务商密码服务器SP的身份标识SPID作为公钥将该签名值$SIGN_{TO\text{-}RKTPID}(TPID)$、电力物联网终端身份标识TPID进行加密,得到加密请求信息$ENC_{SPID}(SIGN_{TO\text{-}RKTPID}(TPID)|TPID)$,并将该加密请求信息发送给服务商密码服务器SP。

[0128] (4)服务商密码服务器SP的密钥管理装置KMC利用自身私钥RK_{SPID}对加密请求信息$ENC_{SPID}(SIGN_{TO\text{-}RKTPID}(TPID)|TPID)$进行解密,得到电力物联网终端身份标识TPID及其签名$SIGN_{TO\text{-}RKTPID}(TPID)$。

[0129] (5)服务商密码服务器SP的密钥管理装置KMC利用电力物联网终端身份标识TPID和电力物联网终端密码服务器TP-OEM的标识密码公共参数$Pram_{TO}$验证签名$SIGN_{TO\text{-}RKTPID}(TPID)$。

[0130] (6)若验证通过,服务商密码服务器SP的密钥管理装置KMC将电力物联网终端身份标识TPID安全发送给密钥生成装置KGC,由密钥生成装置KGC生成相应的服务私钥$SP\text{-}RK_{TPID}$。

[0131] (7)服务商密码服务器SP的密钥生成装置KGC将服务私钥$SP\text{-}RK_{TPID}$安全发送给密钥管理装置KMC。

[0132] (8)服务商密码服务器SP的密钥管理装置KMC使用电力物联网终端密码服务器TP-OEM的标识密码公共参数$Pram_{TO}$和电力物联网终端身份标识TPID对服务私钥$SP\text{-}RK_{TPID}$进行加密,得到加密服务私钥$ENC_{TPID}(SP\text{-}RK_{TPID})$,将该加密服务私钥后发送给电力物联网终端TP。

[0133] (9)电力物联网终端TP利用出厂私钥$TO\text{-}RK_{TPID}$对加密服务私钥$ENC_{TPID}(SP\text{-}RK_{TPID})$进行解密,得到服务私钥$SP\text{-}RK_{TPID}$,至此完成身份验证和安全获取服务私钥。

[0134] 电力物联网边缘接入设备终端首次接入服务终端进行身份认证和获取服务私钥的执行过程与电力物联网终端首次接入服务终端进行身份和获取服务私钥的过程类似,具体过程如下:

[0135] (1)当边缘接入设备终端出厂时,边缘接入设备密码服务器CPS向边缘接入设备终端标识密码模块中内置边缘接入设备终端身份标识CPID(公钥)及其对应的出厂私钥$GP\text{-}RK_{GPID}$。

[0136] (2)服务商密码服务器SP通过可信公开渠获取边缘接入设备终端密码服务器GPS的标识密码公共参数$Pram_{GP}$。

[0137] (3)边缘接入设备终端GP向服务商密码服务器SP发送身份验证和服务私钥请求信息。边缘接入设备终端GP使用其出厂私钥TO-RK_{GPID}对其身份标识GPID进行签名$SIGN_{GP-RKGPID}$(GPID),并使用服务商密码服务器SP的身份标识SPID作为公钥将该签名值$SIGN_{GP-RKGPID}$(GPID)、边缘接入设备终端身份标识GPID进行加密,得到加密请求信息ENC_{SPID}($SIGN_{GP-RKGPID}$(GPID)||GPID),并将该加密请求信息发送给服务商密码服务器SP。

[0138] (4)服务商密码服务器SP的密钥管理装置KMC利用自身私钥RK_{SPID}对加密请求信息ENC_{SPID}($SIGN_{GP-RKGPID}$(GPID)||GPID)进行解密,得到边缘接入设备终端身份标识GPID及其签名$SIGN_{GP-RKGPID}$(GPID)。

[0139] (5)服务商密码服务器SP的密钥管理装置KMC利用边缘接入设备终端身份标识GPID和边缘接入设备终端密码服务器GPS的标识密码公共参数$Pram_{GP}$验证签名$SIGN_{GP-RKGPID}$(GPID)。

[0140] (6)若验证通过,服务商密码服务器SP的密钥管理装置KMC将边缘接入设备终端身份标识GPID安全发送给密钥生成装置KGC,由密钥生成装置KGC生成相应的服务私钥SP-RK_{GPID}。

