(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 107395567 A
(43)申请公布日 2017.11.24

(21)申请号 201710461378.5

(22)申请日 2017.06.16

(71)申请人 深圳市盛路物联通讯技术有限公司
地址 518000 广东省深圳市南山区南山街道科技园科技中三路5号国人通信大厦B栋328室

(72)发明人 杜光东

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
代理人 张全文

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

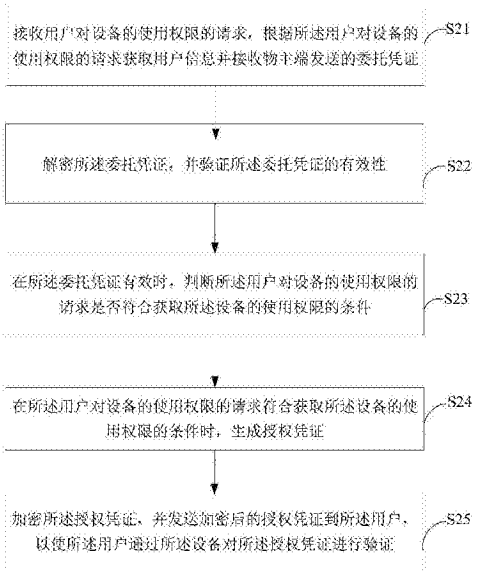
权利要求书2页 说明书14页 附图8页

(54)发明名称

一种基于物联网的设备使用权限获取方法及系统

(57)摘要

本发明适用于物联网信息安领域，提供了一种物联网的设备使用权限获取方法及系统。所述方法包括：根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；解密并验证所述委托凭证的有效性，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；符合时生成授权凭证；加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。用户通过请求代理端获取设备的使用权限，代理端根据用户的请求向物主端获取委托凭证等信息，避免了用户与物主的直接信息交换，既可以保护物主的个人信息安全，又能满足用户对设备的权限获取请求。



CN 107395567 A

1.一种基于物联网的设备使用权限获取方法，其特征在于，所述基于物联网的设备权限获取方法包括：

接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

解密所述委托凭证，并验证所述委托凭证的有效性；

在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

2.根据权利要求1所述的基于物联网的设备使用权限获取方法，其特征在于，所述解密所述委托凭证，并验证所述委托凭证的有效性，具体包括：

解密所述委托凭证，得到所述委托凭证的生成时间及委托内容；

判断所述委托凭证的生成时间是否在有效期内；

当所述委托凭证的生成时间在有效期内时，调用预先存储的委托信息，匹配所述委托内容与所述委托信息，根据匹配结果最终判断所述委托凭证的有效性。

3.根据权利要求2所述的基于物联网的设备使用权限获取方法，其特征在于，所述在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件，具体包括：

在所述委托凭证有效时，获取所述用户对设备的使用权限的请求携带的ID信息；

获取与所述ID信息对应的用户信用等级；

在所述用户信用等级符合要求时，判定所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件，否则，判定所述用户对设备的使用权限的请求不符合获取所述设备的使用权限的条件。

4.根据权利要求1所述的基于物联网的设备使用权限获取方法，其特征在于，在所述接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求，获取用户信息并接收物主端发送的委托凭证之前，包括：

接收服务器发送的认证信息、物主信息以及处于正常状态下的设备信息。

5.根据权利要求1-4任一项所述的基于物联网的设备使用权限获取方法，其特征在于，在所述加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证之后，包括：

接收所述设备对所述授权凭证的验证结果，并发送所述验证结果到所述物主端。

6.一种基于物联网的设备使用权限获取系统，其特征在于，所述基于物联网的设备权限获取系统包括：

委托凭证获取单元，用于接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

委托凭证验证单元，用于解密所述委托凭证，并验证所述委托凭证的有效性；

条件判断单元，用于在所述委托凭证有效时，判断所述用户对设备的使用权限的请求

是否符合获取所述设备的使用权限的条件；

授权凭证生成单元，用于在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

授权凭证加密单元，用于加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

7.根据权利要求6所述的基于物联网的设备使用权限获取系统，其特征在于，所述委托凭证验证单元，具体包括：

解密模块，用于解密所述委托凭证，得到所述委托凭证的生成时间及委托内容；

初步判断模块，用于判断所述委托凭证的生成时间是否在有效期内；

匹配模块，用于当所述委托凭证的生成时间在有效期内时，调用预先存储的委托信息，匹配所述委托内容与所述委托信息，根据匹配结果最终判断所述委托凭证的有效性。

8.根据权利要求7所述的基于物联网的设备使用权限获取系统，其特征在于，所述条件判断单元，具体包括：

ID获取模块，用于在所述委托凭证有效时，获取所述用户对设备的使用权限的请求携带的ID信息；

信用等级获取模块，用于获取与所述ID信息对应的用户信用等级；

条件判断模块，用于在所述用户信用等级符合要求时，判定所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件，否则，判定所述用户对设备的使用权限的请求不符合获取所述设备的使用权限的条件。

9.一种基于物联网的设备使用权限获取系统，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至5任一项所述基于物联网的设备使用权限获取方法的步骤。

10.一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程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至5任一项所述基于物联网的设备使用权限获取方法的步骤。

一种基于物联网的设备使用权限获取方法及系统

技术领域

[0001] 本发明实施例属于物联网信息安全领域，尤其涉及一种物联网的设备使用权限获取方法及系统。

背景技术

[0002] 物联网即物物相连的互联网，它被预言为继互联网之后全球信息产业的又一次科技与经济浪潮，受到各国政府、企业和学术界的重视，美国、欧盟、日本等甚至将其纳入国家和区域信息化战略。目前物联网应用在发展过程中面临很多问题。首先，从物联网体系架构可以看到，物联网终端种类繁多，日常生活生产中绝大多数的设施都可以通过射频技术将其连接到物联网系统内，因此，如何有效的管理这些终端设施是物联网应用首先要考虑的一个问题；其次，目前按终端的位置属性或类型属性对终端进行分组管理，一个应用可能会涉及一个以上的终端组，这样对应用来讲开发和维护比较复杂，并且这样的布局也不利于对各个终端的充分利用。由于物联网中各种设施都在某种程度上隶属于个人或集体，而在各种设施利用过程中避免不了各种信息的传递，因此，无论是解决如何有效管理物联网中不断增加的各种设备问题还是解决如何有效的利用物联网中各种设施问题，都还面临着同一个问题---如何有效的保护物联网中各种设施的拥有者隐私的问题。

[0003] 例如，在物联网中对于一个城市的各种设施和公共服务而言，城市中的每个用户既可以是提供者也可以是使用者，也就是说，用户可以通过物联网将自己的个人设施或其他资源共享，如汽车、停车位、房屋等，从而帮助政府更有效合理地管理和利用城市设施及个人资源，改善交通、医疗、教育、旅游等各领域的管理效率和服务质量，促进城市的和谐发展。在如此开放分享的城市物联网环境中，物联网设备有可能被多次分享使用，因此共享设备的使用权可以从物主传递到不同的用户(比如由物主传递到物主的朋友或朋友的朋友等)；在各种设施的使用权转移过程中存在许多信息的传递，然而，现有技术还无法保证这一信息传递过程的安全性，并且也无法对物主的身份等隐私信息进行有效保护。

发明内容

[0004] 本发明实施例提供了一种基于物联网的设备使用权限获取方法及系统，旨在解决现有技术物联网中各种设施的使用权转移时无法保证转移的信息的安全性及无法保护物主隐私信息的问题。

[0005] 本发明实施例第一方面，提供了一种基于物联网的设备使用权限获取方法，所述基于物联网的设备权限获取方法包括：

[0006] 接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0007] 解密所述委托凭证，并验证所述委托凭证的有效性；

[0008] 在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

[0009] 在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0010] 加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0011] 优选地，所述解密所述委托凭证，并验证所述委托凭证的有效性，具体包括：

[0012] 解密所述委托凭证，得到所述委托凭证的生成时间及委托内容；

[0013] 判断所述委托凭证的生成时间是否在有效期内；

[0014] 当所述委托凭证的生成时间在有效期内时，调用预先存储的委托信息，匹配所述委托内容与所述委托信息，根据匹配结果最终判断所述委托凭证的有效性。

[0015] 优选地，所述在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件，具体包括：

[0016] 在所述委托凭证有效时，获取所述用户对设备的使用权限的请求携带的ID信息；

[0017] 获取与所述ID信息对应的用户信用等级；

[0018] 在所述用户信用等级符合要求时，判定所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件，否则，判定所述用户对设备的使用权限的请求不符合获取所述设备的使用权限的条件。

