



(12) 发明专利申请

(10) 申请公布号 CN 114093060 A

(43) 申请公布日 2022. 02. 25

(21) 申请号 202111338360.9

(22) 申请日 2015.06.18

(30) 优先权数据

951/14 2014.06.23 CH

(62) 分案原申请数据

201580029795.1 2015.06.18

(71) 申请人 励智识别技术有限公司

地址 瑞士维茨康市

(72) 发明人 马塞·普拉斯 保罗·施图德斯

(74) 专利代理机构 北京中安信知识产权代理事务
所(普通合伙) 11248

代理人 张小娟

(51) Int. Cl.

G07C 9/00 (2020.01)

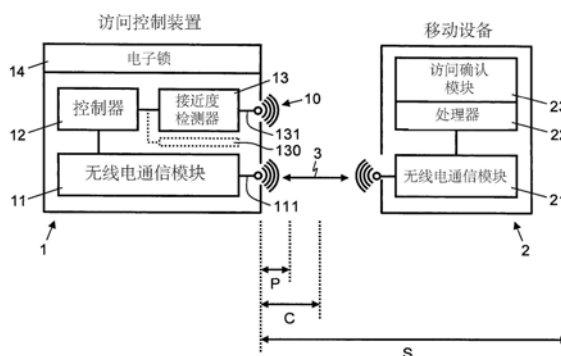
权利要求书3页 说明书10页 附图4页

(54) 发明名称

电子访问控制装置及访问控制方法

(57) 摘要

电子访问控制装置(1)包括无线电通信模块(11),所述无线电通信模块用于通过直接无线通信链路(3)与移动设备(2)在第一射频频带内进行无线数据交换。所述访问控制装置具有控制器(12),所述控制器连接到所述无线电通信模块用于使用从所述移动设备接收的访问密钥生成访问控制信号。所述电子访问控制装置进一步包括接近度检测器(13),所述接近度检测器用于使用与所述第一射频频带不同的第二射频频带内的射频在确定的接近度(P)检测移动设备。所述控制器连接到所述接近度检测器并且仅当在所述电子访问控制装置确定接近度检测到所述移动设备时才控制所述无线电通信模块与所述移动设备建立所述直接无线通信链路。



1. 一种电子访问控制装置(1), 包括:

无线电通信模块(11), 所述无线电通信模块被配置成用于通过在所述无线电通信模块(11)与移动设备(2)之间的直接无线通信链路(3)与移动设备(2)进行无线数据交换;

访问确认模块(23), 可在移动设备(2)的处理器(22)上执行, 并被配置成用于控制所述移动设备(2)的处理器(22)从所述移动设备(2)的用户接收确认指令, 以及用于响应于所述确认指令向所述访问控制装置(1)的所述无线电通信模块(11)传输确认消息; 和

控制器(12), 所述控制器连接到所述无线电通信模块(11)并且被配置成控制所述无线电通信模块(11)经由直接无线通信链路(3)将访问确认模块(23)传输至移动设备(2), 和, 在经由所述直接无线通信链路(3)接收来自移动设备(2)的确认消息后, 使用经由直接无线通信链路(3)从移动设备(2)接收的访问密钥, 生成访问控制信号。

2. 如权利要求1所述的访问控制装置(1), 其中, 所述访问确认模块(23)被进一步配置成用于控制所述移动设备(2)的所述处理器(22)将访问密钥包括在所述确认消息中, 并且所述控制器(12)被进一步配置成用于使用所述包括在确认信息中的访问密钥生成访问控制信号。

3. 如权利要求1或2所述的访问控制装置(1), 其中, 所述控制器(12)被进一步配置成用于检查移动设备(2)的信号强度是否高于位于距访问控制装置(1)的确定近距离(C)内的移动设备(2)的信号强度阈值, 如果移动设备(2)的信号强度大于信号强度阈值, 则经由直接无线通信链路(3)将访问确认模块(23)传输至移动设备(2)。

4. 如权利要求1至3之一所述的访问控制装置(1), 其中, 所述控制器(12)被进一步配置成用于控制所述无线电通信模块(11)向所述移动设备(2)传输所述可执行的访问确认模块(23), 所述访问确认模块(23)被配置成用于控制所述移动设备(2)的处理器(22)通过移动设备(2)的指纹传感器和移动设备(2)的图形用户界面中的至少一个, 从所述移动设备(2)的用户接收确认指令。

5. 如权利要求1至3之一所述的访问控制装置(1), 其中, 所述控制器(12)被进一步配置成用于控制所述无线电通信模块(11)向所述移动设备(2)传输可执行的访问确认模块(23), 所述可执行的访问确认模块(23)被配置成用于控制所述移动设备(2)的处理器(22)运行如下至少一个: 通过用户输入的授权信息进行验证, 和通过移动设备(2)的指纹传感器输入用户的指纹进行验证; 和, 在肯定的验证时, 生成包括在访问密钥中的肯定性确认消息。