[0141] (7)服务商密码服务器SP的密钥生成装置KGC将服务私钥SP-RK_{GPID}安全发送给密钥管理装置KMC。

[0142] (8)服务商密码服务器SP的密钥管理装置KMC使用边缘接入设备终端密码服务器GPS的标识密码公共参数$Pram_{GP}$和边缘接入设备终端身份标识GPID对服务私钥SP-RK_{GPID}进行加密,得到加密服务私钥ENC_{GPID}(SP-RK_{GPID}),将该加密服务私钥后发送给边缘接入设备终端GP。

[0143] (9)边缘接入设备终端GP利用出厂私钥GP-RK_{GPID}对加密服务私钥ENC_{GPID}(SP-RK_{GPID})进行解密,得到服务私钥SP-RK_{GPID},至此完成身份验证和安全获取服务私钥。

[0144] 步骤五:安全通信。在服务商密钥服务器和电力物联网终端之间完成身份验证并获取服务私钥,电力物联网边缘接入设备终端和服务商密钥服务器之间完成身份验证并获取服务私钥后,电力物联网终端、电力物联网边缘接入设备以及服务之间可以利用其内置的标识密码模块(Identity-Based Cryptographic Module,IBCM)进行双向认证和密钥协商,并进行安全通信。

[0145] 本实施例提供的电力物联网身份认证系统,通过服务器获取终端密码服务器的标识密码公共参数;终端获取服务器发送的第二公钥并获取终端密码服务器的终端身份标识和私钥,根据终端身份标识、终端身份标识对应的私钥和第二公钥,生成加密请求信息,并将加密请求信息发送至服务器;服务器接收终端发送的加密请求信息,对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名,根据标识密码公共参数和第一公钥对所述签名进行验签,若验签通过,则生成对应加密请求信息的服务私钥,对服务私钥进行加密,并将加密后的服务私钥发送至终端;终端接收服务器发送的加密服务私钥,并对加密服务私钥进行解密,得到服务器对应的服务私钥。由于第一公钥和第二公钥分别由终端的身份标识号和服务商密码服务器的身份标识号唯一确定,而终端的身份标识号和服务商密码服务器的身份标识号是不变的,进而保证了第一公钥和第二公钥的真实性和固定性,无需通过第三方来保证其真实性,同时,服务私钥可以根据第一公钥生成,进而保证了服务私钥的真实性,确保了电力物联网系统安全高效运行。通过获取的服务私钥进行身份认证以实

现终端与服务之间的安全通信,无需进行额外的在线身份验证,在满足了电力物联网系统的应用要求的基础上,降低了物联网系统互联互通的复杂度,提升了用户体验。

[0146] 实施例8

[0147] 本发明实施例还提供一种非暂态计算机存储介质,所述计算机存储介质存储有计算机可执行指令,该计算机可执行指令可执行上述任意方法实施例中的物联网身份认证方法。其中,所述存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)、随机存储记忆体(Random Access Memory,RAM)、快闪存储器(Flash Memory)、硬盘(Hard Disk Drive,缩写:HDD)或固态硬盘(Solid-State Drive,SSD)等;所述存储介质还可以包括上述种类的存储器的组合。

[0148] 显然,上述实施例仅仅是为清楚地说明所作的举例,而并非对实施方式的限定。对于所属领域的普通技术人员来说,在上述说明的基础上还可以做出其它不同形式的变化或变动。这里无需也无法对所有的实施方式予以穷举。而由此所引伸出的显而易见的变化或变动仍处于本发明创造的保护范围之中。