[0019] 优选地，在所述接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求，获取用户信息并接收物主端发送的委托凭证之前，包括：

[0020] 接收服务器发送的认证信息、物主信息以及处于正常状态下的设备信息。

[0021] 优选地，在所述加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证之后，包括：

[0022] 接收所述设备对所述授权凭证的验证结果，并发送所述验证结果到所述物主端。

[0023] 本发明实施例的第二方面，提供一种基于物联网的设备使用权限获取系统，所述基于物联网的设备权限获取系统包括：

[0024] 委托凭证获取单元，用于接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0025] 委托凭证验证单元，用于解密所述委托凭证，并验证所述委托凭证的有效性；

[0026] 条件判断单元，用于在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

[0027] 授权凭证生成单元，用于在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0028] 授权凭证加密单元，用于加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0029] 优选地，所述委托凭证验证单元，具体包括：

[0030] 解密模块，用于解密所述委托凭证，得到所述委托凭证的生成时间及委托内容；

[0031] 初步判断模块，用于判断所述委托凭证的生成时间是否在有效期内；

[0032] 匹配模块，用于当所述委托凭证的生成时间在有效期内时，调用预先存储的委托信息，匹配所述委托内容与所述委托信息，根据匹配结果最终判断所述委托凭证的有效性。

[0033] 优选地，所述条件判断单元，具体包括：

[0034] ID获取模块，用于在所述委托凭证有效时，获取所述用户对设备的使用权限的请求携带的ID信息；

[0035] 信用等级获取模块，用于获取与所述ID信息对应的用户信用等级；

[0036] 条件判断模块，用于在所述用户信用等级符合要求时，判定所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件，否则，判定所述用户对设备的使用权限的请求不符合获取所述设备的使用权限的条件。

[0037] 优选地，所述基于物联网的设备使用权限获取系统，还包括：

[0038] 信息接收单元，用于接收服务器发送的认证信息、物主信息以及处于正常状态下的设备信息。

[0039] 优选地，所述基于物联网的设备使用权限获取系统，还包括：

[0040] 验证结果接收单元，用于接收所述设备对所述授权凭证的验证结果，并发送所述验证结果到所述物主端。

[0041] 在本发明实施例中，由代理端接收用户发送的对设备的使用权限的请求，然后根据用户的请求向物主端获取委托凭证，对获取到的委托凭证解密后验证其有效性，在判断出所接收到的委托凭证为有效的委托凭证后，对用户进行判断，已确定当前用户是否符合获取所请求设备的使用权限的条件。在用户符合获取所请求设备的使用权限的条件时才生成授权凭证，授权用户获取使用权限。这一过程中，用户通过请求代理端获取设备的使用权限，代理端根据用户的请求向物主端获取委托凭证等信息，避免了用户与物主的直接信息交换，既可以保护物主的个人信息安全，又能满足用户对设备的权限获取请求。

附图说明

[0042] 图1是现有技术中物联网系统中各种设备分布的结构示意图；

[0043] 图2是本发明第一实施例提供的一种基于物联网的设备使用权限获取方法的流程图；

[0044] 图3是第一实施例提供的图2中步骤S22的具体流程图；

[0045] 图4是第一实施例提供的图2中步骤S23的具体流程图；

[0046] 图5是本发明第二实施例提供的一种基于物联网的设备使用权限获取方法的流程图；

[0047] 图6是本发明第三实施例提供的一种基于物联网的设备使用权限获取方法的流程图；

[0048] 图7是本发明第四实施例提供的一种基于物联网的设备使用权限获取系统的结构图。

[0049] 图8是本发明第五实施例提供的一种基于物联网的设备使用权限获取系统的结构图；

[0050] 图9是本发明第六实施例提供的一种基于物联网的设备使用权限获取系统的结构图。

具体实施方式

[0051] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对

本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0052] 本发明实施例中，代理端根据用户对公共资源中设备使用权限的请求，接收物主端发送的带有加密信息的委托凭证；对所述委托凭证解密后，验证其有效性，并确定所述用户是否有获取所请求设备的使用权限，在判定出用户有获取所述设备使用权限后，生成授权凭证，对所述授权凭证加密后发送到所述用户。此过程中由物主端委托代理端管理其拥有的并作为公共资源使用的设备，在代理端判定发送使用权限请求的用户对所请求设备具有合法的使用权时，直接发送授权凭证到所述用户，无需涉及物主的身份信息，避免了用户与物主间的直接信息传递，从而保护了物主的私人信息。

[0053] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0054] 实施例一：

[0055] 图1示出了现有技术中物联网系统中各种设备分布的结构示意图，如图1中所示物联网作为一个管理平台可以应用在智能运输、建筑、医疗、环境保护、公共安全、移动POS、供应链、农业、林业、水务、金融等多个方面。在公共安全方面物联网可以通过管理平台统一接收各方传递的安全信息，并将各种安全保障设备通过互联网接入物联网管理系统中，当接收到某一方面待处理安全隐患时，由物联网管理系统调度附近相关设备处理安全隐患。

[0056] 在应用于城市中各种公共资源时，城市中的每个用户都可以将自己拥有的设备作为公共资源供大家来使用，以达到节约资源，最大程度利用各种设备的目的。此时，只需通过网络将每个用户的各种设备连接起来，在其他用户需要使用另一用户的设备时，经物主授权即可使用。这一过程中对每个用户而言既是公共资源的提供者也是公共资源的受益者。当用户需要使用某一物主设备时，必然会与物主发生信息的交互，以获得使用权限，但现有技术很难保证这一信息交互过程中，交互双方个人信息的安全性，并且，对于一个物主可以有无数的用户向其请求某一设备的使用权限，在于多个用户进行信息交互时，物主的个人信息可能被多个用户获知，完全不利于对物主个人信息的保护。

[0057] 因此，图2示出了本发明第一实施例提供的一种基于物联网的设备使用权限获取方法及系统的流程图，详述如下：

[0058] 步骤S21，接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0059] 具体地，首先在物联网系统中设置代理端，在用户需要获取某一设备的使用权时，可以通过自身智能终端发送请求到代理端，代理端根据用户对设备使用权限的请求，向物主端请求委托权限，物主端接收到代理端的请求，调用并查看所拥有的设备的使用情况，筛选出当前正处于空闲状态的设备，查看这些处于空闲状态的设备是否处于正常的可使用状态，对于可以正常使用的设备设置其对外使用的时间信息及地点信息；物主端将可正常使用的设备的数量，设备的当前位置，某一特定设备可对外使用的时间信息以及可对外使用的地点信息、代理端的权限范围以及用户必须具备的条件等信息整合成委托凭证发送给代理端。

[0060] 例如，某一城市市民可将自己的雨伞、自行车、私家车甚至闲置的房屋通过无线射频识别技术(Radio Frequency Identification，RFID)接入物联网系统中，若有用户向代理端发送物主房屋使用权限，则代理端向物主端请求委托凭证，物主端将目前闲置的房屋

的对外使用时间，使用的方式(如用户只能用于自己居住，不得用于生产、制造，不得对房屋随意改造等)等信息整合后生成委托凭证发送给代理端。

[0061] 优选地，物主端在发送所述委托凭证到代理端前对所述委托凭证进行加密，发送加密后的委托凭证到代理端，代理端对所接收到的加密后的委托凭证进行解密，方可获取委托凭证。事先对委托凭证进行加密，避免委托凭证在发送过程中被篡改。

[0062] 该步骤中，在代理端向物主端请求委托凭证时，物主端会整合当前可对外使用的设备的各种信息形成委托凭证，代理端通过委托凭证中包含的各种信息，响应用户对某一设备的使用权限的请求。此过程中由代理端直接向用户授权，避免了用户与物主的直接信息交换，有效的保护了物主的个人信息。并且在物主端向代理端发送的委托凭证中包含有设备的使用权限并规定了代理端的权限，因此，既能充分的利用现有设备又能充分尊重物主意愿，达到了物主与用户共赢的效果。

