(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 104094274 B
(45)授权公告日 2017.03.22

(21)申请号 201380008135.6

(22)申请日 2013.01.18

(65)同一申请的已公布的文献号
申请公布号 CN 104094274 A

(43)申请公布日 2014.10.08

(30)优先权数据
102012201810.7 2012.02.07 DE
102012203354.8 2012.03.02 DE

(85)PCT国际申请进入国家阶段日
2014.08.06

(86)PCT国际申请的申请数据
PCT/EP2013/050896 2013.01.18

(87)PCT国际申请的公布数据
WO2013/117404 DE 2013.08.15

(73)专利权人 联邦印刷有限公司
地址 德国柏林

(72)发明人 法克·迪特里克
曼弗雷德·皮斯克

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 戴建波

(51)Int.Cl.
G06F 21/57(2006.01)
G06F 21/44(2006.01)
G06F 21/70(2006.01)
G06Q 50/06(2006.01)
H04W 4/00(2006.01)

审查员 马璐璐

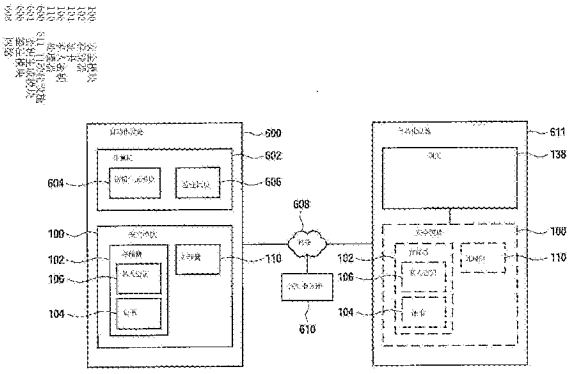
权利要求书2页 说明书10页 附图4页

(54)发明名称

智能表的个性化方法或者智能表网关安全模块的个性化方法

(57)摘要

本发明公开了一种通过第一计算机系统(150)对智能表或智能表网关安全模块(100)进行个性化的方法;其中,智能表(142、144、146、148)能获得与能源消耗相关的测量数据;安全模块(100)具有密保功能,用于执行智能表(142、144、146、148)或智能表网关(138)所接收到的测量数据与能源供应商和/或测量单位操作员的第二计算机系统(166)之间的密钥通讯;该方法包括以下步骤:-准备安全模块(100);-由第一计算机系统生成非对称密钥对,并将该密钥对储存到安全模块(100);-将该密钥对的公共密钥进行签注,以获取证书,并将该证书储存到安全模块(100)和/或公共索引服务器(610)中;其中,签注是通过第一计算机系统(150)进行的;安全模块(100)是如此设置的,在存储所述密钥对之后,只允许智能表(142、144、146、148)或智能表网关(138)与第一计算机系统(150)之间的初始通讯;只有通过第一计算机系统(150)的初始通讯,安全模块(100)才能激活与第二计算机系统(166)之间的通讯。



CN 104094274 B

1.一种通过第一计算机系统(150)对智能表或智能表网关安全模块(100)进行个性化的方法;其中,所述智能表(142、144、146、148)能获得与能源消耗相关的测量数据;所述安全模块(100)具有密保功能,用于执行智能表(142、144、146、148)或智能表网关(138)所接收到的测量数据与能源供应商和/或测量单位操作员的第二计算机系统(166)之间的密钥通讯;该方法包括以下步骤:

-准备安全模块(100);

-由第一计算机系统生成非对称密钥对,并将该密钥对储存到安全模块(100);

-将该密钥对的公共密钥进行签注,以获取证书,并将该证书储存到安全模块(100)和/或公共索引服务器(610)中;其中,所述的签注是通过第一计算机系统(150)进行的;所述的安全模块(100)是如此设置的,在存储所述密钥对之后,只允许智能表(142、144、146、148)或智能表网关(138)与第一计算机系统(150)之间的初始通讯;只有通过第一计算机系统(150)的初始通讯,所述安全模块(100)才能激活与第二计算机系统(166)之间的通讯;

其中,所述的安全模块(100)分配有明确的识别码(128);其中,所述的方法进一步包括将所述识别码(128)存储在所述安全模块(100)中的步骤;其中,所述的签注也包括对所述识别码(128)进行签注;

所述的方法进一步包括在所述智能表(142、144、146、148)或智能表网关(138)中安装安全模块(100)的步骤,其中,该安装是通过在安全模块(100)和智能表(142、144、146、148)或智能表网关(138)之间的不可逆的连接过程而实现的;

其中,为了安全模块(100)与智能表(142、144、146、148)或智能表网关(138)的相互连接,在智能表(142、144、146、148)或智能表网关(138)中启动如此的连接过程,其中,通过该连接过程在安全模块(100)与智能表(142、144、146、148)或智能表网关(138)之间建立不可分离的逻辑连接;

其中,所述不可分离的逻辑连接包括将所述证书和/或安全模块(100)明确的识别码(128)不可逆地复制到智能表(142、144、146、148)或智能表网关(138)的存储区中。

2.如权利要求1所述的方法,其中,所述的证书包含所述安全模块(100)的公共密钥和/或明确的识别码(128)。

3.如权利要求1或2所述的方法,其中,所述安全模块(100)的识别码(128)是指安全模块(100)的公共密钥或者安全模块(100)的IPv6地址。

4.如权利要求1或2所述的方法,其中,所述的第一计算机系统是安全的、封闭的第一自动化设施(600)的一部分,其中:

-将密钥对和/或证书和/或识别码(128)存储在安全模块(100)中是在第一自动化设施(600)中进行的;或者

-将密钥对和/或证书和/或识别码(128)存储在安全模块(100)中是在第二封闭的自动化设施(611)中进行的;其中,在这种情况下,非对称密钥对和/或签注和/或识别码(128)是从第一自动化设施(600)通过加密的通讯连接传输给第二自动化设施(611)的。

5.如权利要求4所述的方法,其中,所述的安全的、封闭的第一自动化设施(600)是指信任中心。

6.如权利要求4所述的方法,其中,在智能表(142、144、146、148)或智能表网关(138)中安装安全模块(100)是在第二自动化设施(611)之内进行的。

7.如权利要求1或2所述的方法，其中，准备好的安全模块(100)没有进行个性化，其中，只有将密钥对和/或证书存储到安全模块(100)中才进行安全模块(100)的个性化。

