

身份认证系统、方法、装置、设备及计算机可读存储介质

本申请实施例要求于 2020 年 11 月 12 日提交的申请号为 202011262480.0、发明名称为“身份认证系统、方法、装置、设备及计算机可读存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请实施例中。

技术领域

本申请实施例涉及安全技术领域，特别涉及一种身份认证系统、方法、装置、设备及计算机可读存储介质。

背景技术

在园区网或企业网等场景中，用户在购置了大量的终端设备之后，如物联网设备（Internet of things, IoT）、路由器、交换机、手机、个人电脑（personal computer, PC）机等，通常需要对购置的终端设备做统一的管理，如分配身份标识（identity document, ID）、下发配置信息等，以便终端设备在接入园区网或企业网时能够被正确识别，且能够与其他设备互联互通。而在对终端设备进行统一管理之前也需要对终端设备进行身份认证，以保证接入园区网或企业网的终端设备为园区或企业购置的设备。

在相关技术中，园区或企业的注册设备中存储有购置的所有终端设备的媒体接入控制（media access control, MAC）地址集合，终端设备入网时，首先搜索网络信号，在搜索到网络信号后，确定搜索到注册设备，之后向注册设备发送认证请求，认证请求携带终端设备的 MAC 地址，如果注册设备验证认证请求携带的 MAC 地址包含在自身存储的 MAC 地址集合中，则对终端设备的身份认证通过。

然而，由于 MAC 地址可以随意伪造或者篡改，因此，这种身份认证方法并不安全。另外，采用该方法时，如果终端设备搜索到恶意设备的网络信号，而向恶意设备发送认证请求，那么恶意设备也可以假装对终端设备的身份验证通过，进而在终端设备上植入信息，如恶意代码等，这样也是不安全的。

发明内容

本申请实施例提供了一种身份认证系统、方法、装置、设备及计算机可读存储介质，能够提高身份认证的安全性。所述技术方案如下：

第一方面，提供了一种身份认证系统，所述身份认证系统具有实现下述第二方面、第三方面、第四方面中身份认证方法行为的功能，请参照下述第二方面、第三方面、第四方面中的相关介绍。该身份认证系统包括终端设备、注册设备和授权设备，终端设备与授权设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系。

终端设备用于向注册设备发送第一认证请求，第一认证请求携带第一认证码，第一认证码根据第一对称密钥生成；

注册设备用于接收第一认证请求，根据第一认证请求生成第二认证请求，向授权设备发送第二认证请求，第二认证请求携带第一认证码；

授权设备用于接收第二认证请求，根据第一对称密钥和所有权关系记录验证第一认证码，在验证通过后向注册设备发送第一认证确认消息，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成；

注册设备还用于接收第一认证确认消息，根据第一认证确认消息确定第二认证确认消息，向终端设备发送第二认证确认消息，第二认证确认消息携带第二认证码；

终端设备还用于接收第二认证确认消息，根据第一对称密钥验证第二认证码，在验证通过后确定终端设备与注册设备的双向身份认证通过。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

第二方面，提供了一种身份认证方法，该方法由终端设备执行，终端设备与授权设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，该方法包括：

终端设备发送第一认证请求，第一认证请求携带第一认证码，第一认证码根据第一对称密钥生成；终端设备接收第二认证确认消息，第二认证确认消息是根据第一对称密钥和所有权关系记录对第一认证码验证通过后确定的，第二认证确认消息携带第二认证码，第二认证码由授权设备根据第一对称密钥生成；终端设备根据第一对称密钥验证第二认证码，在验证通过后确定终端设备与注册设备的双向身份认证通过。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

可选地，第一认证请求还携带第一 ID 和第一密钥参数，第一密钥参数包含第一认证向量（authentication vector，AV）的明文或密文，第一 ID 为终端设备的原所有者为终端设备配置的 ID；第一 AV 包含第一随机参数和第一防重放攻击参数，第一随机参数由终端设备生成，第一随机参数包含第一随机数 N1 和第二随机数 N2 中的至少一项；第一认证码根据第一对称密钥、第一 ID 和第一 AV 生成。

也即是，第一认证请求还携带终端设备的第一 ID，授权设备根据所有权关系记录验证第一认证请求携带的第一 ID，以确保终端设备是销售范围内的设备。第一认证请求还携带第一密钥参数，授权设备获取第一密钥参数中的第一随机参数和第一防重放攻击参数，根据第一防重放攻击参数验证本次身份认证是否受到重放攻击，第一随机参数用于授权设备验证第一认证码，也即验证终端身份的合法性。

可选地，第一 AV 的密文使用终端设备与授权设备共享的密钥加密得到。例如，使用第一对称密钥加密，或者根据第一对称密钥派生出来的密钥加密，以提高身份认证的安全性。

可选地，第一认证请求还携带第一身份信息，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个；第一认证码根据第一对称密钥、第一 ID、第一 AV 以及第一身份信息生成。也即是，第一认证请求还携带终端设备的接入网络的信息，授权设备根据所有权关系记录验证第一身份信息，以确保注册设备与所销售的终端设备的身份绑定关系。可选地，第一身份信息是终端设备在通过网络搜索到注册设备，向注册设备发送入网请求之后，注册设备响应给终端设备的信息。

可选地，第二认证确认消息还携带第二密钥参数；终端设备根据第一对称密钥验证第二认证码，包括：终端设备根据第一对称密钥和第二密钥参数生成对称验证密钥；终端设备根据对称验证密钥验证第二认证码。

也即是，授权设备将生成第二认证码所用的第二密钥参数响应给终端设备，终端设备根据第一对称密钥和第二密钥参数验证第二认证码，实现对称密钥验证授权设备的签名合法性。需要说明的是，前述第一认证码可以理解为终端设备的签名，第二认证码可以理解为授权设备的签名。

可选地，终端设备确定终端设备与注册设备的双向身份认证通过之后，还包括：终端设备根据第一对称密钥和第一派生参数，生成通道安全密钥，第一派生参数根据第二密钥参数确定；终端设备与注册设备之间基于通道安全密钥建立第一安全传输通道；终端设备根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权，第二派生参数根据第二密钥参数确定。

也即是，在终端设备与注册设备通过授权设备实现基于对称密钥的双向身份认证之后，终端设备与注册设备还能够基于授权设备的响应，建立安全传输通道以及协商第二对称密钥，也即，第一对称密钥仅在终端设备与授权设备之间共享，在终端设备与注册设备协商第二对称密钥之后，第二对称密钥仅在终端设备与注册设备之间共享，作为终端设备与注册设备之间新的设备密钥。

可选地，终端设备根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥，包括：终端设备生成随机数 N4，并将 N4 通过第一安全传输通道发送给注册设备，N4 用于注册设备根据 N4 和第二协商密钥生成第二对称密钥，以及根据 N4 和第二对称密钥生成第三认证码，第二协商密钥由授权设备根据第二派生参数生成并发送给注册设备；终端设备根据 N4 和第二派生参数生成第二对称密钥；终端设备接收注册设备发送的第一协商确认消息，第一协商确认消息携带第三认证码；终端设备根据自身生成的第二对称密钥和 N4 验证第三认证码，在验证通过后，将第二对称密钥更新为自身与注册设备之间的设备密钥，并向注册设备发送第二协商确认消息，第二协商确认消息用于指示注册设备将第二对称密钥更新为自身与终端设备之间的设备密钥。

也即是，终端设备与注册设备之间根据终端设备生成的随机数 N4 来协商第二对称密钥。

可选地，终端设备根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥，包括：终端设备接收注册设备通过第一安全传输通道发送的随机数 N5，N5 由注册设备随机生成，N5 用于注册设备根据 N5 和第二协商密钥生成第二对称密钥，并将第二对称密钥更新为自身与终端设备之间的设备密钥；终端设备根据 N5 和第二派生参数生成第二对

称密钥，将第二对称密钥更新为自身与注册设备之间的设备密钥。

也即是，终端设备与注册设备之间也能够根据注册设备生成的随机数 N_5 来协商第二对称密钥。

可选地，终端设备根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥之后，还包括：终端设备接收注册设备通过第一安全传输通道发送的第二 ID 和配置信息中的至少一个，第二 ID 是终端设备的当前所有者为终端设备生成的 ID，例如注册设备为终端设备生成的 ID，或注册设备所属网络中的控制器为终端设备生成的 ID，配置信息为终端设备的当前所有者为终端设备下发的配置文件。第二 ID 为终端设备在注册设备所属网络范围内唯一的 ID，第二 ID 也用于终端设备接入注册设备所属网络时的入网身份鉴权。

第三方面，提供了一种身份认证方法，该方法由注册设备执行，该方法包括：

注册设备接收第一认证请求，第一认证请求携带第一认证码，第一认证码由终端设备根据第一对称密钥生成，终端设备与授权设备共享第一对称密钥；注册设备根据第一认证请求生成第二认证请求，向授权设备发送第二认证请求，第二认证请求携带第一认证码；注册设备接收第一认证确认消息，第一认证确认消息是授权设备根据第一对称密钥和终端设备的所有权关系记录对第一认证码验证通过后确定的，授权设备存储有该所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成；注册设备根据第一认证确认消息确定第二认证确认消息，向终端设备发送第二认证确认消息，第二认证确认消息携带第二认证码，第二认证确认消息用于指示终端设备根据第一对称密钥对第二认证码验证通过后确定终端设备与注册设备的双向身份认证通过。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

可选地，第一认证请求还携带第一 ID，第一 ID 为终端设备的原所有者为终端设备配置的 ID，第二认证请求还携带第一认证请求中的第一 ID，第二认证请求还携带第一身份信息，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个。

可选地，在第一认证请求未携带第一身份信息的情况下，第二认证请求中携带的第一身份信息由注册设备添加。

可选地，第二认证请求还携带注册设备的身份签名，注册设备的身份签名是注册设备使用私钥对第一认证请求和第一身份信息进行的签名。

可选地，注册设备的身份信息包括注册设备身份相关的数字证书和注册设备身份相关的数字证书的摘要中的至少一个。

可选地，第一认证确认消息还携带密钥更新信息，密钥更新信息使用注册设备与授权设备共享的对称密钥加密保护，或者，密钥更新信息使用注册设备的公钥加密保护；

注册设备接收第一认证确认消息之后，还包括：注册设备从密钥更新信息中获取通道安

全密钥；注册设备向终端设备发送第二认证确认消息之后，还包括：注册设备与终端设备之间基于通道安全密钥建立第一安全传输通道；注册设备根据密钥更新信息，与终端设备之间通过第一安全传输通道协商第二对称密钥，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。

也即是，注册设备与终端设备还能够根据授权设备的响应，建立安全传输通道，以及协商第二对称密钥。

可选地，注册设备根据密钥更新信息，与终端设备之间通过第一安全传输通道协商第二对称密钥之后，还包括：注册设备通过第一安全传输通道向终端设备发送第二 ID 和配置信息中的至少一个，第二 ID 是终端设备的当前所有者为终端设备生成的 ID，配置信息为终端设备的当前所有者为终端设备下发的配置文件。第二 ID 为终端设备在注册设备所属网络范围内唯一的 ID，第二 ID 也用于终端设备接入注册设备所属网络时的入网身份鉴权。

第四方面，提供了一种身份认证方法，该方法由授权设备执行，授权设备与终端设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，该方法包括：

授权设备接收第二认证请求，第二认证请求携带第一认证码，第一认证码由终端设备根据第一对称密钥生成；授权设备根据第一对称密钥和所有权关系记录验证第一认证码；在验证通过后，授权设备发送第一认证确认消息，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成，第二认证码指示终端设备根据第一对称密钥对第二认证码验证通过后确定终端设备与注册设备的双向身份认证通过。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

可选地，第二认证请求还携带第一 ID、第一密钥参数和第一身份信息，第一密钥参数由终端设备生成，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个，第一 ID 为终端设备的原所有者为终端设备配置的 ID，所有权关系记录包含第一 ID 与第一身份信息之间的映射关系；授权设备接收第二认证请求之后，还包括：授权设备根据所有权关系记录验证第一 ID，以及验证第一身份信息；授权设备根据第一对称密钥和所有权关系记录验证第一认证码，包括：授权设备根据所有权关系记录、第一 ID、第一对称密钥和第一密钥参数，验证第一认证码。

也即是，授权设备根据所有权关系记录验证终端设备与注册设备的身份。另外，将终端设备生成第一认证码所用的第一密钥参数发送给授权设备，授权设备根据第一密钥参数和第一对称密钥实现基于对称密钥的方式验证第一认证码。

可选地，第一认证确认消息还携带第二密钥参数，第二密钥参数包含第二 AV 的明文或密文，第二 AV 的密文是使用授权设备与终端设备共享的密钥得到；第二 AV 包含第二防重放攻击参数，第二认证码根据第一对称密钥和第二 AV 生成，第一认证确认消息还用于终端设

备根据第一对称密钥和第二密钥参数验证第二认证码。

也即是，授权设备的响应还携带第二密钥参数，终端设备能够根据第二密钥参数和第一对称密钥实现基于对称密钥的方式验证第二认证码，以确保授权设备的签名合法性。

可选地，第一认证确认消息还携带密钥更新信息，密钥更新信息根据第一对称密钥和第二 AV 生成；密钥更新信息用于注册设备获取与终端设备之间建立第一安全传输通道所需的通道安全密钥，以及与终端设备之间通过第一安全传输通道协商第二对称密钥，第二密钥参数还用于终端设备确定生成通道安全密钥所需的第一派生参数，以及确定与注册设备之间通过第一安全传输通道协商第二对称密钥所需的第二派生参数，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。

也即是，授权设备的响应中还携带密钥更新信息，注册设备能够从该密钥更新信息中获取通道安全密钥，以与终端设备之间建立安全传输通道，注册设备还能够从密钥更新信息中获取协商密钥与终端设备之间协商第二对称密钥。终端设备能够根据授权设备响应的第二密钥参数确定生成通道安全密钥的参数，以及根据第二密钥参数确定协商第二对称密钥的参数。

第五方面，提供了一种身份认证装置，所述身份认证装置具有实现上述第二方面中身份认证方法行为的功能。所述身份认证装置包括一个或多个模块，该一个或多个模块用于实现上述第二方面所提供的身份认证方法。

