(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 111641507 A
(43)申请公布日 2020.09.08

(21)申请号 202010420278.X

(22)申请日 2020.05.18

(71)申请人 湖南智领通信科技有限公司
地址 410000 湖南省长沙市长沙高新开发区岳麓西大道588号芯城科技园3栋11层

(72)发明人 朱世立 刘浩

(74)专利代理机构 长沙国科天河知识产权代理有限公司 43225
代理人 董惠文

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)

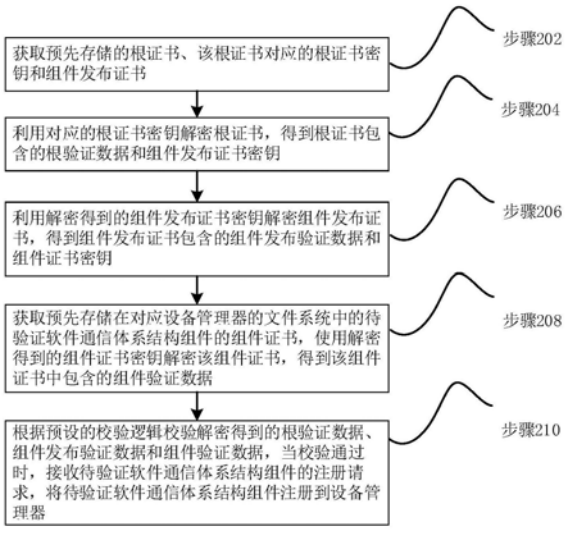
权利要求书2页 说明书11页 附图2页

(54)发明名称

一种软件通信体系结构组件注册管理方法和装置

(57)摘要

本申请涉及一种软件通信体系结构组件注册管理方法和装置。所述方法包括:获取预先存储的根证书、对应的根证书密钥和组件发布证书,获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书;利用根证书密钥解密根证书,得到根验证数据和组件发布证书密钥;利用组件发布证书密钥解密组件发布证书,得到组件发布验证数据和组件证书密钥;利用组件证书密钥解密组件证书,得到组件验证数据;当上述验证数据均通过校验时,将待验证组件注册到设备管理器。上述方法利用软件通信体系结构中的组件注册机制,使组件在验证通过后才能运行,解决了软件通信体系结构系统的开发成果保护问题,有利于推动其开发工作和成果应用的产业化发展。



CN 111641507 A

1.一种软件通信体系结构组件注册管理方法,包括:

获取预先存储的根证书、所述根证书对应的根证书密钥和组件发布证书;

利用所述根证书密钥解密所述根证书,得到所述根证书包含的根验证数据和组件发布证书密钥;

利用所述组件发布证书密钥解密所述组件发布证书,得到所述组件发布证书包含的组件发布验证数据和组件证书密钥;

获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书,使用所述组件证书密钥解密所述组件证书,得到所述组件证书包含的组件验证数据;

根据预设的校验逻辑校验所述根验证数据、所述组件发布验证数据和所述组件验证数据,当校验通过时,接收所述待验证软件通信体系结构组件的注册请求,将所述待验证软件通信体系结构组件注册到设备管理器。

2.根据权利要求1所述的方法,其特征在于,利用所述组件发布证书密钥解密所述组件发布证书,得到所述组件发布证书包含的组件发布验证数据和组件证书密钥的步骤包括:

获取预设的所述组件发布证书的级数N;

当N=2时,利用所述组件发布证书密钥解密第2级组件发布证书,得到所述第2级组件发布证书中包含的第1级组件发布证书密钥;

当N≥3时,利用所述组件发布证书密钥解密第N级组件发布证书,得到所述第N级组件发布证书中包含的第N-1级组件发布证书密钥;利用第n级组件发布证书密钥解密第n级组件发布证书,得到所述第n级组件发布证书中包含的第n-1级组件发布证书密钥,其中2≤n≤N-1;

利用所述第1级组件发布证书密钥解密第1级组件发布证书,得到所述第1级组件发布证书中包含的所述组件发布验证数据和所述组件证书密钥。

3.根据权利要求1所述的方法,其特征在于,所述根据预设的校验逻辑校验所述根验证数据、所述组件发布验证数据和所述组件验证数据,当校验通过时,接收所述待验证软件通信体系结构组件的注册请求,将所述待验证软件通信体系结构组件注册到所述设备管理器的步骤之后,还包括:

根据预设的注册顺序,向所述待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令,所述验证控制指令用于控制所述待验证软件通信系统结构组件的所述下一软件通信系统结构组件开始进行验证。

4.根据权利要求1所述的方法,其特征在于,所述根证书密钥、所述组件发布证书密钥和所述组件证书密钥采用的加密算法为非对称加密算法,所述非对称加密算法包括RSA密码算法、ECC椭圆权限密码算法和数字验证数据算法。