[0063] 步骤S22，解密所述委托凭证，并验证所述委托凭证的有效性；

[0064] 该步骤中，代理端接收到加密后的委托凭证后对所述委托凭证进行解密，获取所述委托凭证的内容，委托凭证生成的时间等信息以验证所述委托凭证的有效性。

[0065] 如图3所示，优选地，所述解密所述委托凭证，并验证所述委托凭证的有效性，具体包括：

[0066] 步骤S221，解密所述委托凭证，得到所述委托凭证的生成时间及委托内容；

[0067] 步骤S222，判断所述委托凭证的生成时间是否在有效期内；

[0068] 步骤S223，当所述委托凭证的生成时间在有效期内时，调用预先存储的委托信息，匹配所述委托内容与所述委托信息，根据匹配结果最终判断所述委托凭证的有效性。

[0069] 具体地，由于代理端接收到的委托凭证是经物主端通过代理端的公钥加密后的委托凭证，因此，代理端必须通过自身私钥对所接收到的委托凭证进行解密才可以获得其中内容。物主端将委托凭证加密后再发送至代理端，避免了委托凭证在发送过程被篡改的危险，保护了物主及其设备的安全。代理端解密委托凭证后获取委托凭证的生成时间信息及委托内容。所述委托内容包括设备的当前位置、对外开放的时间、对外开放的地点、请求使用权限的用户必须满足的条件、代理端的代理权限等。

[0070] 其中所述对外开放时间包括指设备可以供物主之外的人的使用时间，例如可以将某种设备的对外开放时间设定成每周工作日的上午8:00-12:00，设定设备对外开放时间不仅可以满足物主自身使用需求，也可以在物主不需要使用该设备时，提供给他人使用，以充分发挥设备的功用；所述对外开放地点包括物主之外的用户可以使用设备的地点，可以预先在设备上安装定位系统，设备通过自带的定位系统判断自身所处的位置，因此，可以限定设备必须在物主所在市区或物主所在市区的某个范围内使用，若设备定位系统发现所述设备在预先设置的对外开放地点以外则立即向代理端发送预警，提醒代理端关注此设备，以保证设备的安全，保障物主的资产安全；所述请求使用权限的用户必须满足的条件包括用户的信用等级、用户请求的使用权限的范围等；所述代理端的代理权限指物主端赋予代理端的可以对物主的设备的处理权限，物主端既可以在委托凭证中明确的限定代理端的代理权限范围，也可以规定代理端可以根据实际情况自主行使代理权限。

[0071] 优选地，所述委托凭证中还可以包括：物主的个人信息、物主拥有的设备的参数，所述物主的个人信息包括：物主身份唯一确认凭证，物主联系方式等，所述物主拥有的设备

的参数包括:设备数量,设备的型号,设备的简要使用说明等。

[0072] 该步骤中,代理端将解密委托凭证后获取的委托凭证的生成时间与预先设置的有效期进行对比,以初步确定所述委托凭证的有效性。所述有效期可以为从接受到用户的使用权限请求开始的十分钟内,或半小时内,或一天内;有效期的具体设置根据用户所请求的设备不同而不同,可根据实际情况进行设定,这里不做限制。验证所接收到的委托凭证是否在有效期内,可以避免物主端在接收到代理端委托凭证请求时,不能及时处理,而在物主端有时间处理时,距离用户发出请求时已经过很长一段时间,造成用户不再需要此设备的使用权限,而代理端又赋予了其使用权的状况。即避免代理端对用户的无效授权。若所述委托凭证的生成时间在有效期范围内,则初步判定所述委托凭证为有效的委托凭证。

[0073] 在初步确定所述委托凭证为有效委托凭证时,调用预先存储的委托信息,对比所述委托凭证内容与所述委托信息是否一致,所述委托信息为经权威认证机构认证过的物主端与代理端之间的代理协议,包括物主端物主的个人信息、物主端委托代理端代理的代理年限、代理端的负责人的个人信息等。在所述委托凭证中的物主个人信息与所述委托信息中的物主的个人信息一致时,最终判定所述委托凭证为有效委托凭证;将所述委托凭证中的物主的个人信息与所述委托信息中物主的个人信息进行匹配,以确定物主身份真实唯一,同时也确定该代理端对该物主端具有合法的代理权限。

[0074] 该步骤中,代理端通过解密所述委托凭证以获取所述委托凭证的生成时间,通过所述委托凭证的时间初步判定委托凭证的有效性,避免了代理端对用户的无效授权。然后通过解密后的委托凭证中的物主端物主个人信息与事先存储的物主个人信息相匹配以确定物主身份及代理端代理的合法性。

[0075] 步骤S23,在所述委托凭证有效时,判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件;

[0076] 该步骤中,在确定物主端发送的委托凭证为有效委托凭证后,调用发送请求的用户的个人信息,由于委托凭证中事先规定了对特定设备请求其使用权限的用户必须满足一定的条件,因此,这里将用户的个人信息与委托凭证中规定的用户必须具备的条件进行匹配,在用户符合条件时才给予其使用权限。

[0077] 如图4所示,优选地,所述在所述委托凭证有效时,判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件,具体包括:

[0078] 步骤S231,在所述委托凭证有效时,获取所述用户对设备的使用权限的请求携带的ID信息;

[0079] 步骤S232,获取与所述ID信息对应的用户信用等级;

[0080] 步骤S233,在所述用户信用等级符合要求时,判定所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件,否则,判定所述用户对设备的使用权限的请求不符合获取所述设备的使用权限的条件。

[0081] 具体地,确定物主端发送的委托凭证为有效委托凭证后,调用接收到的用户发送对设备的使用权限请求时包含的用户信息,通过用户信息中的ID信息调用用户的信用等级,将用户的信用等级与预设的信用等级相对比,只有在用户信用等级大于或等于预设的信用等级时,才判断用户为合法的用户,符合获取设备的使用权限的条件,否则,判定用户不符合获取所请求设备的使用权限的条件。

[0082] 该步骤中，首先对用户的ID信息进行验证以确定用户的合法性，在用户为合法用户时再对其信用程度进行校验，只有满足一定信用等级用户才会被授予使用权限，用户信用程度高说明其信誉好，有助于对物主设备的保护。

[0083] 步骤S24，在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0084] 该步骤中，事先对根据用户对设备使用权限的请求判断用户是否符合授权使用条件再生成授权凭证，只对符合授权条件的用户生成授权凭证，避免了不必要的授权凭证的生成。例如有些用户发送对公共自行车设备的使用权限请求，虽然请求本身是合法的，但判断用户的条件时，发现用户由于自身条件等原因不符合授权要求，则此情况下不生成授权凭证。

[0085] 步骤S25，加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0086] 该步骤中，代理端对生成的授权凭证进行加密，发送加密后的授权凭证给用户。保证了用户接受到的授权凭证不会被肆意修改。用户接受到完整的授权凭证后通过设备对解密后的授权凭证进行验证，验证通过后即可得到设备的使用权。

[0087] 本发明第一实施例中，代理端根据用户对设备的使用权限的请求，接收物主端发送的加密后的委托凭证；对所述委托凭证解密后，验证其有效性，并确定所述用户是否有获取所请求设备的使用权限，在判定出用户有获取所述设备使用权限后，生成授权凭证，对所述授权凭证加密后发送到所述用户。此过程中由物主端委托代理端管理其拥有的并作为公共资源使用的设备，在代理端判定发送使用权限请求的用户对所请求设备具有合法的使用权时，直接发送授权凭证到所述用户，无需涉及物主的身份信息，避免了用户与物主间的直接信息传递，从而保护了物主的私人信息。

[0088] 应理解，在本发明实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0089] 实施例二：

[0090] 图5示出了本发明第二实施例提供的一种基于物联网的设备使用权限获取方法的流程图；如图5所示，所述基于物联网的设备使用权限获取方法包括：

[0091] 步骤S51，接收服务器发送的认证信息，物主信息以及处于正常状态下的设备信息；

[0092] 该步骤中，首先由服务器对代理端进行审查判定，当代理端满足预设的条件时，则认定其为合法的代理端；合法的代理端才享有代理权限，并发送认证信息到合法的代理端。服务器统计一定范围内物联网系统中处于正常使用状态下的各种设备，以及所述设备的物主信息，将这些信息整合后发送到具有代理权限的代理端。所述认证信息包括：服务器根据对代理端的调查结果生成的对代理端的信用评价，代理端的代理时间期限等。另外，在用户发送设备的使用权限请求时，也可以先查看代理端是否有认证信息，或根据代理端的认证信息中的信用评价对代理端做出选择。

[0093] 步骤S52，接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0094] 步骤S53，解密所述委托凭证，并验证所述委托凭证的有效性；

