



(12) 发明专利申请

(10) 申请公布号 CN 116743386 A

(43) 申请公布日 2023. 09. 12

(21) 申请号 202310226391.8

(22) 申请日 2023.03.09

(30) 优先权数据

22161420.9 2022.03.10 EP

(71) 申请人 西门子股份公司

地址 德国慕尼黑

(72) 发明人 安娜·帕尔明

(74) 专利代理机构 北京康信知识产权代理有限

责任公司 11240

专利代理师 沈敬亭

(51) Int.Cl.

H04L 9/32 (2006.01)

H04L 9/40 (2022.01)

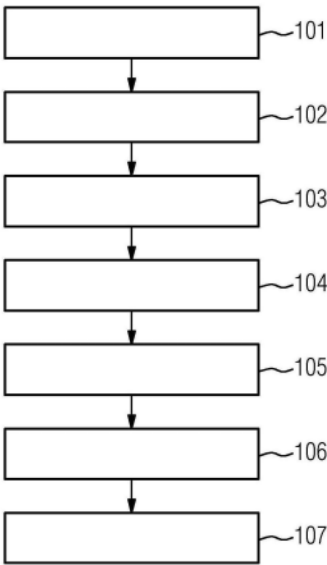
权利要求书2页 说明书8页 附图2页

(54) 发明名称

用于签发证书的方法和以计算机实施的注册机构

(57) 摘要

本申请涉及用于签发证书的方法和以计算机实施的注册机构,尤其提出一种用于通过技术设施的认证机构(5)向技术设施的设施部件(2)签发具有特定证书配置文件的证书的方法,其中在将由设施部件(2)提出的证书申请传输至认证机构(5)之前自动地检查:是否能够由设施部件(2)使用特定的证书配置文件,和是否允许在技术设施中将特定的证书配置文件分配给设施部件(2),其中对于两个检查都成功的情况,将证书申请传输至认证机构(5),对于证书申请检查成功的情况,所述认证机构为设施部件(2)签发具有特定的证书配置文件的所申请的证书。



1. 一种用于通过技术设施的认证机构(5)向所述技术设施的设施部件(2)签发具有特定的证书配置文件的证书的方法,其中,在将由所述设施部件(2)提出的证书申请传输至所述认证机构(5)之前自动地检查:

是否能够由所述设施部件(2)使用特定的所述证书配置文件,以及

是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2),

其中,针对两个检查都成功的情况将所述证书申请传输至所述认证机构(5),所述认证机构针对对于所述证书申请的检查成功的情况为所述设施部件(2)签发已申请的具有特定的所述证书配置文件的所述证书。

2. 根据权利要求1所述的方法,其中,由所述设施部件(2)自动检查是否能够由所述设施部件(2)使用特定的所述证书配置文件,使得所述设施部件(2)仅针对检查成功的情况才提出证书申请。

3. 根据权利要求2所述的方法,其中,基于事先由所述设施部件(2)的制造商、所述设施部件(2)的原始装备制造商或所述技术设施的操作员存储在所述设施部件(2)上的信息,所述设施部件(2)自动地检查是否能够由所述设施部件(2)使用特定的所述证书配置文件。

4. 根据权利要求3所述的方法,其中,尤其针对所述设施部件(2)的功能扩展的情况,定期地或以事件控制的方式更新所述信息,其中,能够由所述技术设施的操作员触发更新或自动地更新。

5. 根据前述权利要求中任一项所述的方法,其中,由所述技术设施的注册机构(4)检查:是否能够由所述设施部件(2)使用特定的所述证书配置文件,以及是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件,其中,响应于由所述设施部件(2)发出给所述注册机构的所述证书申请,所述注册机构(4)执行检查,并且其中,仅针对两个检查都成功的情况,所述注册机构(4)才将所述证书申请传输至所述认证机构(5)。

6. 根据至少权利要求2和5所述的方法,其中,所述设施部件(2)通知注册机构(4):所述设施部件(2)自身已经成功肯定了是否能够由所述设施部件(2)使用特定的所述证书配置文件的检查结果。

7. 根据权利要求1至6中任一项所述的方法,其中,基于操作员的预设来检查:是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2)。

8. 根据权利要求1至7中任一项所述的方法,其中,基于所述技术设施的自动化设置来检查:是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2)。