5.根据权利要求1所述的方法,其特征在于,所述根证书还包含根证书有效性标识,所述组件发布证书还包含组件发布证书有效性标识,所述组件证书还包含组件证书有效性标识;

所述根据预设的校验逻辑校验所述根验证数据、所述组件发布验证数据和所述组件验证数据,当校验通过时,接收所述待验证软件通信体系结构组件的注册请求,将所述待验证软件通信体系结构组件注册到所述设备管理器的步骤之前,还包括:

获取所述根证书有效性标识、所述组件发布证书有效性标识和所述组件证书有效性标

识；

当所述根证书有效性标识、所述组件发布证书有效性标识和所述组件证书有效性标识的状态均为有效时，获取所述根验证数据、所述组件发布验证数据和所述组件验证数据。

6.一种软件通信体系结构组件注册管理装置，包括：

证书获取模块，用于获取预先存储的根证书、所述根证书对应的根证书密钥和组件发布证书；

根证书解密模块，用于利用所述根证书密钥解密所述根证书，得到所述根证书包含的根验证数据和组件发布证书密钥；

组件发布证书解密模块，用于利用所述组件发布证书密钥解密所述组件发布证书，得到所述组件发布证书包含的组件发布验证数据和组件证书密钥；

组件证书解密模块，用于获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，使用所述组件证书密钥解密所述组件证书，得到所述组件证书包含的组件验证数据；

组件注册控制模块，用于根据预设的校验逻辑校验所述根验证数据、所述组件发布验证数据和所述组件验证数据，当校验通过时，接收所述待验证软件通信体系结构组件的注册请求，将所述待验证软件通信体系结构组件注册到设备管理器。

7.根据权利要求6述的装置，其特征在于，所述组件发布证书解密模块用于：

获取预设的所述组件发布证书的级数N；

当N＝2时，利用所述组件发布证书密钥解密第2级组件发布证书，得到所述第2级组件发布证书中包含的第1级组件发布证书密钥；

当N≥3时，利用所述组件发布证书密钥解密第N级组件发布证书，得到所述第N级组件发布证书中包含的第N-1级组件发布证书密钥；利用第n级组件发布证书密钥解密第n级组件发布证书，得到所述第n级组件发布证书中包含的第n-1级组件发布证书密钥，其中2≤n≤N-1；

利用所述第1级组件发布证书密钥解密第1级组件发布证书，得到所述第1级组件发布证书中包含的所述组件发布验证数据和所述组件证书密钥。

8.根据权利要求6所述的装置，还包括：

组件验证控制模块，用于根据预设的注册顺序，向所述待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令，所述验证控制指令用于控制所述待验证软件通信系统结构组件的所述下一软件通信系统结构组件开始进行验证。

9.一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至5中任一项所述方法的步骤。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

一种软件通信体系结构组件注册管理方法和装置

技术领域

[0001] 本发明设计软件通信体系结构,尤其涉及一种软件通信体系结构的组件波形保护方法。

背景技术

[0002] 软件通信体系结构(SCA,Software Communication Architecture)规范是美军在实施联合战术无线电系统计划过程中提出的一个标准规范集,它为软件无线电台的设计提供了一种与实现无关的开放式结构。组件是软件通信体系结构中的一个重要概念,是软件通信体系结构使用其标准规范集中的一组标准定义和描述的具有统一的接口、属性和功能的模块。因此软件通信体系结构中的组件具有高度的可移植性,即软件通信体系结构组件的“即插即用”能力,使其可在不同的软件通信体系结构系统之间复用,给基于软件通信体系结构的系统开发带来了多种便利。

[0003] 但软件通信体系结构组件的可移植性也给开发人员带来了相应的风险:由于软件通信体系结构基于一系列公开的通用标准定义其组件接口和组件间的交互,因此针对某个系统开发的组件可以较容易地被复制和移植到其他系统中,用于实现类似功能,无法保护基于软件通信体系结构的软件无线电开发成果,不利于推动基于软件通信体系结构的软件无线电系统开发的产业化发展和商业应用。

发明内容

[0004] 基于此,有必要针对上述技术问题,提供一种能够防止软件通信体系结构组件未经许可被复制、移植的方法、装置、计算机设备和存储介质。

[0005] 一种软件通信体系结构组件管理方法,包括:

[0006] 获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书;

[0007] 利用对应的根证书密钥解密根证书,得到根证书包含的根验证数据和组件发布证书密钥;

[0008] 利用解密得到的组件发布证书密钥解密组件发布证书,得到组件发布证书包含的组件发布验证数据和组件证书密钥;

[0009] 获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书,利用解密得到的组件证书密钥解密该组件证书,得到该组件证书中包含的组件验证数据;

[0010] 根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据,当校验通过时,接收待验证软件通信体系结构组件的注册请求,将待验证软件通信体系结构组件注册到设备管理器。