也即是，提供了一种身份认证装置，该装置应用于终端设备，终端设备与授权设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，该装置包括：

发送模块，用于发送第一认证请求，第一认证请求携带第一认证码，第一认证码根据第一对称密钥生成；

接收模块，用于接收第二认证确认消息，第二认证确认消息是根据第一对称密钥和所有权关系记录对第一认证码验证通过后确定的，第二认证确认消息携带第二认证码，第二认证码由授权设备根据第一对称密钥生成；

验证模块，用于根据第一对称密钥验证第二认证码，在验证通过后确定终端设备与注册设备的双向身份认证通过。

可选地，第一认证请求还携带第一 ID 和第一密钥参数，第一密钥参数包含第一认证向量 AV 的明文或密文，第一 ID 为终端设备的原所有者为终端设备配置的 ID；

第一 AV 包含第一随机参数和第一防重放攻击参数，第一随机参数由终端设备生成，第一随机参数包含第一随机数 N1 和第二随机数 N2 中的至少一项；

第一认证码根据第一对称密钥、第一 ID 和第一 AV 生成。

可选地，第一认证请求还携带第一身份信息，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个；

第一认证码根据第一对称密钥、第一 ID、第一 AV 以及第一身份信息生成。

可选地，第二认证确认消息还携带第二密钥参数；

验证模块包括：

第一生成子模块，用于根据第一对称密钥和第二密钥参数生成对称验证密钥；

验证子模块，用于根据对称验证密钥验证第二认证码。

可选地，该装置还包括：

生成模块，用于根据第一对称密钥和第一派生参数，生成通道安全密钥，第一派生参数根据第二密钥参数确定；

建立模块，用于与注册设备之间基于通道安全密钥建立第一安全传输通道；

协商模块，用于根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权，第二派生参数根据第二密钥参数确定。

可选地，协商模块包括：

第二生成子模块，用于生成随机数 N4，并将 N4 通过第一安全传输通道发送给注册设备，N4 用于注册设备根据 N4 和第二协商密钥生成第二对称密钥，以及根据 N4 和第二对称密钥生成第三认证码，第二协商密钥由授权设备根据第二派生参数生成并发送给注册设备；

第三生成子模块，用于根据 N4 和第二派生参数生成第二对称密钥；

第一接收子模块，用于接收注册设备发送的第一协商确认消息，第一协商确认消息携带第三认证码；

第一更新子模块，用于根据自身生成的第二对称密钥和 N4 验证第三认证码，在验证通过后，将第二对称密钥更新为自身与注册设备之间的设备密钥，并向注册设备发送第二协商确认消息，第二协商确认消息用于指示注册设备将第二对称密钥更新为自身与终端设备之间的设备密钥。

可选地，协商模块包括：

第二接收子模块，用于接收注册设备通过第一安全传输通道发送的随机数 N5，N5 由注册设备随机生成，N5 用于注册设备根据 N5 和第二协商密钥生成第二对称密钥，并将第二对称密钥更新为自身与终端设备之间的设备密钥；

第二更新子模块，用于根据 N5 和第二派生参数生成第二对称密钥，将第二对称密钥更新为自身与注册设备之间的设备密钥。

第六方面，提供了一种身份认证装置，所述身份认证装置具有实现上述第三方面中身份认证方法行为的功能。所述身份认证装置包括一个或多个模块，该一个或多个模块用于实现上述第三方面所提供的身份认证方法。

也即是，提供了一种身份认证装置，该装置应用于注册设备，该装置包括：

第一接收模块，用于接收第一认证请求，第一认证请求携带第一认证码，第一认证码由终端设备根据第一对称密钥生成，终端设备与授权设备共享第一对称密钥；

第一发送模块，用于根据第一认证请求生成第二认证请求，向授权设备发送第二认证请求，第二认证请求携带第一认证码；

第二接收模块，用于接收第一认证确认消息，第一认证确认消息是授权设备根据第一对称密钥和终端设备的所有权关系记录对第一认证码验证通过后确定的，授权设备存储有该所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成；

第二发送模块，用于根据第一认证确认消息确定第二认证确认消息，向终端设备发送第

第二认证确认消息，第二认证确认消息携带第二认证码，第二认证确认消息用于指示终端设备根据第一对称密钥对第二认证码验证通过后确定终端设备与注册设备的双向身份认证通过。

可选地，第一认证请求还携带第一 ID，第一 ID 为终端设备的原所有者为终端设备配置的 ID，第二认证请求还携带第一认证请求中的第一 ID，第二认证请求还携带第一身份信息，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个。

可选地，第二认证请求还携带注册设备的身份签名，注册设备的身份签名是注册设备使用私钥对第一认证请求和第一身份信息进行的签名。

可选地，注册设备的身份信息包括注册设备身份相关的数字证书和注册设备身份相关的数字证书的摘要中的至少一个。

可选地，第一认证确认消息还携带密钥更新信息，密钥更新信息使用注册设备与授权设备共享的对称密钥加密保护，或者，密钥更新信息使用注册设备的公钥加密保护；

该装置还包括：

获取模块，用于从密钥更新信息中获取通道安全密钥；

建立模块，用于与终端设备之间基于通道安全密钥建立第一安全传输通道；

协商模块，用于根据密钥更新信息，与终端设备之间通过第一安全传输通道协商第二对称密钥，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。

第七方面，提供了一种身份认证装置，所述身份认证装置具有实现上述第四方面中身份认证方法行为的功能。所述身份认证装置包括一个或多个模块，该一个或多个模块用于实现上述第四方面所提供的身份认证方法。

也即是，提供了一种身份认证装置，该装置应用于授权设备，授权设备与终端设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，该装置包括：

接收模块，用于接收第二认证请求，第二认证请求携带第一认证码，第一认证码由终端设备根据第一对称密钥生成；

第一验证模块，用于根据第一对称密钥和所有权关系记录验证第一认证码；

发送模块，用于在验证通过后，授权设备发送第一认证确认消息，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成，第二认证码指示终端设备根据第一对称密钥对第二认证码验证通过后确定终端设备与注册设备的双向身份认证通过。

可选地，第二认证请求还携带第一 ID、第一密钥参数和第一身份信息，第一密钥参数由终端设备生成，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个，第一 ID 为终端设备的原所有者为终端设备配置的 ID，该所有权关系记录包含第一 ID 与第一身份信息之间的映射关系；

该装置还包括：

第二验证模块，用于根据所有权关系记录验证第一 ID，以及验证第一身份信息；

第一验证模块包括：

验证子模块，用于根据所有权关系记录、第一 ID、第一对称密钥和第一密钥参数，验证第一认证码。

可选地，第一认证确认消息还携带第二密钥参数，第二密钥参数包含第二 AV 的明文或密文，第二 AV 的密文是使用授权设备与终端设备共享的密钥得到；

第二 AV 包含第二防重放攻击参数，第二认证码根据第一对称密钥和第二 AV 生成，第一认证确认消息还用于终端设备根据第一对称密钥和第二密钥参数验证第二认证码。

可选地，第一认证确认消息还携带密钥更新信息，密钥更新信息根据第一对称密钥和第二 AV 生成；

密钥更新信息用于注册设备获取与终端设备之间建立第一安全传输通道所需的通道安全密钥，以及与终端设备之间通过第一安全传输通道协商第二对称密钥，第二密钥参数还用于终端设备生成通道安全密钥，以及与注册设备之间通过第一安全传输通道协商第二对称密钥，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。

第八方面，提供了一种身份认证设备，所述身份认证设备包括处理器和存储器，所述存储器用于存储执行上述第二方面、第三方面或第四方面所提供的身份认证方法的程序，以及存储用于实现上述第二方面、第三方面或第四方面所提供的身份认证方法所涉及的数据。所述处理器被配置为用于执行所述存储器中存储的程序。所述存储设备的操作装置还可以包括通信总线，该通信总线用于该处理器与存储器之间建立连接。

第九方面，提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述第二方面、第三方面或第四方面所述的身份认证方法。

第十方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第二方面、第三方面或第四方面所述的身份认证方法。

上述第一方面、第三方面、第四方面、第五方面、第六方面、第七方面、第八方面、第九方面和第十方面所获得的技术效果与第二方面中对应的技术手段获得的技术效果近似，在这里不再赘述。

本申请实施例提供的技术方案至少能够带来以下有益效果：

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

附图说明

图 1 是本申请实施例提供的一种身份认证方法所涉及的系统架构图；

图 2 是本申请实施例提供的另一种身份认证方法所涉及的系统架构图；

图 3 是本申请实施例提供的一种计算机设备的结构示意图；

图 4 是本申请实施例提供的一种身份认证方法的流程图；

图 5 是本申请实施例提供的一种 EST 阶段的流程图；
图 6 是本申请实施例提供的另一种身份认证方法的流程图；
图 7 是本申请实施例提供的一种身份认证装置的结构示意图；
图 8 是本申请实施例提供的另一种身份认证装置的结构示意图；
图 9 是本申请实施例提供的又一种身份认证装置的结构示意图；
图 10 是本申请实施例提供的又一种身份认证装置的结构示意图；
图 11 是本申请实施例提供的又一种身份认证装置的结构示意图。

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

图 1 是本申请实施例提供的一种身份认证方法所涉及的系统架构图。参见图 1，该系统架构包括终端设备 101、注册设备 102 和授权设备 103。其中，终端设备 101 与注册设备 102 能够通过有线或无线方式与注册设备 102 连接以进行通信，注册设备 102 能够与授权设备 103 通过有线或无线方式连接以进行通信。

终端设备 101 用于向注册设备 102 发送第一认证请求，第一认证请求携带第一认证码，第二认证码根据第一对称密钥生成。

在本申请实施例中，终端设备 101 在出厂时被植入第一对称密钥，第一对称密钥是终端设备 101 与授权设备 103 共享的设备密钥，第一对称密钥作为一个对称密钥，本申请实施例基于对称密钥实现终端设备 101 与注册设备 102 的双向身份认证。

可选地，终端设备 101 在出厂时还被植入第一 ID，第一 ID 是终端设备 101 的原所有者为终端设备 101 配置的 ID，第一认证请求还携带第一 ID。

注册设备 102 用于接收终端设备 101 发送的第一认证请求，根据第一认证请求生成第二认证请求，向授权设备 103 发送第二认证请求。示例性地，在第一认证请求不携带注册设备 102 的身份信息的情况下，注册设备 102 将自身的身份信息添加在第一认证请求中，得到第二认证请求。

可选地，注册设备 102 存储有终端设备 101 的购置记录，注册设备 102 根据购置记录验证第一认证请求携带的第一 ID，在验证通过后根据第一认证请求生成第二认证请求，向授权设备 103 发送第二认证请求。

授权设备 103 存储有终端设备 101 的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，授权设备 103 用于在接收到第二认证请求之后，根据第一对称密钥和该所有权关系记录对第二认证请求进行验证，例如根据该所有权关系记录验证第一 ID、验证注册设备的身份信息，根据该所有权关系记录和第一对称密钥验证第一认证码。在验证通过后，授权设备 103 向注册设备 102 发送第一认证确认消息，第一认证确认

消息用于指示授权终端设备 101 与注册设备 102 所属网络的所有权关系。其中，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成。

注册设备 102 还用于在接收授权设备 103 发送的第一认证确认消息之后，确定终端设备的身份合法性，根据第一认证确认消息确定第二认证确认消息，向终端设备 101 发送第二认证确认消息，第二认证确认消息携带第二认证码。

终端设备 101 还用于接收注册设备 102 发送第二认证确认消息，根据第一对称密钥验证第二认证确认消息携带的第二认证码，在验证通过后确定终端设备 101 与注册设备 102 的双向身份认证通过。

可选地，上述身份认证的过程可以看作一个授权互信阶段。

可选地，终端设备 101 还用于在部署之后通过网络搜索注册设备 102，在搜索到注册设备 102 之后，首先向注册设备 102 发送入网请求，在注册设备 102 根据该入网请求响应终端设备 101 之后，终端设备 101 再生成第一认证请求。也即是，在授权互信阶段之前，还包括一个入网发现阶段。

可选地，终端设备 101 可能不支持互联网协议（Internet protocol，IP）栈，也即不具备生成 IP 包的功能，例如一些不支持 IP 协议栈的物联网设备，在这种情况下，该系统架构还包括入网代理设备 104，入网代理设备 104 与注册设备 102 通过有线或无线方式连接进行通信。终端设备 101 通过网络搜索并连接上入网代理设备 104 后，通过入网代理设备 104 向注册设备 102 发送消息，入网代理设备 104 用于接收终端设备 101 向注册设备 102 发送的消息，并封装为 IP 包后转发给注册设备 102，入网代理设备 104 还用于接收并转发注册设备 102 向终端设备 101 发送的消息，以实现终端设备 101 与注册设备 102 之间的网络通信。

可选地，无论终端设备 101 是否支持 IP 栈，该系统架构中均可以还包括入网代理设备 104，也即通过入网代理设备 104 实现终端设备 101 与注册设备 102 之间的通信。

可选地，终端设备 101 还用于在确定终端设备 101 与注册设备 102 的双向身份认证通过之后，与注册设备 102 之间建立第一安全传输通道来协商第二对称密钥，第二对称密钥用于终端设备 101 接入注册设备 102 所属网络时的入网身份鉴权。

也即是，第一对称密钥作为旧的设备密钥，旧的设备密钥仅在终端设备 101 与授权设备 103 之间共享，用于通过授权设备 103 实现上述双向身份认证，第二对称密钥作为终端设备 101 与注册设备 102 之间协商出的新的设备密钥，新的设备密钥仅在终端设备 101 与注册设备 102 之间共享，用于终端设备 101 接入注册设备 102 所属网络时的入网身份鉴权。

可选地，终端设备 101 还用于在与注册设备 102 协商第二对称密钥之后，接收注册设备 102 下发的第二 ID 和配置信息等中的至少一个。注册设备 102 还用于在与注册设备 102 协商第二对称密钥之后，向终端设备 101 下发第二 ID 和配置信息等中的至少一个。第二 ID 为终端设备 102 的当前所有者为终端设备 101 分配的新的身份标识，配置信息为终端设备 101 的当前所有者为终端设备 101 下发的配置文件，注册设备 102 下发的第二 ID 也用于终端设备 101 接入注册设备 102 所属网络时的入网身份鉴权。