8.如权利要求1或2所述的方法，其中，安全模块(100)是以芯片卡形式提供的。

9.如权利要求1或2所述的方法，其进一步包括将第一计算机系统(150)的联系信息存储在安全模块中的步骤，其中，通过该联系信息确定如此界限：只在第一计算机系统上进行初始化通讯。

智能表的个性化方法或者智能表网关安全模块的个性化方法

技术领域

[0001] 本发明涉及一种智能表的个性化方法或者一种智能表网关安全模块的个性化方法、以及一种计算机程序产品。

背景技术

[0002] 就“智能表(或称智能电表)”而言，一般理解为给客户配备的电能消耗计数器，除了可以简单地抄读已消耗的电量外，还可以通过网络为客户或者供电公司提供其它的功能。

[0003] 通过智能电表，客户可以实时得知实际的能源消耗。此处术语“能源消耗”，可以理解为客户在家或者在公司所消耗的任何一种能源的数量。能源形式除了电、水、气之外，还可以是任意其它的能源形式，例如集中供暖。

[0004] 为了抄读能量消耗量，可以在各个消费者处安装智能测量系统，也叫智能计数器，或者“智能电表”。智能电表就是能源消耗计数器。消费者可以是自然人或者法人，消耗各种可测量的能源，例如电、气，水或者热能。使用智能电表的目的是使用智能测量系统根据总需要和电网负荷收取可变的费用，由此可以更好地使用网络。

[0005] 根据BSI TR-03109技术规范，所谓的智能电表网关也称为集中单元，它用来作为中央通讯单元，可以与一个或者多个智能电表通讯。为此，网关在“家庭区域网络(Home Area Network)”和“广域网络(Wide Area Network)”与设备进行通讯。家庭区域网络包括所有与网关连接的智能电表以及消费者的私人计算单元。私人计算单元用于生成由智能电表抄读到的实际能源消耗值的相关信息。广域网络则可用于网关与授权市场参与者之间的通讯。例如，网关可以将智能电表的所有数据收集起来，并将其提供给一个上级收集单位，例如能源供应商或者测量单位操作员。

发明内容

[0006] 此处，本发明的目的是提供一种智能电表的个性化方法或者一种智能电表网关安全模块的个性化方法，以及相应的计算机程序产品。

[0007] 本发明的独立权利要求提供了实现上述发明目的的技术方案，而从属权利要求则给出了本发明的优选实施方式。

[0008] 通过第一计算机系统，可以实现一种智能电表安全模块的个性化方法或者智能电表网关安全模块的个性化方法；其中，智能电表可以获得与能源消耗相关的测量数据；安全模块具有密保功能，用于执行智能电表或者智能电表网关所接收到的测量数据与能源供应商和/或测量单位操作员的第二计算机系统之间的密钥通讯；该方法包括以下步骤：

[0009] -准备安全模块；

[0010] -由第一计算机系统生成非对称密钥对，并将其储存到安全模块；

[0011] -将密钥对的公共密钥进行签注，用于获取证书，并将证书储存到安全模块和/或公共索引服务器中；其中，签注是通过第一计算机系统进行的；安全模块是如此设置的，在

储存密钥对之后，安全模块只允许智能电表和/或智能电表网关与第一计算机系统之间的初始通讯；只有通过第一计算机系统的初始通讯，安全模块才能激活与第二计算机系统之间的通讯。

[0012] 本发明的具体实施方式具有如下优点：通过初始化过程，能够以更安全、清晰、可行的方式，实现智能电表和授权市场参与者(例如能源供应商或者测量单位操作员)之间的安全通讯。此处，第一计算机系统优选是可信赖单位的计算机系统，也称为“信任中心(Trust Center)”或者“可信服务管理平台(Trusted Service Manager)”或者“可信服务管理(TSM)”。

[0013] 安全模块在其初始化状态是如此设置的，只有第一计算机系统的可信赖单位在成功通过认证后，才能与安全模块进行通讯。由此保证只托付这些单位来设置智能电表中与费用相关的配置，这些单位可以是授权的市场参与者，例如测量单位操作员和能源供应商本身；同样，终端消费者也可以设为可信赖的对象。“与费用相关的配置”可作如下理解：通过智能电表的这种配置，确定谁有权计算由智能电表抄读到的能源数量；另外，由此也可以确定，哪些人(例如终端消费者和授权的市场参与者)可以使用智能电表哪些范围内的功能以及信息。因为这些设置都是由可信赖单位单方面执行的，从而保证排除未授权第三方非法使用这些功能和信息。上述信息包括：例如智能电表的地点信息、由智能电表测量到的数值、储存区的地点信息或者储存区中包含的数值。

[0014] 一般来说，由谁来准备安全模块不重要，也就是说，此处是否由可信赖单位处理此事不重要。另外，一般来说，是否由可信赖的有关单位执行存储过程也不重要。安全模块在准备阶段的移交状态下没有设置任何的保密资料。未授权人员通过安全模块不能进行任何操作，因为在没有证书的情况下，第一计算机系统不能执行任何授权的密码操作。只有在储存非对称密钥对的私人密钥时，必须保证安全模块和第一计算机系统之间必要的通讯是安全防窃听的。

[0015] 在数据存储到安全模块后，这些对于未授权人员来说就无意义了，因为只有第一计算机系统才能与安全模块进行通讯，从而修改或者执行上述设置。

[0016] 根据本发明一具体实施方式，安全模块具有明确的识别码；其中，本发明的方法还另外包括将识别码储存在安全模块中的步骤；其中，签注的步骤也包括将识别码进行签注。这一具体实施方式的优点在于，稍后凭借识别码运行安全模块给测量单位操作员或者能量供应商传输能源消耗数据时，安全模块可以清楚地验证安全模块、进而验证终端消费者。如果在使用识别码的情况下，安全模块由此与智能电表和/或网关建立了不可逆地自动连接，那么也可以清楚地验证智能电表和/或网关，由此可以有效阻止其它智能电表或者网关的“假冒”。

