

一种证书续签的方法、装置、系统、介质及设备

本文要求在 2018 年 6 月 25 日提交中国专利局、申请号为 201810659585.6、发明名称为“一种证书续签的方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本文中。

技术领域

本文涉及互联网技术领域，尤其涉及一种证书续签的方法、装置、系统、介质及设备。

背景技术

随着物联网（Internet of Things, IoT）规模的快速增涨，IoT设备的数量也快速增加，从而引起人们对IoT设备的安全性的极大关注。

目前IoT设备的安全问题主要集中在数据加密和身份认证等方面。进行数据加密和身份认证目前均是基于公钥密码基础设施（Public Key Infrastructure, 简称PKI）体系来实现的。现有的PKI安全体系中，每个IoT设备均从认证机构（Certification Authority, 简称CA）获取一个CA签发的证书，并且还获取一个与此证书对应的私钥，其中证书用于标识IoT设备的身份。后续的处理过程中，IoT设备在需要进行身份认证以及数据加密的时候，需要使用证书和私钥进行相应处理。

例如，需要进行IoT设备的身份认证时，IoT设备使用自身私钥签名向校验方申请进行身份认证，校验方使用IoT设备的证书对此IoT设备的签名进行校验，从而确认IoT设备身份。

再例如，进行数据加密传输时，数据发送方使用IoT设备的证书对数据进行加密后，将加密数据发送至IoT设备，IoT设备接收到加密数据后，使用此IoT设备的私钥对加密数据进行解密。

从上述身份认证和数据加密传输的过程可知，涉及IoT设备安全性的主要因素为证书的有效性。证书是有时限性的，证书到达使用时限时需要对证书进行续签，如果没有对证书进行续签，就会导致证书失效，从而危害IoT设备的安全性。

相关技术中进行证书续签的方法具有以下缺点：

一，IoT设备由于地理分散较广，无法及时的对证书进行续签，导致证书失效。

二，采用集中式的方式实现证书的续签，即只设置一个中心CA用于实现证书续签，所有IoT设备均在此中心CA进行证书续签，导致中心CA处理压力较大，尤其在IoT设备数量急剧增长的背景下，中心CA容易在处理压力下出现故障，从影响证书续签用户的体验。

三，采用人工方式向中心CA申请续签，续签效率慢。

并且，现在的CA证书体系基本采用的是两级体系，具体包括：中心CA生成根证书，并生成与此根证书对应的根私钥，将根证书和根私钥进行物理隔离。基于根私钥生成二级证书，并且生成与二级证书对应的二级私钥。中心CA为IoT设备签发其它证书时，均使用此二级私钥进行签发，例如为IoT设备签发续签证书时，也使用此二级私钥进行签发。中心CA对二级私钥一般不进行远程物理隔离，只是储存于安全芯片中，以方便快速调用。二级私钥签发的证书一般不允许继续行使签发功能，例如：IoT设备证书只能用于其本身业务，而无法继续签发其他证书。