可选地，该系统架构还包括控制器，控制器与注册设备 102 通过有线或无线方式连接以进行通信。注册设备 102 还用于在协商第二对称密钥之后，向控制器发送配置请求，控制器用于在接收到该配置请求之后，生成第二 ID，向注册设备 102 发送第二 ID、配置信息等，注册设备 102 将第二 ID、配置信息等下发给终端设备 101。或者，控制器用于在接收到该配置

请求之后，直接向终端设备 101 发送第二 ID、配置信息等。可选地，配置请求中携带第一 ID 和第二对称密钥，控制器还用于存储、管理和维护终端设备与对应的设备密钥的映射关系，例如，对应存储第一 ID、第二 ID 与第二对称密钥。

可选地，上述建立第一安全传输通道来协商第二对称密钥，以及后续下发第二 ID、配置信息等的过程，可以看作一个基于安全传输的注册（enrollment over secure transport, EST）阶段，也即是，在授权互信阶段之后，还包括一个 EST 阶段。

需要说明的是，本申请实施例仅以一个终端设备 101 的身份认证过程为例进行介绍，该系统架构中可以包括多个终端设备 101，例如该多个终端设备 101 为园区或企业购买的一批物联网设备，该多个终端设备 101 中的每个终端设备 101 部署之后均可以按照上述所介绍的方法，通过注册设备 102 和授权设备 103 进行身份认证。

可选地，该系统架构包括多个注册设备 102，该多个注册设备 102 中的每个注册设备 102 用于对该多个终端设备 101 中的至少一个终端设备 101 进行身份认证，控制器用于与该多个注册设备 102 进行通信，该多个终端设备 101 的新的 ID 和配置信息的管理和下发统一由控制器处理，而该多个注册设备 102 需要代替该多个终端设备 101 向控制器申请新的 ID 和配置信息，该多个注册设备 102 还用于把新的设备密钥（第二对称密钥）发送给控制器统一维护和管理。

在本申请实施例中，终端设备 101 为物联网设备（Internet of things, IoT）、路由器、交换机、手机、个人电脑（personal computer, PC）机等中任何一种，注册设备 102 为服务器、网关设备等设备，授权设备 103 为服务器，服务器是指一台服务器，或者由多台服务器构成的服务器集群，或者一个云计算服务中心。入网代理设备 104 为交换机、路由器、无线保真（wireless fidelity, WiFi）设备等。

图 2 是本申请实施例提供的另一种身份认证方法所涉及的系统架构图。该系统架构包括终端设备、入网代理设备（join proxy, JP）、注册设备（registrer, REG）、控制器（controller, CON）和授权设备。可选地，JP、REG 和 CON 可以看作一个客户网络系统。

接下来参照图 2 对本申请实施例提供的身份认证方法的一个实施例进行简单介绍。

在本申请实施例中，终端设备与授权设备共享第一对称密钥（SK_{old}），授权设备存储有终端设备的所有权关系记录。可选地，注册设备存储有终端设备的购置记录。

1、终端设备通过入网发现（discovery）搜索到 JP。

2、终端设备通过 JP 向 REG 发送第一认证请求（voucher request, VReq1），第一认证请求携带第一认证码，第一认证码根据 SK_{old} 生成。

3、REG 与授权设备之间建立安全传输层（transport layer security, TLS）通道。

4、REG 通过 TLS 通道向授权设备发送第二认证请求（VReq2），第二认证请求携带第一认证码。可选地，注册设备先根据购置记录验证第一认证请求。

5、授权设备根据 SK_{old} 和所有权关系记录验证第二认证请求，验证通过后响应注册设备第一认证确认消息（voucher response, VResp1），第一认证确认消息携带第二认证码，第二认证码根据 SK_{old} 生成，第一认证确认消息指示终端设备与注册设备所属网络的所有权关系。

6、REG 根据授权设备的响应确定第二认证确认消息（VResp2），将第二认证确认消息通过 JP 发送给终端设备。终端设备验证第二认证确认消息之后，双向身份认证通过。

7、可选地，终端设备与 REG 之间基于授权设备的响应，建立 TLS 通道并协商第二对称密钥 (SK_{new})。

8、REG 向 CON 发送配置请求。

9、CON 向 REG 响应第二 ID (ID_{new})、配置信息。

10、REG 将 ID_{new} 、配置信息通过 JP 下发给终端设备。

请参考图 3，图 3 是根据本申请实施例示出的一种计算机设备的结构示意图。可选地，该计算机设备为图 1 或图 2 中所示的终端设备 101、注册设备 102 或授权设备 103。该计算机设备包括一个或多个处理器 301、通信总线 302、存储器 303 以及一个或多个通信接口 304。

处理器 301 为一个通用中央处理器 (central processing unit, CPU)、网络处理器 (NP)、微处理器、或者为一个或多个用于实现本申请方案的集成电路，例如，专用集成电路 (application-specific integrated circuit, ASIC)、可编程逻辑器件 (programmable logic device, PLD) 或其组合。可选地，上述 PLD 为复杂可编程逻辑器件 (complex programmable logic device, CPLD)、现场可编程逻辑门阵列 (field-programmable gate array, FPGA)、通用阵列逻辑 (generic array logic, GAL) 或其任意组合。

通信总线 302 用于在上述组件之间传送信息。可选地，通信总线 302 分为地址总线、数据总线、控制总线等。为便于表示，图中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

可选地，存储器 303 为只读存储器 (read-only memory, ROM)、随机存取存储器 (random access memory, RAM)、电可擦可编程只读存储器 (electrically erasable programmable read-only memory, EEPROM)、光盘 (包括只读光盘 (compact disc read-only memory, CD-ROM)、压缩光盘、激光盘、数字通用光盘、蓝光光盘等)、磁盘存储介质或者其它磁存储设备，或者是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其它介质，但不限于此。存储器 303 独立存在，并通过通信总线 302 与处理器 301 相连接，或者，存储器 303 与处理器 301 集成在一起。

通信接口 304 使用任何收发器一类的装置，用于与其它设备或通信网络通信。通信接口 304 包括有线通信接口，可选地，还包括无线通信接口。其中，有线通信接口例如以太网接口等。可选地，以太网接口为光接口、电接口或其组合。无线通信接口为无线局域网 (wireless local area networks, WLAN) 接口、蜂窝网络通信接口或其组合等。

可选地，在一些实施例中，计算机设备包括多个处理器，如图 3 中所示的处理器 301 和处理器 305。这些处理器中的每一个为一个单核处理器，或者一个多核处理器。可选地，这里的处理器指一个或多个设备、电路、和/或用于处理数据 (如计算机程序指令) 的处理核。

在具体实现中，作为一种实施例，计算机设备还包括输出设备 306 和输入设备 307。输出设备 306 和处理器 301 通信，能够以多种方式来显示信息。例如，输出设备 306 为液晶显示器 (liquid crystal display, LCD)、发光二极管 (light emitting diode, LED) 显示设备、阴极射线管 (cathode ray tube, CRT) 显示设备或投影仪 (projector) 等。输入设备 307 和处理器 301 通信，能够以多种方式接收用户的输入。例如，输入设备 307 是鼠标、键盘、触摸屏设备或传感设备等。

在一些实施例中，存储器 303 用于存储执行本申请方案的程序代码 310，处理器 301 能

够执行存储器 303 中存储的程序代码 310。该程序代码 310 中包括一个或多个软件模块，该计算机设备能够通过处理器 301 以及存储器 303 中的程序代码 310，来实现下文图 4 实施例提供的身份认证方法。

图 4 是本申请实施例提供的一种身份认证方法的流程图。请参考图 4，该方法包括如下步骤。

步骤 401：终端设备向注册设备发送第一认证请求，第一认证请求携带第一认证码，第一认证码根据第一对称密钥生成，第一对称密钥为终端设备与授权设备共享的密钥。

在本申请实施例中，终端设备与授权设备共享第一对称密钥，也即终端设备在出厂时被植入第一对称密钥，例如，终端设备的硬件或固件中被植入第一对称密钥。

其中，第一对称密钥作为一个对称密钥，用于通过授权设备实现对终端设备与注册设备的双向身份认证。也即是，本申请实施例提供了一种基于对称密码技术的身份认证机制，能够实现园区网或企业网中终端设备的安全入网。

在本申请实施例中，终端设备根据第一对称密钥生成第一认证码，根据第一认证码生成第一认证请求，第一认证请求携带第一认证码，终端设备将第一认证请求发送给注册设备。在另一些实施例中，认证码也可以称为消息鉴别码、消息认证码、消息签名等。可选地，终端设备通过入网代理设备将第一认证请求发送给注册设备。

需要说明的是，在本申请实施例中，终端设备根据第一对称密钥生成携带第一认证码的第一认证请求的实现方式有很多，接下来详细介绍其中的一种实现方式。

在本申请实施例中，第一认证码根据第一对称密钥、第一 ID 和第一 AV 生成。其中，第一 ID 为终端设备的原所有者为终端设备配置的 ID，原所有者为终端设备的制造商或者集成商等。终端设备在出厂时还被植入第一 ID，例如，终端设备的硬件或固件中被植入第一 ID。第一 AV 包含第一随机参数和第一防重放攻击参数，第一随机参数由终端设备生成，第一随机参数包含第一随机数 N1 和第二随机数 N2 中的至少一项。

可选地，第一认证请求还携带第一 ID 和第一密钥参数，第一密钥参数包含第一 AV 的明文或密文，第一 AV 的密文使用终端设备与授权设备共享的密钥加密。

在本申请实施例中，终端设备首先生成用于派生密钥的随机数 N1 和 N2 中的至少一项，以及生成第一防重放攻击参数 CT，之后生成第一 AV，第一 AV 包括 N1 和 N2 中的至少一项，以及第一防重放攻击参数。终端设备根据第一 AV 生成第一密钥参数，第一密钥参数包含第一 AV 的明文或密文，也即第一密钥参数包含第一 AV 或者包含加密后的第一 AV。然后，终端设备根据第一 ID 和第一 AV 确定第一安全杂凑算法的输入数据，根据第一对称密钥确定第一安全杂凑算法的输入密钥，并基于第一安全杂凑算法通过所确定的输入密钥对所确定的输入数据进行处理得到第一认证码。

可选地，第一安全杂凑算法为一种密钥相关的哈希运算认证码（hash-based message authentication code, HMAC）算法，HMAC 算法可以使用安全散列算法（secure hash algorithm, SHA）256、SHA512、国产哈希算法 SM3 等算法实现。

可选地，终端设备将第一对称密钥作为第一安全杂凑算法的输入密钥，或者，终端设备根据第一对称密钥基于密钥派生算法生成派生密钥，将该派生密钥作为第一安全杂凑算法的输入密钥。其中，密钥派生算法使用密钥导出函数（key derivation function, KDF）、基于 HMAC

的 KDF (HMAC-based KDF, HKDF) 等实现。例如, 终端设备根据第一对称密钥和第一随机参数 (N1 和 N2 中的至少一项), 基于密钥派生算法生成派生密钥。可选地, 终端设备将第一 ID 和第一 AV 作为第一安全杂凑算法的输入数据。

需要说明的是, 在第一密钥参数携带加密后的第一 AV 的情况下, 能够降低第一密钥参数被盗窃而泄露的概率, 提高身份认证的安全性。可选地, 终端设备根据第一对称密钥基于密钥派生算法生成对称加密密钥, 终端设备使用该对称加密密钥加密第一 AV 得到第一密钥参数。

可选地, 终端设备生成随机数 N0, 根据第一对称密钥和 N0 基于密钥派生算法生成对称加密密钥, 终端设备使用该对称加密密钥加密第一 AV 后得到第一密钥参数。在这种情况下, 终端设备根据第一 ID、第一 AV 和 N0 确定第一安全杂凑算法的输入数据, 第一认证请求还携带 N0。其中, 密钥派生算法可以使用 KDF、HKDF 等实现。可选地, 终端设备加密第一 AV 所用的加密函数可以使用高级加密标准 (advanced encryption standard, AES)、SM4 等对称密码算法实现。

由前述对图 1 所示系统架构的介绍可知, 终端设备在部署之后先通过网络搜索注册设备, 在搜索到注册设备之后, 终端设备先向注册设备发送入网请求, 在注册设备根据该入网请求响应终端设备之后, 终端设备再生成第一认证请求。

也即是, 在终端设备向注册设备发送第一认证请求之前, 终端设备先向注册设备发送入网请求, 终端设备接收注册设备发送的第一应答消息, 其中, 第一应答消息携带第一身份信息, 第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个, 注册设备的身份信息包括注册设备身份相关的数字证书和注册设备身份相关的数字证书的摘要中的至少一个。可选地, 该过程可以看作终端设备在发送第一认证请求之前的一个入网发现阶段。

在第一应答消息携带第一身份信息的情况下, 第一认证码根据第一对称密钥、第一 ID、第一 AV 以及第一身份信息生成, 第一认证请求还携带第一身份信息。例如, 终端设备将第一 ID、第一 AV 和第一身份信息, 作为第一安全杂凑算法的输入数据, 以生成第一认证码。

示例性地, 在第一应答消息携带注册设备身份相关的数字证书的情况下, 终端设备将第一 ID、第一 AV 和注册设备身份相关的数字证书, 作为第一安全杂凑算法的输入数据, 在这种情况下, 第一认证请求还携带注册设备身份相关的数字证书。在第一应答消息携带注册设备的数字证书的摘要的情况下, 终端设备将第一 ID、第一 AV 和注册设备身份相关的数字证书的摘要, 作为第一安全杂凑算法的输入数据, 在这种情况下, 第一认证请求还携带注册设备身份相关的数字证书的摘要。

需要说明的是, 在本申请实施例中, 为了提高身份认证的安全性, 本申请实施例提供的身份认证方法还能够防重放攻击, 由前述可知, 第一 AV 包含第一防重放攻击参数。也即是, 为了防重放攻击, 终端设备能够生成第一防重放攻击参数。