[0017] 根据本发明另一具体实施方式，通过安全模块的识别码，可以直接或间接地通过网关为智能电表设置了存储区的识别码，由此保证安全模块和存储区之间不可分离地相互连接起来，这样，安全模块的准确定位与存储区的准确定位是一致的。如果存储区位于智能电表网关内，就可以确保以后网关不会通过非法方式由其它网关代替。例如，可以阻止“黑客”网关将数值提供给测量单位操作员，这些“黑客”网关只是偶尔地与相应的智能电表连接，其根本没有进行实际能源消耗数据的抄读。上述存储区可以只通过安全模块由第一计算机系统来书写，并且根据识别码可清楚地定位此存储区。在这种情况下，使用其它网关和

其它存储区原则上是不可能的，因为就第一计算机系统而言，其不会启动与能源读取的相关数据。

[0018] 根据本发明一具体实施方式，安全模块的识别码是指安全模块的公共密钥或者安全模块的IPv6地址。使用安全模块的公共密钥作为安全模块的识别码、从而作为存储区的识别码的优点在于，由此可以准备全球唯一标识符(GUID)，它几乎是绝对安全的。简单地分配一个尽可能长的公共密钥就可以实现对识别码的简单管理。在安全模块的识别码是IPv6地址的情况下，通过简单的方式，就可以通过现有网络对安全模块进行准确地定位。

[0019] 根据本发明另一具体实施方式，证书包含安全模块的公共密钥和/或识别码。该公共密钥是分配给私人密钥的，私人密钥储存在安全模块的受保护的存储区内。该证书可以根据公钥基础设施(PKI)标准生成，例如根据X.509标准生成。

[0020] 根据本发明一具体实施方式，本发明的方法还包括在智能电表或者智能电表网关中安装安全模块的步骤，其中，该安装是通过执行在安全模块和智能电表或者智能电表网关之间的不可逆且不可分离的连接过程而实现的。“不可分离”或者“不可逆”的意思可以理解为安全模块和智能电表或者智能电表网关之间建立持续地连接，由此保证安全模块的功能。只要尝试将安全模块与智能电表或者智能电表网关分离，就导致安全模块进入不可用状态，也就是无功能状态。这可以通过安全模块的电子自我销毁、自我失活、或者物理销毁或失活来保证。在最简单的情况下，安全模块可以锁在智能电表或者智能电表网关的外壳中，这样“拆开”铸件连接，就会导致安全模块的销毁。

[0021] 优选地，为了安全模块与智能电表或者智能电表网关的相互连接，启动智能电表或者智能电表网关的连接过程，其中，通过该连接过程在安全模块和智能电表或者智能电表网关之间建立不可分离的逻辑连接。例如，这种不可分离的逻辑连接包括将安全模块的证书和/或识别码不可逆地复制到分配给智能电表或者网关的存储区中。

[0022] 根据本发明一具体实施方式，第一计算机系统是安全的、封闭的第一自动化设施的一部分，其中：

[0023] -将密钥对和/或证书和/或识别码存储在安全模块中是同样在第一自动化设施中进行的；或者

[0024] -将密钥对和/或证书和/或识别码存储在安全模块中是在第二封闭的自动化设施中进行的；其中，在这种情况下，非对称密钥对和/或签名和/或识别码从第一自动化设施通过加密的通讯连接传输给第二自动化设施。

[0025] 优选地，安全的、封闭的第一自动化设施是指信任中心。信任中心定义为公钥基础设施(PKI)可信赖机构，它为使用者和通讯伙伴提供安全服务。信任中心可以接受认证单位或者密码管理中心的基本功能。在上述描述中非常重要的是，第一自动化设施是指部件的积聚体，它在安全的、空间封闭的自动化环境中生成不对称密钥对和证书。另外，这还意味着可以在第一自动化设施中，各部件以预定方式共同作用，能够实现集中控制和中央调控。这同样也适用于上述的第二封闭自动化设施。因此，两个自动化设施是分离的，或者是“空间分离”的，因为两个自动化设施中都进行各自的自动化过程，不形成中央控制。

[0026] 根据本发明一具体实施方式，在智能电表或者智能电表网关中安装安全模块是在第二自动化设施之内进行的。该安装一定不能在第一自动设施中进行，或者不能由第一自动化设施来执行。这样，可以通过简单的方式，通过储存密钥和证书来准备大量的安全模

块，在稍后任意的时间任意的地点与硬件“智能电表”或者“智能电表网关”进行逻辑连接。仍然可以确保，在之后的任意时点，只通过第一计算机系统激活与第二计算机系统的通讯。

[0027] 根据本发明一具体实施方式，安全模块是以芯片卡形式提供的。第一计算机系统的操作员预先设置了芯片卡形式的安全模块，它将信息存储在芯片卡中，第一计算机系统成功认证了安全模块后，稍后执行初始化过程或者激活过程。

[0028] 根据本发明一具体实施方式，准备好的安全模块没有进行个性化，其中，只有将密钥对和/或证书储存到安全模块中才进行安全模块的个性化。此处，术语“个性化”是指清楚地确定安全模块的标志特征，该标志特征使得该安全模块能够被唯一地确定，从而可以清楚地与其它安全模块区分开来。

[0029] 根据本发明另一具体实施方式，本发明的方法还包括将第一计算机系统的联系信息储存在安全模块中的步骤，其中，通过该联系信息确定如此界限：只在第一计算机系统上进行初始化通讯。这样，在存储过程中同时也可以清楚地确定，只有第一计算机系统被激活用于与安全模块建立联系。所有其它计算机系统不能进行这种初始化读取数据。例如，可以将第一计算机系统的明确标识，例如其姓名或者其公共密钥，作为信息储存在安全模块中。之后，第一计算机系统通过它自己的证书对安全模块进行认证。

[0030] 另一方面，本发明涉及一种计算机程序产品，其具有处理器可执行的指令，以执行上述方法的步骤。

[0031] 下面，借助附图来详细地描述本发明的优选具体实施方式。其中：

附图说明

[0032] 图1显示了用于执行上述方法的系统的框图；

[0033] 图2显示了用于与智能电表之测量数据进行通讯的系统的框图；

[0034] 图3显示了用于初始化存储区之方法的流程图；

[0035] 图4显示了用于准备安全模块之方法的流程图。

具体实施方式

[0036] 在下面的具体实施方式中，相同的元件采用相同的附图标记。

[0037] 图1显示了用于个性化安全模块的各种自动化设施的布局方框图。下面只以图1左侧的形式为例进行叙述，其中，安全模块100通过自动化设施600完全地进行个性化。