[0095] 步骤S54，在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

[0096] 步骤S55，在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0097] 步骤S56，加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0098] 本实施例中步骤S52-步骤S56与实施例一中步骤S21-步骤S25分别对应，在此不再赘述。

[0099] 本发明第二实施例中在接收用户发送的对设备的使用权限的请求，首先接收服务器发送的认证信息，物主信息即可被利用的设备的信息；由于代理端具有为物主个人信息保密的义务，因此，该步骤中首先对代理端进行认证，确定其合法性，既可以保证物主设备的安全也可以保证物主及用户的个人信息不被随意泄漏。

[0100] 应理解，在本发明实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0101] 实施例三

[0102] 图6示出了本发明第三实施例提供的一种基于物联网的设备使用权限获取方法的流程图；如图6所示，所述基于物联网的设备使用权限获取方法包括：

[0103] 步骤S61，接收服务器发送的认证信息，物主信息以及处于正常状态下的设备信息；

[0104] 步骤S62，接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0105] 步骤S63，解密所述委托凭证，并验证所述委托凭证的有效性；

[0106] 步骤S64，在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

[0107] 步骤S65，在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0108] 步骤S66，加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0109] 本实施例中步骤S61-步骤S66与实施例二中步骤S51-步骤S56分别对应，在此不再赘述。

[0110] 步骤S67，接收所述设备对所述授权凭证的验证结果，并发送所述验证结果到所述物主端。

[0111] 该步骤中，用户接收到代理端发送的授权凭证后，用自己的私钥对加密后的授权凭证进行解密，以获得使用权限，用户将授权凭证中包含的信息发送到设备后，设备对接收到的信息进行验证，验证通过则对用户开放使用权限，并将所述验证结果发送到代理端，以供对其进行记录存档，并发送验证结果到物主端，以使物主得知自己设备的被使用情况。

[0112] 本发明第三实施例中用户得到所请求设备的授权凭证后，由设备对授权凭证中包

含信息进行验证，验证通过则对用户开放使用权限，并发送验证结果到代理端，代理端记录后再发送验证结果到物主端，这一过程中避免了用户与物主的直接通信，既保护了物主个人信息不被泄漏也可保证用户个人的安全。

[0113] 应理解，在本发明实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0114] 实施例四

[0115] 图7示出了本发明第四实施例提供的一种基于物联网的设备使用权限获取系统的结构图，该基于物联网的设备使用权限获取系统可应用于各种移动终端中。为了便于说明，仅示出了与本发明实施例相关的部分。

[0116] 如图7所述，所述基于物联网的设备使用权限获取系统包括：委托凭证获取单元71，委托凭证验证单元72，条件判断单元73，授权凭证生成单元74，授权凭证加密单元75，其中：

[0117] 委托凭证获取单元71，用于接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0118] 具体地，首先在物联网系统中设置代理端，在用户需要获取某一设备的使用权时，可以通过自身智能终端发送请求到代理端，代理端根据用户对设备使用权限的请求，向物主端请求委托权限，物主端接收到代理端的请求，调用并查看所拥有的设备的使用情况，筛选出当前正处于空闲状态的设备，查看这些处于空闲状态的设备是否处于正常的可使用状态，对于可以正常使用的设备设置其对外使用的时间信息及地点信息；物主端将可正常使用的设备的数量，设备的当前位置，某一特定设备可对外使用的时间信息以及可对外使用的地点信息、代理端的权限范围以及用户必须具备的条件等信息整合成委托凭证发送给代理端。

[0119] 例如，某一城市市民可将自己的雨伞、自行车、私家车甚至闲置的房屋通过无线射频识别技术(Radio Frequency Identification，RFID)接入物联网系统中，若有用户向代理端发送物主房屋使用权限，则代理端向物主端请求委托凭证，物主端将目前闲置的房屋的对外使用时间，使用的方式(如用户只能用于自己居住，不得用于生产、制造，不得对房屋随意改造等)等信息整合后生成委托凭证发送给代理端。

[0120] 优选地，物主端在发送所述委托凭证到代理端前对所述委托凭证进行加密，发送加密后的委托凭证到代理端，代理端对所接收到的加密后的委托凭证进行解密，方可获取委托凭证。事先对委托凭证进行加密，避免委托凭证在发送过程中被篡改。

[0121] 该步骤中，在代理端向物主端请求委托凭证时，物主端会整合当前可对外使用的设备的各种信息形成委托凭证，代理端通过委托凭证中包含的各种信息，响应用户对某一设备的使用权限的请求。此过程中由代理端直接向用户授权，避免了用户与物主的直接信息交换，有效的保护了物主的个人信息。并且在物主端向代理端发送的委托凭证中包含有设备的使用权限并规定了代理端的权限，因此，既能充分的利用现有设备又能充分尊重物主意愿，达到了物主与用户共赢的效果。

[0122] 委托凭证验证单元72，用于解密所述委托凭证，并验证所述委托凭证的有效性；

[0123] 该步骤中，代理端接收到加密后的委托凭证后对所述委托凭证进行解密，获取所

述委托凭证的内容，委托凭证生成的时间等信息以验证所述委托凭证的有效性。

[0124] 优选地，所述委托凭证验证单元，具体包括：

[0125] 解密模块，用于解密所述委托凭证，得到所述委托凭证的生成时间及委托内容；

[0126] 初步判断模块，用于判断所述委托凭证的生成时间是否在有效期内；

[0127] 匹配模块，用于当所述委托凭证的生成时间在有效期内时，调用预先存储的委托信息，匹配所述委托内容与所述委托信息，根据匹配结果最终判断所述委托凭证的有效性。

[0128] 具体地，由于代理端接收到的委托凭证是经物主端通过代理端的公钥加密后的委托凭证，因此，代理端必须通过自身私钥对所接收到的委托凭证进行解密才可以获得其中内容。物主端将委托凭证加密后再发送至代理端，避免了委托凭证在发送过程被篡改的危险，保护了物主及其设备的安全。代理端解密委托凭证后获取委托凭证的生成时间信息及委托内容。所述委托内容包括设备的当前位置、对外开放的时间、对外开放的地点、请求使用权限的用户必须满足的条件、代理端的代理权限等。

[0129] 其中所述对外开放时间包括指设备可以供物主之外的人的使用时间，例如可以将某种设备的对外开放时间设定成每周工作日的上午8:00-12:00，设定设备对外开放时间不仅可以满足物主自身使用需求，也可以在物主不需要使用该设备时，提供给他人使用，以充分发挥设备的功用；所述对外开放地点包括物主之外的用户可以使用设备的地点，例如，设备通过自带的定位系统判断自身所处的位置，因此，可以限定设备必须在物主所在市区或物主所在市区的某个范围内使用，若设备定位系统发现所述设备在预先设置的对外开放地点以外则立即向代理端发送预警，提醒代理端关注此设备，以保证设备的安全，保障物主的资产安全；所述请求使用权限的用户必须满足的条件包括用户的信用等级、用户请求的使用权限的范围等；所述代理端的代理权限指物主端赋予代理端的可以对物主的设备的处理权限，物主端既可以在委托凭证中明确的限定代理端的代理权限范围，也可以规定代理端可以根据实际情况自主行使代理权限。

[0130] 优选地，所述委托凭证中还可以包括：物主的个人信息、物主拥有的设备的参数，所述物主的个人信息包括：物主身份唯一确认凭证，物主联系方式等，所述物主拥有的设备的参数包括：设备数量，设备的型号，设备的简要使用说明等。

[0131] 该步骤中，代理端将解密委托凭证后获取的委托凭证的生成时间与预先设置的有效期进行对比，以初步确定所述代理凭证的有效性。所述有效期可以为从接受到用户的使用权限请求开始的十分钟内，或半小时内，或一天内；有效期的具体设备根据用户所请求的设备不同而不同，可根据实际情况进行设定，这里不做限制。验证所接收到的委托凭证是否在有效期内，可以避免物主端在接收到代理端委托凭证请求时，不能及时处理，而在物主端有时间处理时，距离用户发出请求时已经过很长一段时间，造成用户不再需要此设备的使用权限，而代理端又赋予了其使用权的状况。即避免代理端对用户的无效授权。若所述委托凭证的生成时间在有效期范围内，则初步判定所述委托凭证为有效的委托凭证。