可选地, 在本申请实施例中, 防重放攻击的方式为基于随机数的方式、基于时间戳的方式、基于计数器的方式、基于随机数和时间戳的方式等中的任意一种, 相应的, 第一防重放攻击参数是指第三随机数、第一时间戳、第一计数值、第三随机数附上第一时间戳中的一种。其中, 第一时间戳是指终端设备生成第一防重放攻击参数的时刻。

可选地, 第一认证请求还携带授权设备的统一资源定位符 (uniform resource locator, URL),

第一认证请求携带的 URL 用于注册设备与该 URL 对应的授权设备通信以进行身份认证。

示例 1, 终端设备生成第一认证请求 VReq1 的过程包括:

1、生成随机数 $N0=Rand()$, $N1=Rand()$, $N2=Rand()$, 其中, $Rand()$ 是一个安全且标准的伪随机数生成函数。生成第一防重放攻击参数 CT_1 。

2、生成对称认证密钥 $Key_1=HKDF(SK_{old}, N1)$, 其中, $HKDF()$ 可以是基于 SHA256 实现的安全的密钥派生算法。

3、生成对称加密密钥 $Key_C=HKDF(SK_{old}, N0)$ 。

4、生成第一认证向量 $AV_1=\{N1, N2, CT_1\}$, AV_1 包括 $N1$ 、 $N2$ 和 CT_1 。

5、使用 Key_C 加密 AV_1 , 得到 $EAV_1=E(Key_C, AV_1)$, 其中, $E()$ 可以是基于 SM4 实现的对称加密算法。

6、计算第一认证码 $AuthC=HMAC(Key_1, (ID_{old}, CertR, N1, N2))$, 其中, ID_{old} 为第一 ID, $CertR$ 为第一身份信息。

7、得到携带 ID_{old} 、 $N0$ 、 EAV_1 、 $CertR$ 、授权设备的 URL (可选地)、 $AuthC$ 的第一认证请求 VReq1。

由上述可知, 第一认证消息携带第一 ID、第一密钥参数 (加密或者不加密的第一 AV)、第一身份信息 (可选地)、授权设备的 URL (可选地)、第一认证码、 $N0$ (可选地)。其中, 第一 AV 包含第一随机参数和第一防重放攻击参数。

步骤 402: 注册设备接收第一认证请求, 根据第一认证请求生成第二认证请求, 向授权设备发送第二认证请求, 第二认证请求携带第一认证码。

在本申请实施例中, 注册设备在接收到第一认证请求之后, 根据第一认证请求生成第二认证请求, 向授权设备发送第二认证请求, 第二认证请求携带第一认证码。例如注册设备直接将第一认证请求作为第二认证请求, 转发给授权设备。

可选地, 在本申请实施例中, 注册设备存储有终端设备的购置记录, 在第一认证请求携带第一 ID 的情况下, 注册设备根据购置记录验证第一认证请求携带的第一 ID, 如果第一 ID 包含在购置记录内, 则注册设备确定对该终端设备属于园区或企业购置的设备范围, 根据第一认证请求生成第二认证请求, 向授权设备发送第二认证请求。其中, 购置记录中包括购买者 (如园区或企业) 所购买的所有终端设备的 ID。可选地, 购置记录存储在购置数据库中, 注册设备可以从购置数据库中获取购置记录。

在本申请实施例中在第一认证请求携带第一 ID 的情况下, 第二认证请求还携带第一认证中的第一 ID。第二认证请求还携带第一身份信息, 第一身份信息包括所述注册设备的身份信息和所述注册设备所属网络的身份信息中的至少一个。在第一认证请求未携带第一身份信息的情况下, 注册设备将第一身份信息添加在第一认证请求中, 得到第二认证请求。在第一认证请求携带第一身份信息的情况下, 注册设备将第一认证请求作为第二认证请求。

示例性地, 如果第一认证请求携带注册设备身份相关的数字证书, 则注册设备将第一认证请求作为第二认证请求, 或者, 注册设备将注册设备所属网络的身份信息增加在第一认证请求中得到第二认证请求。如果第一认证请求携带注册设备身份相关的数字证书的摘要, 则注册设备将第一认证请求作为第二认证请求, 或者, 注册设备将身份相关的数字证书和注册设备所属网络的身份信息添加在第一认证请求中得到第二认证请求。

可选地, 由前述可知, 第一认证请求还携带第一密钥参数, 第一密钥参数包含第一 AV 的

明文或密文，为了防重放攻击，第一 AV 包含第一防重放攻击参数，在这种情况下，第二认证请求也同样还携带第一密钥参数。

由前述可知，授权设备的 URL 是第一认证请求可选择携带的，基于此，在第一认证请求不携带授权设备的 URL 的情况下，注册设备根据第一 ID 从授权数据库中获取授权设备的 URL。其中，授权数据库中存储有多个授权设备的 URL 与多个终端设备的 ID 的对应关系，例如，一个授权设备的 URL 对应该授权设备所销售的一批终端设备的 ID，注册设备根据该对应关系获取与第一 ID 对应的 URL，将获取的 URL 作为第二认证请求的接收者。

可选地，如果第一认证请求还携带授权设备的 URL，注册设备可以选择在获取该 URL 之后，将第一认证请求中携带的该 URL 删除，这样，得到的第二认证请求将不携带授权设备的 URL。

可选地，为了保证注册设备与授权设备之间通信的安全性，注册设备与授权设备之间基于注册设备的数字证书建立第二安全传输通道（TLS 通道），注册设备通过第二安全传输通道向授权设备发送第二认证请求。或者，注册设备与授权设备之间传输的消息需要基于注册设备的私钥（如与数字证书中的公钥对应的私钥）加密，或者基于注册设备与授权设备共享的对称密钥加密，也即通过加密消息来保证通信安全。

需要说明的是，如果在本次身份认证之前，授权设备未获取过注册设备的公钥（如数字证书中的公钥），或者授权设备未与注册设备共享对称密钥，那么为了保证通信安全，在注册设备未与授权设备之间建立 TLS 通道，注册设备需要确保注册设备的公钥携带在第二认证请求中，以将公钥发送给授权设备。例如，在第一认证请求未携带注册设备身份相关的数字证书的情况下，注册设备将自身身份相关的数字证书添加在第一认证请求中，得到第二认证请求。

可选地，第二认证请求还携带注册设备的身份签名，注册设备的身份签名是注册设备使用私钥第一认证请求和第一身份信息进行的签名。如果授权设备信任注册设备，第二认证请求也可以不携带注册设备的身份签名。

示例 2，在示例 1 的基础上，注册设备接收到第一认证请求后确定第二认证请求的过程包括：

1、从 VReq1 中获取 ID_{old}，根据购置记录验证 ID_{old}，如果购置记录中不存在 ID_{old}，则返回错误。如果购置记录中存在 ID_{old}，则继续下一步。

2、如果 VReq1 中不携带第一身份信息，则注册设备将第一身份信息增加在 VReq1 中得到 VReq2。例如 VReq1 不携带注册设备身份相关的数字证书，则注册设备将注册设备身份相关的数字证书增加在 VReq1 中得到 VReq2。可选地，则注册设备将注册设备的身份签名增加在 VReq2 中。

由上述可知，第二认证请求携带第一 ID、第一密钥参数、第一认证码、第一身份信息（可选地，在生成第一认证码时的输入数据包含第一身份信息的情况下携带）、授权设备的 URL（可选地）、N0（可选地，第一认证请求携带的情况下携带）、注册设备的身份签名（可选地）。

步骤 403：授权设备接收第二认证请求，根据第一对称密钥和所有权关系记录验证第一认证码，在验证通过后向注册设备发送第一认证确认消息，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系。

在本申请实施例中，授权设备在接收到第二认证请求之后，根据第一对称密钥和存储的

终端设备的所有权关系记录验证第二认证请求携带的第一认证码，在验证通过后向注册设备发送第一认证确认消息，第一认证确认消息用于授权终端设备与注册设备所属网络的所有权关系。

需要说明的是，授权设备中存储有终端设备的所有权关系记录（例如销售记录），该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，例如，该所有权关系记录中记录有销售商已销售的所有终端设备的 ID 与购买者信息的对应关系，也即所有权关系记录包含第一 ID 和第一身份信息之间的映射关系。授权设备中还存储有密钥数据库，密钥数据库中存储销售商所销售的所有终端设备的 ID 与设备密钥之间的映射关系，例如，密钥数据库中包含第一 ID 和第一对称密钥的映射关系。可选地，授权设备未存储密钥数据库，而是在所有权关系记录中记录与终端设备的 ID 对应的设备密钥，也即是，所有权关系记录中存储有销售商已销售的所有终端设备的 ID，以及与每个 ID 对应的设备密钥和购买者信息，授权设备从密钥数据库中获取与第一 ID 对应的第一对称密钥。在本申请实施例中，授权设备根据所有权关系记录、第一 ID、第一对称密钥和第一密钥参数，验证第一认证码。

在第一认证码根据第一对称密钥、第一 ID 和第一 AV 生成的情况下，授权设备在接收到第二认证请求之后，从第二认证请求中获取第一 ID 和第一密钥参数，从第一密钥参数中获取第一 AV，根据所有权关系记录验证第一 ID。在验证通过后，授权设备从密钥数据库中获取与第一 ID 对应的第一对称密钥。可选地，在所有权关系记录中存储有销售商已销售的所有终端设备的 ID，以及与每个 ID 对应的设备密钥和购买者信息的情况下，授权设备从所有权关系记录中获取与第一 ID 对应的第一对称密钥。授权设备获取第一对称密钥之后，根据第一对称密钥、第一 ID 和第一 AV 验证第一认证码。

示例性地，授权设备根据第一对称密钥确定第一安全杂凑算法的输入密钥，将第一 ID 和第一 AV 作为第一安全杂凑算法的输入数据，基于第一安全杂凑算法用所确定的输入密钥对所确定的输入数据进行处理，得到第一校验码，如果第一校验码与第一认证码相同，则验证通过，如果第一校验码与第一认证码不同，则验证失败。

在第一认证码根据第一对称密钥、第一 ID、第一 AV 和第一身份信息生成的情况下，授权设备从第二认证请求中获取第一 ID 和第一密钥参数，从第一密钥参数中获取第一 AV，从所有权关系记录中获取与第一 ID 对应的第一身份信息，从密钥映射数据库中获取与第一 ID 对应的第一对称密钥，授权设备根据第一对称密钥、第一 ID、第一 AV 和第一身份信息，验证第一认证码。

示例性地，授权设备根据第一对称密钥确定第一安全杂凑算法的输入密钥，将第一 ID、第一 AV 和第一身份信息作为第一安全杂凑算法的输入数据，基于第一安全杂凑算法用所确定的输入密钥对所确定的输入数据进行处理，得到第一校验码，如果第一校验码与第一认证码相同，则验证通过，如果第一校验码与第一认证码不同，则验证失败。

可选地，在终端设备将第一对称密钥作为第一安全杂凑算法的输入密钥的情况下，授权设备也将第一对称密钥作为第一安全杂凑算法的输入密钥。在终端设备根据第一对称密钥基于密钥派生算法生成派生密钥，将该派生密钥作为第一安全杂凑算法的输入密钥的情况下，授权设备也根据第一对称密钥基于该密钥派生算法生成派生密钥，将生成的派生密钥作为第一安全杂凑算法的输入密钥。也即是，授权设备验证第一认证码所采用的算法，与终端设备生成第一认证码所采用的算法需要相同，这是个对称验证的过程，以保证验证的准确性。

可选地,在第二认证请求还携带第一ID和第一身份信息的情况下,授权设备在接收到第二认证请求之后,先根据所有权关系记录验证第一ID和第一身份信息。示例性地,在本申请实施例中,授权设备需要验证第二认证请求中携带的第一ID是否包含在所有权关系记录中,验证第一认证请求中携带的第一身份信息是否与所有权关系记录中记录的第一ID对应的第一身份信息一致。在确认这两个验证均通过后,授权设备根据第一ID从密钥数据库中获取第一对称密钥,从第二认证请求中获取第一密钥参数,从第一密钥参数中获取第一AV,根据第一对称密钥、第一ID、第一AV和第一身份信息,并基于第一安全杂凑算法验证第一认证码。

可选地,在第一密钥参数携带未加密的第一AV的情况下,授权设备直接从第一密钥参数中获取第一AV。在第一密钥参数携带加密的第一AV的情况下,第二认证请求还携带加密第一AV所使用的随机数N0,授权设备从第二认证请求中获取N0后,根据第一对称密钥和N0基于密钥派生算法生成对称加密密钥,授权设备使用该对称加密密钥解密第一密钥参数后,得到第一AV。其中,授权设备解密第一密钥参数所用的解密函数与终端设备加密第一AV所使用的加密函数对应。

可选地,由前述可知,为了防重放攻击,第一认证请求和第二认证请求还携带第一防重放攻击参数,例如第一AV还包含第一防重放攻击参数。在这种情况下,授权设备在接收到第二认证请求之后,需要从第二认证请求获取第一AV,从第一AV中获取第一防重放攻击参数,并根据第一防重放攻击参数验证第二认证请求是否为重放攻击,在确定第二认证请求不是重放攻击,且授权设备对第一ID、第一身份信息以及第一认证码均验证通过之后,确定授权终端设备与注册设备所属网络的所有权关系。

示例3,假设第一认证请求VReq1和第二认证请求VReq2均携带ID_{old}、EAV₁、CertR、授权设备的URL(可选地)、AuthC,也即在上述示例1和示例2的基础上,授权设备验证第二认证请求VReq2的过程包括:

1、从VReq2中获取ID_{old},根据ID_{old}从密钥数据库中获取SK_{old},如果密钥数据库中不存在SK_{old},则返回错误。如果密钥数据库中不存在SK_{old},则继续下一步。

2、从VReq2中获取第一身份信息,从所有权关系记录中查找ID_{old},以及与ID_{old}对应的第一身份信息,如果所有权关系记录中包括该ID_{old},且对应的第一身份信息与从VReq2中获取的第一身份信息一致,则验证通过。

3、从VReq2中获取N0和EAV₁,并根据N0和SK_{old}解密EAV₁得到AV₁,从AV₁中获取N1、N2和CT,根据CT验证VReq2是否为重放攻击。如果是重放攻击,则返回错误。如果不是重放攻击,则继续下一步。