[0011] 其中一个实施例中,利用所述组件发布证书密钥解密所述组件发布证书,得到所述组件发布证书包含的组件发布验证数据和组件证书密钥的步骤包括:

[0012] 获取预设的组件发布证书的级数N;

[0013] 当N=2时,利用组件发布证书密钥解密第2级组件发布证书,得到第2级组件发布

证书中包含的第1级组件发布证书密钥；

[0014] 当N≥3时，利用组件发布证书密钥解密第N级组件发布证书，得到第N级组件发布证书中包含的第N-1级组件发布证书密钥；利用第n级组件发布证书密钥解密第n级组件发布证书，得到第n级组件发布证书中包含的第n-1级组件发布证书密钥，其中2≤n≤N-1；

[0015] 利用第1级组件发布证书密钥解密第1级组件发布证书，得到第1级组件发布证书中包含的组件发布验证数据和组件证书密钥。

[0016] 其中一个实施例中，在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之后，还包括：

[0017] 根据预设的注册顺序，向待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令，该验证控制指令用于控制该待验证软件通信系统结构组件的下一软件通信系统结构组件开始进行验证。

[0018] 其中一个实施例中，根证书密钥、组件发布证书密钥和组件证书密钥采用的加密算法为非对称加密算法，包括RSA密码算法、ECC椭圆权限密码算法和数字验证数据算法。

[0019] 其中一个实施例中，根证书还包含根证书有效性标识，组件发布证书还包含组件发布证书有效性标识，组件证书还包含组件证书有效性标识。在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之前，还包括：

[0020] 获取根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识；

[0021] 当根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识的状态均为有效时，获取根验证数据、组件发布验证数据和组件验证数据。

[0022] 一种软件通信体系结构组件注册管理装置，包括：

[0023] 证书获取模块，用于获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书；

[0024] 根证书解密模块，用于利用根证书密钥解密根证书，得到该根证书包含的根验证数据和组件发布证书密钥；

[0025] 组件发布证书解密模块，用于利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥；

[0026] 组件证书解密模块，用于获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，利用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据；

[0027] 组件注册控制模块，用于根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器。

[0028] 其中一个实施例中，组件发布证书解密模块用于：

[0029] 获取预设的组件发布证书的级数N；

[0030] 当N＝2时，利用组件发布证书密钥解密第2级组件发布证书，得到第2级组件发布证书中包含的第1级组件发布证书密钥；

[0031] 当N≥3时，利用组件发布证书密钥解密第N级组件发布证书，得到第N级组件发布证书中包含的第N-1级组件发布证书密钥；利用第n级组件发布证书密钥解密第n级组件发布证书，得到第n级组件发布证书中包含的第n-1级组件发布证书密钥，其中2≤n≤N-1；

[0032] 利用第1级组件发布证书密钥解密第1级组件发布证书，得到第1级组件发布证书中包含的组件发布验证数据和组件证书密钥。

[0033] 其中一个实施例中，还包括组件验证控制模块，用于根据预设的注册顺序，向待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令，该验证控制指令用于控制该待验证软件通信系统结构组件的下一软件通信系统结构组件开始进行验证。

[0034] 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现以下步骤：

[0035] 获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书；

[0036] 利用对应的根证书密钥解密根证书，得到根证书包含的根验证数据和组件发布证书密钥；

[0037] 利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥；

[0038] 获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，利用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据；

[0039] 根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器。

[0040] 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时时实现以下步骤：

[0041] 获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书；

[0042] 利用对应的根证书密钥解密根证书，得到根证书包含的根验证数据和组件发布证书密钥；

[0043] 利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥；

[0044] 获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，利用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据；

[0045] 根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器。

[0046] 上述软件通信体系结构组件注册管理方法、装置、计算机设备和存储介质，在基于软件通信体系结构设计的设备中预存设备组件的组件证书，并对根证书、组件发布证书和组件证书进行多级嵌套的加密，使得设备组件在注册到设备管理器之前，需要解密其对应的根证书和组件发布证书，获取根证书验证数据、组件发布证书验证数据和组件证书的密钥，再解密组件证书获取组件证书验证数据；并且仅在根证书验证数据、组件发布证书验证数据和组件证书验证数据均校验通过时，才允许该组件注册到设备管理器。上述软件通信体系结构组件注册管理方法、装置、计算机设备和存储介质，利用软件通信体系结构中的组

件注册机制，使得组件必须在验证通过后才能运行，解决了保护基于软件通信体系结构的软件无线电开发成果的问题，有利于推动基于软件通信体系结构的软件无线电系统开发的产业化发展和商业应用。