[0038] 自动化设施600配置了一台计算机602，它具有密钥生成模块604和签注模块606。通过密钥生成模块604，计算机602可以生成不对称密钥对。通过签注模块606，计算机600可以将模块604生成的公共密钥进行签注，由此生成证书104。为此，模块606借助自动化设施600的私人密钥而对所生成的公共密钥进行加密。

[0039] 密钥对生成之后，特别是私人密钥106可以保存到安全模块100的存储器102中，其中必须保证，在安全模块100之外不能读取私人密钥106。此处，例如在存储了私人密钥106之后，安全模块100在一单独步骤中直接“关闭”。

[0040] 证书104优选通过网络608保存在公共索引服务器610中；也可以将证书直接保存在存储器102中。

[0041] 将安全模块100个性化之后，可以在单独的工作步骤中将其与智能电表或者智能

电表网关138阻隔开。它不能安装在自动化设施600中，而可以在例如自动化设施611中进行。将安全模块100安装到网关138中，就在网关和安全模块之间建立了不可逆的逻辑连接，同样也是物理连接。关于这一点，稍后还会详细介绍。

[0042] 上述个性化方法的替代方案可以是，取代在自动化设施600中“现场”个性化，而是通过网络608在自动化设施611中执行个性化方法。此处，图1右侧中用虚线示出了安全模块100。在这种情况下，还像之前那样，由计算机602生成非对称密钥对。然后将私人密钥106传输给自动化设施611，在使用网络608的情况下通过密保通讯连接传输给安全模块100的存储器102。

[0043] 两个自动化设施600和611在空间上和逻辑上都是互相分离的。它们是“自动化设备”，各自的自动化流程在空间上都是完全分开控制的。

[0044] 因此，例如可以给自动化设施610配置传送芯片卡的传送带，在自动化设施610内部的中央控制下，按照特定的节奏将芯片卡输送给阅读器或者书写器。在这种情况下，芯片卡就是安全元件。然后，芯片卡阅读器或者书写器在芯片卡上针对私人密钥106以及证书104执行上述书写过程。接着，还可以包装好完成个性化的芯片卡，准备自动发货。

[0045] 由此，完全分离的自动化设施611可以使用中央控制单元，且此中央控制单元只对自动化设施611有效，收到发货后打开芯片卡，并将其安装到相应的网关38。

[0046] 如果自动化设施611中的安全模块100如之前所描述的一样，就减少了自动化设施600生成密钥并将其传输给自动化设施611的工作步骤。此处，自动化设施611接受具有这种密钥的芯片卡所限定的上述功能。

[0047] 图2显示了一种总系统的方框图，它使用图1所显示的安全模块100对存储区进行初始化。接下来，与图3所显示的用于初始化存储区的步骤一起，无特殊限制地介绍了对网关138的存储区136进行初始化，网关中安装了所归属的大量的智能电表142、144、146、148。

[0048] 智能电表142-148用于抄读各种能源的消耗值，例如气(智能电表142)、水(智能电表144)、电(智能电表146)以及其它没有详细介绍的能源形式(智能电表148)。智能电表通过相应的通讯连接192与网关138的接口118连接。

[0049] 安全模块100与网关138稳固地、不可分地连接起来。这样，网关138与安全模块100的组合就形成了一个不可分的单元140。网关138和安全模块100通过各个接口118或者116相互通讯。通过接口116，还可以与授权市场参与者、第三方或者相关单位通讯，其不在由单元140和智能电表142-148所形成的网络中。安全模块100和其它通讯参与者之间的通讯则通过通讯连接190来实现，它可以是电线连接，或者是通过移动电信通讯网络或因特网实现的通讯连接。

[0050] 安全模块100具有电子存储器102，它具有受保护的存储区106和108。受保护的存储区106用于储存安全模块100的私人密钥，存储区108则用于储存安全模块的标识符“全球唯一标识符(GUID)”。全球唯一标识符(GUID)例如可以是安全模块100的IPv6地址，它可以由图1所显示的自动化设施610生成，并通过上述储存私人密钥106的方法储存在安全模块中。存储过程可以由自动化设施610执行，或者由自动化设施611执行。

[0051] 另外，电子存储器102可以配置存储区104，用于储存证书。证书中包含公共密钥，该公共密钥分配给在受保护的存储区106中所存储的私人密钥。证书也可以根据公钥基础设施(PKI)标准生成，例如根据X.509标准。

[0052] 证书不是必须储存在安全模块100的电子存储器102中。可以替代或者可以补充的是，将证书储存在公共索引服务器中，见图1。

[0053] 安全模块100具有处理器110，用于执行程序指令112和114。通过执行程序指令112“密码协议”，例如可以认证有关单位150或者能源供应商166对于安全模块100的可信度。密码协议例如可以是以对称密钥或者非对称密钥对为基础的口令/应答协议。

[0054] 当然也可以反过来验证安全模块对于有关单位或者能源供应商的可信度。

[0055] 程序指令114用于对安全模块100与可信赖的有关单位150或者能源供应商166之间的数据传输进行点对点的加密。对于点对点的加密可以使用对称密钥，例如在执行安全模块100和其它参与者150或者166之间的密码协议时进行约定。

[0056] 与安全模块100相似的是，可信赖的有关单位150也配置了一个电子存储器152和受保护的存储区156，用于储存可信赖单位的私人密钥。存储器152中也可以含有可信赖单位的证书。此证书同时也可以储存在中央证书服务器中。

[0057] 另一方面，可信赖的有关单位150的处理器158中配有上述与安全模块100有关的程序指令112和114，用于执行密码协议和点对点加密。密码协议和点对点加密可用于通过接口164与能源供应商166或者安全模块100实现的通讯。证书154包含分配给储存在受保护的存储区156中的私人密钥的公共密钥。

[0058] “能源供应商”166是能源供应商的计算机系统，它配置了一个电子存储器168和一个处理器178。另外，这个计算机系统还有一个接口186，通过它可以实现与可信赖单位150或者安全模块之间的通讯。

[0059] 能源供应商的电子存储器168具有带私人密钥的受保护的存储区172，私人密钥还分配了一个公共密钥，它包含在证书170中，同样也包含在电子存储器168中。另外，存储器168中设有一个存储区用于一项或者多项应用，这些应用可以实现例如与费用相关的网关138配置。在电子存储器168中同样也可以储存由网关138所接收到的测量数据176。