发明内容

本文提供一种证书续签的方法、装置、系统及介质。

根据本文的一方面，提供一种证书续签方法，包括：

卫星认证机构 CA 从中心 CA 接收权限设置信息，所述权限设置信息包括用于指示只执行续签处理的权限信息；

卫星 CA 接收设备发送的续签请求；

判断是否满足续签条件；

确定满足续签条件，生成新的设备证书，所述新的设备证书是使用所述卫星 CA 的三级证书所对应的私钥进行签名生成的；

将生成的新的设备证书发送至所述设备。

上述证书续签方法还具有以下特点：

所述卫星 CA 接收设备发送的续签请求之前，所述方法还包括：所述卫星 CA

从所述中心 CA 接收设备标识集合；

所述判断是否满足续签条件之前，所述方法还包括：确定所述设备的标识属于所述设备标识集合。

上述证书续签方法还具有以下特点：

所述续签请求还包括证书签名请求，所述证书签名请求还包括过期时间；

所述续签条件包括：当前时间距所述证书签名请求的过期时间的时间差值小于预设时长。

上述证书续签方法还具有以下特点：

所述卫星 CA 接收设备发送的续签请求的同时还接收所述设备的当前证书；

所述续签请求还包括证书签名请求；

所述续签条件包括：所述证书签名请求中的信息与所述卫星 CA 中已保存的所述设备的当前证书的信息相同。

上述证书续签方法还具有以下特点：

所述方法还包括：

所述卫星 CA 从中心 CA 接收所述三级证书，所述三级证书是所述中心 CA 根据所述卫星 CA 的唯一标识信息生成的。

上述证书续签方法还具有以下特点：

所述卫星 CA 包括签发单元和私钥管理单元；

所述签发单元，设置为在判断所述卫星 CA 需要生成所述新的设备证书时，向所述私钥管理单元发送连接请求，在与所述私钥管理单元连接成功后，向所述私钥管理单元发送所述证书签名请求；还用于从所述私钥管理单元接收所述新的设备证书；

所述私钥管理单元，设置为从所述签发单元接收连接请求，在与所述签发单元建立连接后，使用所述卫星 CA 的三级证书所对应的私钥对所述证书签名请求进行签名，将签名生成的新的设备证书发送至所述签发单元；

或者，所述卫星 CA 包括签发单元；

所述签发单元，设置为在判断所述卫星 CA 需要生成所述新的设备证书时，

向所述私钥管理单元发送连接请求，在与所述私钥管理单元连接成功后，向所述私钥管理单元发送所述证书签名请求；还用于从所述私钥管理单元接收所述新的设备证书；所述新的设备证书是所述私钥管理单元从所述签发单元接收连接请求，在与所述签发单元建立连接后，使用所述卫星 CA 的三级证书所对应的私钥对所述证书签名请求进行签名生成的。

根据本文的另一方面，提供一种证书续签装置，应用于卫星 CA，包括：

第一接收模块，设置为从中心 CA 接收权限设置信息，所述权限设置信息包括用于指示只执行续签处理的权限信息；

第二接收模块，设置为接收设备发送的续签请求；

判断模块，设置为判断是否满足续签条件；

生成模块，设置为在所述判断模块确定满足续签条件时，生成新的设备证书，所述新的设备证书是使用所述卫星 CA 的三级证书所对应的私钥进行签名生成的；

发送模块，设置为将生成的新的设备证书发送至所述设备。

上述证书续签装置还具有以下特点：

所述装置还包括：

第三接收模块，设置为在所述第二接收模块接收设备发送的续签请求之前，从所述中心 CA 接收设备标识集合；

确定模块，设置为确定所述设备的标识属于所述设备标识集合，在确定所述设备的标识属于所述设备标识集合后，触发所述判断模块。

上述证书续签装置还具有以下特点：

所述续签请求还包括证书签名请求，所述证书签名请求还包括过期时间；

所述续签条件包括：当前时间距所述证书签名请求的过期时间的时间差值小于预设时长。

上述证书续签装置还具有以下特点：

所述第二接收模块，还用于在接收设备发送的续签请求的同时还接收所述设备的当前证书；

所述续签请求还包括证书签名请求；

所述续签条件包括：所述证书签名请求中的信息与所述卫星 CA 中已保存的所述设备的当前证书的信息相同。

上述证书续签装置还具有以下特点：

所述装置还包括：

第四接收模块，设置为从中心 CA 接收所述三级证书，所述三级证书是所述中心 CA 根据所述卫星 CA 的唯一标识信息生成的。

上述证书续签装置还具有以下特点：

所述装置还包括签发单元和私钥管理单元；

所述签发单元，设置为在判断所述卫星 CA 需要生成所述新的设备证书时，向所述私钥管理单元发送连接请求，在与所述私钥管理单元连接成功后，向所述私钥管理单元发送所述证书签名请求；还用于从所述私钥管理单元接收所述新的设备证书；

所述私钥管理单元，设置为从所述签发单元接收连接请求，在与所述签发单元建立连接后，使用所述卫星 CA 的三级证书所对应的私钥对所述证书签名请求进行签名，将签名生成的新的设备证书发送至所述签发单元；