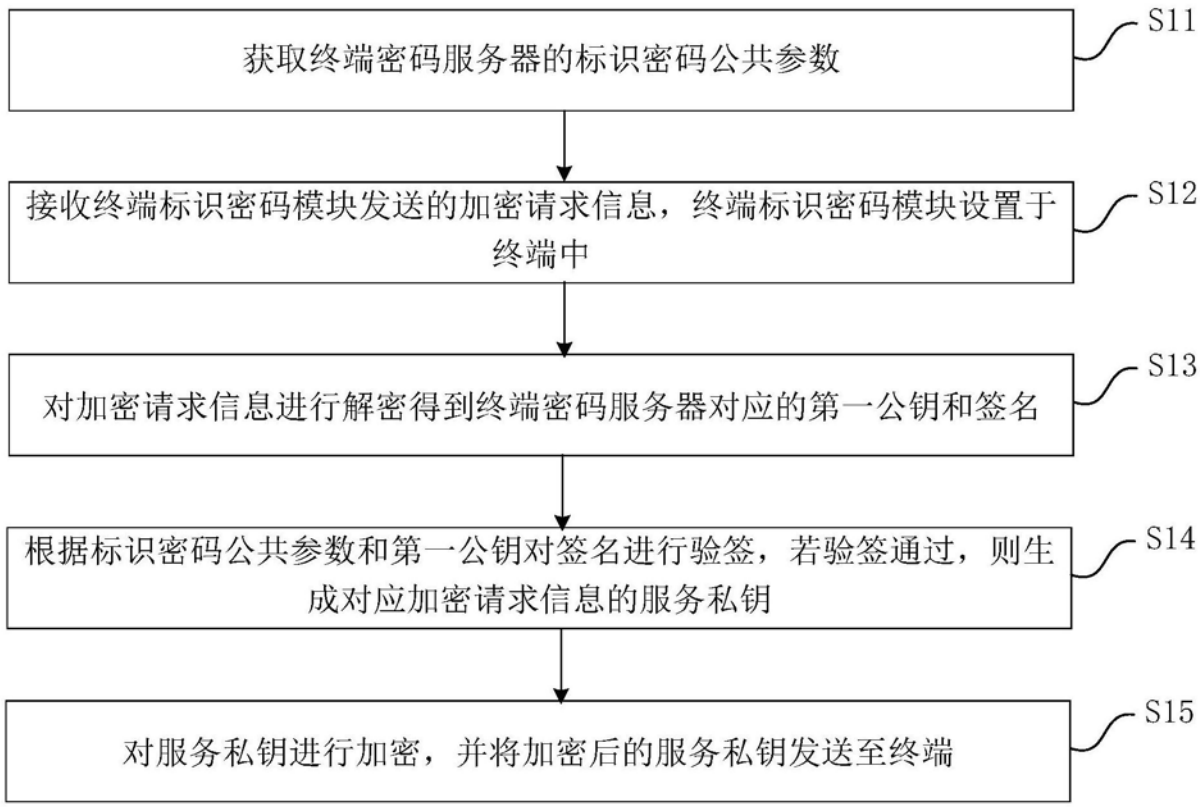

获取终端密码服务器的标识密码公共参数
S11
接收终端标识密码模块发送的加密请求信息，终端标识密码模块设置于终端中
S12
对加密请求信息进行解密得到终端密码服务器对应的第一公钥和签名
S13
根据标识密码公共参数和第一公钥对签名进行验签，若验签通过，则生成对应加密请求信息的服务私钥
S14
对服务私钥进行加密，并将加密后的服务私钥发送至终端
S15

