



(12) 发明专利申请

(10) 申请公布号 CN 115885499 A

(43) 申请公布日 2023. 03. 31

(21) 申请号 202180050896.2

(22) 申请日 2021.08.10

(30) 优先权数据

20191531.1 2020.08.18 EP

(85) PCT国际申请进入国家阶段日

2023.02.17

(86) PCT国际申请的申请数据

PCT/EP2021/072237 2021.08.10

(87) PCT国际申请的公布数据

W02022/037997 DE 2022.02.24

(71) 申请人 西门子股份公司

地址 德国慕尼黑

(72) 发明人 R·福尔克 S·弗里斯

(74) 专利代理机构 中国专利代理(香港)有限公司
72001

专利代理师 臧永杰 刘春元

(51) Int.Cl.

H04L 9/40 (2022.01)

H04L 9/32 (2006.01)

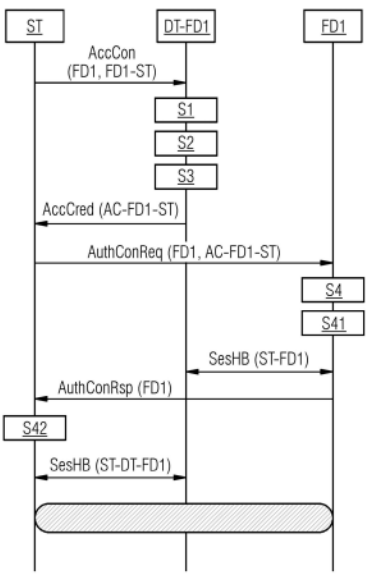
权利要求书2页 说明书9页 附图3页

(54) 发明名称

在设备处对通信伙伴进行认证

(57) 摘要

一种用于在设备处对通信伙伴(ST)进行认证的方法,其中除了物理设备实现(FD1)之外,还存在至少一个分配给所述设备的虚拟设备实现(TD-FD1),所述方法具有以下步骤:-在所述两个设备实现中的第一设备实现中接收(S1)通信伙伴(ST)的访问权限,-通过所述第一设备实现检验(S2)所述访问权限,以及-如果所述访问权限被认为是允许的,则从所述第一设备实现向所述通信伙伴(ST)提供(S3)权限证明(AC),以及-允许(S4)通过所述通信伙伴(ST)借助于所述权限证明(AC)访问所述两个设备实现中的第二设备实现。



1. 一种用于在设备处对通信伙伴 (ST) 进行认证的方法, 其中除了物理设备实现 (FD1) 之外, 还存在至少一个分配给所述设备的虚拟设备实现 (TD-FD1), 所述方法具有以下步骤:

- 在所述两个设备实现中的第一设备实现中接收 (S1) 通信伙伴 (ST) 的访问权限,
- 通过所述第一设备实现检验 (S2) 所述访问权限, 以及
- 如果所述访问权限被认为是允许的, 则从所述第一设备实现向所述通信伙伴 (ST) 提供 (S3) 用于通过所述通信伙伴 ST 访问所述第二设备实现的权限证明 (AC), 以及
- 允许 (S4) 通过所述通信伙伴 (ST) 借助于所述权限证明 (AC) 访问所述两个设备实现中的第二设备实现。

2. 根据权利要求1所述的方法, 其中所述权限证明 (AC) 是用于接入认证的接入权限证明和/或用于所授予的访问权的访问权限证明。

3. 根据前述权利要求中任一项所述的方法, 其中所述权限证明 (AC) 的有效性是在时间上有限的。

4. 根据前述权利要求中任一项所述的方法, 其中借助于所述权限证明 (AC) 对所述第二设备实现的访问的次数是有限的。

5. 根据前述权利要求中任一项所述的方法, 其中如果在所述第一设备实现和所述通信伙伴 (ST) 之间的连接被终止, 则所述权限证明 (AC) 被撤销或不被更新。

6. 根据前述权利要求中任一项所述的方法, 其中所述权限证明 (AC) 是数字证书或密码密钥或接入令牌。

7. 根据前述权利要求中任一项所述的方法, 其中所述权限证明 (AC) 包括以下信息中的至少一个:

- 所述通信伙伴 (ST) 的证书的标识符,
- 所述通信伙伴 (ST) 的授权信息,
- 针对所述通信伙伴 (ST) 的访问的时间限制和/或地理限制,
- 可用通信媒介的限制,
- 可用通信协议的限制,
- 关于所述通信伙伴 (ST) 的安全状态的信息,
- 所述权限证明 (AC) 的完整性校验值。

8. 根据前述权利要求中任一项所述的方法, 其中所述权限证明 (AC) 在建立安全的通信连接时从所述第一设备实现被传送给所述通信伙伴 (ST) 和/或从所述通信伙伴 (ST) 被传送给所述第二设备实现。

9. 根据前述权利要求中任一项所述的方法, 其中所述权限证明 (AC) 经由经认证的现有通信连接从所述第一设备实现被传送给所述通信伙伴 (ST) 和/或从所述通信伙伴 (ST) 被传送给所述第二设备实现。

10. 根据前述权利要求中任一项所述的方法, 其中所述第二设备实现的地址信息附加地从所述第一设备实现被提供给所述通信伙伴 (ST)。

11. 根据前述权利要求中任一项所述的方法, 其中在通过所述第一设备实现检验所述访问权限时, 检验所述通信伙伴 (ST) 的当前配置的完整性和/或允许性。

12. 根据前述权利要求中任一项所述的方法, 其中所述第一设备实现将关于所述设备的配置的信息传送给所述通信伙伴 (ST)。

13. 一种设备,所述设备包括物理设备实现 (FD1) 和所分配的虚拟设备实现 (TD-FD1), 所述物理设备实现和所分配的虚拟设备实现被构造用于

- 在所述两个设备实现中的第一设备实现中接收通信伙伴 (ST) 的访问权限,
- 通过所述第一设备实现检验所述访问权限,以及
- 如果所述访问权限被认为是允许的,则从所述第一设备实现向所述通信伙伴 (ST) 提供用于通过所述通信伙伴 ST 访问所述第二设备实现的权限证明 (AC), 以及
- 允许通过所述通信伙伴 (ST) 借助于所述权限证明 (AC) 访问所述两个设备实现 (FD1、DT-FD1) 中的第二设备实现。