或者，所述装置包括签发单元；

所述签发单元，设置为在判断所述卫星 CA 需要生成所述新的设备证书时，向所述私钥管理单元发送连接请求，在与所述私钥管理单元连接成功后，向所述私钥管理单元发送所述证书签名请求；还用于从所述私钥管理单元接收所述新的设备证书；所述新的设备证书是所述私钥管理单元从所述签发单元接收连接请求，在与所述签发单元建立连接后，使用所述卫星 CA 的三级证书所对应的私钥对所述证书签名请求进行签名生成的。

根据本文的另一方面，提供一种证书续签系统，其中包括中心 CA 和至少一个卫星 CA，所述卫星 CA 包括上述证书续签装置。

根据本文的另一方面，提供一种计算机可读存储介质，其上存储有计算机程序，其中，所述计算机程序被执行时实现上述方法的步骤。

根据本文的另一方面，提供一种计算机设备，包括处理器、存储器和存储于所述存储器上的计算机程序，其中，所述处理器执行所述计算机程序时实现上述方法的步骤。

本文通过设置分布式的 CA 结构以及功能有限的卫星 CA，由功能有限的卫星 CA 分担中心 CA 的处理压力，并且，使 IoT 设备就近接入卫星 CA 从而快速有效的实现证书续签。

附图说明

构成本文的一部分的附图用来提供对本文的进一步理解，本文的示意性实施例及其说明用于解释本文，并不构成对本文的不当限定。在附图中：

图 1 是根据一示例性实施例示出的实施例中 CA 分布结构示意图；

图 2 是根据一示例性实施例示出的实施例中证书续签方法的流程图；

图 3 是根据一示例性实施例示出的实施例中证书续签装置的结构图；

图 4 是根据一示例性实施例示出的一种计算机装置的框图。

具体实施方式

为使本文实施例的目的、技术方案和优点更加清楚，下面将结合本文实施例中的附图，对本文实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本文一部分实施例，而不是全部的实施例。基于本文中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本文保护的范围。需要说明的是，在不冲突的情况下，本文中的实施例及实施例中的特征可以相互任意组合。

本文中涉及到的设备可以典型的是 IoT 设备，本文中简称为设备。

如图 1 所示，本文中将 CA 设置为分布式结构，即包括中心 CA 和与中心 CA 连接的一个以上卫星 CA。设置卫星 CA 时可以按地理位置设置（例如，在热点位置区域设置较多的卫星 CA），也可以根据设备密度设置（例如，在设备密度较大的区域设置较多的卫星 CA）。卫星 CA 数量越多则 IoT 设备的用户体验就越好。

如图 2 所示，证书续签方法的包括：

步骤 201, 卫星 CA 从中心 CA 接收权限设置信息, 此权限设置信息包括用于指示只执行续签处理的权限信息;

步骤 202, 卫星 CA 接收设备发送的续签请求;

步骤 203, 判断是否满足续签条件;

步骤 204, 确定满足续签条件时, 生成新的设备证书, 此新的设备证书是使用上述卫星 CA 的三级证书所对应的私钥进行签名生成的;

步骤 205, 将生成的新的设备证书发送至上述设备。

此方法还包括步骤 206, 卫星 CA 向中心 CA 上报此次签发行为, 并从中心 CA 接收确认此次签发行为的信息。中心 CA 在进行进一步验证时, 将不合法的续签确认为无效续签, 这样即使三级证书的私钥遭到泄露, 伪造的证书也无法使用, 从而保证了安全性。

本方在现有的二级体系的基础上引入了引入第三级证书的概念, 即使用 CA 的二级私钥签发一个可以继续签发其他证书的三级证书。卫星 CA 可以使用此三级证书, 但卫星 CA 的功能是受限的, 卫星 CA 只负责进行证书续签, 设备在需要进行证书首签时需与中心 CA 交互, 由中心 CA 处理。并且, 卫星 CA 没有吊销证书的权力。

步骤 202 之前, 此方法还包括: 卫星 CA 从中心 CA 接收设备标识集合。步骤 203 之前, 此方法还包括: 确定上述设备的标识属于设备标识集合。因此, 卫星 CA 除了在功能上受限外, 在处理对象上也是受限的, 即卫星 CA 只能对中心 CA 为其分配的各设备进行续签, 不能对设备标识集合之外的其它设备进行续签。

步骤 203 中续签条件包括以下条件中的至少一个, 典型的情况下包括下述两个条件:

条件一, 续签请求还包括证书签名请求, 证书签名请求还包括过期时间。续签条件包括: 当前时间距证书签名请求的过期时间的时间差值小于预设时长。

条件二, 卫星 CA 接收设备发送的续签请求的同时还接收上述设备的当前证书。续签请求还包括证书签名请求。续签条件包括: 证书签名请求中的信息与卫星 CA 中已保存的设备的当前证书的信息相同;

其中，卫星 CA 接收设备发送的续签请求的同时还接收设备的当前证书，可以防止证书过期时间被恶意篡改，从而保证续签的准确性；

续签条件中的信息是指公钥内容、通用名称、有效日期、证书用途等公知的参数信息。续签请求还包括签名值，续签条件中还包括：通过此签名值验证证书签名请求成功。

步骤 203 中判断不满足续签条件时，向设备发送拒绝续签的信息。

步骤 204 中的三级证书是中心 CA 根据卫星 CA 的唯一标识信息生成的，卫星 CA 从中心 CA 接收此三级证书。从而，各个卫星 CA 的三级证书各不相同。

本方法中的卫星 CA 中采用了安全措施来确保三级证书对应的私钥的安全，具体的，采用私钥与签发分离的处理方式。现有技术中使用同一芯片保存私钥并签发证书。本方法中，签发单元和私钥管理单元位于不同的实体中。具体实现方式是以下方式中的一种：

方式一

卫星 CA 包括签发单元和私钥管理单元。

签发单元设置为在判断卫星 CA 需要生成新的设备证书时，向私钥管理单元发送连接请求，在与私钥管理单元连接成功后，向私钥管理单元发送证书签名请求；还设置为从私钥管理单元接收新的设备证书；

私钥管理单元设置为从签发单元接收连接请求，在与签发单元建立连接后，使用卫星 CA 的三级证书所对应的私钥对证书签名请求进行签名，将签名生成的新的设备证书发送至签发单元。

方式二

卫星 CA 包括签发单元，私钥管理单元位于卫星 CA 之外的实体中，例如可以位于中心 CA 中。

签发单元设置为在判断卫星 CA 需要生成新的设备证书时，向私钥管理单元发送连接请求，在与私钥管理单元连接成功后，向私钥管理单元发送证书签名请求；还设置为从私钥管理单元接收新的设备证书；新的设备证书是私钥管理单元从签发单元接收连接请求，在与签发单元建立连接后，使用卫星 CA 的三级证书所对应的私钥对证书签名请求进行签名生成的。

私钥管理单元设置为从签发单元接收连接请求，在与签发单元建立连接后，使用卫星 CA 的三级证书所对应的私钥对证书签名请求进行签名，将签名生成的新的设备证书发送至签发单元。

其中，签发单元与私钥管理单元进行连接时，需要进行验证后才可以成功连接，此验证过程包括以下操作中的至少一种：TLS 双向认证、IP 白名单筛选。

卫星 CA 向中心 CA 上报所有续签行为，以便于中心 CA 根据各卫星 CA 的续签行为进行安全审计。

本方法可以实现中心 CA 的去中心化，减少中心 CA 的处理压力，在设备需要续签时，无需像现有技术中一样，连接唯一的中心 CA，从而可以减少中心 CA 的处理压力，并且卫星 CA 的功能受限，设备只在需要续签时才连接，从而防止卫星 CA 的功能过多导致的安全性问题。