9. 根据权利要求8所述的方法,其中,由基于机器学习的系统检测所述技术设施的所述自动化设置的改变,其中,所述系统必要时自动地匹配用于检查是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2)的基础。

10. 根据权利要求1至9中任一项所述的方法,其中,以视觉方式给所述技术设施的操作员呈现是否能够由所述设施部件(2)使用特定的所述证书配置文件的检查的结果、以及是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2)的检查的结果。

11. 根据权利要求1至10中任一项所述的方法,其中,在所述技术设施的档案中存储是否能够由所述设施部件(2)使用特定的所述证书配置文件的检查的结果、以及是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2)的检查的结果。

12. 一种用于技术设施的控制系统以计算机实施的注册机构(4), 所述注册机构设计用于从所述技术设施的设施部件(2)接收由所述设施部件(2)提出的证书申请, 并且所述注册机构设计用于, 在将所述证书申请传输至所述技术设施的认证机构(5)之前自动地检查是否能够由所述设施部件(2)使用特定的所述证书配置文件, 并且检查是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2), 并且其中, 所述注册机构(4)设计用于, 针对两个检查都成功的情况将所述证书申请传输至所述认证机构(5)。

13. 根据权利要求12所述的以计算机实施的注册机构(4), 所述注册机构设计用于, 基于操作员的预设和/或基于所述技术设施的自动化设置来检查是否允许在所述技术设施中将特定的所述证书配置文件分配给所述设施部件(2)。

14. 一种包括根据权利要求12或13所述的以计算机实施的注册机构(4)、认证机构(5)和至少一个设施部件(2)的系统, 其中, 所述系统设计用于执行根据权利要求1至11中任一项所述的方法。

用于签发证书的方法和以计算机实施的注册机构

技术领域

[0001] 本发明涉及一种签发证书的方法。本发明还涉及一种计算机实施的注册服务和一种系统。

背景技术

[0002] 安全通信协议、例如HTTPS或OPC UA越来越多地进入技术设施中(更准确地说进入在离散的、和工艺过程的设施中)。使用所述协议的前提是使用根据X.509标准的所谓的数字证书。

[0003] 除了安全通信之外,为了最佳地保护(工业)技术设施,需要与不同的安全要求、例如“Security by Default默认安全”和“Least Functionality最少功能”一致地遵守安全的设备配置。根据当前的安全设计,使用所谓的制造商设备证书(根据IEEE802.1AR的IDevID证书)依照安全设计来检查真实性,进行指配和随后安全配置(即根据上述安全设计和基于其的安全策略)。只有这样,设施部件才允许申请所需的客户特定的证书(根据IEEE802.1AR的LDevID证书),并且然后利用所述证书与其通信伙伴进行安全通信。

[0004] 技术设施的部件通常与多于一个通信伙伴进行通信,并且在此使用多于一种的安全通信协议。例如,工业自动化系统(AS)通常能够通过HTTPS将其基于Web的用户界面提供用于用户访问(其中,使用配属的TLS服务器证书),并且同时(作为OPC UA服务器)通过OPC UA与配属的OPC UA客户端通信。因此,设施部件通常应申请多个证书(LDevID证书),其中,从安全角度来看建议为每个使用目的的申请或使用专用证书。

[0005] 根据当前的PKI设计,经由扮演智能网关角色的注册机构(英文Registration authority (RA))申请对通信所需的证书的。智能设施部件(例如网络部件或工业控制器以及OS/ES服务器和工业边缘部件)为此生成相应的证书申请并且将其传输至注册机构,其中,智能设施部件支持证书管理协议,例如根据RFC4210或根据Lightweight轻量级CMP配置文件的证书管理协议(CMP)。

[0006] 由于通常为特定目的签发的每个证书在其使用寿命期间不仅在初始进行申请,而且也应该/能够更新和/或撤销,所以例如上述CMP协议提供不同的所谓的CMP消息,根据所述CMP消息能够识别证书申请(或相应的底层的用例)的相应类型。例如,如果注册机构得到由设施部件发送的所谓的IR消息(“Initial Request初始请求”),则其识别出是特定证书的初始(首次)申请。注册机构通过CR或RR消息识别用于更新或撤销现有证书的申请。