[0060] 处理器178具有程序指令180，用于抄读由网关138送来的消耗数据和其它内容，由此执行方法步骤，根据接收到的测量数据(程序指令182)计算能源消耗。同时也可以设置执行密码协议112的程序指令以及未介绍的执行点对点加密的程序指令，通过这些程序指令可以与可信赖单位150或者安全模块100建立安全通讯。

[0061] 如果现在给能源供应商166分配了一个新客户，例如可以在初次安装了智能电表142-148，并准备好带安全模块102的网关138之后再启动安全模块的初始化过程。如果新客户(终端消费者)或者指定的技术有关单位已经安装过智能电表，初始化过程就有可能出现冲突，就会向能源供应商166发送相应的通知。通知中应该优选包含安全模块100的全球唯一标识符(GUID)108，因为安全模块100可以清楚地针对能源供应商166进行认证。

[0062] 能源供应商166通过接口186，例如通过相应网页上的网络接口接收到通知后，就建立了到达可信赖单位150的通讯通道。这个步骤在图3中用附图标记200标示出来了。可信赖的有关单位可以是例如所谓的“可信服务管理(TSM)”，一家在电子通讯程序中证明通讯伙伴身份的官方认证单位。

[0063] 在下面的描述中，从原则上来说，自动化设施600及它的计算机602与可信赖的有关单位150是相同的。

[0064] 在第200步建立了通讯通道后，在第202步验证能源供应商166。此处，可信赖的有

关单位150检查能源供应商的证书170。例如，可信赖的有关单位150在检验证书时执行口令/应答程序，由此产生一个随机验证码，它与证书170中包含的能源供应商166的公共密钥一起加密，并传送给能源供应商166。紧接着，能源供应商166可以用其私人密钥172解密随机验证码，并以明文形式发回。如果可信赖单位150接收到的随机验证码与之前所描述的随机验证码一致，实际上能源供应商166就通过了验证。

[0065] 执行了步骤202及选择性执行口令/应答程序后，紧接着在第204步，可以通过能源供应商166和可信赖单位150之间的通讯连接，建立点对点的加密通道。此处可以使用可信赖单位的处理器158的程序指令114。

[0066] 在第204步建立了通讯通道后，可信赖单位150在第206步接收请求开启能源供应商166的能源抄读应用174，并传输给网关138的存储器136。为了清楚地说明存储器136或者网关138，请求中应将初始化存储器136、并将存储器136中含有的网关138的全球唯一标识符(GUID)128发送给可信赖的有关单位。存储器136的全球唯一标识符(GUID)128优选与安全模块100的存储器102的全球唯一标识符(GUID)108一致。

[0067] 通过在第206步接收全球唯一标识符(GUID)，可信赖的有关单位150清楚定位需要的网关138，以启动应用174。此处，在接下来的步骤208中，可信赖单位150通过通讯连接190建立到达安全模块100的通讯通道。可信赖单位150针对安全模块100进行验证，验证包括安全模块100的口令/应答程序以及安全模块对证书154的检验。此处，安全模块100生成一个随机验证码，和可信赖单位150的公共密钥一起加密，并发送给可信赖单位150。可信赖单位150用其私人密钥156解密这个加密随机验证码，并将明文格式的解密随机验证码发回给安全模块100。如果安全模块确定接收到的解密随机验证码与它的原始加密随机验证码一致，则表示可信赖单位通过验证。

[0068] 本发明方法继续进行到第212步，在可信赖单位150和安全模块100之间建立点对点加密通讯通道。这一步可以应用安全模块100的处理器110的程序指令114。

[0069] 第214步，安全模块100从可信赖单位接收能源抄读应用174。

[0070] 此时可以发现其优点在于，如果可信赖单位将最常使用的能源抄读应用事先存放在可信赖单位的本地存储器中，就不需要在签订新用户时总是让能源供应商166给可信赖单位150发送应用174。

[0071] 在第214步接收到能源抄读应用后，安全模块100将应用储存到网关138的存储器136中。如果应用174是关于抄读水电能源消耗的应用，应用就作为应用132保存在存储器136中。应用的作用是直接处理智能电表144的能源消耗数据。与此相似的是，存储器136可以包含气能源抄读应用(134)以及抄读其它能源形式的其它应用程序130。图2第216步标示了网关138中的安全模块100储存能源抄读应用的过程。

[0072] 对安全模块100在第214步接收能源抄读应用可以补充的是，可以从可信赖单位150接收能源供应商资格证书或者网络数据元件的详细规格说明，这些同样也储存在存储器136的其它资格125中。资格证书或者测量数据元件的详细规格说明可以事先规定允许从网关138接收的关于能源供应商166的信息。此处，例如可以事先由可信赖单位150定义每个能源供应商的特殊资质，这些资质对于所有的能源供应商166都全球有效，原则上来说将能源抄读应用发送给安全模块，再发送给网关138。

[0073] 同时还可以得到可信赖单位150的配置数据。这些配置数据可以涉及智能电表和/

或其网关的技术配置。

[0074] 凭借程序指令，处理器126执行数据抄读122。此时，网关138的作用就是抄读例如智能电表144和智能电表146的能源消耗测量数据。相应的测量数据则储存在存储器136的储存区124中。原则上来说，测量数据124由很多测量数据元件组成，例如包括：测量数据抄读时间，各个时间的单个测量数据点，测量数据的产生信息(例如电流强度、电压、水压、水温、气压)。测量数据124可以通过应用程序130、132和134执行其它评价，这些评价同样作为“数据测量元件”保存在存储区124中。例如评价出的测量数据可以是累积能源消耗值。

[0075] 上述资格证书125以及测量数据元件的规格说明可以事先规定，能源供应商126的哪些数据测量元件124允许被读取。另外，还可以事先规定允许读取的资料的详细程度。详细地，准时地读取测量数据124是不被大家所期望的，因为通过短暂的测量时间间隔就可以知道电器对能源的消耗情况，并且由此可以了解到用户的特点，但是同样终端用户也得不到利益。

[0076] 如上所述，安全模块100和网关138优选不可分地连接在一起。例如将其形成一个结构单元140，如图2图形所示。为了形成单元140，可以执行图4流程图中介绍的程序步骤。