图1

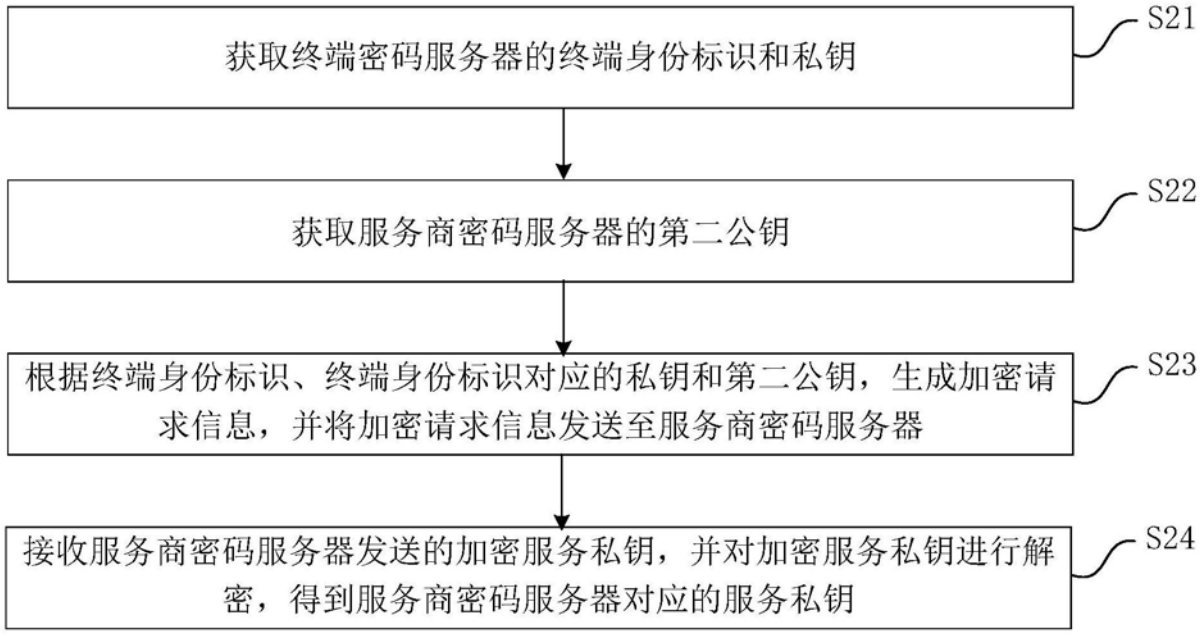

获取终端密码服务器的终端身份标识和私钥
S21
获取服务商密码服务器的第二公钥
S22
根据终端身份标识、终端身份标识对应的私钥和第二公钥，生成加密请求信息，并将加密请求信息发送至服务商密码服务器
S23
接收服务商密码服务器发送的加密服务私钥，并对加密服务私钥进行解密，得到服务商密码服务器对应的服务私钥
S24