[0007] 即使所有证书类型、例如TLS服务器、TLS客户端、OPC UA服务器或OPC UA客户端证书都能够从纯技术角度由相同的认证机构(英文Certification Authority (CA))签发,而关于安全性推荐推荐为每个使用目的或每个通信协议(例如TLS、OPC UA)分离、进而使用专用的认证机构。原因在于,如果设备为不同目的、或者为设备使用的通信协议使用多个不同的证书,其中,通信协议由相同认证机构签发并且认证机构做出妥协,则该设备不能够再经由安全的通信协议进行通信,因为它的(唯一的)由做出妥协的认证机构签发和认证的证书因此不再是值得信赖的。

[0008] 即使在根据上述建议使用不同的认证机构为不同的使用目的/通信协议签发证书的情况下,证书申请通常经由(中央的)注册机构(RA)进行。在此,注册机构能够例如根据证书申请的内容或根据http/https路径来识别所计划得到的证书的使用目的,其中,所述注册机构经由http/https路径获得证书申请。

[0009] 如果执行相应的配置,则注册机构通常能够将不同的证书申请转发给不同的负责的认证机构。为此需要提到的是,在使用CMP协议时,原则上可行的是,设施部件相应地在“接收者”字段中说明要寻址的认证机构。然而,这样的前提是,所述设施部件“知道”不同的认证机构和其与不同的证书配置文件的关联,而这在实践中是罕见的情况。通常,设施部件仅知道注册机构(或在分区段的网络的情况下知道负责的本地的注册机构(LRA))作为证书申请的响应伙伴。

[0010] 注册机构通常对其收到的证书申请进行如下检查:

[0011] (I) 检查是否存在申请人的清单条目,在注册机构的清单中(或在专用清单)中包含特定的包含在证书申请中的、鉴别申请人(尤其其ID)的数据,即对所述注册机构而言是否知道该申请人。如果检查结果不正常:证书申请将被拒绝。如果检查结果正常,则转到步骤II。

[0012] (II) 检查证书申请、更确切地说其根据RFC5280的签名是否正确和有效(这大致意味着:证书申请的签名与证书申请“匹配”)。如果检查结果不正常:证书申请被拒绝。如果检查结果正常,则转到步骤(III)。

[0013] (III) 检查用于签署证书申请的证书是否由(对注册机构已知的)认证机构签发,注册机构与所述认证机构已经具有信任关系(这例如能够意味着配属的“证书链”“相应地存放在注册机构的配置中和/或其“证书库”中)。如果检查结果不正常:证书申请被拒绝。如果检查结果正常,则将证书申请转发给相应的(例如在CMP消息中指定或在配置中指定的)认证机构。

[0014] 在EP 3 258 662 A1中公开一种用于在认证机构中注册智能电气设备的方法。

[0015] US 5 745 574 A公开一种具有多个认证机构的安全基础设施。

[0016] EP 3 287 925 A1公开一种用于将证书传递到设施中的设备上的计算设备。

[0017] 在W0 2020/078750 A1中公开一种用于在自动化系统中安全运行工业自动化设备的方法。在所述方法的范畴中,描述用于接收和转发证书申请的注册机构。

[0018] 现有技术是:每个成功经历检查(I)至(III)的证书申请都被转发给相应的(在注册机构中配置的)认证机构,这能够导致可能签发许多不必要的证书。由此尤其产生以下问题:

[0019] -通信量增加(这或者能够导致危害技术设施的正常运行和危害技术设施可用性),因为设施部件在初始申请的范畴中将不必要的证书申请传输至注册机构,所述注册机构然后转发给负责的认证机构,所述认证机构然后将多余的证书经由注册机构传输至申请人,并且由于所有签发的(也还有多余的)证书都在其到期前不久更新,这又导致不必要的管理耗费/通信量;

[0020] -增加设施部件的存储需求,所述设施部件将所有多余的证书存储在其“证书库”中并且将配属的加密密钥存储在配属的“密钥库”中(在理想情况下是硬件绑定的),其中,该问题尤其在资源贫乏的设备(英文:约束设备(Constraint Devices))中视作为是特别严