[0077] 第400步，首先要准备安全模块100。紧接着执行第402步，将密钥材料和/或证书储存到安全模块中。例如，为此可以给安全模块设置相应的密钥单元，它可以单独由私人密钥产生。另一种方式，可以由可信赖单位生成私人密钥，并将其保存在一个外部不可进入的存储区的安全模块中。从属于私人密钥的公共密钥随着证书由可信赖单位进行签注储存在安全模块的存储器102中，或者储存在公共索引服务器中。另外，在第402步还可以将可信赖单位的联系方式储存在安全模块中，通过联系方式可以规定对可信赖单位的初始通讯的限制。也就是说，第402步将密钥材料储存好后，只有可信赖单位在初始化步骤中可以成功读取安全模块。

[0078] 紧接着，在第404步将芯片卡形式的安全模块安装到网关，由此安全模块与网关之间就建立了不可分的连接。例如，安全模块和网关可以相互电子连接，如果将安全模块与网关分离，将会导致安全模块自动毁坏。

[0079] 在第404步将安全模块插入网关后，安全模块100和网关138在第406步自动形成逻辑连接。例如，安全模块的全球唯一标识符(GUID)108作为全球唯一标识符(GUID)128不可逆地写入网关138的存储器136中。此处，从安全模块100出发应该保证，只有当全球唯一标识符(GUID)108与128一致时，才可以通过能源供应商166启动与网关138之间的通讯，准备测量数据元件。

[0080] 可信赖单位成功验证安全模块后，安全模块现在就可以通过安全传输接收可信赖单位的数据。这些数据之后可以用于初始化分配给上述网关的存储区以及将数据储存在存储区。在这些数据的基础上，就可以绕开可信赖单位与能源供应商和/或测量单位操作员的其它任一计算机系统建立通讯。储存好的数据都详细说明了其它的计算机系统。通过这些储存在存储区的数据，与其它计算机系统建立通讯连接。

[0081] 附图标记清单

[0082] ----------

[0083] 100 安全模块

[0084] 102 存储器

[0085]	104	证书
[0086]	106	私人密钥
[0087]	108	GUID
[0088]	110	处理器
[0089]	112	密码协议
[0090]	114	点对点加密
[0091]	116	接口
[0092]	118	接口
[0093]	120	数据传输
[0094]	122	数据抄读
[0095]	124	测量数据
[0096]	125	资格权利
[0097]	126	处理器
[0098]	128	GUID
[0099]	130	应用程序
[0100]	132	应用程序
[0101]	134	应用程序
[0102]	136	存储器
[0103]	138	网关
[0104]	140	单元
[0105]	142	智能表
[0106]	144	智能表
[0107]	146	智能表
[0108]	148	智能表
[0109]	150	可信赖的单位
[0110]	152	存储器
[0111]	154	证书
[0112]	156	私人密钥
[0113]	158	处理器
[0114]	164	接口
[0115]	166	能源供应商
[0116]	168	存储器
[0117]	170	证书
[0118]	172	私人密钥
[0119]	174	应用程序
[0120]	176	测量数据
[0121]	178	处理器
[0122]	180	数据抄读
[0123]	182	消耗计算

[0124]	186	接口
[0125]	188	通讯连接
[0126]	190	通讯连接
[0127]	192	通讯连接
[0128]	600	自动化设施
[0129]	602	计算机
[0130]	604	密钥生成模块
[0131]	606	签注模块
[0132]	608	网络
[0133]	610	索引服务器
[0134]	611	自动化设施