14. 根据权利要求13所述的设备,其中所述虚拟设备实现 (TD-FD1) 是根据开放平台通信统一架构标准的OPC UA服务器。

15. 根据权利要求13或14所述的设备,其中所述虚拟设备实现 (TD-FD1) 被构造在中央服务器 (13)、边缘服务器 (12) 上或被构造在所述设备的物理设备实现 (FD1、...、FD5) 上。

16. 一种计算机程序产品,所述计算机程序产品包括能够直接被加载到数字计算机的存储器中的非易失性计算机可读介质,包括适用于执行根据权利要求1至12中任一项所述的方法的步骤的程序代码部分。

在设备处对通信伙伴进行认证

技术领域

[0001] 本发明涉及一种用于在设备处对通信伙伴进行认证的方法,其中除了物理设备实现之外,还存在至少一个分配给所述设备的虚拟设备实现。

背景技术

[0002] 经由网络连接对设备、诸如现场设备、控制设备、物联网(IoT)设备等的访问必须被认证,以便防止通过未经授权方的访问。在工业环境中,访问不仅可以通过自动化系统的其他设备进行,而且例如可以通过服务技术人员进行,所述服务技术人员经由基于网络的本地服务接口或经由远程维护接入(Fernwartungszugang)来访问设备。

[0003] 在工业环境中,数字孪生(也称为Digital Twin(数字孪生)或管理壳或Administration Shell)的概念日益起重要作用。在此,通过数字孪生实现真实对象的虚拟表示。

[0004] 出版物SIEMENS AG(西门子公司)等:“Digital-Twin-Zertifikat”(PRIOR ART PUBLISHING GMBH,PRIOR ART PUBLISHING GMBH,MANFRED-VON-RICHTHOFEN-STR.9,12101BERLIN GERMANY,Bd.www.priorartregister.com,2019年2月21日(2019-02-21),1-5页,XP007022409)描述不仅分配给物理对象而且分配给其数字孪生的数字孪生证书。数字孪生证书包含分配给真实对象或其数字孪生的两个公钥条目以及数字孪生的链接(URL)。物理对象使用数字孪生证书,以便在检验方处进行认证。随后,检验方可以通过第二公钥对数字孪生的以加密的方式传送的数据进行解密并且从而访问所述数据。

[0005] WO 2019/243429 A1公开一种用于客户端设备安全地访问云服务器中的云服务的方法,其中该访问通过第三方的服务器上的应用程序被提供。

[0006] 为服务技术人员或其他通信伙伴设立和管理访问权限以及设立和管理相对应的检验数据是耗费的。从而,例如密码信息、公钥证书或甚至权限信息必须在用户数据库中被设立和管理。此外,在工业环境中,通信网络此外通常与外部通信网络隔离,使得不能使用中央安全服务、诸如目录服务或认证服务器。

[0007] 此外,这样的设备通常具有低的计算能力或通过电池被供电,使得在那里应该避免耗费的查询或操作。

发明内容

[0008] 因此,本发明的任务是以尽可能节能和节省容量的方式设计针对这样的设备的接入认证,并且仍然保证足够的保护和灵活的访问可能性。

[0009] 该任务通过在独立权利要求中描述的特征来解决。本发明的有利改进方案在从属权利要求中示出。

[0010] 根据第一方面,本发明涉及一种用于在设备处认证通信伙伴的方法,其中除了物理设备实现之外,还存在至少一个分配给所述设备的虚拟设备实现,所述方法具有以下步骤:

- [0011] -在所述两个设备实现中的第一设备实现中接收通信伙伴的访问权限，
- [0012] -通过第一设备实现检验访问权限，以及
- [0013] -如果所述访问权限被认为是允许的，则从所述第一设备实现向所述通信伙伴提供用于通过所述通信伙伴访问所述第二设备实现的权限证明 (Berechtigungsnachweis)，以及
- [0014] -允许通过所述通信伙伴借助于所述权限证明访问所述两个设备实现中的第二设备实现。
- [0015] 这能够实现通信伙伴对第二设备实现的简化的接入。如果第二设备实现从通信伙伴接收权限证明，则第二设备实现在无其他检验的情况下或以减小的检验范围允许访问。由此可以在两个设备实现之间划分例如用于检验参数的任务，并且从而减轻每个单独的设备实现的负担。因此，不需要所有要检验的参数或关于此的信息在两个设备实现上可用和被管理。在此，通信伙伴可以将访问权限要么传送给物理设备实现要么传送给虚拟设备实现。如果由物理设备实现接收访问权限，则该物理设备实现是第一设备实现并且相应地虚拟设备实现是第二设备实现。相反地，如果访问权限从通信伙伴被发送给虚拟设备实现并且在那里被接收，则该虚拟设备实现是第一设备实现。在成功地检验之后，虚拟设备实现将权限证明提供给通信伙伴，所述权限证明允许访问物理设备实现，所述物理设备实现于是表示第二设备实现。访问权限例如是密码、访问代码、访问令牌、生物认证信息或者在使用秘密/公共密码密钥或包含公钥的数字证书的情况下的密码认证信息。
- [0016] 在一种有利的实施方式中，权限证明是用于通信伙伴在第二设备实现处进行接入认证的接入权限证明和/或用于授予通信伙伴的对第二设备实现的访问权的访问权限证明。
- [0017] 因此，通信伙伴可以通过所获得的权限证明在第二设备实现处进行认证/或也可以在那里例如根据不同的安全等级访问权来检验或授予访问权限。
- [0018] 在一种有利的实施方式中，权限证明的有效性是时间上有限的。
- [0019] 由此可以减少权限证明的滥用。时间限制例如可以是受限制的有效期限或者也可以是预先给定的时间间隔，在所述时间间隔内权限证明是有效的。由此限制何时可以执行针对第二设备实现的接入认证。在预先给定的有效期限之后，不允许通信伙伴进一步访问第二设备实现。另一方面，通过权限实现的时间上有限的有效性可以限制所建立的连接可以最大保持存在多长时间。
- [0020] 在一种有利的实施方式中，借助于权限证明对第二设备实现的访问的次数是有限的。
- [0021] 例如，权限证明可以是仅可使用一次的，例如可用于仅建立一次与第二设备实现的连接。这允许对用于第二设备实现的权限证明的使用进行灵活限制，并且因此防止对第二设备实现的权限证明的不期望的不受限制的使用。为此，第二设备实现可以将所使用的权限证明录入所使用的权限证明的列表中。由此可以识别对已经使用的权限证明的重新使用并且可以拒绝该权限证明。
- [0022] 在一种有利的实施方式中，如果在所述第一设备实现与所述通信伙伴之间的连接被终止，则所述权限证明被撤销或不被更新。
- [0023] 这允许通信伙伴的连接耦合到两个设备实现。因此仅只要当对第一设备实现的访