附图说明

[0047] 图1为一个实施例中软件通信体系结构组件注册管理方法的应用场景图；

[0048] 图2为一个实施例中软件通信体系结构组件注册管理方法的流程示意图；

[0049] 图3为另一个实施例中软件通信体系结构组件注册管理方法的流程示意图；

[0050] 图4为一个实施例中计算机设备的内部结构图。

具体实施方式

[0051] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0052] 本申请提供的软件通信体系结构组件管理方法，可以基于软件通信体系结构开发的软件无线电设备中，如图1所示，该软件无线电设备包含n个组件，还包括预先存储有组件证书的证书存储模块。该软件无线电设备需要新增组件m和组件j。

[0053] 在一个实施例中，如图2所示，提供了一种软件通信体系结构组件管理方法，以该方法应用于图1中的软件无线电设备为例进行说明，包括以下步骤：

[0054] 步骤202：获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书；

[0055] 步骤204：利用对应的根证书密钥解密根证书，得到根证书包含的根验证数据和组件发布证书密钥；

[0056] 步骤206：利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥；

[0057] 步骤208：获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，利用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据；

[0058] 具体地，当设备中需要添加新的组件时，需要先将组件对应的证书存储到设备中，随后添加新的组件：获取存储在软件无线电设备中的组件m和组件j对应的组件证书，利用步骤206中获得的组件证书密钥解密该组件证书，得到其中的组件验证数据。

[0059] 步骤210：根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器。

[0060] 当各步骤得到的根验证数据、组件发布验证数据和组件验证数据校验通过时，证明组件m和组件j是由设备厂商经过管理机构授权后发布的组件，允许其注册到该软件无线电设备对应的设备管理器。

[0061] 其中，根证书是整个证书体系的基础，基于一个根证书可以生成多个组件发布证书，使用根证书的密钥对组件发布证书验证数据进行加密，生成组件发布证书；类似地，基于一个组件发布证书，使用组件发布证书的密钥对组件证书验证数据进行加密，也可以生成多个组件证书。

[0062] 在实际应用中，根证书的生成和管理可以由管理机构负责。管理机构下辖的设备厂商根据其实际需求，向管理机构提交获取组件发布证书请求，并提交生成组件发布证书所需的数据。管理机构对该设备厂商进行审核后，向设备厂商提供包括组件发布证书密钥、组件发布证书验证数据在内的组件发布证书数据。设备厂商在开发软件通信体系结构组件时，可针对一个设备中的全部组件或针对单个组件生成唯一的组件证书密钥和组件证书验证数据，使用该设备厂商的组件发布证书密钥加密组件证书密钥和对应的组件证书验证数据，生成组件证书。管理机构和厂商负责确保其各级证书密钥和证书数据的保密性，以基于多级证书的组件验证过程的有效性。

[0063] 该设备对应的根证书、组件发布证书可以存储在验证服务器等该设备可以访问的设备中，组件证书是该软件无线电设备出厂时，预先存储在设备中的。此外，设备厂商需要修改组件的注册逻辑，使其在根验证数据、组件发布验证数据和组件验证数据的逻辑校验通过时，才向设备管理器发送组件注册请求。进行验证时，可以将根证书和组件发布证书下载到组件所在的设备中进行解密和验证，也可以将根证书、组件发布证书和组件证书下载到其他的设备中进行验证，并将验证结果返回给组件所在的设备，完成验证过程。通过这种验证方式，即使组件被移植到其他系统，因为无法同时复制存储在设备中的组件证书，或者无法获得对应的根证书和组件发布证书，因此组件无法完成验证过程，也不能注册到设备管理器。

[0064] 上述软件通信体系结构组件注册管理方法，在基于软件通信体系结构设计的设备中预存设备组件的组件证书，并对根证书、组件发布证书和组件证书进行多级嵌套的加密，使得设备组件在注册到设备管理器之前，需要解密其对应的根证书和组件发布证书，获取根证书验证数据、组件发布证书验证数据和组件证书的密钥，再解密组件证书获取组件证书验证数据；并且仅在根证书验证数据、组件发布证书验证数据和组件证书验证数据均校验通过时，才允许该组件注册到设备管理器。上述软件通信体系结构组件注册管理方法利用软件通信体系结构中的组件注册机制，使得组件必须在验证通过后才能运行，解决了保护基于软件通信体系结构的软件无线电开发成果的问题，有利于推动基于软件通信体系结构的软件无线电系统开发的产业化发展和商业应用。

[0065] 其中一个实施例中，利用所述组件发布证书密钥解密所述组件发布证书，得到所述组件发布证书包含的组件发布验证数据和组件证书密钥的步骤包括：

[0066] 获取预设的组件发布证书的级数N；

[0067] 当N＝2时，利用组件发布证书密钥解密第2级组件发布证书，得到第2级组件发布证书中包含的第1级组件发布证书密钥；

[0068] 当N≥3时，利用组件发布证书密钥解密第N级组件发布证书，得到第N级组件发布证书中包含的第N-1级组件发布证书密钥；利用第n级组件发布证书密钥解密第n级组件发布证书，得到第n级组件发布证书中包含的第n-1级组件发布证书密钥，其中2≤n≤N-1；