重的;和

[0021] -增加技术设施的清单中或“证书存储库”中的存储需求,根据当前的预设,应当保存在相应环境中签发的所有证书。

发明内容

[0022] 本发明所基于的目的是:提出一种用于向技术设施的设施部件签发证书的方法,其避免之前列举的缺点,并且能够实现技术设施的更有效的证书管理。

[0023] 在根据本发明的、用于通过技术设施的认证机构向技术设施的设施部件签发具有特定的证书配置文件的证书的方法中,在将由设施部件提出的证书申请传输至认证机构之前,自动地检查:

[0024] -是否能够由设施部件使用特定的证书配置文件,和

[0025] -是否允许在技术设施中将特定的证书配置文件分配给设施部件,

[0026] 其中,对于两个检查都成功的情况,将证书申请传输至认证机构,对于证书申请检查成功的情况,所述认证机构为设施部件签发具有特定的证书配置文件的申请的证书。

[0027] 将证书理解为确认特定属性(在该情况下为机器、设备、应用程序等的特定属性)的数字数据集。证书的真实性和完整性通常能够借助于加密方法来验证。由认证机构为技术设施中的设施部件的使用来签发证书,认证机构也称为所谓的“颁发CA(认证机构(Certification Authority))”。这种颁发CA通常始终在线,并基于收到的证书申请,为不同的申请人签发证书,颁发CA用自己的颁发CA证书对证书申请进行签名。通过以下方式确保颁发CA的可信性,即其自身的颁发CA证书通过位于被保护的环境中的受信任的根认证机构(也称为“根CA”)的证书来签名。在此,应注意,根CA大部分时间离线,并且仅当其应为配属的颁发CA签发证书时,才(在遵守最严格的安全预防措施的情况下)激活或接通。根CA能够位于技术设施之外。

[0028] 技术设施能够是出自过程工业,例如化学、制药、石化工业的设施、或来自食品和饮料行业的设施。借此,也包括来自其中例如生产所有类型的汽车或物品的生产工业的任何设施。适合于执行根据本发明的方法的技术设施也能够来自能源生产领域。风力涡轮机、太阳能设施或用于产生能源的发电厂同样包括在术语“技术设施”中。

[0029] 技术设施的设施部件能够是任何设备或计算机实施的应用程序,所述应用程序需要通过一个或多个证书进行身份验证以与技术设施的其他部件进行通信。技术设施的设施部件能够例如是泵、阀、马达、加热炉等设备,但也能够是软件程序。

[0030] 为了获得设施部件需要与技术设施内的其他设施部件交互的证书,设施部件必须提出向认证机构提交的证书申请(直接或间接地经由下面解释的注册机构提出)。因此,换言之,证书申请是设施部件向技术设施的认证机构的申请,认证机构为设施部件签发证书

[0031] 证书具有特定的证书配置文件(英文Certificate Profile)。在此,证书配置文件包括证书的类型。例如,类型能够是TLS(传输层安全(Transport Layer Security))服务器证书、TLS客户端证书、OPC UA(开放平台通信统一架构(Open Platform Communications Unified Architecture))服务器证书或OPC UA客户端证书。根据分配的证书类型和可能其他附加的要求,证书配置文件能够包括根据ITU-T标准X.509的特定的证书属性及其值。在此,在根据所述证书配置文件的验证中,拒绝每个不包含所有确定的属性和值的证书申请。

通过证书配置文件规定/确定的属性和/或值越多,验证就越严格和准确。

[0032] 在本发明的范畴中自动检查特定的证书配置文件是否能够由设施部件使用。因此意味着,检查要向认证机构提交证书申请的设施部件在技术上为此是否能够使用由其所申请的、具有特定的证书配置文件的证书。例如,如果实际上不支持OPC UA的设施部件申请OPC UA服务器证书,或者如果不能作为TLS服务器的设施部件申请TLS服务器证书,则情况并非如此。

[0033] 在第二检查阶段的范围内检查是否应提交证书申请的设施部件分配技术设施中的特定的证书配置文件。换言之,在检查使用具有特定证书配置文件的证书的基本能力之后,还在技术设施内的实际需要方面检查在技术设施中使用具有特定的证书配置文件的证书的基本能力。然后,例如如果设施部件尽管能够作为Web服务器(这就是检查的第一阶段仍然会成功的原因),而检查的第二阶段不会成功,然而该功能在技术环境的相应的运行时环境的上下文中是不期望的。由于检查的第二阶段不成功,整个检查不会成功,这就是为什么在这种情况下不会将证书申请传输至认证机构的原因。