问也存在时,对第二设备实现的访问才是可能的。

[0024] 在一种有利的实施方式中,所述权限证明是数字证书或密码密钥或接入令牌。

[0025] 数字证书例如可以是具有根据公钥基础设施方法的公钥的证书或属性证书。这样的证书例如根据X.509标准被结构化,并且包含非对称密码方法的公钥。权限证明可以是密码密钥、尤其是对称密码方法的密钥。如果权限证明是接入令牌,例如根据OAuth(开放授权(Open Authorization))或JSON(JavaScript对象表示法(JavaScript Objekt Notation))网络或SAML(安全断言标记语言(Security Assertion Markup Language))标准的令牌,则从而提供关于例如对受保护的资源并且在这里尤其是对第二设备实现中的资源的访问的授权的信息。通过使用这些已知的数据结构,仅用于集成这些已知的结构的小的变化耗费是必要的。

[0026] 在一种有利的实施方式中,权限证明包括以下信息中的至少一个:通信伙伴的证书的标识符、通信伙伴的授权信息、针对所述通信伙伴的接入的时间限制和/或地理限制、可用通信媒介的限制、可用通信协议的限制、关于所述通信伙伴的安全状态的信息、权限证明的身份校验值。

[0027] 关于通信伙伴的安全状态的信息可以说明:所述通信伙伴的配置和/或所述通信伙伴的固件/软件状况是否是允许的。由此可以防止受操纵的设备可能被使用用于访问。

[0028] 因此,可以通过权限证明将大量的其他信息从第一设备实现传送给第二设备实现,并且由此可以将在第一设备实现中收集的信息和检验结果告知给第二设备实现。在第一和第二设备实现之间的通信此外是可能的,并且尤其是对于传送关于已经发生的鉴权的信息是有意义的。

[0029] 在一种有利的实施方式中,所述权限证明在建立安全的通信连接时从第一设备实现被传送给通信伙伴和/或从通信伙伴被传送给第二设备实现。

[0030] 例如,在根据传输层安全协议TLS建立通信连接时,权限证明可以从第一设备实现在TLS握手内被传送给通信伙伴。因此,权限证明在早的时间点对于通信伙伴准备好,并且已经在该时间点可以考虑访问权限等。

[0031] 在一种有利的实施方式中,所述权限证明经由经认证的现有通信连接从第一设备实现被传送给通信伙伴和/或从通信伙伴被传送给第二设备实现。

[0032] 这可以例如在根据超文本传递协议http连接的连接的头部部分中被传送。在此,权限证明的传输的类型的每个组合、即在连接建立时或在经认证的现有通信连接上对于两个通信连接、即一方面对于第一设备实现和通信伙伴之间的第一通信连接以及对于在通信伙伴和第二设备实现之间的第二通信连接是可能的。例如,权限证明可以在建立安全的通信连接时从第一设备实现被传送到通信伙伴,而权限证明在通信伙伴和第二设备实现之间经由经认证的现有通信连接被传送。

[0033] 在一种有利的实施方式中,所述第二设备实现的地址信息附加地从第一设备实现被提供给通信伙伴。

[0034] 这使得通信伙伴容易正确地寻址第二设备实现。

[0035] 在一种有利的实施方式中,在通过第一设备实现检验接入权限时,检验所述通信伙伴的当前配置的完整性和/或允许性。

[0036] 在此,例如可以检验安装在通信伙伴上的固件/软件是否是有效的并且准许的

(freigegeben), 所谓的补丁级别 (Patch Level)、即固件或软件的升级状况是否处于当前状况。此外, 可以检验病毒扫描程序是否是激活的和/或是否存在当前病毒模式 (Virusmuster)。通常, 这也被称为“零信任接入”或也为“零信任访问 (Zero Trust Access)”。因为这些检验通常是耗费的, 所以如果在与通信伙伴进行连接建立时由第一设备实现执行通信伙伴的完整性的这些检验, 则是有利的。于是可以对第二设备实现确认由第一设备实现签发的权限证明: 通信伙伴的完整性已经成功地被检验。第一设备实现可以对通信伙伴的所确定的和检验的配置以密码保护的方式进行编码, 使得第二设备实现可以在内容上对所述信息进行检验, 但是不必自身再次采集和评估所述信息。

[0037] 在一种有利的实施方式中, 第一设备实现将关于设备的配置的信息传送给通信伙伴。

[0038] 这能够实现针对通信伙伴的较少的检验耗费。如果通信伙伴已经通过第一设备实现检验了关于第一设备的配置的该信息并且将其归类为允许的, 则所述通信伙伴使用所提供的权限证明用于访问第二设备实现, 而不对关于设备配置的信息进行重新检验。由于物理设备及其数字孪生是两个以一致的方式配置的设备实现, 因此可以避免重新检验。