[0132] 在初步确定所述委托凭证为有效委托凭证时，调用预先存储的委托信息，对比所述委托凭证内容与所述委托信息是否一致，所述委托信息为经权威认证机构认证过的物主端与代理端之间的代理协议，包括物主端物主的个人信息、物主端委托代理端代理的代理年限、代理端的负责人的个人信息等。在所述委托凭证中的物主个人信息与所述委托信息中的物主的个人信息一致时，最终判定所述委托凭证为有效委托凭证；将所述委托凭证中

的物主的个人信息与所述委托信息中物主的个人信息进行匹配，以确定物主身份真实唯一，同时也确定该代理端对该物主端具有合法的代理权限。

[0133] 该步骤中，代理端通过解密所述委托凭证以获取所述委托凭证的生成时间，通过所述委托凭证的时间初步判定委托凭证的有效性，避免了代理端对用户的无效授权。然后通过解密后的委托凭证中的物主端物主个人信息与事先存储的物主个人信息相匹配以确定物主身份及代理端代理的合法性。

[0134] 条件判断单元73，用于在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

[0135] 该步骤中，在确定物主端发送的委托凭证为有效委托凭证后，调用发送请求的用户的个人信息，由于委托凭证中事先规定了对特定设备请求其使用权限的用户必须满足一定的条件，因此，这里将用户的个人信息与委托凭证中规定的用户必须具备的条件进行匹配，在用户符合条件时才给予其使用权限。

[0136] 优选地，所述条件判断单元73，具体包括：

[0137] ID获取模块，用于在所述委托凭证有效时，获取所述用户对设备的使用权限的请求携带的ID信息；

[0138] 信用等级获取模块，用于获取与所述ID信息对应的用户信用等级；

[0139] 条件判断模块，用于在所述用户信用等级符合要求时，判定所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件，否则，判定所述用户对设备的使用权限的请求不符合获取所述设备的使用权限的条件。

[0140] 具体地，确定物主端发送的委托凭证为有效委托凭证后，调用接收到的用户发送对设备的使用权限请求时包含的用户信息，通过用户信息中的ID信息调用用户的信用等级，将用户的信用等级与预设的信用等级相对比，只有在用户信用等级大于或等于预设的信用等级时，才判断用户为合法的用户，符合获取设备的使用权限的条件，否则，判定用户不符合获取所请求设备的使用权限的条件。

[0141] 该步骤中，首先对用户的ID信息进行验证以确定用户的合法性，在用户为合法用户时再对其信用程度进行校验，只有满足一定信用等级用户才会被授予使用权限，用户信用程度高说明其信誉好，有助于对物主设备的保护。

[0142] 授权凭证生成单元74，用于在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0143] 具体地，事先对根据用户对设备使用权限的请求判断用户是否符合授权使用条件再生成授权凭证，只对符合授权条件的用户生成授权凭证，避免了不必要的授权凭证的生成。例如有些用户发送对公共自行车设备的使用权限请求，虽然请求本身是合法的，但判断用户的条件时，发现用户由于自身条件等原因不符合授权要求，则此情况下不生成授权凭证。

[0144] 授权凭证加密单元75，用于加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0145] 具体地，代理端对生成的授权凭证进行加密，发送加密后的授权凭证给用户。保证了用户接受到的授权凭证不会被肆意修改。用户接受到完整的授权凭证后通过设备对解密后的授权凭证进行验证，验证通过后即可得到设备的使用权。

[0146] 本发明第四实施例中，代理端根据用户对设备的使用权限的请求，接收物主端发送的加密后的委托凭证；对所述委托凭证解密后，验证其有效性，并确定所述用户是否有获取所请求设备的使用权限，在判定出用户有获取所述设备使用权限后，生成授权凭证，对所述授权凭证加密后发送到所述用户。此过程中由物主端委托代理端管理其拥有的并作为公共资源使用的设备，在代理端判定发送使用权限请求的用户对所请求设备具有合法的使用权时，直接发送授权凭证到所述用户，无需涉及物主的身份信息，避免了用户与物主间的直接信息传递，从而保护了物主的私人信息。

[0147] 实施例五：

[0148] 图8示出了本发明第五实施例提供的一种基于物联网的设备使用权限获取系统的结构图；如图8所示，所述基于物联网的设备使用权限获取系统包括：

[0149] 信息接收单元81，用于接收服务器发送的认证信息、物主信息以及处于正常状态下的设备信息。

[0150] 具体地，首先由服务器对代理端进行审查判定，当代理端满足预设的条件时，则认定其为合法的代理端；合法的代理端才享有代理权限，并发送认证信息到合法的代理端。服务器统计一定范围内物联网系统中处于正常使用状态下的各种设备，以及所述设备的物主信息，将这些信息整合后发送到具有代理权限的代理端。所述认证信息包括：服务器根据对代理端的调查结果生成的对代理端的信用评价，代理端的代理时间期限等。另外，在用户发送设备的使用权限请求时，也可以先查看代理端是否有认证信息，或根据代理端的认证信息中的信用评价对代理端做出选择。

[0151] 委托凭证获取单元82，用于接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0152] 委托凭证验证单元83，用于解密所述委托凭证，并验证所述委托凭证的有效性；

[0153] 条件判断单元84，用于在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

[0154] 授权凭证生成单元85，用于在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0155] 授权凭证加密单元86，用于加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0156] 本实施例中委托凭证获取单元82、委托凭证验证单元83、条件判断单元84、授权凭证生成单元85、授权凭证加密单元86与实施例四中委托凭证获取单元71、委托凭证验证单元72、条件判断单元73、授权凭证生成单元74、授权凭证加密单元75分别对应，在此不再赘述。

[0157] 本发明第五实施例中在接收用户发送的对设备的使用权限的请求，首先接收服务器发送的认证信息，物主信息即可被利用的设备的信息；由于代理端具有为物主个人信息保密的义务，因此，该步骤中首先对代理端进行认证，确定其合法性，既可以保证物主设备的安全也可以保证物主及用户的个人信息不被随意泄漏。

[0158] 实施例六：

[0159] 图9示出了本发明第六实施例提供的一种基于物联网的设备使用权限获取系统的结果图；如图9所示，所述基于物联网的设备使用权限获取系统包括：

[0160] 信息接收单元91，用于接收服务器发送的认证信息、物主信息以及处于正常状态下的设备信息。

[0161] 委托凭证获取单元92，用于接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证；

[0162] 委托凭证验证单元93，用于解密所述委托凭证，并验证所述委托凭证的有效性；

[0163] 条件判断单元94，用于在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件；

[0164] 授权凭证生成单元95，用于在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证；

[0165] 授权凭证加密单元96，用于加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证。

[0166] 本实施例中信息接收单元91、委托凭证获取单元92、委托凭证验证单元93、条件判断单元84、授权凭证生成单元95、授权凭证加密单元96与实施例四中信息接收单元81、委托凭证获取单元82、委托凭证验证单元83、条件判断单元84、授权凭证生成单元85、授权凭证加密单元86分别对应，在此不再赘述。

[0167] 验证结果接收单元97，用于接收所述设备对所述授权凭证的验证结果，并发送所述验证结果到所述物主端。

[0168] 该步骤中，用户接收到代理端发送的授权凭证后，用自己的私钥对加密后的授权凭证进行解密，以获得使用权限，用户将授权凭证中包含的信息发送到设备后，设备对接收到的信息进行验证，验证通过则对用户开放使用权限，并将所述验证结果发送到代理端，以供对其进行记录存档，并发送验证结果到物主端，以使物主得知自己设备的被使用情况。

[0169] 本发明第六实施例中用户得到所请求设备的授权凭证后，由设备对授权凭证中包含信息进行验证，验证通过则对用户开放使用权限，并发送验证结果到代理端，代理端记录后再发送验证结果到物主端，这一过程中避免了用户与物主的直接通信，既保护了物主个人信息不被泄漏也可保证用户个人的安全。

[0170] 应理解，在本发明实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0171] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0172] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0173] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或

讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0174] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0175] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[0176] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0177] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