图2

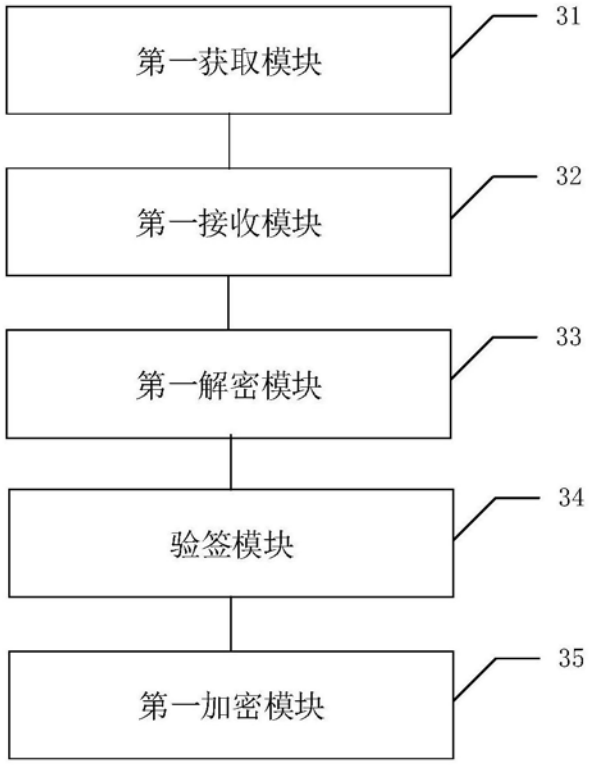

第一获取模块
31
第一接收模块
32
第一解密模块
33
验签模块
34
第一加密模块
35

图3

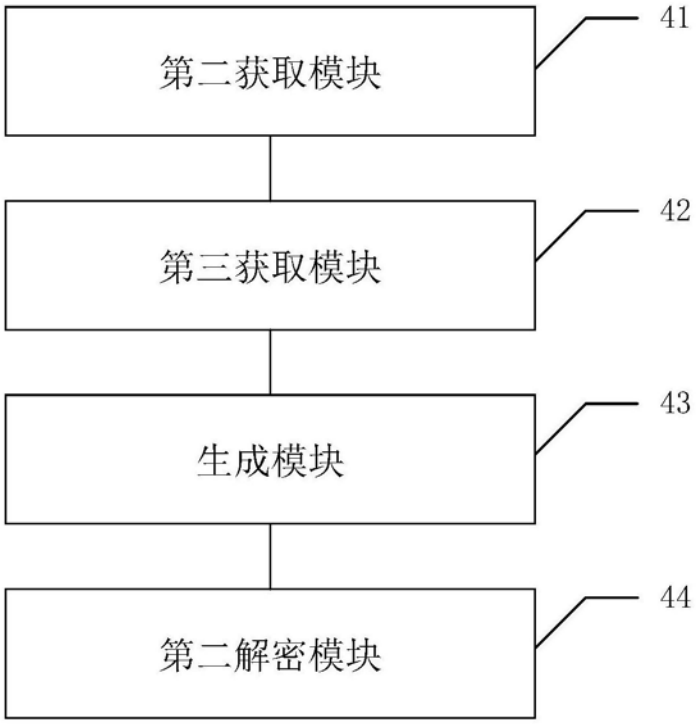

第二获取模块
41
第三获取模块
42
生成模块
43
第二解密模块
44

图4

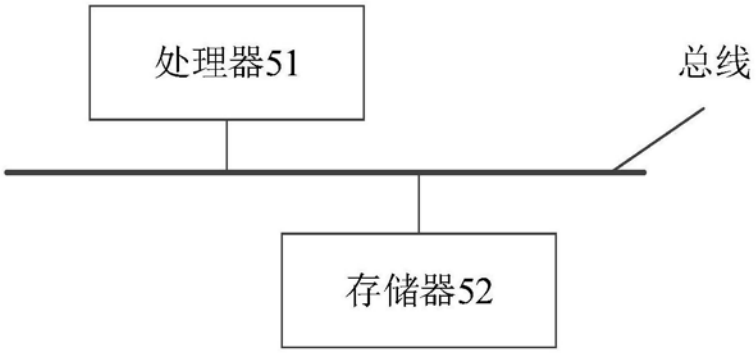


图5

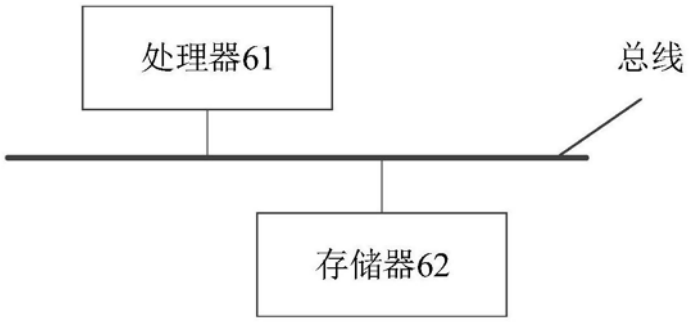


图6

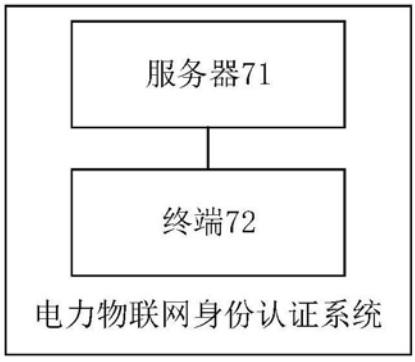


图7

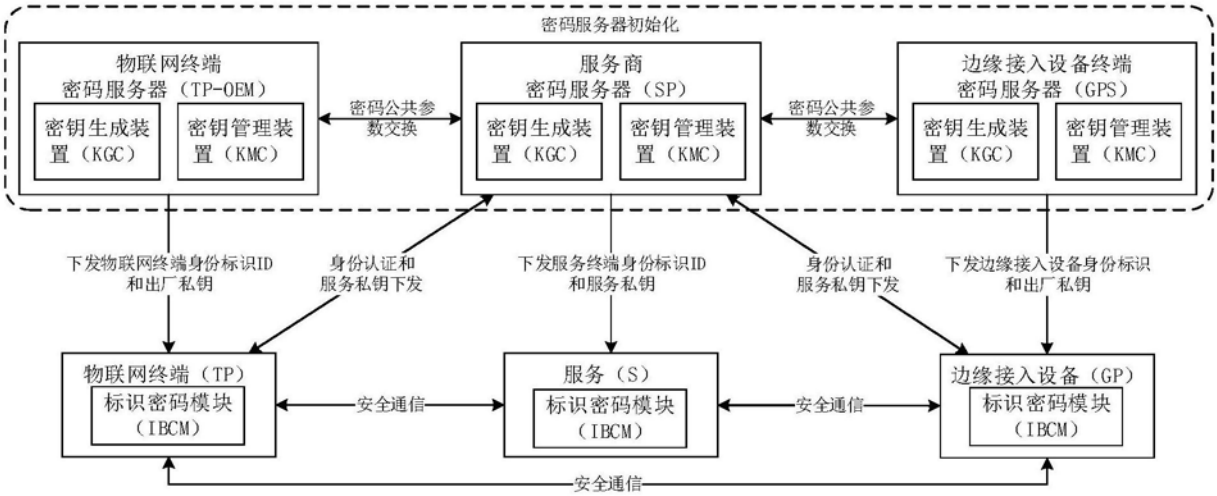

密码服务器初始化
物联网终端
密码服务器（TP-OEM）
密钥生成装置（KGC）
密钥管理装置（KMC）
密码公共参数交换
服务商
密码服务器（SP）
密钥生成装置（KGC）
密钥管理装置（KMC）
密码公共参数交换
边缘接入设备终端
密码服务器（GPS）
密钥生成装置（KGC）
密钥管理装置（KMC）
下发物联网终端身份标识ID和出厂私钥