[0039] 本发明的第二方面涉及一种设备, 所述设备包括物理设备实现和所分配的虚拟设备实现, 所述物理设备实现和所分配的虚拟设备实现被构造用于

[0040] - 在所述两个设备实现中的第一设备实现中接收通信伙伴的访问权限,

[0041] - 通过第一设备实现检验访问权限, 以及

[0042] - 如果所述访问权限被认为是允许的, 则从第一设备实现向通信伙伴提供用于通过所述通信伙伴访问第二设备实现的权限证明, 以及

[0043] - 允许通过所述通信伙伴借助于所述权限证明访问所述两个设备实现中的第二设备实现。

[0044] 对于不仅具有物理设备实现而且具有虚拟设备实现、例如数字孪生的这样的设备, 尤其是在零信任认证的范围中进行的复杂检验不能由真实设备、也就是说物理设备实现执行, 而是被转移到其数字孪生、也即虚拟设备实现上。设备的物理设备实现可以例如是数字孪生现在分配给的旧设备。通过数字孪生可以灵活地配置和升级 (aktualisiert): 对于零信任接入需要哪些信息以及可以如何传送所述信息。

[0045] 在一种有利的实施方式中, 所述虚拟设备实现被构造为根据开放平台通信统一架构标准的 OPC UA 服务器。

[0046] 如果 OPC UA 服务器例如被实施为物理设备实现上的集成虚拟设备实现, 则可能的是, 在访问设备时, 例如在控制数据通信或访问集成设备网络服务器时, 设备提供用于访问设备内部虚拟设备实现的权限证明。特别地, 在建立安全的通信连接时, 可以设立对物理设备实现的 OPC UA 服务器的临时接入, 并且可以将权限证明传送给通信伙伴。从而通信伙伴可以访问作为物理设备实现上的虚拟设备实现的 OPC UA 服务器。

[0047] 在一种有利的实施方式中, 所述虚拟设备实现被构造在中央服务器、边缘服务器上或被构造在所述设备的物理设备实现上。

[0048] 中央服务器或者定位在自动化网络的边缘处的边缘服务器提供与设备本身相比更大的计算能力并且通常包括其他数据库, 诸如配置或调试数据库, 可以通过所述其他数据库以低的传输带宽快速地访问关于设备以及关于通信伙伴的大数量的数据, 并且从而可

以查询针对设备的访问权限以及通信伙伴的非常高效的检验。

[0049] 本发明的第三方面涉及一种计算机程序产品,所述计算机程序产品包括能够直接被加载到数字计算机的存储器中的非易失性计算机可读介质,包括适用于执行该方法的步骤的程序代码部分。

[0050] 只要在以下描述中未另外说明,术语“接收”、“检验”、“提供”、“允许”等就优选地涉及改变和/或产生数据和/或将数据转化成其他数据的动作和/或过程和/或处理步骤,其中数据尤其是可以被表示为物理参量或者可以作为物理参量存在,例如作为电脉冲。设备并且其中尤其是物理设备实现以及虚拟设备实现可以包括一个或多个处理器。结合本发明,处理器可以例如被理解为主处理器、微处理器或微控制器。例如,它也可以是虚拟处理器或是软CPU。

[0051] 计算机程序产品、诸如计算机程序构件例如可以作为存储介质、诸如存储卡、USB棒、CD-ROM、DVD或也以从网络中的服务器可下载的文件的形式被提供或供应。这可以例如在无线通信网络中通过将对应的文件传输到计算机程序产品或计算机程序构件上进行。

附图说明

[0052] 根据本发明的方法和根据本发明的设备的实施例在附图中示例性示出并且根据以下描述更详细地被阐述。其中:

[0053] 图1以示意图示出并入到设施网络中的根据本发明的设备的实施例;

[0054] 图2以消息流程图的形式示出根据本发明的方法的第一实施例;和

[0055] 图3以消息流程图的形式示出根据本发明的方法的第二实施例,其中分别具有物理设备实现和虚拟设备实现的两个设备执行认证。

具体实施方式

[0056] 彼此对应的部分在所有图中配备有相同的附图标记。

[0057] 图1示出具有多个设备的通信网络。所述设备例如是现场设备,所述现场设备与工业设施的通信网络连接。每个设备均包括物理设备实现FD1、FD2、FD3、FD4、FD5和至少一个所分配的虚拟设备实现DT-FD1、DT-FD2、DT-FD3、DT-FD4、DT-FD5。物理设备实现FD1、FD2、FD3与子网络10、例如自动化网络连接。子网络10经由边缘服务器12与开放网络11连接。边缘服务器12提供用于与设施网络的布置在子网络10之外的组件协作的传递函数。物理设备实现FD4、FD5直接与开放网络11、例如办公网络或公共互联网连接。经由开放网络11连上中央服务器、例如云服务器,所述中央服务器集中地为设施网络提供计算能力和存储容量。

[0058] 给物理设备实现FD1、FD2分别分配两个虚拟设备实现DT-FD1、DT-FD2。虚拟设备实现DT-FD1、DT-FD2分别布置在边缘服务器12和云服务器13中。针对物理设备实现FD3的虚拟设备实现DT-FD3布置在物理设备实现FD3内并且附加地布置在中央服务器13中。分配给物理设备实现FD4和FD5的虚拟设备实现DT-FD4和DT-FD5仅仅布置在中央服务器13中。虚拟设备实现通常也被称为数字孪生,并且例如可以被构造为应用程序。虚拟设备实现尤其是也可以被构造为OPC UA服务器。

[0059] 可以通过访问OPC UA服务器来查询关于物理设备实现的信息。OPC UA服务器可以被构造在物理设备实现之外,例如被构造在边缘服务器12中或中央服务器14中。但是,虚拟