[0034] 根据本发明的方法能够成功地防止在技术设施中签发多余的证书,由此,能够为优化通信和维持技术设施的正常运行和可用性做出牢固基础的贡献。

[0035] 能够由设施部件自动执行是否能够由设施部件使用特定的证书配置文件的检查,如此,使得设施部件仅针对检查成功的情况才提出证书申请。因此,对于设施部件不支持具有特定的证书配置文件的证书的情况,则根本不会提出任何证书申请(进而也不传输至认证机构)。对于设施部件支持多个证书配置文件的情况,则能够将证书配置文件组合在一个设备配置文件中,以便更清楚并且简化在制造商侧上还有在操作使用环境中管理证书配置文件,并使其更可靠。

[0036] 为此,关于设施部件能够使用哪些证书配置文件的信息优选地存储在设施部件上。所述信息能够由设施部件的制造商、设施部件的原始设备制造商(OEM)或设施部件的操作员/运营商在技术设施中存储在设施部件上。

[0037] 优选地定期更新或以事件控制的方式更新信息,特别地对于设施部件的功能扩展的情况更新信息,其中,更新能够以通过操作员/用户触发或自动地进行。这种事件例如也能够是通过ECC算法或特定的国家/地区特定的算法替换包含在相关的证书配置文件中的、用于加密和/或形成签名的RSA算法。

[0038] 附加于或替代于通过设施部件本身进行的检测的(第一)阶段之外,能够由技术设施的注册机构检查是否能够由设施部件使用特定的证书配置文件的检查,以及检查是否允许在技术设施中将特定的证书配置文件分配给设施部件,其中,注册机构执行响应于由设施部件发出给注册机构的证书申请来执行检查,并且其中,注册机构仅针对两个检查都成功的情况才将证书申请传输至认证机构。

[0039] 在此,对于(第一)检查是否能够由设施部件使用特定的证书配置文件所需的信息能够由技术设施的运营商/操作员存储在注册机构中。基于所述信息,在两阶段检查的第一阶段的范畴中,注册机构能够检查设施部件的证书申请。当设施部件本身不能够检查要生成的证书申请的证书配置文件是否能够由设施部件使用时,该检查特别有意义。例如,如果在检查的第一阶段的范畴中注册机构确定已经申请了(由于其功能范围或其支持的通信协议)不被设施部件支持的证书配置文件(例如OPC UA),则注册机构拒绝证书申请,进而拒绝

将其转发给认证机构。

[0040] 在设施部件设计用于执行检查的第一阶段的前提下,设施部件能够通知注册机构:已经由设施部件本身成功地执行了是否能够由设施部件使用特定的证书配置文件的检查。响应于此,注册机构能够放弃重新检查是否能够由设施部件使用特定的证书配置文件,以便节省资源。

[0041] 能够基于操作员的预设来进行检查的第二阶段,即检查在技术设施中是否允许将特定的证书配置文件与设施部件相关联。为此,例如注册机构的用户界面的操作员例如能够利用适当的输入掩码来进行操作。操作员能够使用所谓的申请人配置文件作为其自己限定的或第三方先前限定的模板。在这种申请人配置文件中概括证实配置文件,所述证书配置文件允许被分配给技术设施中的设施部件。使用申请人配置文件简化了第二检查的配置。

[0042] 替代地或附加地,能够基于技术设施的自动化设置来进行是否允许在技术设施中将特定的证书配置文件分配给设施部件的检查。典型地,在自动化设置中描述技术设施的设施部件之间的通信关系,所述通信关系对设施部件分别需要何种证书类型具有直接影响。例如,注册机构能够读取所述自动化设置,更确切地说读取相应的文件,并且自动地用于第二检查阶段。为此,不需要操作员的任何干预,但是其中不排除这种干预。

[0043] 在此,技术设施的自动化设置的变化能够由基于机器学习的系统检测,其中,该系统在需要的情况下自动地适配用于是否允许在技术设施中将特定的证书配置文件分配给设施部件的检查的基础。

[0044] 优选地,是否能够由设施部件使用特定的证书配置文件的检查的结果和是否允许在技术设施中将特定的证书配置文件分配给设施部件的检查的结果以视觉方式呈现给技术设施的操作员。随后,所述操作员能够触发可能的后续动作,以便对结果做出适当的反应。