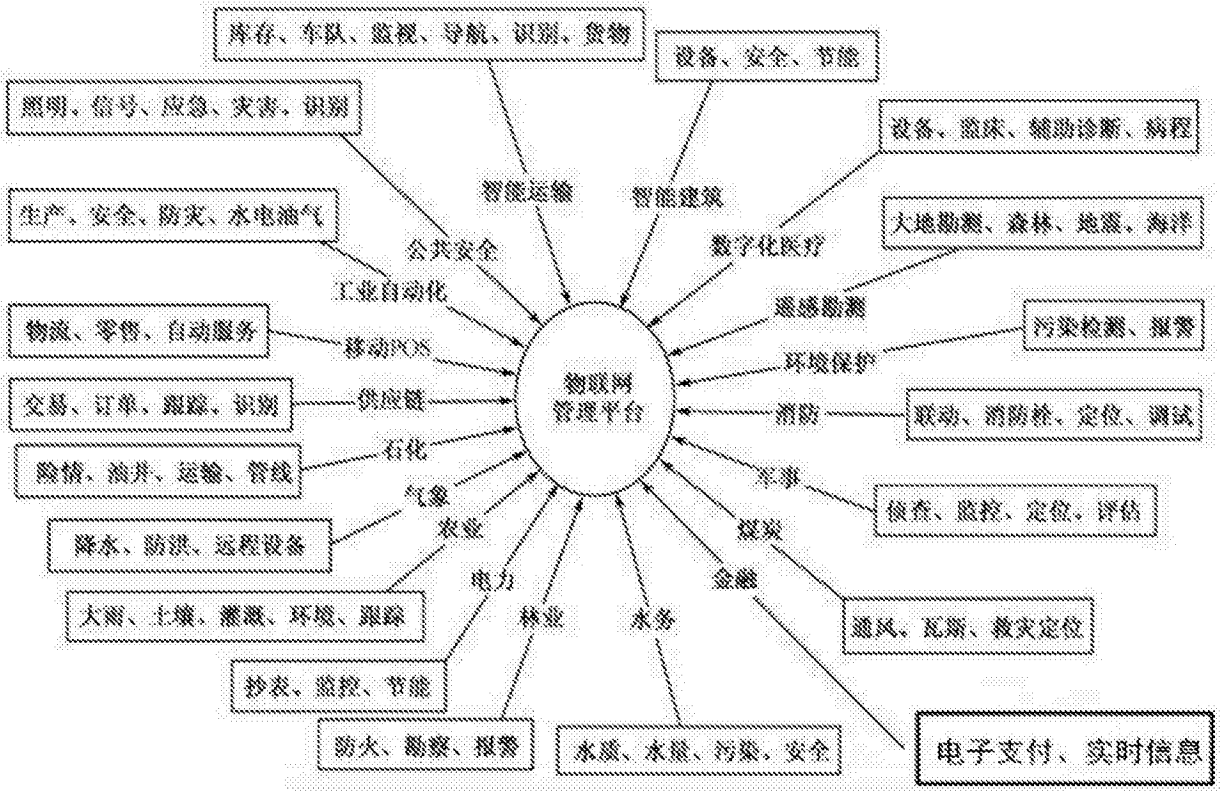

库存、车队、监视、导航、识别、货物
设备、安全、节能
照明、信号、应急、灾害、识别
设备、监床、辅助诊断、病程
智能运输
智能建筑
生产、安全、防灾、水电油气
大地勘测、森林、地震、海洋
公共安全
数字化医疗
工业自动化
遥感勘测
物流、零售、自动服务
移动POS
污染检测、报警
环境保护
交易、订单、跟踪、识别
供应链
物联网
管理平台
消防
联动、消防栓、定位、调试
险情、油井、运输、管线
石化
军事
侦查、监控、定位、评估
气象
降水、防洪、远程设备
农业
煤炭
电力
大雨、土壤、灌溉、环境、跟踪
金融
通风、瓦斯、救灾定位
林业
水务
抄表、监控、节能
防火、勘察、报警
水质、水量、污染、安全
电子支付、实时信息

图1

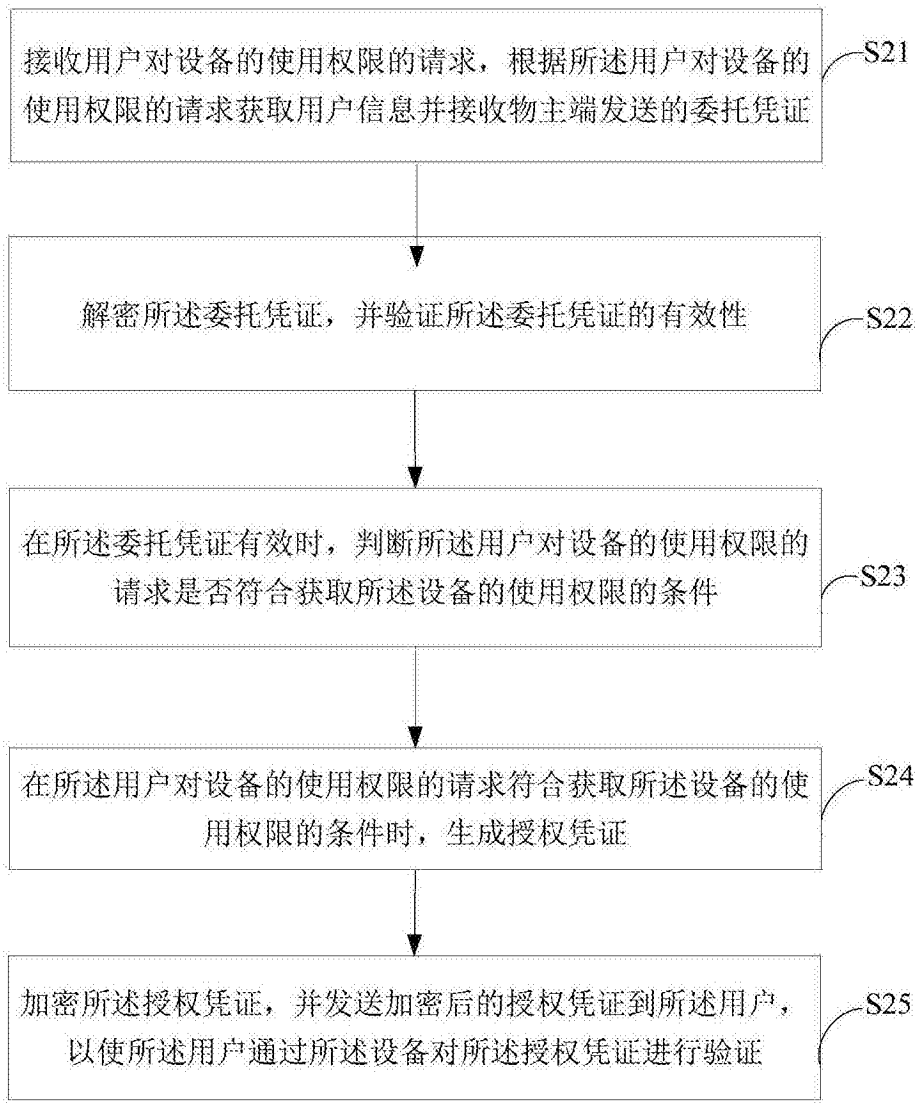

接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证
S21
解密所述委托凭证，并验证所述委托凭证的有效性
S22
在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件
S23
在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证
S24
加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证
S25

图2

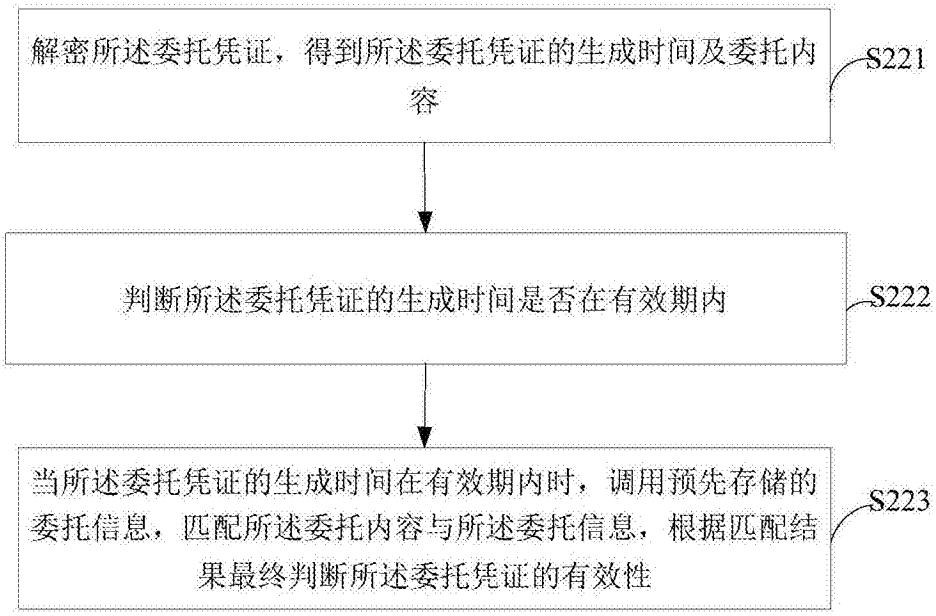

解密所述委托凭证，得到所述委托凭证的生成时间及委托内容
S221
判断所述委托凭证的生成时间是否在有效期内
S222
当所述委托凭证的生成时间在有效期内时，调用预先存储的委托信息，匹配所述委托内容与所述委托信息，根据匹配结果最终判断所述委托凭证的有效性
S223