设备实现的OPC UA服务器也可以以在设备本身上的OPC UA应用服务的形式来实施,诸如对于物理和虚拟设备实现FD3、DT-FD3。在这种情况下,物理设备实现FD3本身可以向通信伙伴提供用于访问集成到物理设备实现中的OPC UA服务器的权限证明。如果通信伙伴可以访问两个设备实现中的第一设备实现、例如物理设备实现FD3,则所述通信伙伴也自动地获得对第二设备实现、在这里虚拟设备实现DT-FD3、在这种情况下设备的OPC UA服务器的访问。如果服务的多个实例在物理设备实现FD3上分开地运行,则这尤其是有意义的。例如经由经认证的HTTPS通信连接,通信伙伴尤其是可以访问物理设备实现的网络服务器。

[0060] 图2现在示出具体的实施例,其中通信伙伴ST、例如服务技术人员与设备的虚拟设备实现DT-FD1连接并且查询权限证明。该设备在图2中首先以虚拟设备实现DT-FD1及其物理设备实现FD1示出。

[0061] 首先,通信伙伴ST在两个设备实现中的第一设备实现、在这里虚拟设备实现DT-FD1处进行认证。在此,在第一方法步骤S1中,虚拟设备实现DT-FD1接收通信伙伴ST的访问权限。第一设备实现现在检验访问权限,参见方法步骤S2,并且在方法步骤S3中向通信伙伴ST提供权限证明AC,在图2中对于用于通过通信伙伴ST访问物理设备实现FD1的权限证明称为AC-FD1-ST。权限证明AC在这里例如通过确认消息ACC-Cred从虚拟设备实现DT-FD1被传送给通信伙伴ST。

[0062] 通信伙伴ST随后将包含权限证明AC的认证请求AuthConReq发送给第二设备实现、在这里物理设备实现FD1。在第二设备实现中检验权限证明AC,并且随后向通信伙伴ST授予对第二设备实现FD1的访问。这利用从第二设备实现向通信伙伴ST的确认消息AuthConRsp被确认。如在所示的示例中那样,权限证明AC可以是用于通信伙伴ST在第二设备实现处进行接入认证的接入权限证明。但是,权限证明AC也可以作为用于通信伙伴对第二设备实现的经授予的访问权的访问权限证明。因此,可以访问第一设备实现的通信伙伴ST也可以访问第二设备实现。

[0063] 不需要在两个设备实现上管理关于接入鉴权(Zugangsauthentifizierung)的信息和关于访问权限的信息。从而减少管理耗费,并且避免两个设备实现之间的原则上不一致的接入数据配置。尤其是,这也能够实现:物理设备实现FD1不仅直接获得和检验通信伙伴ST的访问权限,而且附加地获得用于准许(Freigabe)所分配的虚拟设备实现DT-FD1的访问的权限证明AC。此外可能的是,不仅从物理设备实现FD1而且从虚拟设备实现DT-FD1关于关键行动获得日志消息,所述关键行动例如在审核时被需要。

[0064] 所签发的权限证明AC的有效性可能是在时间上有限的。该使用限制可以在权限证明AC之内、但是也可以在权限证明AC之外被传送。为此,权限证明可以例如包含时间戳。在此,有效期限可以说明其中向第二设备实现的接入认证或访问请求是允许的时间间隔或者所建立的通信连接可以最大保持存在多长时间。也可能的是,通过权限证明AC对第二设备实现的访问的次数是有限的。例如,权限证明AC可以是仅可使用一次的,也就是说仅有利用于建立一次与第二设备实现的连接。

[0065] 如果在通信伙伴ST和第一设备实现、在这里虚拟设备实现DT-FD1之间的通信连接被终止,则所签发的权限证明AC例如被撤销或不再被更新。因此,仅只要当对第一设备实现的访问也存在时,对第二设备实现的访问才是可能的。如果与第一设备实现的连接、例如通信会话被终止,则由此对第二设备实现的访问也不再是可能的。这例如可以通过所谓的心

跳机制被实现,所述心跳机制与相应的权限证明AC关联。为此,在第一和第二设备实现、在这里DT-FD1和FD1之间建立网络连接,其中两个设备实现相互被通知:所述设备实现准备运行并且仍然可以履行其任务,即仍然活着(am Leben)。这样的“心跳”或“Heartbeat”连接(参见SesHB)在方法步骤S41中在第一和第二设备实现之间以及在方法步骤S42中在通信伙伴和第一设备实现之间被建立。

[0066] 在所阐明的示例中,虚拟设备实现DT-FD1可以签发权限证明AC,所述权限证明能够实现通信伙伴ST对虚拟设备实现DT-FD1、即数字孪生的访问。所传送的并且因此签发的权限证明AC可以例如是数字证书、密码密钥或接入令牌(Zugangstoken),其能够实现对设备的特定服务或资源的访问权限或者对此有权利。

[0067] 权限证明AC可以例如包含证书的指纹作为通信伙伴ST的证书的标识符。说明证书的序列号和签发者同样是可能的。可替代地,权限证明AC也可以包含或引用通信伙伴ST以及两个设备实现DT-FD1、FD1必须知道和使用的机密。在此,证书的该标识符或者甚至整个权限证明AC以密码方式被加密。权限证明AC此外可以包含授权信息、诸如通信伙伴ST的角色或针对特定行动的属性。权限证明AC此外可以包含时间限制,诸如访问的时间点或持续时间和/或在访问时通信伙伴ST的地理位置。此外,权限证明AC可以包含可使用的通信媒介的限制,例如仅通过有线连接或通过无绳通信连接借助于W-LAN或移动无线电接入。

[0068] 权限证明AC此外可以包含关于通信伙伴ST的安全状态的信息。这样的安全状态例如可以通过通信伙伴ST中的本地代理被确定,所述本地代理定期地检验通信伙伴ST的系统状态。此外,权限证明AC可以包含权限证明AC的完整性校验值。这例如是签名或密码校验和,所述签名或密码校验和使得能够在相应的接收方、即通信伙伴ST或第二设备实现、在这里FD1处检验权限证明AC的完整性。