4、从VReq2中获取AuthC,计算对称验证密钥Key₁'=HKDF(SK_{old},N1),计算第一校验码AuthC'=HMAC(Key₁',(ID_{old},CertR,N1,N2)),验证AuthC'与AuthC是否相同。如果相同,则确定第一认证码验证通过,确定授权终端设备与注册设备所属网络的所有权关系,如果不相同,则确定验证失败,返回错误。

在授权设备确定授权终端设备与注册设备所属网络的所有权关系之后,授权设备生成第一认证确认消息,并向注册设备发送第一认证确认消息。其中,第一认证确认消息携带第二认证码,第二认证码根据第一对称密钥生成。

接下来介绍授权设备生成第一认证确认消息的一种实现方式。

在本申请实施例中,第一认证确认消息携带第二密钥参数和第二认证码。授权设备确定

第二 AV，授权设备根据第二 AV 生成第二密钥参数，第二密钥参数携带第二 AV 或加密后的第二 AV，第二 AV 使用授权设备与终端设备共享的密钥加密，例如使用第一对称密钥加密。之后，授权设备根据第一对称密钥确定第二安全杂凑算法的输入密钥，根据第一 ID 和第二 AV 确定第二安全杂凑算法的输入数据，并基于第二安全杂凑算法通过所确定的输入密钥对所确定的输入数据处理得到第二认证码。其中，第二 AV 包含第二防重放攻击参数，或者，第二 AV 包含第一随机参数和第二防重放攻击参数，或者，第二 AV 包含第二随机参数和第二防重放攻击参数，或者，第二 AV 包含第一随机参数、第二随机参数和第二防重放攻击参数。其中，第二随机参数由授权设备生成，第二随机参数包含至少一个随机数。

其中，授权设备生成第二防重放攻击参数的实现方式为：授权设备根据第一防重放攻击参数，生成第二防重放攻击参数。需要说明的是，在第一防重放攻击参数是指第一随机数的情况下，第二防重放攻击参数是指第二随机数，第一随机数与第二随机数不同。在第一防重放攻击参数是指第一时间戳的情况下，第二防重放攻击参数是指第二时间戳，第二时间戳是指授权设备生成第二防重放攻击参数的时刻。在第一防重放攻击参数是指第一计数值的情况下，第二防重放攻击参数是指第二计数值，第二计数值是在第一计数值的基础上累加 1 得到的。在第一防重放攻击参数是指第一随机数附上第一时间戳的情况下，第二防重放攻击参数是指第二随机数附上第二时间戳。

授权设备确定第二 AV 的第一种实现方式为：授权设备将第二防重放攻击参数作为第二 AV。授权设备确定第二 AV 的第二种实现方式为：授权设备从第一 AV 中获取第一随机参数（如 N1 和 N2），授权设备将第一随机参数和第二防重放攻击参数作为第二 AV。授权设备确定第二 AV 的第三种实现方式为：授权设备生成第二随机参数，第二随机参数包含至少一个随机数（如随机数 N3），授权设备将第二随机参数和第二防重放攻击参数作为第二 AV。授权设备确定第二 AV 的第四种实现方式为：授权设备从第一 AV 中获取第一随机参数，授权设备生成第二随机参数，第二随机参数包含至少一个随机数（如随机数 N3），授权设备将第一随机参数、第二随机参数和第二防重放攻击参数作为第二 AV。

可选地，授权设备将第一对称密钥作为第二安全杂凑算法的输入密钥。或者，授权设备根据第一对称密钥基于密钥派生算法生成派生密钥，将该派生密钥作为第二安全杂凑算法的输入密钥。授权设备将第一 ID 和第二 AV 作为第二安全杂凑算法的输入数据，或者，将第一 ID、第二 AV 和第一身份信息作为第二安全杂凑算法的输入数据。需要说明的是，授权设备生成第二认证码时所采用的密钥派生算法，与终端设备生成第一认证码时采用的密钥派生算法相同或不同，第二安全杂凑算法与上述第一安全杂凑算法相同或不同。

可选地，第一认证确认消息还携带第一 ID，第一认证确认消息指示注册设备向第一 ID 对应的终端设备发送授权设备的响应。

由上述可知，本申请实施例中的第一对称密钥作为旧的设备密钥，旧的设备密钥仅在终端设备和授权设备之间共享，第一对称密钥用于终端设备与授权设备实现上述身份认证的过程。由于终端设备后续接入注册设备所属的网络时，仍需要入网身份鉴权，因此，注册设备与终端设备之间需要根据授权设备的响应来协商第二对称密钥，第二对称密钥仅在终端设备与注册设备之间共享，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。

在本申请实施例中，第一认证确认消息还携带密钥更新信息，密钥更新信息由授权设备生成，密钥更新信息使用注册设备与授权设备共享的对称密钥加密保护，或者，密钥更新信

息使用注册设备的公钥加密保护。该密钥更新信息用于注册设备获取与终端设备之间建立第一安全传输通道所需的通道安全密钥，以及与终端设备之间通过第一安全传输通道协商第二对称密钥。第一认证确认消息携带的第二密钥参数还用于终端设备确定生成该通道安全密钥所需的第一派生参数，以及确定与注册设备之间通过第一安全传输通道协商第二对称密钥所需的第二派生参数。

接下来介绍授权设备生成密钥更新信息的一种实现方式。

在本申请实施例中，授权设备在确定第二 AV 之后，根据第一对称密钥和第二 AV 生成密钥更新信息。在一种实现方式中，授权设备根据第二 AV 确定第一派生参数和第二派生参数，根据第一派生参数和第一对称密钥基于密钥派生算法生成第一协商密钥，根据第二派生参数和第一对称密钥基于密钥派生算法生成第二协商密钥，授权设备根据第一协商密钥和第二协商密钥确定密钥更新信息。

示例性地，假设第二 AV 包含第二防重放攻击参数，或者，第二 AV 包含第一随机参数和第二防重放攻击参数，第一随机参数包含 N1 和 N2，那么授权设备将 N1 作为第一派生参数，将 N2 作为第二派生参数。假设第二 AV 包含第二随机参数和第二防重放攻击参数，或者，第二 AV 包含第一随机参数、第二随机参数和第二防重放攻击参数，第一随机参数包含 N1 和 N2，第二随机参数包含 N3，那么授权设备将 N1 和 N3 作为第一派生参数，将 N2 和 N3 作为第二派生参数。可选地，授权设备也可以生成更多的随机数，用于确定第一派生参数和第二派生参数，本申请实施例对此不作限定。例如，在第一随机参数包含 N1 的情况下，授权设备生成随机数 N3 和 N6，授权设备将 N1 和 N3 作为第一派生参数，将 N1 和 N6 作为第二派生参数。或者，授权设备生成随机数 N3 和 N6，将 N3 作为第一派生参数，将 N6 作为第二派生参数。

授权设备根据第一派生参数基于密钥派生算法生成第一协商密钥，根据第二派生参数基于密钥派生算法生成第二协商密钥。示例性地，假设第一派生参数包含 N1 和 N3，第二派生参数包含 N2 和 N3，那么，第一协商密钥 $K_{R1} = \text{HKDF}(\text{SK}_{\text{old}}, N1, N3)$ ，第二协商密钥 $K_{R2} = \text{HKDF}(\text{SK}_{\text{old}}, N2, N3)$ 。

需要说明的是，第一协商密钥与第一派生参数对应，第二协商密钥与第二派生参数对应。密钥更新信息包含第一协商密钥和第二协商密钥，第一协商密钥和第二协商密钥是授权设备提供给注册设备的信息，也即注册设备能够获取的信息，第一协商密钥和第二协商密钥中的一个作为后续注册设备所确定的通道安全密钥，另一个作为注册设备生成第二对称密钥的依据。第二密钥参数包含的第二 AV 或者加密的第二 AV 是授权设备提供给终端设备的信息，也即终端设备能够获取第二 AV，并根据第二 AV 确定第一派生参数和第二派生参数，第一派生参数和第二派生参数中的一个作为终端设备生成通道安全密钥的依据，另一个作为终端设备生成第二对称密钥的依据。其中，注册设备与终端设备所确定的通道安全密钥相同，所生成的第二对称密钥也相同。

本申请实施例中，以第一协商密钥作为注册设备获取的通道安全密钥，第二协商密钥作为注册设备生成第二对称密钥的依据，以第一派生参数用于终端设备生成通道安全密钥，第二派生参数用于终端设备生成第二对称密钥的依据为例，在下文步骤 405 中将对此详细介绍。

可选地，为了保证注册设备与授权设备之间通信的安全性，授权设备与注册设备之间基于注册设备的数字证书建立安全传输通道来进行通信，也即，授权设备通过安全传输通道将

第一认证确认消息发送给注册设备。或者，授权设备使用从注册设备的数字证书中获取的公钥对密钥更新信息加密，或使用授权设备与注册设备之间共享的对称密钥对密钥更新信息加密，将加密后的密钥更新信息携带在第一认证确认消息中，授权设备将携带加密的密钥更新信息的第一认证确认消息发送给注册设备。或者，授权设备使用注册设备的公钥对第一认证确认消息加密，或使用授权设备与注册设备之间共享的对称密钥加密第一认证确认消息，将加密后的第一认证确认消息发送给注册设备。

可选地，无论注册设备与授权设备之间是否建立安全传输通道进行通信，授权设备均可以通过加密密钥更新信息或者加密第一认证确认消息的方式，保证通信的安全性。也即是，密钥更新信息使用注册设备的公钥加密得到，或者，使用授权设备与注册设备之间的对称密钥加密得到。

示例 4，在上述示例 3 的基础上，授权设备生成第一认证确认消息（voucher response，VResp1）的过程包括：

1、生成随机数 $N3 = \text{Rand}()$ 。

2、生成第二认证向量 $AV_2 = \{N1, N2, N3, CT+\}$ 。

3、生成第二认证码 $\text{AuthS} = \text{HMAC}(\text{Key}_1', (\text{ID}_{\text{old}}, \text{CertR}, N1, N2, N3))$ 。

4、计算第一协商密钥 $K_{R1} = \text{HKDF}(\text{SK}_{\text{old}}, N1, N3)$ ，第二协商密钥 $K_{R2} = \text{HKDF}(\text{SK}_{\text{old}}, N2, N3)$ 。

5、使用注册设备的数字证书中给出的第一公钥 PK_R 加密 K_{R1} 和 K_{R2} ，得到密钥更新信息 $\text{EKV} = \text{E}(\text{PK}_R, K_{R1}, K_{R2})$ 。其中， $\text{E}()$ 可以使用 RAS、SM3 或其他基于椭圆曲线的公钥算法实现。

6、得到携带 ID_{old} 、 AV_2 、 AuthS 和 EKV 的第一认证确认消息 VResp1。

由上述可知，第一认证确认消息携带第一 ID（可选地）、第二密钥参数、第二认证码和密钥更新信息（可选地）。其中，密钥更新信息包含第一协商密钥和第二协商密钥，密钥更新信息为明文或密文。

步骤 404：注册设备接收第一认证确认消息，根据第一认证确认消息确定第二认证确认消息，向终端设备发送第二认证确认消息，第二认证确认消息携带第二认证码。

在本申请实施例中，注册设备在接收到第一认证确认消息之后，确定终端设备的身份合法性，也即对于注册设备来说，确认终端设备的身份认证通过。之后，注册设备根据第一认证确认消息确定第二认证确认消息，并向终端设备发送第二认证确认消息，第二认证确认消息携带第二认证码。例如，注册设备将第一认证确认消息作为第二认证确认消息转发给终端设备。

由前述可知，为了后续注册设备与终端设备之间建立第一安全传输通道协商第二对称密钥，第一认证确认消息还携带密钥更新信息，密钥更新信息包含第一协商密钥和第二协商密钥，密钥更新信息为明文或密文。

在密钥更新信息为明文的情况下，注册设备在接收到第一认证确认消息之后，从第一认证确认消息中获取密钥更新信息，并存储第一协商密钥和第二协商密钥，供后续与终端设备之间建立安全传输通道以及协商第二对称密钥使用。之后，注册设备将密钥更新信息从第一认证确认消息中删除后得到第二认证确认消息。

在密钥更新信息为密文的情况下，注册设备在接收到第一认证确认消息之后，从第一认

证确认消息中获取密钥更新信息，并使用与注册设备的公钥对应的私钥解密密钥更新信息，或者，使用注册设备与授权设备之间共享的对称密钥解密密钥更新信息，得到第一协商密钥和第二协商密钥。之后，注册设备将第一认证确认消息作为第二认证确认消息转发给终端设备。

可选地，在密钥更新信息加密或者未加密的情况下，注册设备均可以将密钥更新信息从第一认证确认消息中删除后得到第二认证确认消息。

可选地，第一认证确认消息使用注册设备的公钥加密，或使用注册设备与授权设备之间共享的对称密钥加密的情况下，注册设备在接收到第一认证确认消息之后，使用与该公钥对应的私钥或该对称密钥解密第一认证确认消息，从解密后的第一认证确认消息中获取密钥更新信息，并存储第一协商密钥和第二协商密钥。

示例 5，在上述示例 4 的基础上，注册设备根据第一认证确认消息 VResp1 确定第二认证确认消息 VResp2 的过程包括：

1、从 VResp1 中获取 EKV，使用与公钥 PK_R 对应的私钥解密 EKV，得到 K_{R1} 和 K_{R2}，并存储 K_{R1} 和 K_{R2}。

2、将 VResp1 作为 VResp2 发送给终端设备。需要说明的是，如果 VResp1 中的 K_{R1} 和 K_{R2} 未加密，则注册设备需要将 K_{R1} 和 K_{R2} 从中删除 VResp1 后得到 VResp2。

由上述可知，第二认证确认消息携带第一 ID（可选地）、第二密钥参数、第二认证码、密钥更新信息（可选地）。其中，密钥更新信息在加密的情况下选择携带，在未加密的情况下不携带。

步骤 405：终端设备接收第二认证确认消息，根据第一对称密钥验证第二认证码，在验证通过后确定终端设备与注册设备的双向身份认证通过。

在本申请实施例中，终端设备在接收到第二认证确认消息之后，根据第一对称密钥验证第二认证码，在验证通过后确定终端设备与注册设备的双向身份认证通过。需要说明的是，终端设备验证第二认证码所采用的算法，与授权设备生成第二认证码所采用的算法相同，以确保验证的准确性。