[0069] 利用第1级组件发布证书密钥解密第1级组件发布证书，得到第1级组件发布证书中包含的组件发布验证数据和组件证书密钥。

[0070] 具体地，在有多级管理机构或多级设备厂商的情况下，可以通过增加组件发布证书地级数来实现相应的多级授权过程。相应地，组件在进行验证时也需要根据组件发布证书的级数来调整验证过程。

[0071] 当组件发布证书的级数为2时，首先利用解密根证书获得的组件发布证书密钥解密第2级组件发布证书，得到其中包含的第1级组件发布证书密钥；当组件发布证书的级数为3以上时，首先利用解密根证书获得的组件发布证书密钥解密最高一级组件发布证书，得到其中包含的次一级组件发布证书密钥；重复这一过程，直至获得第1级组件发布证书密钥。

[0072] 利用第1级组件发布证书密钥解密第1级组件发布证书，得到第1级组件发布证书中包含的组件发布验证数据和组件证书密钥。

[0073] 本实施例提供的方法可以适用于需要组件需要多级管理和/或多级发布的情况，满足这些情况下的软件通信体系结构组件开发成果保护需求。

[0074] 其中一个实施例中，在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之后，还包括：根据预设的注册顺序，向待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令，该验证控制指令用于控制该待验证软件通信系统结构组件的下一软件通信系统结构组件开始进行验证。

[0075] 组件是软件通信体系结构中最小的功能实体和复用单元，具备特定的信号控制流程或信号处理功能，设备中的各组件间通过信号流向、组件功能等可建立起相应的逻辑关系。本实施例根据组件间的逻辑关系，依次对设备中的各个组件进行验证，必须在上一组件通过验证后，下一组件才能开始验证。相应地，组件中需要增加对应的逻辑，使得组件在收到验证控制指令后开始验证过程。

[0076] 与此相对地，如果各组件可以分别进行验证，则可以在设备中插入其他不需要验证的组件，实现修改设备功能的目的，本实施例可以避免这一问题。

[0077] 其中一个实施例中，根证书密钥、组件发布证书密钥和组件证书密钥采用的加密算法为非对称加密算法，包括RSA密码算法、ECC椭圆权限密码算法和数字验证数据算法。

[0078] 非对称加密算法采用私钥和公钥对来进行加密和解密，发送方使用私钥加密信息，同时可以公开公钥，接收方使用公开的公钥来解密收到的信息。由于私钥不需要通过消息传输，因此非对称加密算法比对称加密算法更加安全；此外，由于用户和其公私钥对是唯一对应的，接收方可以根据公钥来验证信息的来源是否真实，使消息的发送方具有不可抵赖性。

[0079] 具体地，如图3所示，本实施例提供的方法的包括以下步骤：

[0080] 步骤302：获取预先存储的根证书、该根证书对应的根证书公钥和组件发布证书；

[0081] 步骤304：利用对应的根证书公钥解密根证书，得到根证书包含的根验证数据和组件发布证书公钥；

[0082] 步骤306：利用解密得到的组件发布证书公钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书公钥；

[0083] 步骤308：获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，利用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据；

[0084] 步骤310：根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软

件通信体系结构组件注册到设备管理器。

[0085] 其中，根证书是由管理机构使用其私钥加密生成的，组件发布证书是由厂商使用其私钥加密生成的，组件证书是由厂商使用组件证书私钥加密生成并存储在对应设备中的。组件证书和组件证书私钥也可以采用明文的方式存储在对应设备中，在验证时，采用组件证书私钥加密组件证书，再利用解密获得的组件证书公钥解密该组件证书，得到组件证书验证数据。

[0086] 本实施例提供的方法利用了非对称加密算法可靠性高、发送方不可抵赖的特性，能够更好地确保证书验证过程的安全性和可靠性。

[0087] 其中一个实施例中，根证书还包含根证书有效性标识，组件发布证书还包含组件发布证书有效性标识，组件证书还包含组件证书有效性标识。在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之前，还包括：

[0088] 获取根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识；

[0089] 当根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识的状态均为有效时，获取根验证数据、组件发布验证数据和组件验证数据。

[0090] 随着计算能力的加强，破解密码的能力也在相应增强。因此可以根据加密强度等情况给各级证书设置相应的有效期限，当各级证书中存在过期的证书时，则对应的组件不能通过验证。这样能够增强对组件的管理，通过定期更新各级证书，确保持续保护基于软件通信体系结构的系统开发成果。

[0091] 进一步地，根证书、组件发布证书和组件证书中还可以包括证书序列号、版本号、密码算法类型、秘钥长度、哈希算法类型等数据。具体地，当采用对称加密算法时，对各级证书密钥和证书验证数据进行加密；当采用非对称加密算法时，对各级证书验证数据进行加密。各级证书验证数据包括用于哈希运算数据和计算得到的哈希值，用于验证解密结果是否正确。对于各级证书的证书序列号、版本号、密码算法类型、秘钥长度等数据，以采用非对称加密算法时的公钥，可以采用明文传输。这样能够在增加证书信息的同时限制验证过程中需解密数据的数量和种类，以提高验证过程的效率，节约计算资源。