6. 如权利要求1至5之一所述的访问控制装置(1), 其中, 无线电通信模块(11)被配置成用于在第一射频频带内与移动设备(2)进行无线数据交换; 和电子访问控制装置(1)进一步包括接近度检测器(13), 所述接近度检测器(13)被配置成使用区别于第一射频频带的第二射频频带中的射频来检测所述电子访问控制装置(1)的确定接近度(P)内的所述移动设备(2)的存在; 所述控制器(12)连接到所述接近度检测器(13)并且被进一步配置成用于当所述接近度检测器(13)在距电子访问控制装置(1)的确定接近度(P)内检测到移动设备(2)时, 控制所述无线电通信模块(11)与所述移动设备(2)建立所述直接无线通信链路(3)。

7. 如权利要求6所述的访问控制装置(1), 其中, 无线电通信模块(11)被配置成在几米、特别是距离可达十米的短距离(S)的通信链路(3)与移动设备(2)进行无线数据交换; 和接近度检测器(13)被配置为用于在距电子访问控制装置(1)几厘米、特别是在距离可达十厘

米的近接近度(P)内检测移动设备(2)的存在。

8.如权利要求6或7所述的访问控制装置(1),其中,接近度检测器(13)包括RFID读取器,并被配置成用于通过发射电磁场脉冲(10)来检测移动设备(2)的存在,检测在电磁场脉冲(10)发射过程中的返回信号,并使用该返回信号检测移动设备(2)的存在。

9.如权利要求1至8之一所述的访问控制装置(1),其中,所述无线电通信模块(11)包括蓝牙收发器,并且所述控制器(12)被进一步配置成用于控制所述蓝牙收发器通过执行蓝牙连接过程与所述移动设备(2)建立所述直接无线通信链路(3)。

10.如权利要求1至9之一所述的访问控制装置(1),其中,所述访问控制装置(1)进一步包括电子锁(14),并且所述控制器(12)连接到所述电子锁(14)并且被进一步配置成用于向所述电子锁(14)提供所述访问控制信号从而控制所述电子锁(14)执行解锁功能。

11.如权利要求1至10之一所述的访问控制装置(1),其中,所述控制器(12)进一步被配置成定义反映所述访问控制信号的访问状态,和用于控制所述无线电通信模块(11)向所述移动设备(2)传输所述访问状态。

12.一种移动设备(2),其包括:

无线电通信模块(21),其被配置成用于通过在所述无线电通信模块(21)与访问控制装置(1)之间的直接无线通信链路(3)与所述访问控制装置(1)进行无线数据交换;和

处理器(22),其连接到无线电通信模块(21),并被配置为用于控制无线电通信模块(21)经由直接无线通信链路(3)接收来自访问控制装置(1)的可执行的访问确认模块(23),和用于执行访问确认模块(23),并且通过执行访问确认模块(23)来接收来自移动设备(2)的用户的确认指令,响应于该确认指令,通过直接无线通信链路(3)向访问控制装置(1)传输一个确认消息,使用经由直接无线通信链路(3)从移动设备(2)接收的访问密钥,使访问控制装置(1)能够生成访问控制信号。

13.一种访问控制方法,所述方法包括:

通过电子访问控制装置(1)的控制器(12)控制电子访问控制装置(1)的无线电通信模块(11),以建立(S2)与移动设备(2)的用于无线数据交换的直接无线通信链路(3);

通过直接无线通信链路(3)向移动设备(2)传输来自访问控制装置的可执行的访问确认模块(23);

通过移动设备(2)的处理器(22)执行可执行的访问确认模块(23);和

可执行的访问确认模块(23)控制移动设备(2)的处理器(22),使处理器(22)接收来自移动设备(2)的用户的确认指令,响应于所述确认指令,生成确认信息,和通过直接无线通信链路(3)向访问控制装置(1)的无线电通信模块(11)传输所述确认信息,使用经由直接无线通信链路(3)从移动设备(2)接收的访问密钥,使访问控制装置(1)能够生成访问控制信号。

14.如权利要求13所述的方法,其中,该方法进一步包括:可执行的访问确认模块(23)控制移动设备(2)的处理器(22),从而处理器(22)将储存在移动设备(2)中的访问密钥包括入确认消息中,使得访问控制装置(1)使用所述访问密钥能够生成访问控制信号。

15.如权利要求14所述的方法,其中,该方法进一步包括:电子访问控制装置(1)的控制器(12)检查移动设备(2)的信号强度是否高于位于距访问控制装置(1)的确定近距离(C)内的移动设备(2)的信号强度阈值,如果移动设备(2)的信号强度大于所述信号强度阈值,则