[0069] 在建立安全的通信连接时,权限证明AC可以从第一设备实现、在这里DT-FD1被传送给通信伙伴ST和/或从通信伙伴ST被传送给第二设备实现、在这里FD1。尤其是,在根据电信层协议TLS建立连接时,例如在TLS扩展字段中可以在认证和密钥协定期间传送权限证明AC。因此在与第一设备实现TD-FD1进行TLS连接建立时,自动地给通信伙伴ST提供权限证明,然后使用所述权限证明用于与第二设备实现FD1建立连接。

[0070] 除了权限证明AC之外,第二设备实现(在这里FD1)的地址信息可以从第一设备实现(在这里DT-FD1)被提供给通信伙伴ST。这样的地址信息例如是第二设备实现FD1的IP地址或者域名服务器的名称或第二设备实现的URL地址。

[0071] 同样可能的是,经由开放平台通信统一架构协议(Open Plattform Communication Unified Architecture Protokoll)OPC UA提供权限证明AC。权限证明AC作为有效数据经由已经建立和经认证的通信连接、例如超文本传送协议http连接被传送。可替代地,已经可以在建立安全的通信连接时例如在TLS协议中的握手内传输权限证明AC。因此,不必管理用于访问第一或第二设备实现的分开的权限证明AC。此外,因为所提供的权限证明AC比例如在完全认证时所使用的数字证书更紧凑,所以与第二设备实现的连接建立可以更高效地、尤其是更快速地或借助于更小的数据量进行。

[0072] 第一设备实现、在这里虚拟设备实现DT-FD1因此被签发给用于访问物理设备实现FD1的权限证明AC的提供者。相反的情况同样是可能的,其中首先建立与物理设备实现FD1的连接并且经由所述连接设立用于与虚拟设备实现DT-FD1进行连接建立的权限证明AC。根

据X.509标准结构化的数字证书形式的权限证明AC尤其是可以具有以下扩展,用于传送所提到的信息中的一个或多个信息。以下扩展是示例,并且以抽象语法表示法ASN.1来写:

```
AccessControlToken EXTENSION ::= {
    peerAuthentication ::= CHOICE {
        PCertificate          [0] Certificate OPTIONAL,
        FPcertificate         [1] BIT STRING  OPTIONAL -- Fingerprint
    }
    peerAuthorization ::= CHOICE {
        roleInformation       [0] RoleID,
        operations            [1] Operations OPTIONAL,
    }

    deviceState              DevState,
    Validity                  Time
}
```

```
[0073] RoleId ::= INTEGER (-32768..32767) -- predefined role identifications
                                         (e.g. IEC 62351-8)

Operation ::= ENUMERATED { Add (1), Delete (2), Change (3) }

DevState ::= ENUMERATED {
    OsPassed          (1),    -- Operation system has passed security
check
    OsFailed          (2),    -- Operation system has failed security
check
    OsAppPassed       (3),    -- Operation system and installed applica-
tions
                                         have passed security check
    OsAppFailed       (4) }   -- Either operation system or installed
                             applications have failed security check
```

[0074] 这意味着,例如虚拟设备实现DT-FD1可以签发数字证书,所述数字证书能够实现对所分配的物理设备实现FD1的受保护的访问。在此,物理设备实现是实际的物理设备,在图1的示例中是现场设备FD1。作为权限证明的数字证书是自签名证书,所述自签名证书由设备的第一设备实现创立并且由同一设备的第二设备实现检验和接受。为此不必建立和运行通常公认的私钥基础设施(PKI),因为这些特殊证书或权限证明仅由单独的设备本身签发和检验。

[0075] 图3示出用于现场设备FD1访问第二现场设备FD2的实施例,其中设备FD1与设备FD2建立以密码方式受保护的、相互认证的连接。然而,在物理设备实现FD1和FD2之间的实际的、复杂的认证分别通过其数字孪生、即其虚拟设备实现DT-FD1、DT-FD2进行。

[0076] 在此,物理设备实现FD1向其自身的虚拟设备实现DT-FD1提请求。在所示的示例

中,该虚拟设备实现首先将认证请求AuthCon发送给物理设备实现FD2。从那里,请求在内部被移交给其所分配的虚拟设备实现DT-FD2。虚拟设备实现DT-FD2随后利用认证请求发起虚拟设备实现DT-FD1的认证。在此,从虚拟设备实现DT-FD2请求虚拟设备实现DT-FD1的认证。其中虚拟设备实现DT-FD1作为通信伙伴在虚拟设备实现DT-FD2处进行请求的认证的方法步骤用附图标记S1、S2、S3、S4表示。第二设备实现DT-FD2作为通信伙伴在虚拟设备实现DT-FD1处认证的方法步骤是具有所示的附图标记S1'、S2'、S3'和S4'的方法步骤。

[0077] 相应的第一设备实现利用认证请求消息AuthConReq接收通信伙伴的访问权限,参见S1、S1',检验该访问权限,参见S2、S2',并且将权限证明AC-FD1FD2、AC-FD2FD1提供给通信伙伴、在这里即虚拟设备实现DT-FD1或者虚拟设备实现DT-FD2。相应的权限证明AC-FD1FD2、AC-FD2FD1利用消息ACC-Cred从第一设备实现、在这里DT-FD1或DT-FD2被传送给相应的所分配的第二设备实现、在这里FD1或者FD2。物理设备实现FD1随后将具有权限证明AC-FD1FD2的认证请求AuthConReq发送给物理设备实现FD2并且从该物理设备实现获得访问许可,这利用确认消息AuthConRsp被确认,对此也参见绘入的方法步骤S4。相应地,在方法步骤S4'中,在通过第二设备实现FD2的认证请求和其中包含的权限证明AC-FD2FD1之后,第二设备实现FD1允许对物理设备实现FD1的接入。