[0092] 应该理解的是，虽然图2-3的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图2-3中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0093] 一种软件通信体系结构组件注册管理装置，包括：

[0094] 证书获取模块，用于获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书；

[0095] 根证书解密模块，用于利用根证书密钥解密根证书，得到该根证书包含的根验证数据和组件发布证书密钥；

[0096] 组件发布证书解密模块，用于利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥；

[0097] 组件证书解密模块，用于获取预先存储在对应设备中的待验证软件通信体系结构组件的组件证书，利用解密得到的组件证书密钥解密组件证书，得到该组件证书包含的组件验证数据；

[0098] 组件注册控制模块，用于根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器。

[0099] 其中一个实施例中，组件发布证书解密模块用于：

[0100] 获取预设的组件发布证书的级数N；

[0101] 当N＝2时，利用组件发布证书密钥解密第2级组件发布证书，得到第2级组件发布证书中包含的第1级组件发布证书密钥；

[0102] 当N≥3时，利用组件发布证书密钥解密第N级组件发布证书，得到第N级组件发布证书中包含的第N-1级组件发布证书密钥；利用第n级组件发布证书密钥解密第n级组件发布证书，得到第n级组件发布证书中包含的第n-1级组件发布证书密钥，其中2≤n≤N-1；

[0103] 利用第1级组件发布证书密钥解密第1级组件发布证书，得到第1级组件发布证书中包含的组件发布验证数据和组件证书密钥。

[0104] 其中一个实施例中，还包括组件验证控制模块，用于根据预设的注册顺序，向待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令，该验证控制指令用于控制该待验证软件通信系统结构组件的下一软件通信系统结构组件开始进行验证。

[0105] 其中一个实施例中，根证书还包含根证书有效性标识，组件发布证书还包含组件发布证书有效性标识，组件证书还包含组件证书有效性标识。本实施例提供的装置还包括证书有效性识别模块，用于在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之前，获取根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识；当根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识的状态均为有效时，获取根验证数据、组件发布验证数据和组件验证数据。

[0106] 关于软件通信体系结构组件注册管理装置的具体限定可以参见上文中对于软件通信体系结构组件注册管理方法的限定，在此不再赘述。上述软件通信体系结构组件注册管理装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0107] 在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图4所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储根证书、根证书密钥和组件发布证书数据。该计算机设备的网络

接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种软件通信体系结构组件注册管理方法。

[0108] 本领域技术人员可以理解，图4中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0109] 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现以下步骤：

[0110] 获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书；

[0111] 利用对应的根证书密钥解密根证书，得到根证书包含的根验证数据和组件发布证书密钥；

[0112] 利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥；

[0113] 获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，利用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据；

[0114] 根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器。

[0115] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：获取预设的组件发布证书的级数N；当N＝2时，利用组件发布证书密钥解密第2级组件发布证书，得到第2级组件发布证书中包含的第1级组件发布证书密钥；当N≥3时，利用组件发布证书密钥解密第N级组件发布证书，得到第N级组件发布证书中包含的第N-1级组件发布证书密钥；利用第n级组件发布证书密钥解密第n级组件发布证书，得到第n级组件发布证书中包含的第n-1级组件发布证书密钥，其中2≤n≤N-1；利用第1级组件发布证书密钥解密第1级组件发布证书，得到第1级组件发布证书中包含的组件发布验证数据和组件证书密钥。

[0116] 在一个实施例中，处理器执行计算机程序时还实现以下步骤：在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之后：根据预设的注册顺序，向待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令，该验证控制指令用于控制该待验证软件通信系统结构组件的下一软件通信系统结构组件开始进行验证。

[0117] 在一个实施例中，根证书还包含根证书有效性标识，组件发布证书还包含组件发布证书有效性标识，组件证书还包含组件证书有效性标识。处理器执行计算机程序时还实现以下步骤：在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之前，获取根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识；当根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识的状态均为有效时，获取根验证数据、组件发布验证数据和组件验证数据。

[0118] 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时时实现以下步骤：

[0119] 获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书；

[0120] 利用对应的根证书密钥解密根证书，得到根证书包含的根验证数据和组件发布证书密钥；

[0121] 利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥；

[0122] 获取预先存储在待验证软件通信体系结构组件所在设备中的组件证书，利用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据；