由前述可知，第二认证消息携带第二密钥参数和第二认证码，基于此，终端设备根据第一对称密钥和第二密钥参数，验证第二认证码。示例性地，终端设备根据第一对称密钥和第二密钥参数生成对称验证密钥，终端设备根据该对称验证密钥验证第二认证码。

在本申请实施例中，第二认证码由授权设备根据第一对称密钥确定第二安全杂凑算法的输入密钥，根据第一 ID 和第二 AV 确定第二安全杂凑算法的输入数据后，基于第二安全杂凑算法通过所确定的输入密钥对所确定的输入数据处理得到。那么，终端设备验证第二认证码的实现方式为：终端设备从第二认证确认消息中获取第二密钥参数，从第二密钥参数中获取第二 AV，终端设备根据第一对称密钥确定第二安全杂凑算法的输入密钥（对称验证密钥），根据第一 ID 和第二 AV 确定第二安全杂凑算法的输入数据后，基于第二安全杂凑算法通过所确定的输入密钥对所确定的输入数据处理得到。其中，如果第二密钥参数包含第二 AV 的密文，则终端设备使用终端设备与授权设备共享的对称密钥解密第二密钥参数，得到第二 AV。例如，授权设备采用第一对称密钥加密第二密钥参数，那么终端设备采用第一对称密钥解密第二密钥参数。

需要说明的是，如果授权设备将第二对称密钥作为第二安全杂凑算法的输入密钥，那么，

终端设备验证第二认证码时也将第二对称密钥作为第二安全杂凑算法的输入密钥。如果授权设备根据第一对称密钥基于密钥派生算法生成派生密钥后，将该派生密钥作为第二安全杂凑算法的输入密钥，那么，终端设备验证第二认证码时也根据第一对称密钥基于密钥派算法生成派生密钥后，将该派生密钥作为第二安全杂凑算法的输入密钥。也即是，终端设备验证第二认证码的方式要与授权设备生成第二认证码的方式保持一致，以确保验证的准确性。

由前述可知，为了防重放攻击，第二认证确认消息还携带第二防重放攻击参数，其中，第二 AV 包含第二防重放攻击参数。基于此，终端设备在接收到第二认证确认消息之后，先从第二认证确认消息中提取出第二防重放攻击参数，也即从第二 AV 中获取第二防重放攻击参数，终端设备根据第二防重放攻击参数验证第二认证确认消息是否为重放攻击，在确认第二认证确认消息不是重放攻击，且验证第二认证码通过之后，终端设备确定双向身份认证通过，也即表明注册设备被授权设备授权为终端设备的新网络主人。

示例 6，在前述示例 5 的基础上，终端设备验证第二认证确认消息 VResp2 的过程包括：

1、从 VResp2 中获取 N3 和 CT+。

2、根据 CT+验证 VResp2 是否为重放攻击。如果是重放攻击，则返回错误。如果不是重放攻击，则继续下一步。

3、从 VResp2 中获取 AuthS。计算 $\text{AuthS}' = \text{HMAC}(\text{Key}_1, (\text{ID}_{\text{old}}, \text{CertR}, \text{N1}, \text{N2}, \text{N3}))$ 。验证 AuthS' 与 AuthS 是否相同。如果相同，则确定双向身份认证通过。如果不相同，则确定双向身份认证失败，返回错误。

上述终端设备、注册设备与授权设备配合实现终端设备与注册设备的双向身份认证的过程，可以看作入网发现阶段之后的授权互信阶段。

可选地，由前述可知，为了后续终端设备与注册设备之间建立第一安全传输通过协商第二对称密钥，第一认证确认消息和第二认证确认消息还携带密钥更新信息，密钥更新信息用于注册设备获取与终端设备之间建立第一安全传输通道所需的通道安全密钥，以及与终端设备之间通过第一安全传输通道协商第二对称密钥，而第二密钥参数还用于终端设备确定生成该通道安全密钥所需的第一派生参数，以及确定与注册设备之间通过第一安全传输通道协商第二对称密钥所需的第二派生参数。

其中，密钥更新信息携带第一协商密钥和第二协商密钥的明文或密文，第一协商密钥由授权设备根据第一对称密钥和第一派生参数基于密钥派生算法生成，第二协商密钥由授权设备根据第一对称密钥和第二派生参数基于密钥派生算法生成。注册设备能够从密钥更新信息中获取第一协商密钥和第二协商密钥，注册设备将第一协商密钥作为通道安全密钥，根据第二协商密钥生成第二对称密钥。或者，注册设备将第二协商密钥作为通道安全密钥，根据第一协商密钥生成第二对称密钥。

在本申请实施例中，终端设备在确定双向身份认证通过之后，根据第二密钥参数确定第一派生参数，根据第一对称密钥和第一派生参数，生成通道安全密钥，终端设备与注册设备之间基于该通道安全密钥建立第一安全传输通道，终端设备根据第二密钥参数确定第二派生参数，根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥。

在本申请实施例中，终端设备能够从第二认证确认消息中获取第二密钥参数，从第二密钥参数中获取第二 AV，根据第二 AV 确定第一派生参数和第二派生参数，终端设备根据第一对称密钥和第一派生参数生成第一协商密钥，根据第一对称密钥和第二派生参数生成第二协

商密钥。其中，终端设备根据第二 AV 确定第一派生参数和第二派生参数的实现方式，可以参照前述授权设备根据第二 AV 确定第一派生参数和第二派生参数的相关介绍，这里不再赘述。

在本申请实施例中，通道安全密钥与第一协商密钥相同，且终端设备根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥。或者，通道安全密钥与第二协商密钥相同，且终端设备根据第一派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥。

也即是，假设注册设备将获取的第一协商密钥作为通道安全密钥，以及根据第二协商密钥生成第二对称密钥，那么，终端设备将根据第一派生参数生成的第一协商密钥作为通道安全密钥，以及根据第二派生参数生成的第二协商密钥生成第二对称密钥。假设注册设备将获取的第二协商密钥作为通道安全密钥，以及根据第一协商密钥生成第二对称密钥，那么，终端设备将根据第二派生参数生成的第二协商密钥作为通道安全密钥，以及根据第一派生参数生成的第一协商密钥生成第二对称密钥。也即保证注册设备与终端设备所确定的通道安全密钥相同，且注册设备与终端设备各自生成的第二对称密钥也相同。

接下来以通道安全密钥与第一协商密钥相同，且终端设备根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥为例，对终端设备与注册设备之间通过第一安全传输通道协商第二对称密钥的过程进行介绍。

终端设备与注册设备之间通过第一安全传输通道协商第二对称密钥的第一种实现方式：

终端设备生成随机数 N_4 ，将 N_4 通过第一安全传输通道发送给注册设备， N_4 用于指示注册设备根据 N_4 和第二协商密钥生成第二对称密钥，以及根据 N_4 和第二对称密钥生成第三认证码。终端设备根据第二密钥参数确定第二派生参数，根据 N_4 和第二派生参数生成第二对称密钥。终端设备接收注册设备发送的第一协商确认消息，第一协商确认消息携带第三认证码，终端设备根据自身生成的第二对称密钥和 N_4 验证第三认证码，在验证通过后，将第二对称密钥更新为自身与注册设备之间的设备密钥，并向注册设备发送第二协商确认消息，第二协商确认消息用于指示注册设备将第二对称密钥更新为自身与终端设备之间的设备密钥。

可选地，终端设备根据 N_4 和第二协商密钥基于密钥派生算法生成第二对称密钥，注册设备根据 N_4 和第二协商密钥基于相同的密钥派生算法生成第二对称密钥。注册设备基于第三安全杂凑算法生成第三认证码，终端设备基于第三安全杂凑算法验证第三认证码。其中，第三安全杂凑算法与第一安全杂凑算法相同或不同，第三安全杂凑算法与第二安全杂凑算法相同或不同。

可选地，注册设备将第二对称密钥作为第三安全杂凑算法的输入密钥，或者，注册设备根据第二对称密钥基于密钥派生算法生成派生密钥，将该派生密钥作为第三安全杂凑算法的输入密钥。注册设备将 N_4 作为第三安全杂凑算法的输入数据，注册设备基于第三安全杂凑算法通过所确定的输入密钥对所确定的输入数据进行处理得到第三认证码。终端设备根据自身生成的第二对称密钥和 N_4 验证第三认证码的方式，与注册设备生成第三认证码的方式一致，以保证验证的准确性。

示例性地，假设第一协商密钥为 K_{R1} ，第二协商密钥为 K_{R2} ，第二对称密钥为 SK_{new} ，终端设备与注册设备之间基于 K_{R1} 建立 TLS 通道，终端设备生成 N_4 ，通过 TLS 通道将 N_4 发送给注册设备，终端设备计算 $SK_{new}=KDF(K_{R2}, N_4)$ 。注册设备收到 N_4 之后，计算

$SK_{new}=KDF_1(K_{R2}, N4)$, 派生密钥 $AK=KDF_2(SK_{new})$, 响应 $ACK=HMAC_{AK}(N4)$ 。注册设备将响应（也即第一协商确认消息）发送给终端设备。终端设备收到响应之后，验证 ACK ，验证过程为：计算 $AK'=KDF_2(SK_{new})$, $ACK'=HMAC_{AK'}(N4)$, 判断 $ACK'=ACK?$ 也即判断终端设备计算得到的 ACK' 是否与注册设备响应的 ACK 相同。如果相同，则终端设备确认对第三认证码的验证通过。在对第三认证码的验证通过后，终端设备确认与注册设备之间协商确定第二对称密钥，并回复第二协商确认消息给注册设备，注册设备接收到第二协商确认消息之后，确认与终端设备之间协商确定第二对称密钥。

由上述可知，在协商第二对称密钥的第一种实现方式中，由终端设备生成用于协商第二对称密钥的随机数 $N4$ ，并将 $N4$ 同步给注册设备，注册设备和终端设备都将 $N4$ 作为生成第二对称密钥的依据，以相同的方式生成第二对称密钥。

终端设备与注册设备之间通过第一安全传输通道协商第二对称密钥的第二种实现方式：

终端设备接收注册设备通过第一安全传输通道发送的随机数 $N5$ ， $N5$ 由注册设备随机生成， $N5$ 和第二协商密钥用于注册设备生成第二对称密钥。终端设备根据 $N5$ 和第二派生参数生成第二对称密钥，将第二对称密钥更新为自身与注册设备之间的设备密钥。其中，终端设备根据第二派生参数生成第二协商密钥，根据 $N5$ 和第二协商密钥生成第二对称密钥。

在协商第二对称密钥的第二种实现方式中，由注册设备生成用于协商第二对称密钥的随机数 $N5$ ，并将 $N5$ 同步给终端设备，注册设备和终端设备都将 $N5$ 作为生成第二对称密钥的依据，以相同的方式生成第二对称密钥。

需要说明的是，在终端设备与注册设备协商第二对称密钥之后，终端设备与注册设备均保存第二对称密钥，以便后续的入网身份鉴权。

可选地，在终端设备与注册设备通过第一安全传输通道协商第二对称密钥之后，注册设备通过第一安全传输通道向终端设备发送第二 ID 和配置信息中的至少一项，第二 ID 是注册设备为终端设备分配的 ID，也即是，注册设备为终端设备下发新的身份。第二 ID 以及第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。终端设备接收到注册设备发送的第二 ID、配置信息之后，保存第二 ID、配置信息。

可选地，由前述可知，该系统架构还包括控制器，注册设备在协商确认第二对称密钥之后，向控制器发送携带第一 ID 和第二对称密钥的配置请求。控制器接收到该配置请求后，将第二 ID 和配置信息中的至少一项发送给注册设备，注册设备通过第一安全传输通道将第二 ID、配置信息转发给终端设备，或者，由控制器直接将第二 ID、配置信息发送给终端设备。可选地，控制器还用于存储、管理和维护终端设备的 ID 与对应的设备密钥的映射关系，例如，对应存储第一 ID、第二 ID 与第二对称密钥。

上述终端设备与注册设备建立第一安全传输通道协商第二对称密钥的过程，可以看作一个 EST 阶段，接下来参照图 5 对该过程再次解释说明。在图 5 中，该过程包括如下步骤：

1、终端设备与注册设备之间基于第一协商密钥 K_{R1} 建立第一安全传输通道来进行安全通信（TLS for EST）。

2、终端设备生成随机数 $NX=Rand()$ ，计算 $SK_{new}=KDF_1(K_{R2}, NX)$ ，终端设备向注册设备发送携带 NX 的注册（enrollment, Enrol）请求。

3、注册设备计算 $SK_{new}=KDF_1(K_{R2}, NX)$ ，计算 $AK=KDF_2(SK_{new})$, $ACK=HMAC_{AK}(NX)$ ，将响应 ACK （第一协商确认消息）发送给终端设备。

4、终端设备验证 ACK：计算 $AK' = KDF_2(SK_{new})$ ，判断 $ACK == HMAC_{AK'}(NX)$ ？在判断相等后，向注册设备发送第二协商确认消息。

5、注册设备存储 SK_{new} ，并向控制器发送携带 ID_{old} 和 SK_{new} 的配置请求消息（ID 请求）。

6、控制器生成一个新的在园区网或企业网范围内唯一的 ID_{new} ，向注册设备发送携带 ID_{new} 、配置文件（配置信息）的响应消息（ID 响应）。控制器对应存储（ ID_{old} ， ID_{new} ， SK_{new} ）。

7、注册设备转发 ID 响应给终端设备。

8、终端设备存储 ID_{new} 和 SK_{new} ，存储配置文件。

在本申请实施例中，终端设备、注册设备与授权设备通过上述介绍的方法实现身份认证，接下来再次参照图 6 对上述过程进行解释说明。

参见图 6，终端设备包括发现模块、授权模块和 EST 模块，注册设备包括授权模块和 EST 模块，授权设备包括授权模块。

其中，终端设备包括的发现模块具有上述入网发现阶段中终端设备实现的相应功能，例如，发现模块通过搜索发现入网代理设备，通过入网代理设备与注册设备进行通信。

终端设备包括的授权模块具有上述授权互信阶段中终端设备实现的相应功能，例如，该授权模块生成并发送第一认证请求，以及接收并验证第二认证确认消息。注册设备包括的授权模块具有上述授权互信阶段中注册设备实现的相应功能，例如，该授权模块接收第一认证请求和第一认证确认消息、生成并发送第二认证请求和第二认证确认消息。授权设备包括的授权模块具有上述授权互信阶段中授权设备实现的相应功能，例如，该授权模块接收并验证第二认证请求、生成并发送第一认证确认消息。