[0078] 因此,两个虚拟设备实现分别检验通信伙伴、即物理设备实现FD2和FD1。物理设备实现可以例如是已经存在于网络中的设备,所述设备不支持零信任接入检验。

[0079] 可以通过适用于实施相应的方法步骤的对应的设备来实施所有方法步骤。可以由具体特征实施的所有功能都可以是该方法的方法步骤。在本发明的范围内,所有描述和/或绘制的特征可以有利地被相互组合。本发明不限于所描述的实施例。

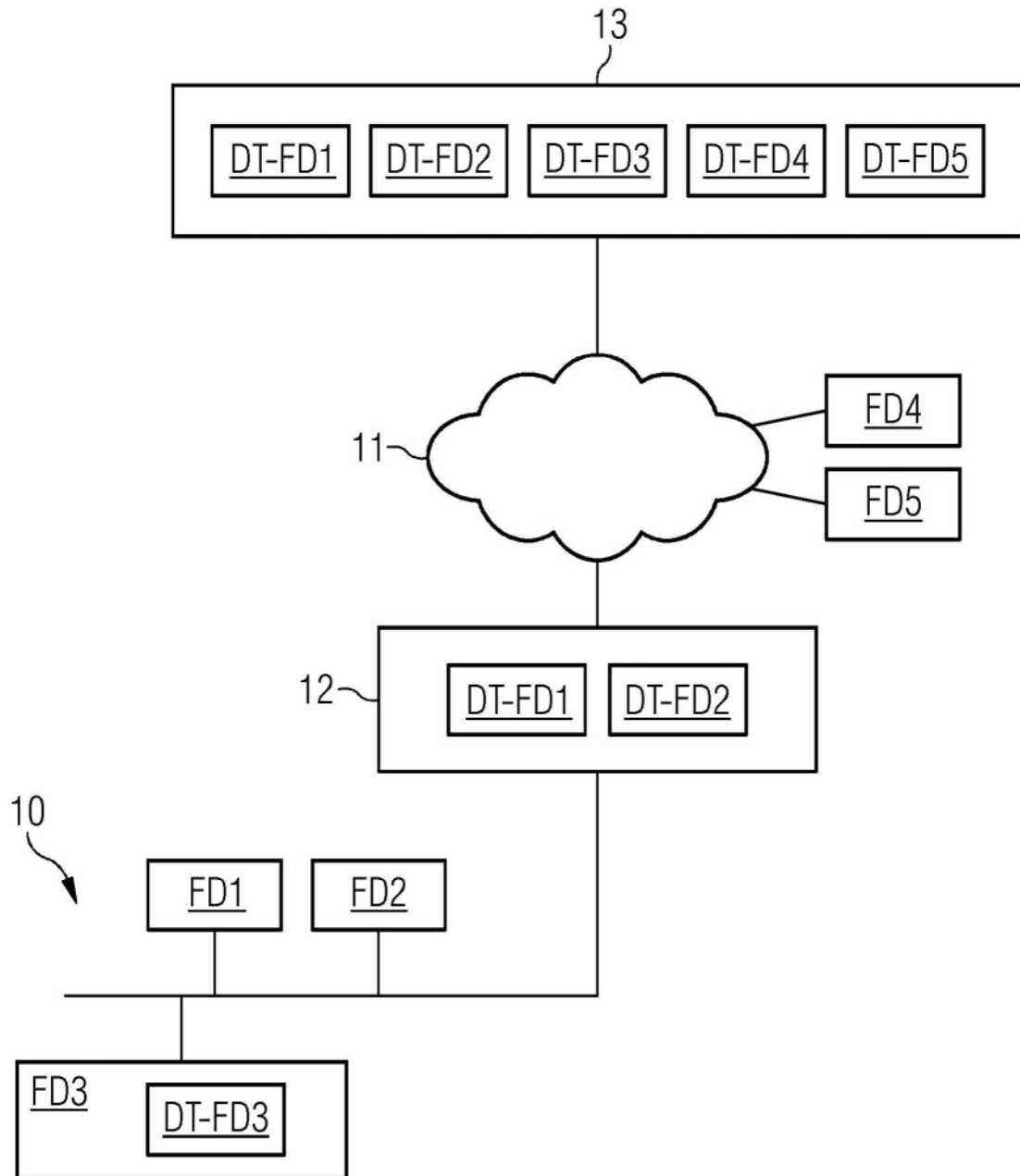


图1

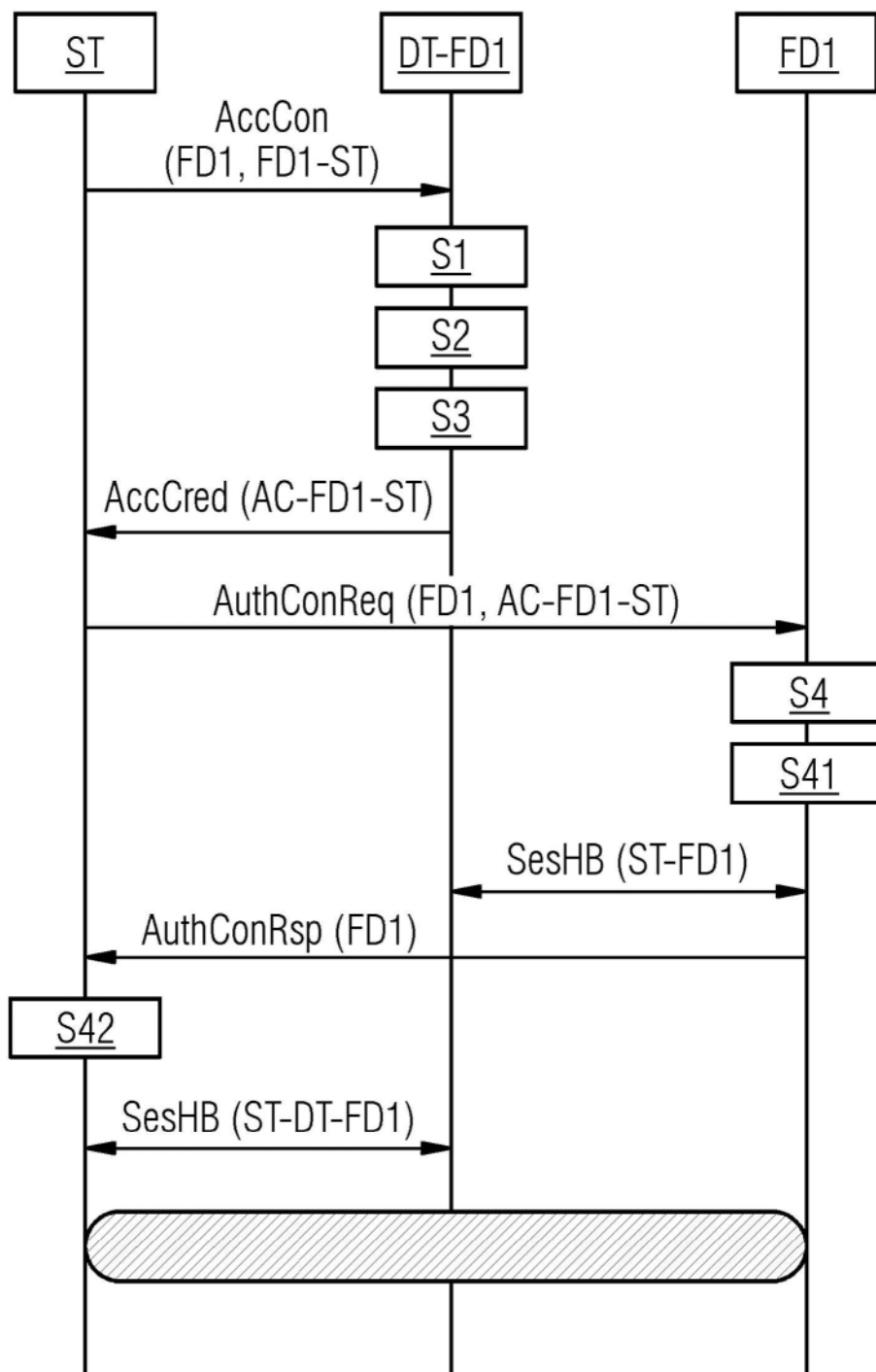


图2

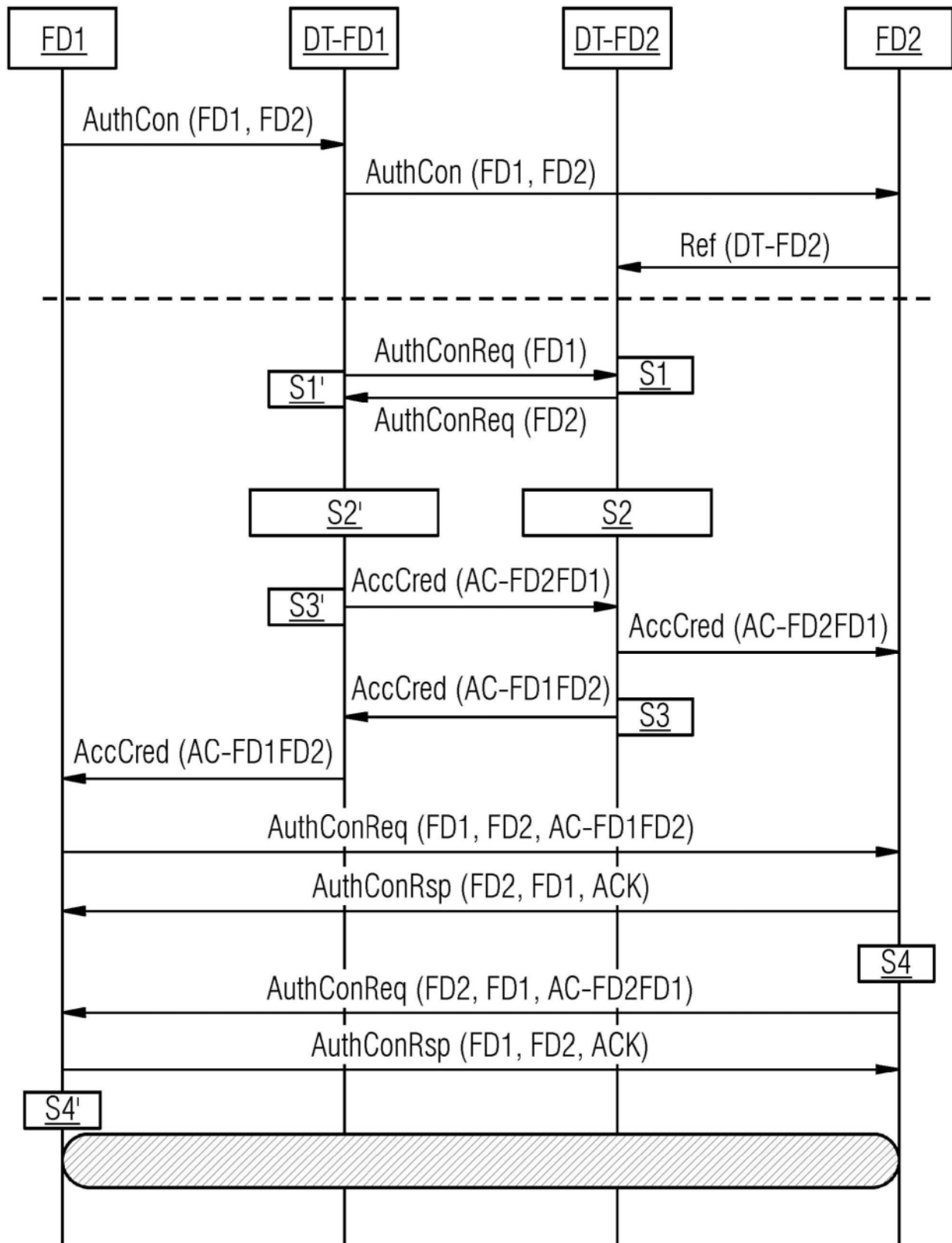


图3