[0123] 根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器。

[0124] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：获取预设的组件发布证书的级数N；当N＝2时，利用组件发布证书密钥解密第2级组件发布证书，得到第2级组件发布证书中包含的第1级组件发布证书密钥；当N≥3时，利用组件发布证书密钥解密第N级组件发布证书，得到第N级组件发布证书中包含的第N-1级组件发布证书密钥；利用第n级组件发布证书密钥解密第n级组件发布证书，得到第n级组件发布证书中包含的第n-1级组件发布证书密钥，其中2≤n≤N-1；利用第1级组件发布证书密钥解密第1级组件发布证书，得到第1级组件发布证书中包含的组件发布验证数据和组件证书密钥。

[0125] 在一个实施例中，计算机程序被处理器执行时还实现以下步骤：在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之后：根据预设的注册顺序，向待验证软件通信系统结构组件的下一软件通信系统结构组件发送验证控制指令，该验证控制指令用于控制该待验证软件通信系统结构组件的下一软件通信系统结构组件开始进行验证。

[0126] 在一个实施例中，根证书还包含根证书有效性标识，组件发布证书还包含组件发布证书有效性标识，组件证书还包含组件证书有效性标识。计算机程序被处理器执行时还实现以下步骤：在根据预设的校验逻辑校验根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器的步骤之前，获取根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识；当根证书有效性标识、组件发布证书有效性标识和组件证书有效性标识的状态均为有效时，获取根验证数据、组件发布验证数据和组件验证数据。

[0127] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM

(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0128] 以上实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0129] 以上所述实施例仅表达了本申请的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本申请构思的前提下,还可以做出若干变形和改进,这些都属于本申请的保护范围。因此,本申请专利的保护范围应以所附权利要求为准。

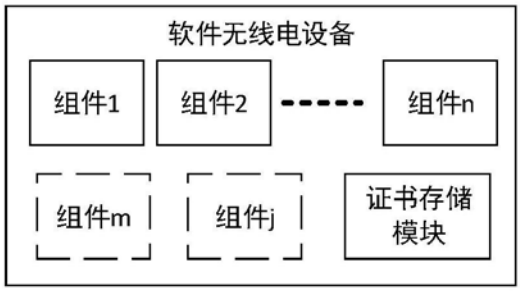

软件无线电设备
组件1
组件2
组件n
组件m
组件j
证书存储模块

图1

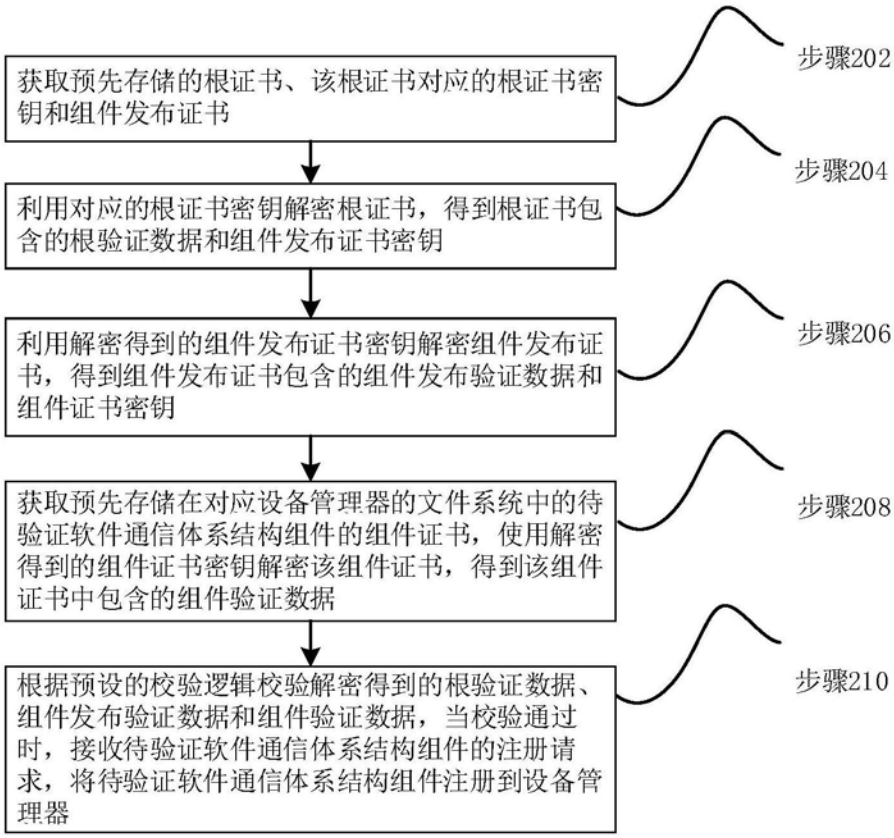

获取预先存储的根证书、该根证书对应的根证书密钥和组件发布证书
步骤202
利用对应的根证书密钥解密根证书，得到根证书包含的根验证数据和组件发布证书密钥
步骤204
利用解密得到的组件发布证书密钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书密钥
步骤206
获取预先存储在对应设备管理器的文件系统中的待验证软件通信体系结构组件的组件证书，使用解密得到的组件证书密钥解密该组件证书，得到该组件证书中包含的组件验证数据
步骤208
根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器
步骤210