终端设备包括的 EST 模块具有上述 EST 阶段中终端设备实现的相应功能，例如，该 EST 模块与注册设备建立第一安全传输通道、协商第二对称密钥以及接收第二 ID 和配置信息。注册设备包括的 EST 模块具有上述 EST 阶段中注册设备实现的相应功能，例如，该 EST 模块与终端设备之间建立第一安全传输通道、协商第二对称密钥以及下发第二 ID 和配置信息。

由上述可知，本申请实施例实现了一种基于对称密钥的远程零接触入网方法，无需手动将终端设备的 MAC 地址录入注册设备的数据库，也无需人工扫描终端设备上的二维码来录入终端设备的身份信息，仅需终端设备支持轻量级的对称密码技术，大大降低了人工成本，且提升了安全性。无需终端设备支持非对称密码技术，降低了终端设备的成本，对于资源受限、成本较低的终端设备具有很大优势。另外，本申请实施例中设备密钥从第一对称密钥更新为第二对称密钥的过程，由终端设备或者注册设备生成随机数，这样能够基于底层的硬件安全保证密钥的安全，无需接受外界（如授权设备）的输入即能更新设备密钥，更加安全。

综上所述，在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

图 7 是本申请实施例提供的一种身份认证装置 700 的结构示意图，该身份认证装置 700 可以由软件、硬件或者两者的结合实现成为计算机设备的部分或者全部，该计算机设备可以为图 3 所示的计算机设备，该计算机设备为上述实施例中的终端设备。在本申请实施例中，

该装置 700 应用于终端设备，终端设备与授权设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系。参见图 7，该装置 700 包括：发送模块 701、接收模块 702 和验证模块 703。

发送模块 701，用于发送第一认证请求，第一认证请求携带第一认证码，第一认证码根据第一对称密钥生成；

接收模块 702，用于接收第二认证确认消息，第二认证确认消息是根据第一对称密钥和所有权关系记录对第一认证码验证通过后确定的，第二认证确认消息携带第二认证码，第二认证码由授权设备根据第一对称密钥生成；

验证模块 703，用于根据第一对称密钥验证第二认证码，在验证通过后确定终端设备与注册设备的双向身份认证通过。

可选地，第一认证请求还携带第一 ID 和第一密钥参数，第一密钥参数包含第一 AV 的明文或密文，第一 ID 为终端设备的原所有者为终端设备配置的 ID；

第一 AV 包含第一随机参数和第一防重放攻击参数，第一随机参数由终端设备生成，第一随机参数包含第一随机数 N1 和第二随机数 N2 中的至少一项；

第一认证码根据第一对称密钥、第一 ID 和第一 AV 生成。

可选地，第一认证请求还携带第一身份信息，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个；

第一认证码根据第一对称密钥、第一 ID、第一 AV 以及第一身份信息生成。

可选地，第二认证确认消息还携带第二密钥参数；

验证模块 703 包括：

第一生成子模块，用于根据第一对称密钥和第二密钥参数生成对称验证密钥；

验证子模块，用于根据对称验证密钥验证第二认证码。

可选地，参见图 8，该装置 700 还包括：

生成模块 704，用于根据第一对称密钥和第一派生参数，生成通道安全密钥，第一派生参数根据第二密钥参数确定；

建立模块 705，用于与注册设备之间基于通道安全密钥建立第一安全传输通道；

协商模块 706，用于根据第二派生参数与注册设备之间通过第一安全传输通道协商第二对称密钥，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权，第二派生参数根据第二密钥参数确定。

可选地，协商模块 706 包括：

第二生成子模块，用于生成随机数 N4，并将 N4 通过第一安全传输通道发送给注册设备，N4 用于注册设备根据 N4 和第二协商密钥生成第二对称密钥，以及根据 N4 和第二对称密钥生成第三认证码，第二协商密钥由授权设备根据第二派生参数生成并发送给注册设备；

第三生成子模块，用于根据 N4 和第二派生参数生成第二对称密钥；

第一接收子模块，用于接收注册设备发送的第一协商确认消息，第一协商确认消息携带第三认证码；

第一更新子模块，用于根据自身生成的第二对称密钥和 N4 验证第三认证码，在验证通过后，将第二对称密钥更新为自身与注册设备之间的设备密钥，并向注册设备发送第二协商确认消息，第二协商确认消息用于指示注册设备将第二对称密钥更新为自身与终端设备之间

的设备密钥。

可选地，协商模块 706 包括：

第二接收子模块，用于接收注册设备通过第一安全传输通道发送的随机数 N5，N5 由注册设备随机生成，N5 用于注册设备根据 N5 和第二协商密钥生成第二对称密钥，并将第二对称密钥更新为自身与终端设备之间的设备密钥；

第二更新子模块，用于根据 N5 和第二派生参数生成第二对称密钥，将第二对称密钥更新为自身与注册设备之间的设备密钥。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

需要说明的是：上述实施例提供的身份认证装置在身份认证时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的身份认证装置与身份认证方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

图 9 是本申请实施例提供的一种身份认证装置 900 的结构示意图，该身份认证装置 900 可以由软件、硬件或者两者的结合实现成为计算机设备的部分或者全部，该计算机设备可以为图 3 所示的计算机设备，该计算机设备为上述实施例中的注册设备。在本申请实施例中，该装置 900 应用于注册设备，参见图 9，该装置 900 包括：第一接收模块 901、第一发送模块 902、第二接收模块 903 和第二发送模块 904。

第一接收模块 901，用于接收第一认证请求，第一认证请求携带第一认证码，第一认证码由终端设备根据第一对称密钥生成，终端设备与授权设备共享第一对称密钥；

第一发送模块 902，用于根据第一认证请求生成第二认证请求，向授权设备发送第二认证请求，第二认证请求携带第一认证码；

第二接收模块 903，用于接收第一认证确认消息，第一认证确认消息是授权设备根据第一对称密钥和终端设备的所有权关系记录对第一认证码验证通过后确定的，授权设备存储有该所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成；

第二发送模块 904，用于根据第一认证确认消息确定第二认证确认消息，向终端设备发送第二认证确认消息，第二认证确认消息携带第二认证码，第二认证确认消息用于指示终端设备根据第一对称密钥对第二认证码验证通过后确定终端设备与注册设备的双向身份认证通过。

可选地，第一认证请求还携带第一 ID，第一 ID 为终端设备的原所有者为终端设备配置的 ID，第二认证请求还携带第一认证请求中的第一 ID，第二认证请求还携带第一身份信息，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个。

可选地，第二认证请求还携带注册设备的身份签名，注册设备的身份签名是注册设备使用私钥对第一认证请求和第一身份信息进行的签名。

可选地，注册设备的身份信息包括注册设备身份相关的数字证书和注册设备身份相关的数字证书的摘要中的至少一个。

可选地，第一认证确认消息还携带密钥更新信息，密钥更新信息使用注册设备与授权设备共享的对称密钥加密保护，或者，密钥更新信息使用注册设备的公钥加密保护；

参见图 10，该装置 900 还包括：

获取模块 905，用于从密钥更新信息中获取通道安全密钥；

建立模块 906，用于与终端设备之间基于通道安全密钥建立第一安全传输通道；

协商模块 907，用于根据密钥更新信息，与终端设备之间通过第一安全传输通道协商第二对称密钥，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

需要说明的是：上述实施例提供的身份认证装置在身份认证时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的身份认证装置与身份认证方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

图 11 是本申请实施例提供的一种身份认证装置 1100 的结构示意图，该身份认证装置 1100 可以由软件、硬件或者两者的结合实现成为计算机设备的部分或者全部，该计算机设备可以为图 3 所示的计算机设备，该计算机设备为上述实施例中的授权设备。在本申请实施例中，该装置 1100 应用于授权设备，授权设备与终端设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系。参见图 11，该装置 1100 包括：接收模块 1101、第一验证模块 1102 和发送模块 1103。

接收模块 1101，用于接收第二认证请求，第二认证请求携带第一认证码，第一认证码由终端设备根据第一对称密钥生成；

第一验证模块 1102，用于根据第一对称密钥和所有权关系记录验证第一认证码；

发送模块 1103，用于在验证通过后，授权设备发送第一认证确认消息，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成，第二认证码指示终端设备根据第一对称密钥对第二认证码验证通过后确定终端设备与注册设备的双向身份认证通过。

可选地，第二认证请求还携带第一 ID、第一密钥参数和第一身份信息，第一密钥参数由终端设备生成，第一身份信息包括注册设备的身份信息和注册设备所属网络的身份信息中的至少一个，第一 ID 为终端设备的原所有者为终端设备配置的 ID，所有权关系记录包含第一

ID 与第一身份信息之间的映射关系；

该装置 1100 还包括：

第二验证模块，用于根据所有权关系记录验证第一 ID，以及验证第一身份信息；

第一验证模块包括：

验证子模块，用于根据所有权关系记录、第一 ID、第一对称密钥和第一密钥参数，验证第一认证码。

可选地，第一认证确认消息还携带第二密钥参数，第二密钥参数包含第二 AV 的明文或密文，第二 AV 的密文是使用授权设备与终端设备共享的密钥得到；

第二 AV 包含第二防重放攻击参数，第二认证码根据第一对称密钥和第二 AV 生成，第一认证确认消息还用于终端设备根据第一对称密钥和第二密钥参数验证第二认证码。

可选地，第一认证确认消息还携带密钥更新信息，密钥更新信息根据第一对称密钥和第二 AV 生成；

密钥更新信息用于注册设备获取与终端设备之间建立第一安全传输通道所需的通道安全密钥，以及与终端设备之间通过第一安全传输通道协商第二对称密钥，第二密钥参数还用于终端设备确定生成通道安全密钥所需的第一派生参数，以及确定与注册设备之间通过第一安全传输通道协商第二对称密钥所需的第二派生参数，第二对称密钥用于终端设备接入注册设备所属网络时的入网身份鉴权。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

需要说明的是：上述实施例提供的身份认证装置在身份认证时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的身份认证装置与身份认证方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

本申请实施例提供了一种身份认证系统，该身份认证系统包括终端设备、注册设备和授权设备，终端设备与授权设备共享第一对称密钥，授权设备存储有终端设备的所有权关系记录，该所有权关系记录描述了终端设备与终端设备的当前所有者的绑定关系；

终端设备用于向注册设备发送第一认证请求，第一认证请求携带第一认证码，第一认证码根据第一对称密钥生成；

注册设备用于接收第一认证请求，根据第一认证请求生成第二认证请求，向授权设备发送第二认证请求，第二认证请求携带第一认证码；

授权设备用于接收第二认证请求，根据第一对称密钥和所有权关系记录验证第一认证码，在验证通过后向注册设备发送第一认证确认消息，第一认证确认消息用于指示授权终端设备与注册设备所属网络的所有权关系，第一认证确认消息携带第二认证码，第二认证码根据第一对称密钥生成；

注册设备还用于接收第一认证确认消息，根据第一认证确认消息确定第二认证确认消息，向终端设备发送第二认证确认消息，第二认证确认消息携带第二认证码；

终端设备还用于接收第二认证确认消息，根据第一对称密钥验证第二认证码，在验证通过后确定终端设备与注册设备的双向身份认证通过。

在本申请实施例中，终端设备与授权设备之间通过共享第一对称密钥，实现基于对称密钥验证身份的方法，这样，在保证对称密钥机密性的情况下，整个身份认证的过程中基于对称密钥生成的认证码不易伪造，能够保证身份认证的安全可靠。另外，本方案通过授权设备实现对终端设备与注册设备的双向身份认证，避免了单向身份认证存在的安全隐患问题，也即本方案的安全性更高。

需要说明的是：上述实施例提供的身份认证系统与身份认证方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意结合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络或其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如：同轴电缆、光纤、数据用户线（digital subscriber line, DSL））或无线（例如：红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质，或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如：软盘、硬盘、磁带）、光介质（例如：数字通用光盘（digital versatile disc, DVD））或半导体介质（例如：固态硬盘（solid state disk, SSD））等。值得注意的是，本申请实施例提到的计算机可读存储介质可以为非易失性存储介质，换句话说，可以是非瞬时性存储介质。

应当理解的是，本文提及的“至少一个”是指一个或多个，“多个”是指两个或两个以上。在本申请实施例的描述中，除非另有说明，“/”表示或的意思，例如，A/B 可以表示 A 或 B；本文中的“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，为了便于清楚描述本申请实施例的技术方案，在本申请的实施例中，采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并不限定一定不同。

以上所述为本申请提供的实施例，并不用以限制本申请，凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

1.一种身份认证系统，其特征在于，所述身份认证系统包括终端设备、注册设备和授权设备，所述终端设备与所述授权设备共享第一对称密钥，所述授权设备存储有所述终端设备的所有权关系记录，所述所有权关系记录描述了所述终端设备与所述终端设备的当前所有者的绑定关系；

所述终端设备用于向所述注册设备发送第一认证请求，所述第一认证请求携带第一认证码，所述第一认证码根据所述第一对称密钥生成；

所述注册设备用于接收所述第一认证请求，根据所述第一认证请求生成第二认证请求，向所述授权设备发送所述第二认证请求，所述第二认证请求携带所述第一认证码；

所述授权设备用于接收所述第二认证请求，根据所述第一对称密钥和所述所有权关系记录验证所述第一认证码，在验证通过后向所述注册设备发送第一认证确认消息，所述第一认证确认消息用于指示授权所述终端设备与所述注册设备所属网络的所有权关系，所述第一认证确认消息携带第二认证码，所述第二认证码根据所述第一对称密钥生成；

所述注册设备还用于接收所述第一认证确认消息，根据所述第一认证确认消息确定第二认证确认消息，向所述终端设备发送所述第二认证确认消息，所述第二认证确认消息携带所述第二认证码；