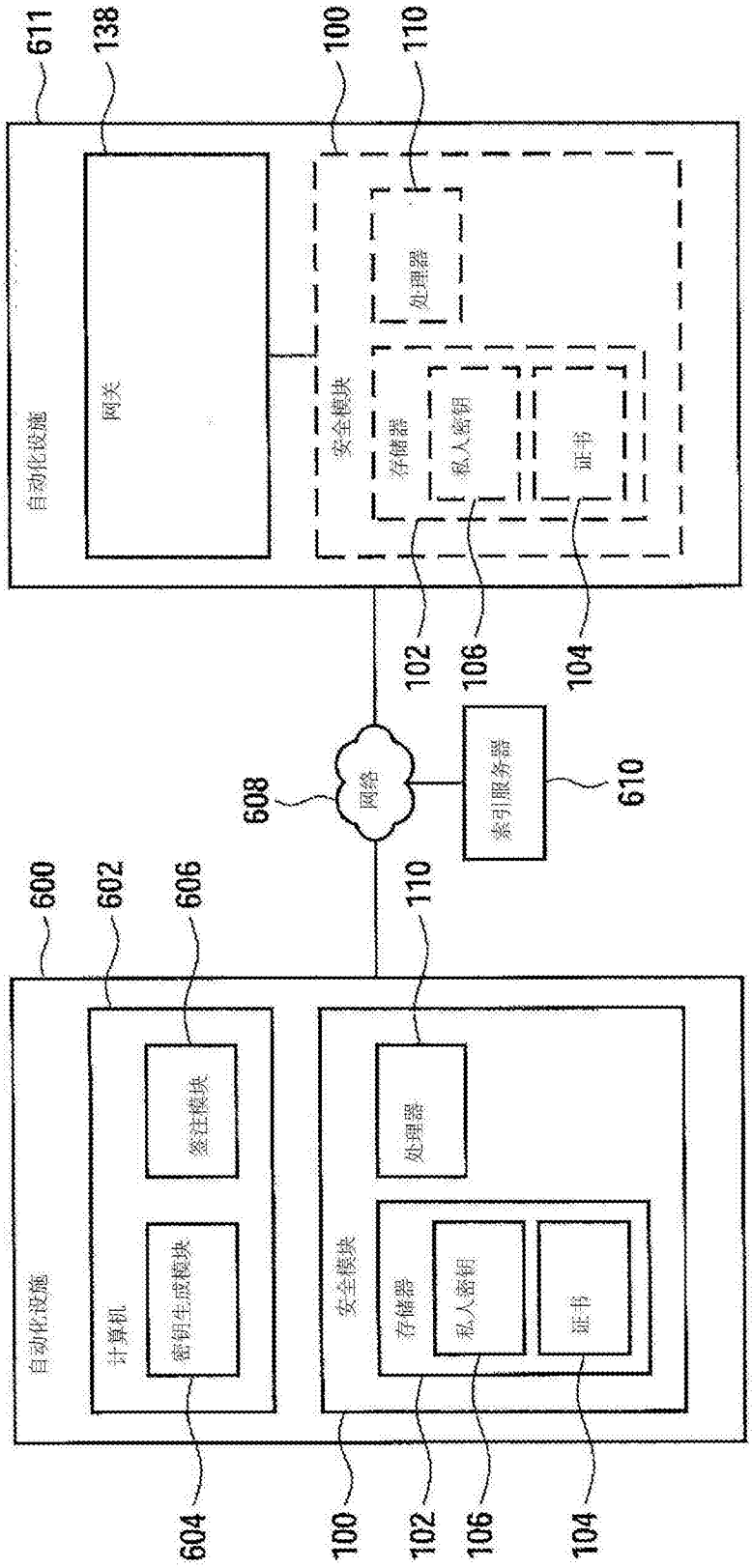

611
138
100
110
自动化设施
网关
安全模块
处理器
存储器
私人密钥
证书
102
106
104
608
网络
索引服务器
610
600
602
606
110
自动化设施
计算机
签注模块
密钥生成模块
处理器
安全模块
存储器
私人密钥
证书
604
100
102
106
104

图1

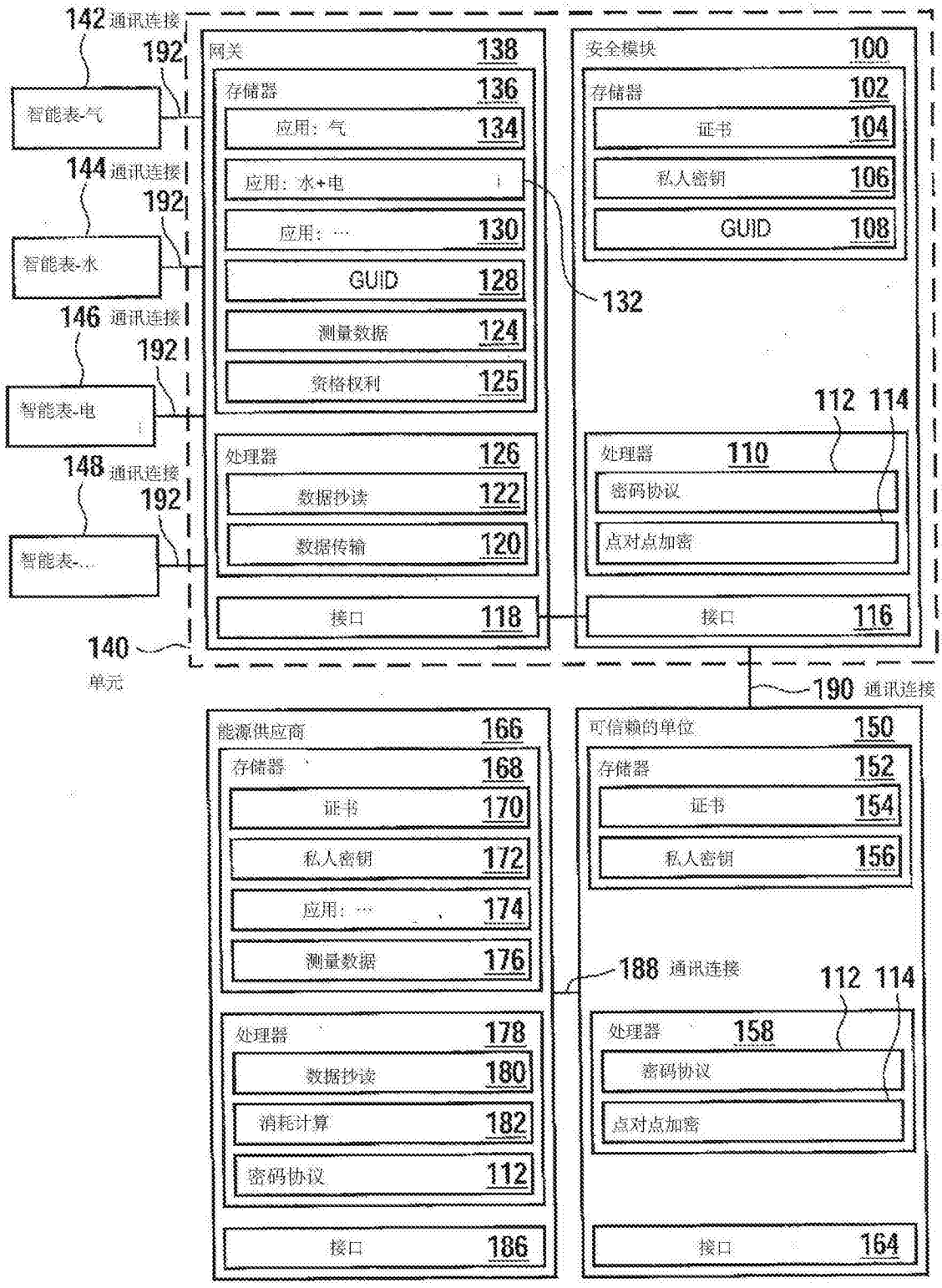

142 通讯连接
192
智能表-气
144 通讯连接
192
智能表-水
146 通讯连接
192
智能表-电
148 通讯连接
192
智能表-...
140
单元
网关 138
存储器 136
应用：气 134
应用：水+电
应用：... 130
GUID 128
测量数据 124
资格权利 125
处理器 126
数据抄读 122
数据传输 120
接口 118
安全模块 100
存储器 102
证书 104
私人密钥 106
GUID 108
132
112 114
处理器 110
密码协议
点对点加密
接口 116
190 通讯连接
能源供应商 166
存储器 168
证书 170
私人密钥 172
应用：... 174
测量数据 176
处理器 178
数据抄读 180
消耗计算 182
密码协议 112
接口 186
188 通讯连接
可信赖的单位 150
存储器 152
证书 154
私人密钥 156
112 114
处理器 158
密码协议
点对点加密
接口 164