图3

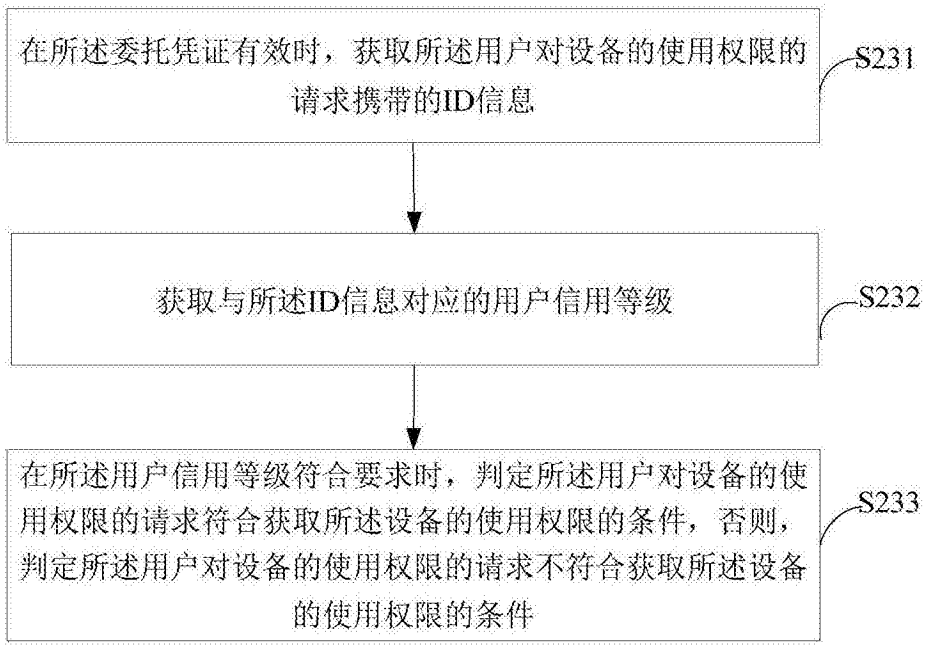

在所述委托凭证有效时，获取所述用户对设备的使用权限的请求携带的ID信息
S231
获取与所述ID信息对应的用户信用等级
S232
在所述用户信用等级符合要求时，判定所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件，否则，判定所述用户对设备的使用权限的请求不符合获取所述设备的使用权限的条件
S233

图4

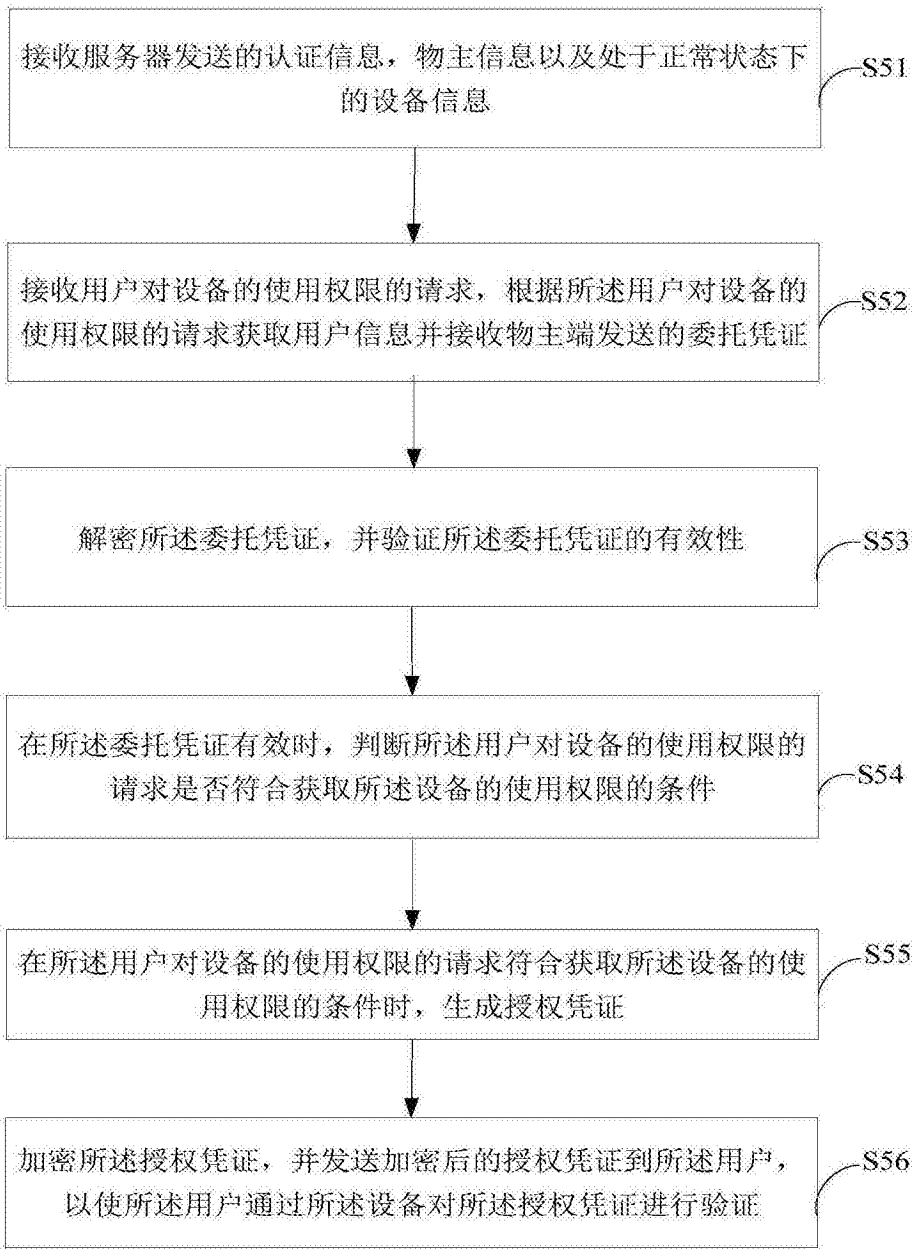

接收服务器发送的认证信息，物主信息以及处于正常状态下的设备信息
S51
接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证
S52
解密所述委托凭证，并验证所述委托凭证的有效性
S53
在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件
S54
在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证
S55
加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证
S56