身份认证和服务私钥下发
下发服务终端身份标识ID和服务私钥
身份认证和服务私钥下发
下发边缘接入设备身份标识和出厂私钥
物联网终端（TP）
标识密码模块（IBCM）
安全通信
服务（S）
标识密码模块（IBCM）
安全通信
边缘接入设备（GP）
标识密码模块（IBCM）
安全通信

图8

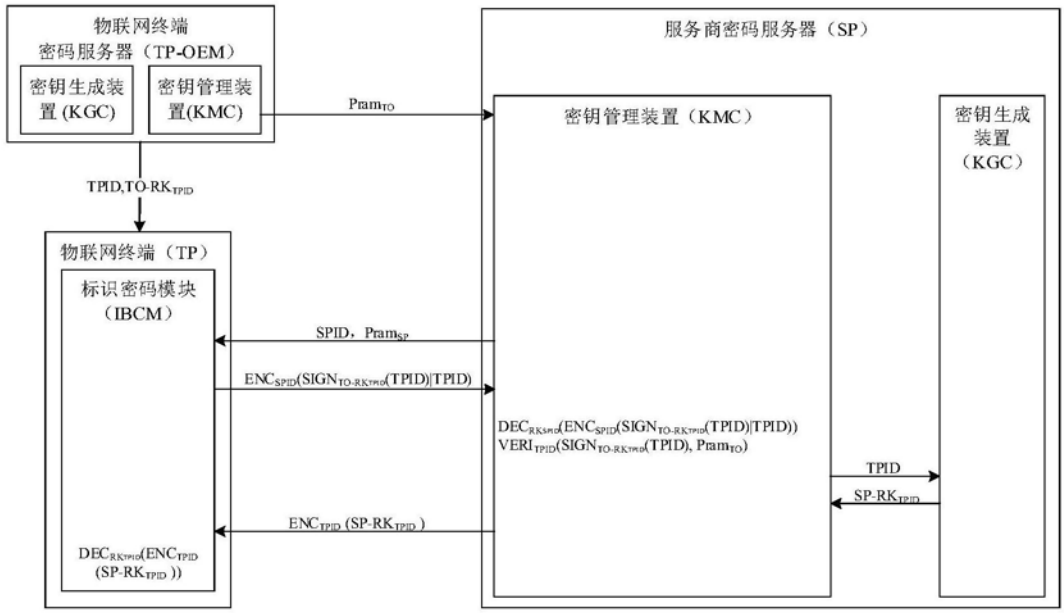

物联网终端
密码服务器（TP-OEM）
密钥生成装置(KGC)
密钥管理装置(KMC)
Pram_TO
服务商密码服务器（SP）
密钥管理装置（KMC）
密钥生成装置（KGC）
TPID,TO-RK_TPID
物联网终端（TP）
标识密码模块（IBCM）
SPID，Pram_SP
ENC_SPID(SIGN_TO-RK_TPID(TPID)|TPID)
DEC_RKSPID(ENC_SPID(SIGN_TO-RK_TPID(TPID)|TPID))
VERI_TPID(SIGN_TO-RK_TPID(TPID), Pram_TO)
TPID
SP-RK_TPID
ENC_TPID (SP-RK_TPID)
DEC_RK_TPID(ENC_TPID (SP-RK_TPID))

图9