图 3 是实施例中证书续签装置的结构图，卫星 CA 包含证书续签装置，证书续签装置包括：

第一接收模块，设置为从中心 CA 接收权限设置信息，权限设置信息包括设置为指示只执行续签处理的权限信息；

第二接收模块，设置为接收设备发送的续签请求；

判断模块，设置为判断是否满足续签条件；

生成模块，设置为在判断模块确定满足续签条件时，生成新的设备证书，新的设备证书是使用卫星 CA 的三级证书所对应的私钥进行签名生成的；

发送模块，设置为将生成的新的设备证书发送至上述设备。

其中，

上述装置还包括：

第三接收模块，设置为在第二接收模块接收设备发送的续签请求之前，从中心 CA 接收设备标识集合；

确定模块，设置为确定上述设备的标识属于设备标识集合，在确定上述设备的标识属于设备标识集合后，触发判断模块。

其中，

续签条件包括以下条件中的至少一个，典型的情况下包括下述两个条件：

条件一，续签请求还包括证书签名请求，证书签名请求还包括过期时间；续签条件包括：当前时间距证书签名请求的过期时间的时间差值小于预设时长。

条件二，第二接收模块还设置为在接收设备发送的续签请求的同时还接收上述设备的当前证书。续签请求还包括证书签名请求；续签条件包括：证书签名请求中的信息与卫星 CA 中已保存的设备的当前证书的信息相同。其中，第二接收模块接收设备发送的续签请求的同时还接收设备的当前证书，可以防止证书过期时间被恶意篡改，从而保证续签的准确性。

续签条件中的信息是指公钥内容、通用名称、有效日期、证书用途等公知的参数信息。续签请求还包括签名值，续签条件中还包括：通过此签名值验证证书签名请求成功。

上述装置还包括：第四接收模块，设置为从中心 CA 接收三级证书，三级证书是中心 CA 根据卫星 CA 的唯一标识信息生成的。

上述装置实现签发功能时可以采用以下方式中的一种实现：

方式一

上述装置还包括签发单元和私钥管理单元；

签发单元，设置为在判断卫星 CA 需要生成新的设备证书时，向私钥管理单元发送连接请求，在与私钥管理单元连接成功后，向私钥管理单元发送证书签名请求；还设置为从私钥管理单元接收新的设备证书；

私钥管理单元，设置为从签发单元接收连接请求，在与签发单元建立连接后，使用卫星 CA 的三级证书所对应的私钥对证书签名请求进行签名，将签名生成的新的设备证书发送至签发单元；

方式二

上述装置包括签发单元，设置为在判断卫星 CA 需要生成新的设备证书时，向私钥管理单元发送连接请求，在与私钥管理单元连接成功后，向私钥管理单元发送证书签名请求；还设置为从私钥管理单元接收新的设备证书；新的设备证书是私钥管理单元从签发单元接收连接请求，在与签发单元建立连接后，使用卫星 CA 的三级证书所对应的私钥对证书签名请求进行签名生成的。

上述装置还包括上报模块，设置为向中心 CA 上报所有续签行为，以便于中心 CA 根据各卫星 CA 的续签行为进行安全审计。

本文实施例还公开了证书续签系统，如图 1 所示，此系统包括中心 CA 和至少一个卫星 CA，卫星 CA 包括上述证书续签装置。此分布式的 CA 结构，设置功能有限的卫星 CA，由功能有限的卫星 CA 分担中心 CA 的处理压力。从而使 IoT 设备就近接入卫星 CA 从而快速有效的实现证书续签。

图 4 是根据一示例性实施例示出的一种用于证书续签的计算机设备的框图。例如，装置可以被提供为一服务器。参照图 4，此装置包括处理器 401，处理器的个数可以根据需要设置为一个或者多个。此装置还包括存储器 402，用于存储可由处理器 401 的执行的指令，例如应用程序。存储器的个数可以根据需要设置一个或者多个。其存储的应用程序可以为一个或者多个。处理器 401 被配置为执行指令，以执行上述证书续签方法。

本领域技术人员应明白，本文的实施例可提供为方法、装置（设备）、或计算机程序产品。因此，本文可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本文可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质上实施的计算机程序产品的形式。计算机存储介质包括在用于存储信息（诸如计算机可读指令、数据结构、程序模块或其他数据）的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质，包括但不限于 RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质等。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

本文是参照根据本文实施例的方法、装置（设备）和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个

流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的物品或者设备中还存在另外的相同要素。

尽管已描述了本文的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本文范围的所有变更和修改。

显然，本领域的技术人员可以对本文进行各种改动和变型而不脱离本文的精神和范围。这样，倘若本文的这些修改和变型属于本文权利要求及其等同技术的范围之内，则本文的意图也包含这些改动和变型在内。

工业实用性

本文通过设置分布式的 CA 结构以及功能有限的卫星 CA，由功能有限的卫星 CA 分担中心 CA 的处理压力，并且，使 IoT 设备就近接入卫星 CA 从而快速有效的实现证书续签。