[0045] 替代于或附加于视觉输出,是否能够由设施部件使用特定的证书配置文件的检查的结果和

[0046] -是否允许在技术设施中将特定的证书配置文件分配给设施部件的检查的结果能够存储在技术设施的档案中,例如存储在为此设计的档案服务器上。

[0047] 在该上下文中,将控制系统理解为计算机辅助的技术系统,所述系统包括用于显示、操作和控制方法技术设施的功能。控制系统还能够包括用于求出测量值的传感器和不同的执行器。此外,控制系统能够包括用于驱控执行器或传感器的所谓的过程相关或生产相关的部件。此外,控制系统还能够具有用于可视化方法技术设施和用于工程设计的构件。将术语控制系统附加地还理解为用于更复杂调节的其他计算单元和用于数据存储和数据处理

的系统。

[0048] 此外,上述目的还通过计算机实施的注册机构或类似的机关或用于技术设施的控制系统

的相应的类似的服务来实现,注册机构设计用于:由技术设施的设施部件接收由设施部件提出的证书申请,并且注册机构设计用于:在将证书申请传输至技术设施的认证机构之前自动地检查是否能够由设施部件使用特定的证书配置文件和是否允许在技术设施中将特定的证书配置文件分配给设施部件,其中,注册机构设计用于对于两个检查都成功的情况,将证书申请传输至认证机构。

[0049] 注册机构例如能够在控制系统的操作员站服务器上实施。在此,将“操作员站服务器”理解为如下服务器,所述服务器中央地检测操作和观察系统的数据,以及通常检测技术设施的控制系统警报和测量值档案并提供给用户。操作员站服务器通常建立与技术设施的自动化系统的通信连接并将技术设施的数据转发给所谓的操作员站客户端,所述操作员站客户端用于操作和观察技术设施的各个功能元件的运行。操作员站服务器能够具有客户端功能,以便访问其他操作员站服务器的数据(存档、消息、标签、变量)。操作员站服务器能够是、但不限于西门子公司SIMATIC PCS7工业工作站服务器。

[0050] 在此,计算机实施的注册机构能够设计用于:基于操作员的预设和/或基于技术设施的自动化设置来执行是否允许在技术设施中将特定的证书配置文件分配给设施部件的检查。

[0051] 上面提出的目的还通过一种系统来实现,该系统包括如上所解释的那样构成的计算机实施的注册机构、认证机构和至少一个设施部件,其中,该系统设计用于执行包括之前解释的方法步骤的方法。

附图说明

[0052] 利用一下结合附图对实施例的描述,更详细地解释本发明的上述特性、特征和优点以及如何实现其的方式和方法。附图示出:

[0053] 图1示出根据本发明的系统的示意图;和

[0054] 图2示出根据本发明的方法的流程图。

具体实施方式

[0055] 在图1中示出系统1,所述系统包括设施部件2、操作员站服务器3与在其上实施的注册机构4、和认证机构5。设施部件2与操作员站服务器3和在其上实施的注册机构4连接。类似于此,认证机构5具有到操作员站服务器3与在其上实施的注册机构4的连接。

[0056] 注册机构4以本身已知的方式设计用于从设施部件2接收证书申请并转发给认证机构5。此外,注册机构4设计用于接收由认证机构5签发的证书并转发给设施部件2。认证机构5设计用于检查证书申请,并且对于满足特定检查标准的情况签发所申请的证书。此外,认证机构5还能够再次撤销已经签发的证书,然而对此在本文中不进一步深入讨论。

[0057] 在图2中示出根据本发明的方法的流程。在第一步骤101中,设施部件2检查是否允许对具有特定的证书配置文件的证书提出证书申请,所述证书的生成由操作员启动或由技术设施的软件部件自动启动。在此,设施部件2本身通过配属的微处理器来检查是否能够由设施部件2使用(是证书申请的主题的)特定的证书配置文件。如果不是这种情况,则拒绝证书申请的生成。

[0058] 对于检查结果成功的情况,将证书申请转发给注册机构4。数据传输能够经由现场总线、例如工业以太网进行。

[0059] 在第二步骤102中,注册机构4接受证书申请并检查申请人是否为其所知。检查以本身已知的方式通过将证书申请的数据(特别是与申请人的身份相关的数据)与和注册机构4相关联的存储器(英文清单(Inventory))进行比较来进行。对于申请人不为注册机构所知4的情况,证书申请被拒绝。对于申请人对其所知的情况,则执行随后的第三步骤103。