图2

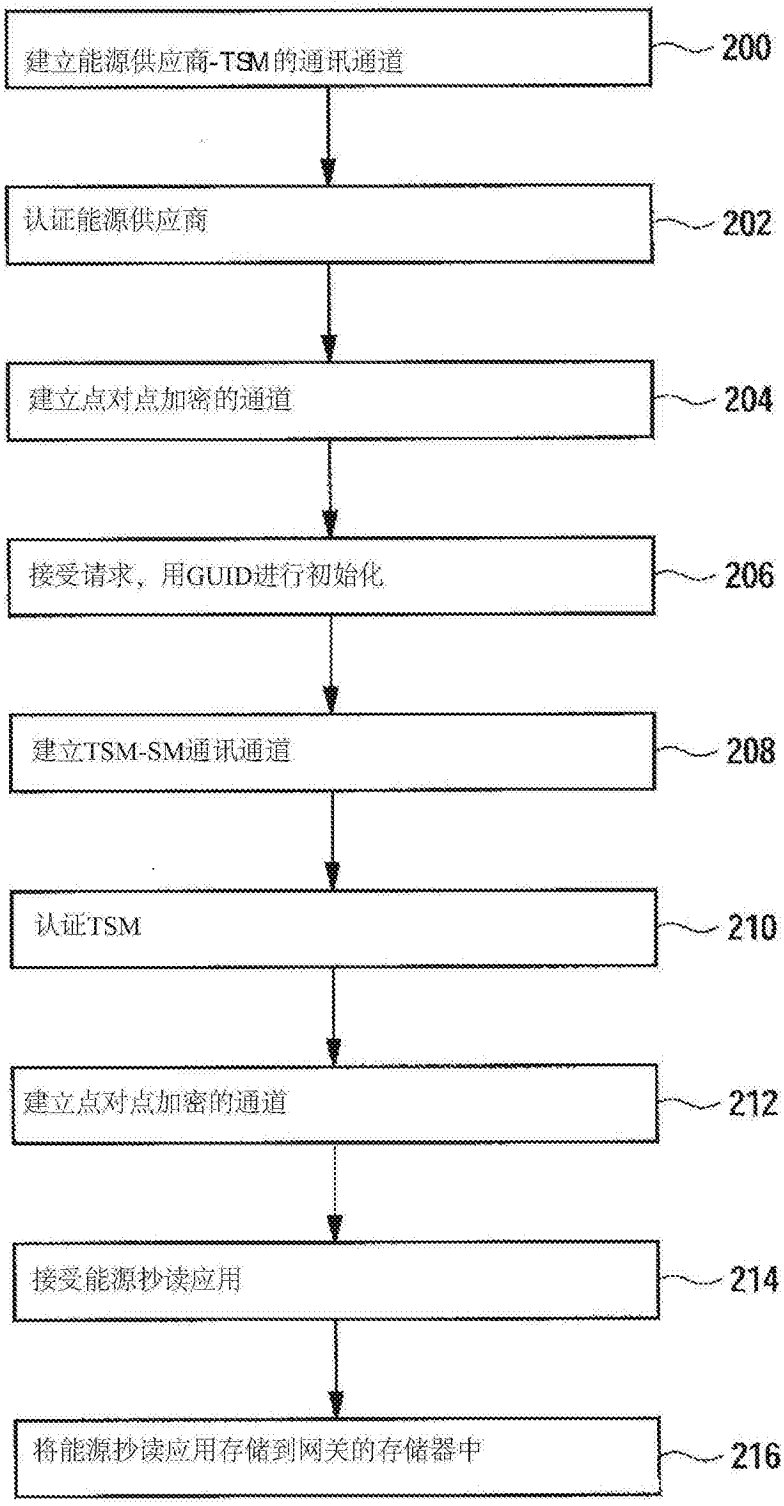

建立能源供应商-TSM的通讯通道
200
认证能源供应商
202
建立点对点加密的通道
204
接受请求，用GUID进行初始化
206
建立TSM-SM通讯通道
208
认证TSM
210
建立点对点加密的通道
212
接受能源抄读应用
214
将能源抄读应用存储到网关的存储器中
216

图3

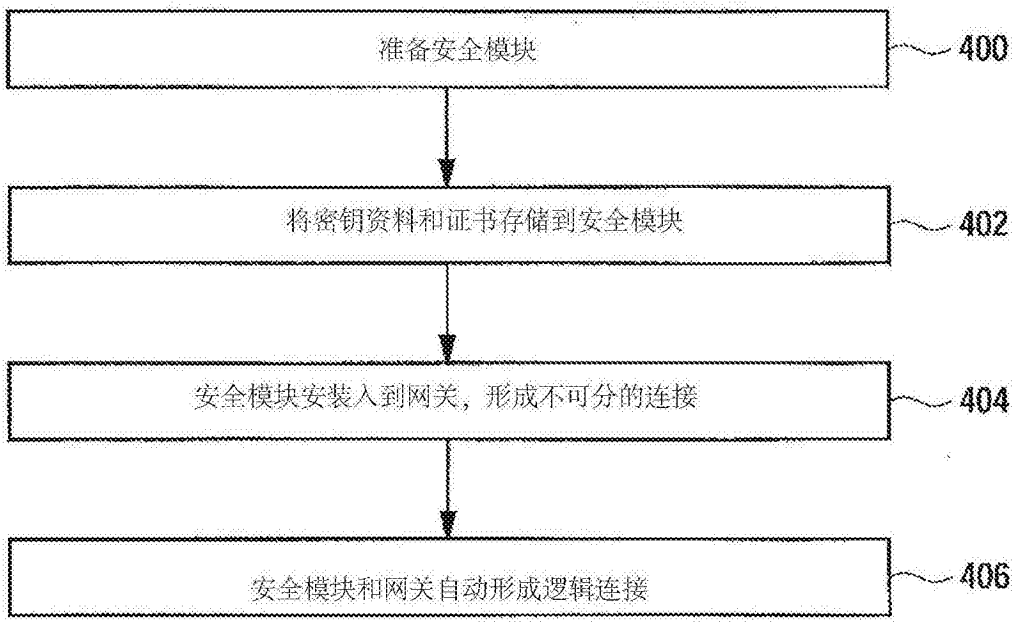

准备安全模块
400
将密钥资料和证书存储到安全模块
402
安全模块安装入到网关，形成不可分的连接
404
安全模块和网关自动形成逻辑连接
406

图4