所述终端设备还用于接收所述第二认证确认消息，根据所述第一对称密钥验证所述第二认证码，在验证通过后确定所述终端设备与所述注册设备的双向身份认证通过。

2.一种身份认证方法，其特征在于，所述方法由终端设备执行，所述终端设备与授权设备共享第一对称密钥，所述授权设备存储有所述终端设备的所有权关系记录，所述方法包括：

所述终端设备发送第一认证请求，所述第一认证请求携带第一认证码，所述第一认证码根据所述第一对称密钥生成；

所述终端设备接收第二认证确认消息，所述第二认证确认消息是根据所述第一对称密钥和所述所有权关系记录对所述第一认证码验证通过后确定的，所述第二认证确认消息携带第二认证码，所述第二认证码由所述授权设备根据所述第一对称密钥生成；

所述终端设备根据所述第一对称密钥验证所述第二认证码，在验证通过后确定所述终端设备与注册设备的双向身份认证通过。

3.如权利要求2所述的方法，其特征在于，所述第一认证请求还携带第一身份标识ID和第一密钥参数，所述第一密钥参数包含第一认证向量AV的明文或密文，所述第一ID为所述终端设备的原所有者为所述终端设备配置的ID；

所述第一AV包含第一随机参数和第一防重放攻击参数，所述第一随机参数由所述终端设备生成，所述第一随机参数包含第一随机数N1和第二随机数N2中的至少一项；

所述第一认证码根据所述第一对称密钥、所述第一ID和所述第一AV生成。

4.如权利要求3所述的方法，其特征在于，所述第一认证请求还携带第一身份信息，所述

第一身份信息包括所述注册设备的身份信息和所述注册设备所属网络的身份信息中的至少一个；

所述第一认证码根据所述第一对称密钥、所述第一 ID、所述第一 AV 以及所述第一身份信息生成。

5.如权利要求 2-4 任一所述的方法，其特征在于，所述第二认证确认消息还携带第二密钥参数；

所述终端设备根据所述第一对称密钥验证所述第二认证码，包括：

所述终端设备根据所述第一对称密钥和所述第二密钥参数生成对称验证密钥；

所述终端设备根据所述对称验证密钥验证所述第二认证码。

6.如权利要求 5 所述的方法，其特征在于，所述终端设备确定所述终端设备与注册设备的双向身份认证通过之后，还包括：

所述终端设备根据所述第一对称密钥和第一派生参数，生成通道安全密钥，所述第一派生参数根据所述第二密钥参数确定；

所述终端设备与所述注册设备之间基于所述通道安全密钥建立第一安全传输通道；

所述终端设备根据第二派生参数与所述注册设备之间通过所述第一安全传输通道协商第二对称密钥，所述第二对称密钥用于所述终端设备接入所述注册设备所属网络时的入网身份鉴权，所述第二派生参数根据所述第二密钥参数确定。

7.如权利要求 6 所述的方法，其特征在于，所述终端设备根据第二派生参数与所述注册设备之间通过所述第一安全传输通道协商所述第二对称密钥，包括：

所述终端设备生成随机数 N4，并将所述 N4 通过所述第一安全传输通道发送给所述注册设备，所述 N4 用于所述注册设备根据所述 N4 和第二协商密钥生成所述第二对称密钥，以及根据所述 N4 和所述第二对称密钥生成第三认证码，所述第二协商密钥由所述授权设备根据所述第二派生参数生成并发送给所述注册设备；

所述终端设备根据所述 N4 和所述第二派生参数生成所述第二对称密钥；

所述终端设备接收所述注册设备发送的第一协商确认消息，所述第一协商确认消息携带所述第三认证码；

所述终端设备根据自身生成的第二对称密钥和所述 N4 验证所述第三认证码，在验证通过后，将所述第二对称密钥更新为自身与所述注册设备之间的设备密钥，并向所述注册设备发送第二协商确认消息，所述第二协商确认消息用于指示所述注册设备将所述第二对称密钥更新为自身与所述终端设备之间的设备密钥。

8.如权利要求 6 所述的方法，其特征在于，所述终端设备根据第二派生参数与所述注册设备之间通过所述第一安全传输通道协商所述第二对称密钥，包括：

所述终端设备接收所述注册设备通过所述第一安全传输通道发送的随机数 N5，所述 N5 由所述注册设备随机生成，所述 N5 用于所述注册设备根据所述 N5 和所述第二协商密钥生成所述第二对称密钥，并将所述第二对称密钥更新为自身与所述终端设备之间的设备密钥；

所述终端设备根据所述 N5 和所述第二派生参数生成所述第二对称密钥，将所述第二对称密钥更新为自身与所述注册设备之间的设备密钥。

9.一种身份认证方法，其特征在于，所述方法由注册设备执行，所述方法包括：

所述注册设备接收第一认证请求，所述第一认证请求携带第一认证码，所述第一认证码由终端设备根据所述第一对称密钥生成，所述终端设备与授权设备共享第一对称密钥；

所述注册设备根据所述第一认证请求生成第二认证请求，向所述授权设备发送所述第二认证请求，所述第二认证请求携带所述第一认证码；

所述注册设备接收第一认证确认消息，所述第一认证确认消息是所述授权设备根据所述第一对称密钥和所述终端设备的所有权关系记录对所述第一认证码验证通过后确定的，所述授权设备存储有所述所有权关系记录，所述所有权关系记录描述了所述终端设备与所述终端设备的当前所有者的绑定关系，所述第一认证确认消息用于指示授权所述终端设备与所述注册设备所属网络的所有权关系，所述第一认证确认消息携带第二认证码，所述第二认证码根据所述第一对称密钥生成；

所述注册设备根据所述第一认证确认消息确定第二认证确认消息，向所述终端设备发送所述第二认证确认消息，所述第二认证确认消息携带所述第二认证码，所述第二认证确认消息用于指示所述终端设备根据所述第一对称密钥对所述第二认证码验证通过后确定所述终端设备与所述注册设备的双向身份认证通过。

10.如权利要求 9 所述的方法，其特征在于，所述第一认证请求还携带第一 ID，所述第一 ID 为所述终端设备的原所有者为所述终端设备配置的 ID，所述第二认证请求还携带所述第一认证请求中的所述第一 ID，所述第二认证请求还携带第一身份信息，所述第一身份信息包括所述注册设备的身份信息和所述注册设备所属网络的身份信息中的至少一个。

11.如权利要求 10 所述的方法，其特征在于，所述第二认证请求还携带所述注册设备的身份签名，所述注册设备的身份签名是所述注册设备使用私钥对所述第一认证请求和所述第一身份信息进行的签名。

12.如权利要求 10 或 11 所述的方法，其特征在于，所述注册设备的身份信息包括所述注册设备身份相关的数字证书和所述注册设备身份相关的数字证书的摘要中的至少一个。

13.如权利要求 9-12 任一所述的方法，其特征在于，所述第一认证确认消息还携带密钥更新信息，所述密钥更新信息使用所述注册设备与所述授权设备共享的对称密钥加密保护，或者，所述密钥更新信息使用所述注册设备的公钥加密保护；

所述注册设备接收所述第一认证确认消息之后，还包括：

所述注册设备从所述密钥更新信息中获取通道安全密钥；

所述注册设备向所述终端设备发送所述第二认证确认消息之后，还包括：

所述注册设备与所述终端设备之间基于所述通道安全密钥建立第一安全传输通道；

所述注册设备根据所述密钥更新信息，与所述终端设备之间通过所述第一安全传输通道

协商第二对称密钥，所述第二对称密钥用于所述终端设备接入所述注册设备所属网络时的入网身份鉴权。

14.一种身份认证方法，其特征在于，所述方法由授权设备执行，所述授权设备与终端设备共享第一对称密钥，所述授权设备存储有所述终端设备的所有权关系记录，所述所有权关系记录描述了所述终端设备与所述终端设备的当前所有者的绑定关系，所述方法包括：

所述授权设备接收第二认证请求，所述第二认证请求携带第一认证码，所述第一认证码由所述终端设备根据所述第一对称密钥生成；

所述授权设备根据所述第一对称密钥和所述所有权关系记录验证所述第一认证码；

在验证通过后，所述授权设备发送第一认证确认消息，所述第一认证确认消息用于指示授权所述终端设备与注册设备所属网络的所有权关系，所述第一认证确认消息携带第二认证码，所述第二认证码根据所述第一对称密钥生成，所述第二认证码指示所述终端设备根据所述第一对称密钥对所述第二认证码验证通过后确定所述终端设备与所述注册设备的双向身份认证通过。

15.如权利要求 14 所述的方法，其特征在于，所述第二认证请求还携带第一 ID、第一密钥参数和第一身份信息，所述第一密钥参数由所述终端设备生成，所述第一身份信息包括所述注册设备的身份信息和所述注册设备所属网络的身份信息中的至少一个，所述第一 ID 为所述终端设备的原所有者为所述终端设备配置的 ID，所述所有权关系记录包含所述第一 ID 与所述第一身份信息之间的映射关系；

所述授权设备接收第二认证请求之后，还包括：

所述授权设备根据所述所有权关系记录验证所述第一 ID，以及验证所述第一身份信息；

所述授权设备根据所述第一对称密钥和所述所有权关系记录验证所述第一认证码，包括：

所述授权设备根据所述所有权关系记录、所述第一 ID、所述第一对称密钥和所述第一密钥参数，验证所述第一认证码。

16.如权利要求 14 或 15 所述的方法，其特征在于，所述第一认证确认消息还携带第二密钥参数，所述第二密钥参数包含第二 AV 的明文或密文，所述第二 AV 的密文是使用所述授权设备与所述终端设备共享的密钥得到；

所述第二 AV 包含第二防重放攻击参数，所述第二认证码根据所述第一对称密钥和所述第二 AV 生成，所述第一认证确认消息还用于所述终端设备根据所述第一对称密钥和所述第二密钥参数验证所述第二认证码。

17.如权利要求 16 所述的方法，其特征在于，所述第一认证确认消息还携带密钥更新信息，所述密钥更新信息根据所述第一对称密钥和所述第二 AV 生成；

所述密钥更新信息用于所述注册设备获取与所述终端设备之间建立第一安全传输通道所需的通道安全密钥，以及与所述终端设备之间通过所述第一安全传输通道协商第二对称密钥，所述第二密钥参数还用于所述终端设备确定生成所述通道安全密钥所需的第一派生参数，以及确定与所述注册设备之间通过所述第一安全传输通道协商所述第二对称密钥所需的第二派

生参数,所述第二对称密钥用于所述终端设备接入所述注册设备所属网络时的入网身份鉴权。

18.一种身份认证装置,其特征在于,所述装置应用于终端设备,所述终端设备与授权设备共享第一对称密钥,所述授权设备存储有所述终端设备的所有权关系记录,所述所有权关系记录描述了所述终端设备与所述终端设备的当前所有者的绑定关系,所述装置包括:

发送模块,用于发送第一认证请求,所述第一认证请求携带第一认证码,所述第一认证码根据所述第一对称密钥生成;

接收模块,用于接收第二认证确认消息,所述第二认证确认消息是根据所述第一对称密钥和所述所有权关系记录对所述第一认证码验证通过后确定的,所述第二认证确认消息携带第二认证码,所述第二认证码由所述授权设备根据所述第一对称密钥生成;

验证模块,用于根据所述第一对称密钥验证所述第二认证码,在验证通过后确定所述终端设备与注册设备的双向身份认证通过。

19.一种身份认证装置,其特征在于,所述装置应用于注册设备,所述装置包括:

第一接收模块,用于接收第一认证请求,所述第一认证请求携带第一认证码,所述第一认证码由所述终端设备根据所述第一对称密钥生成,终端设备与授权设备共享第一对称密钥;

第一发送模块,用于根据所述第一认证请求生成第二认证请求,向所述授权设备发送所述第二认证请求,所述第二认证请求携带所述第一认证码;

第二接收模块,用于接收第一认证确认消息,所述第一认证确认消息是所述授权设备根据所述第一对称密钥和所述终端设备的所有权关系记录对所述第一认证码验证通过后确定的,所述授权设备存储有所述所有权关系记录,所述所有权关系记录描述了所述终端设备与所述终端设备的当前所有者的绑定关系,所述第一认证确认消息用于指示授权所述终端设备与所述注册设备所属网络的所有权关系,所述第一认证确认消息携带第二认证码,所述第二认证码根据所述第一对称密钥生成;

第二发送模块,用于根据所述第一认证确认消息确定第二认证确认消息,向所述终端设备发送所述第二认证确认消息,所述第二认证确认消息携带所述第二认证码,所述第二认证确认消息用于指示所述终端设备根据所述第一对称密钥对所述第二认证码验证通过后确定所述终端设备与所述注册设备的双向身份认证通过。

20.一种身份认证装置,其特征在于,所述装置应用于授权设备,所述授权设备与终端设备共享第一对称密钥,所述授权设备存储有所述终端设备的所有权关系记录,所述所有权关系记录描述了所述终端设备与所述终端设备的当前所有者的绑定关系,所述装置包括:

接收模块,用于接收第二认证请求,所述第二认证请求携带第一认证码,所述第一认证码由所述终端设备根据所述第一对称密钥生成;

第一验证模块,用于根据所述第一对称密钥和所述所有权关系记录验证所述第一认证码;

发送模块,用于在验证通过后,所述授权设备发送第一认证确认消息,所述第一认证确认消息用于指示授权所述终端设备与注册设备所属网络的所有权关系,所述第一认证确认消息携带第二认证码,所述第二认证码根据所述第一对称密钥生成,所述第二认证码指示所述终端设备根据所述第一对称密钥对所述第二认证码验证通过后确定所述终端设备与所述注册

设备的双向身份认证通过。

21.一种身份认证设备，其特征在于，所述身份认证设备包括存储器和处理器；

所述存储器，用于存储计算机程序；

所述处理器，用于执行所述计算机程序实现权利要求 1-8 任一项所述的方法，或者，实现权利要求 9-13 任一项所述的方法，或者，实现权利要求 14-17 任一项所述的方法。

22.一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内存储有计算机程序，所述计算机程序被处理器执行时实现权利要求 1-8 任一项所述的方法，或者，实现权利要求 9-13 任一项所述的方法，或者，实现权利要求 14-17 任一项所述的方法。