[0060] 在第三步103的范畴中,注册机构4检查根据RFC5280证书申请、更准确地说是其签名是否正确和有效。换言之,注册机构4检查证书申请的签名是否与证书申请相匹配。对于检查不成功的情况,证书申请被拒绝。对于检查成功的情况,执行随后的第四步骤104。

[0061] 在第四步骤104的范畴中,注册机构4检查用于对证书申请签名的证书是否由(对注册机构4所知的)认证机构签发,其中,注册机构4已经与认证机构具有信任关系。在此,认证机构能够为图1中所示的认证机构5。信任关系的存在例如能够意味着,配属的证书链被相应地存储在注册机构4的配置存储器中和/或其“证书库”中。对于检查不成功的情况,证书申请被拒绝。对于检查成功的情况,执行随后的第五步骤105。

[0062] 在第五步骤105的范围中,注册机构4检查在证书申请中申请的特定的证书配置文件是否能够被设施部件2(完全)使用。注册机构4能够从证书申请中直接或间接地经由证书申请中引用的来源(例如URL)得出申请哪个证书配置文件。在该情况下,第五步骤105是可选的,因为设施部件2本身已经执行了检查。然而,如果是异质环境/技术设施,在该异质环境/技术设施中不是每个设施部件都能够可验证地执行检查,则推荐通过注册机构4对所有收到的证书申请执行检查。对于检查不成功的情况,证书申请被拒绝。对于检查成功的情况,执行随后的第六步骤106。

[0063] 在第六步骤106的范畴中,注册机构4检查设施部件2是否允许在技术设施中分配特定的证书配置文件。在此,所述注册机构能够基于操作员的预设或基于技术设施的自动化设置来执行检查,其中,所述技术设施尤其能够通过自学系统保持最新。对于检查不成功的情况,证书申请将被拒绝。如果检查成功,则执行随后的第七步骤107。

[0064] 在第七步骤107的范畴中,证书申请被转发给认证机构5。所述认证机构检查证书申请是否有效,并且在成功的情况下,签发所申请的证书。所述证书从认证机构5经由注册机构4传输至设施部件2并在那里存储在证书库中。于是,设施部件2然后例如能够与技术设施的其他的设施部件通信,系统1能够处于技术设施中。

[0065] 通过所描述的发明确保在OT环境/工业设施中,仅如下证书在相应的认证机构中被申请并且由认证机构签发,所述证书满足以下前提:

[0066] -由申请人通过其功能范围支持证书配置文件。

[0067] -申请人在相应工业设施/OT环境的上下文中需要所述证书(或其证书配置文件)。

[0068] 通过本发明基本上能够完全禁止签发多余证书,由此,对于以下显著的改进做出有牢固基础的贡献:

[0069] -对于优化/最小化在设施部件的证书库中存储证书所需的存储空间;

[0070] -对于优化/最小化对于将证书存储在清单/OT环境的元数据库/工业设施中所需的存储器空间;

[0071] -对于优化/最小化用于在OT环境/工业设施中签发的证书的管理耗费/存储库中存储证书所需的存储空间(因为当前根据经验,多余的证书由设施部件或其他机关监控其到期和在到期前不久借助RA/CA的支持相应地更新);

[0072] -对于优化通信量(因为不必要的/多余的证书申请不转发给注册机构或认证机构,并且随后不会发生基于所述证书申请签发(多余的/不必要的)证书以及将这些证书传输至申请人;

[0073] -对于维持OT环境/系统的正常运行和可用性(由于所有上述优点)

[0074] -对于加密敏捷性,因为在本发明中引入的证书特定的设备和申请人配置文件具有非常高的灵活性和可配置性,尤其在当所使用的加密算法已被破坏或(例如在特定国家中)不允许使用时的情况下,所述灵活性和可配置性能够实现通过其他适当算法快速替代算法。

[0075] 尽管详细地通过优选的实施例详细地阐述和描述本发明,然而本发明不受所公开的示例限制,并且能够由本领域技术人员从中推导出其他的变体方案,而不偏离本发明的保护范围。