图2

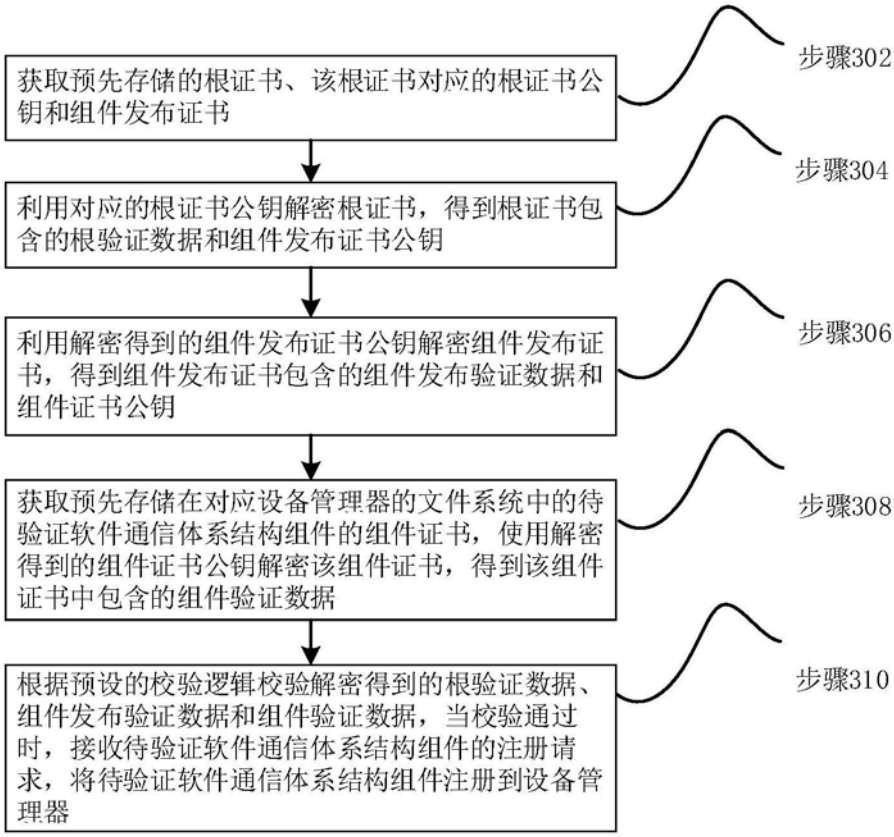

获取预先存储的根证书、该根证书对应的根证书公钥和组件发布证书
步骤302
利用对应的根证书公钥解密根证书，得到根证书包含的根验证数据和组件发布证书公钥
步骤304
利用解密得到的组件发布证书公钥解密组件发布证书，得到组件发布证书包含的组件发布验证数据和组件证书公钥
步骤306
获取预先存储在对应设备管理器的文件系统中的待验证软件通信体系结构组件的组件证书，使用解密得到的组件证书公钥解密该组件证书，得到该组件证书中包含的组件验证数据
步骤308
根据预设的校验逻辑校验解密得到的根验证数据、组件发布验证数据和组件验证数据，当校验通过时，接收待验证软件通信体系结构组件的注册请求，将待验证软件通信体系结构组件注册到设备管理器
步骤310

图3

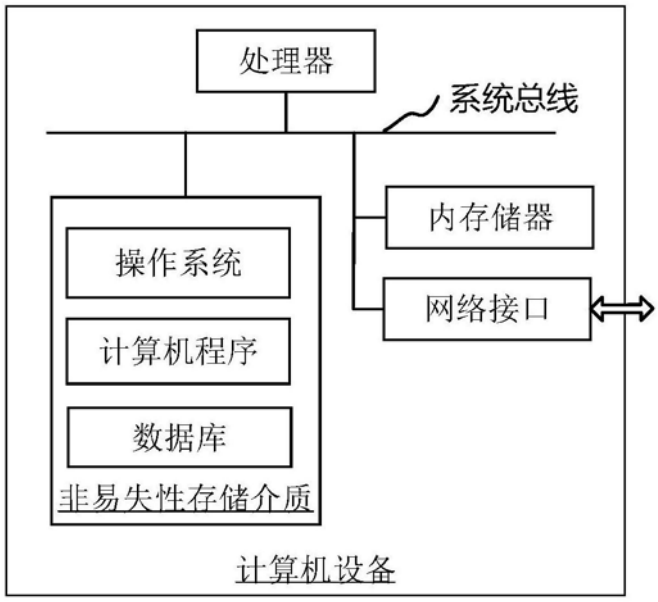

处理器
系统总线
内存储器
网络接口
操作系统
计算机程序
数据库
非易失性存储介质
计算机设备

图4