图5

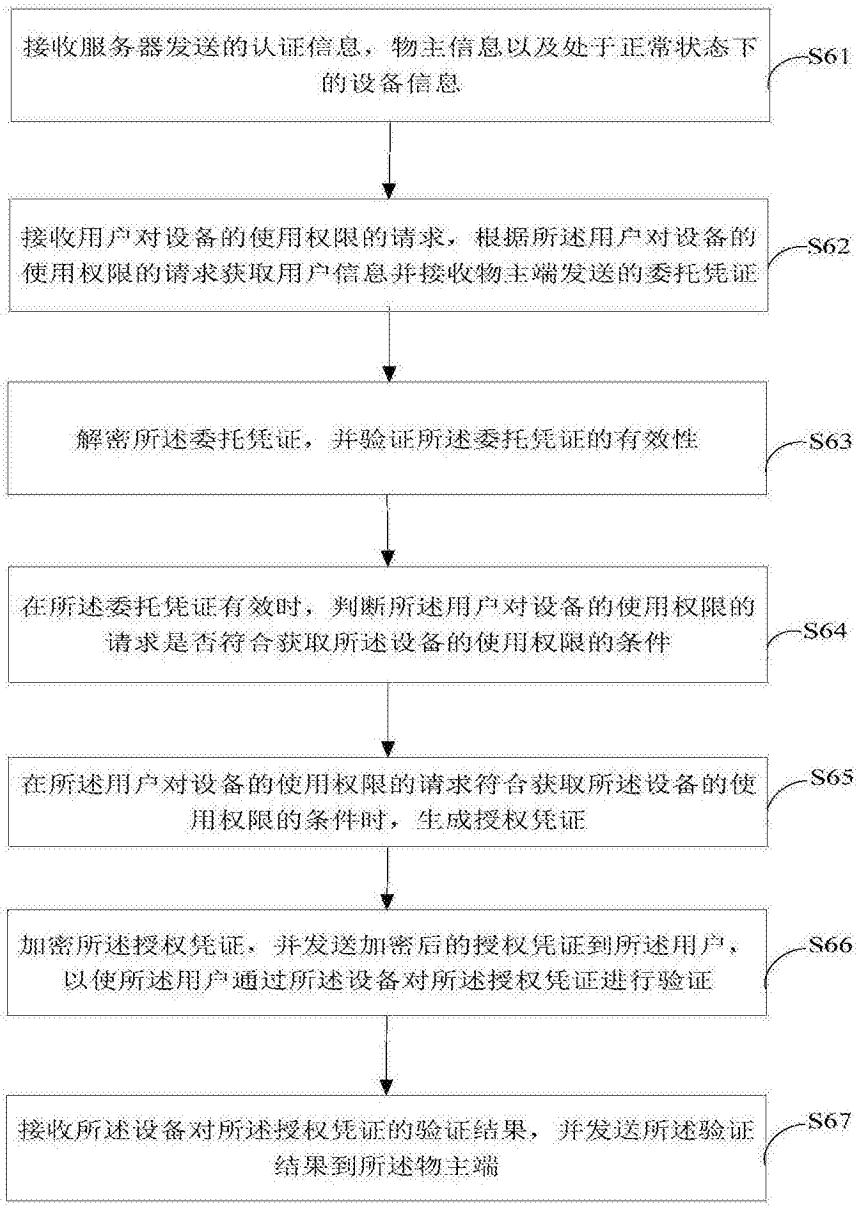

接收服务器发送的认证信息，物主信息以及处于正常状态下的设备信息
S61
接收用户对设备的使用权限的请求，根据所述用户对设备的使用权限的请求获取用户信息并接收物主端发送的委托凭证
S62
解密所述委托凭证，并验证所述委托凭证的有效性
S63
在所述委托凭证有效时，判断所述用户对设备的使用权限的请求是否符合获取所述设备的使用权限的条件
S64
在所述用户对设备的使用权限的请求符合获取所述设备的使用权限的条件时，生成授权凭证
S65
加密所述授权凭证，并发送加密后的授权凭证到所述用户，以使所述用户通过所述设备对所述授权凭证进行验证
S66
接收所述设备对所述授权凭证的验证结果，并发送所述验证结果到所述物主端
S67

图6

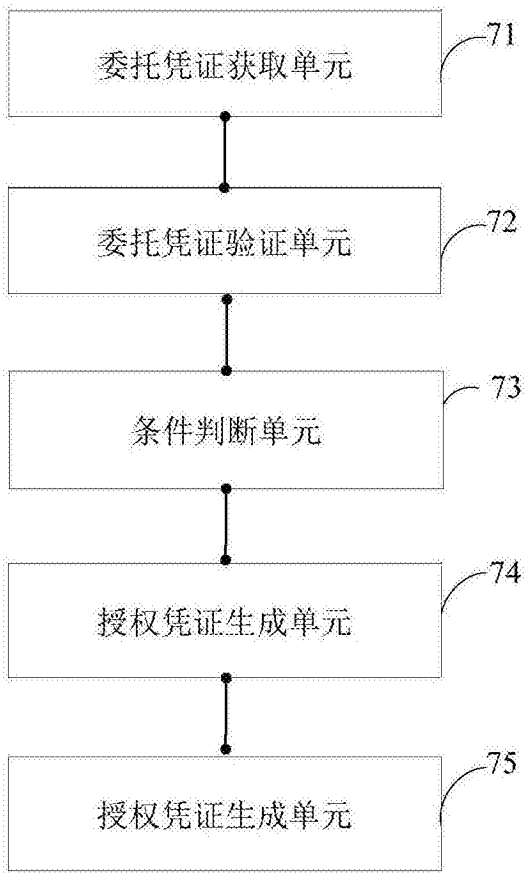


图7

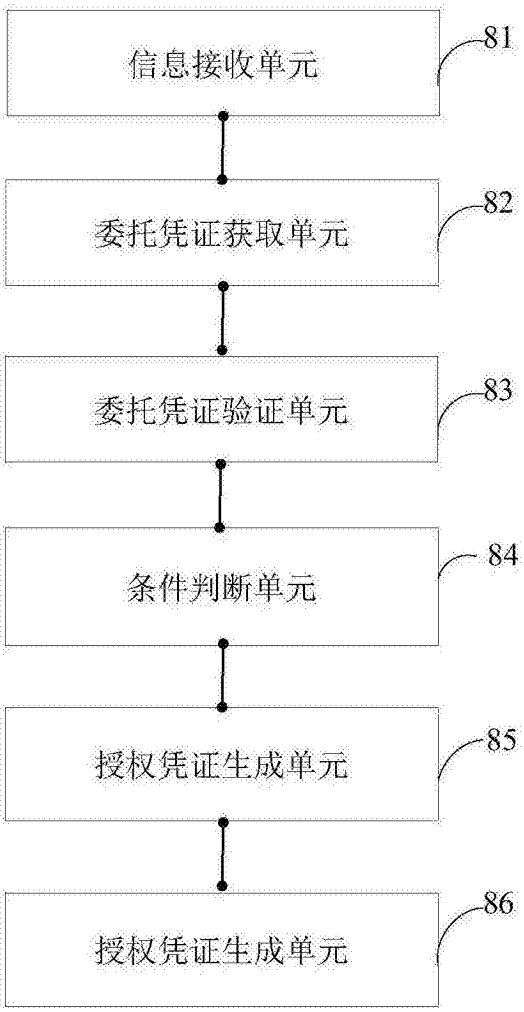

信息接收单元
81
委托凭证获取单元
82
委托凭证验证单元
83
条件判断单元
84
授权凭证生成单元
85
授权凭证生成单元
86

图8

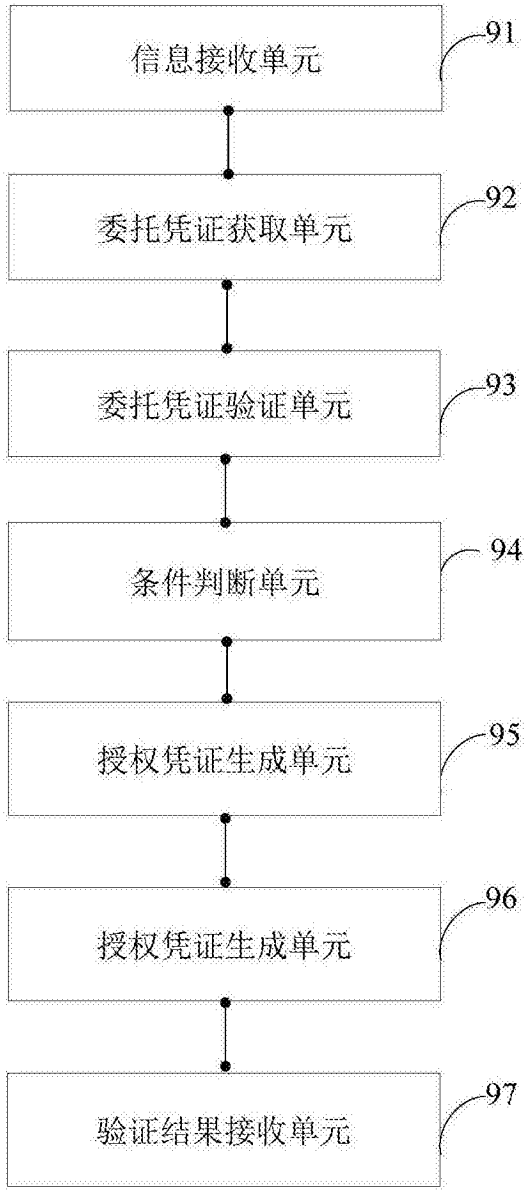

信息接收单元
91
委托凭证获取单元
92
委托凭证验证单元
93
条件判断单元
94
授权凭证生成单元
95
授权凭证生成单元
96
验证结果接收单元
97

图9