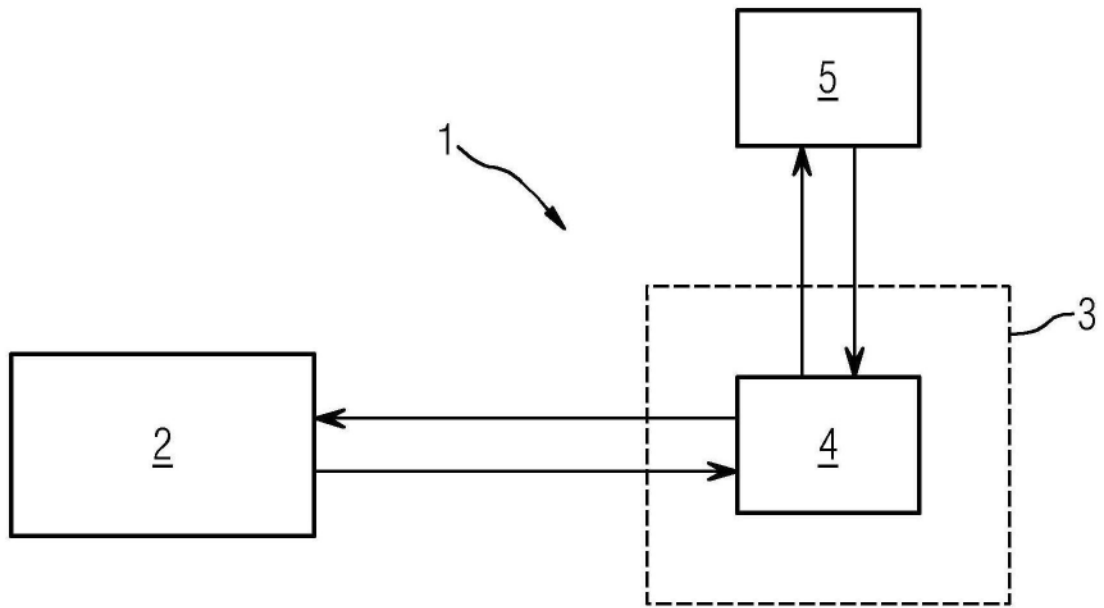


图1

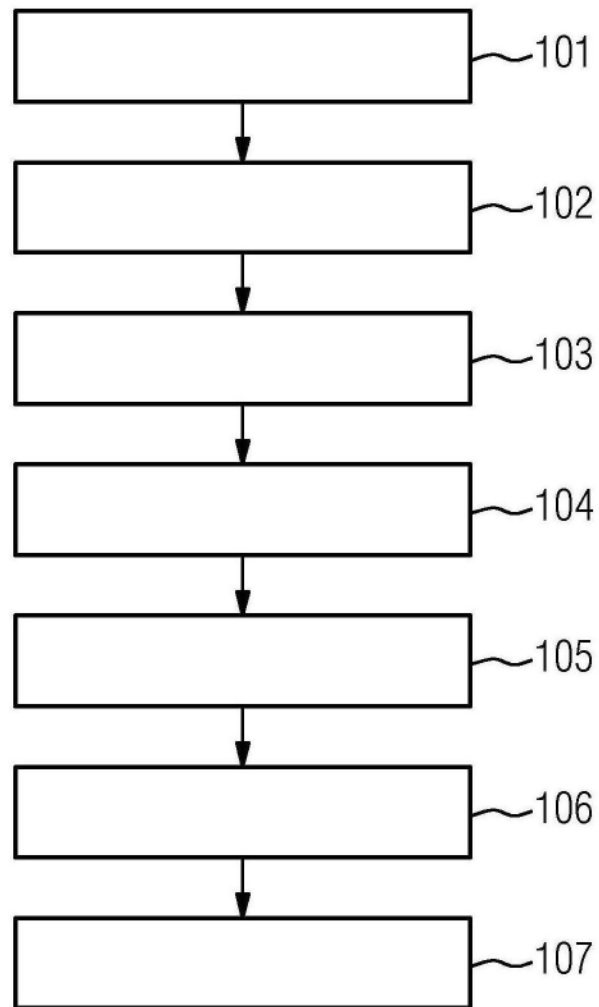


图2