经由直线无线通信链路 (3) 将访问确认模块 (23) 传输至移动设备 (2)。

16. 如权利要求14或15所述的方法,其中,该方法进一步包括:通过所述电子访问控制装置 (1) 的接近度检测器 (13) 使用第二射频频带内的射频,检测 (S1) 在所述电子访问控制装置 (1) 的确定接近度 (P) 内的所述移动设备 (2) 的存在;和当接近度检测器 (13) 在电子访问控制装置 (1) 的确定接近度 (P) 内检测到移动设备 (2) 时,所述电子访问控制装置 (1) 的控制器 (12) 控制所述电子访问控制装置 (1) 的所述无线电通信模块 (11),用于在区别于第二射频频带的第一射频频带内与所述移动设备 (2) 建立 (S2) 直接无线通信链路 (3)。

电子访问控制装置及访问控制方法

[0001] 本申请是申请号为201580029795.1的发明专利申请的分案申请。

[0002] 原案申请日:2015年6月18日。

[0003] 原案发明名称:电子访问控制装置及访问控制方法。

[0004] 原案申请号:201580029795.1,国际申请号:PCT/EP2015/001232。

技术领域

[0005] 本发明涉及一种电子访问控制装置和一种访问控制方法。具体地,本发明涉及一种包括无线电通信模块和控制器的电子访问控制装置,所述无线电通信模块用于与移动设备进行直接无线数据交换,所述控制器连接到所述无线电通信模块用于使用从所述移动设备接收的访问密钥生成访问控制信号。

背景技术

[0006] 许多年来,访问控制系统已经结合无源RFID(射频标识符)应答器使用。这些访问控制系统包括RFID读取器,这些读取器用于以无线方式从RFID应答器读取访问权限或者至少用户标识符以便控制对访问受控区域(诸如建筑物或房间)或访问受控物体(诸如售货机中的商品等等)的访问。当包括有源的基于RFID的通信接口,所谓的NFC接口(近场通信)的移动无线电话(蜂窝电话)出现时,可以将这种移动电话用作访问权限的载体而不是处于RFID卡、加密狗等等形式的无源RFID应答器。通过NFC接口,可以将访问控制与访问控制装置的相应的NFC接口附近的区域内的移动电话的物理存在(例如,附接到或靠近门或闸门)相联系。换言之,NFC接口的短通信范围要求用户的移动电话不要距离有待访问的门或闸门太远,使得未授权人员无法基于存储在有权用户的移动电话上的访问权限错误地得到给定的访问,只要移动电话由有权用户拥有。然而,不是所有类型和品牌的移动电话都配备有NFC接口或其他基于RFID的通信能力。尽管如此,除了用于访问蜂窝电话网络,诸如GSM(全球移动通信系统)或UMTS(通用移动电话系统)的移动无线电通信模块之外,某些类型和品牌的移动电话包括用于建立本地或直接无线通信链路的其他基于无线电的通信模块。例如,这种基于无线电的通信模块包括具有比NFC接口大得多的通信范围(例如,十米到百米)的WLAN(无线局域网)和蓝牙通信接口。尽管这种其他基于无线电的通信模块可以用于与访问控制装置交换访问权限,存在未授权用户可能得到错误访问的风险,仅仅因为有权用户或至少其移动电话位于该访问控制装置的这个延伸通信范围内。

[0007] FR2981823描述了一种相对于集成在汽车中的致动器设备认证标识设备从而执行汽车启动操作的方法。在认证会话中,通过在该标识设备与该致动器设备之间交换认证数据来认证该标识设备。在认证会话期间,使用蓝牙通信该交换认证数据的第一部分,而通过磁感应交换该认证数据的第二部分。在该致动器中,这两部分认证数据汇总。

[0008] US2012/154115描述了一种控制位置跟踪系统中的访问的方法。当移动标签进入房间时,其执行位置更新过程并且链接到该位置跟踪系统的节点并且更新其在该房间中的位置。响应于该位置更新,该位置跟踪系统的位置跟踪装置向该房间中的访问控制装置传

输激活信号从而发起与该移动标签建立通信连接以便协商该移动标签的访问权限。在一个实施例中,该访问控制装置可以设置有接近度传感器,在协商访问权限之后,在该访问控制装置实际上授权或拒绝访问之前,该接近度传感器检测该移动标签的近接近度。

[0009] US2014/049361描述了一种包括与同电子锁相关联的读取器设备通信的移动设备的电子系统。该移动设备和该读取器设备彼此例如经由蓝牙通信并且交换证书、安全数据和位置信息。在一个实施例中,该电子锁还可以包括近接近度范围能力,该能力在具有适当证书的移动设备位于该近接近度范围内时自动地解锁该电子锁。

发明内容

[0010] 本发明的目的是提供不具有现有技术的至少一些缺点的电子访问控制装置和访问控制方法。特别是,本发明的目的是提供一种不局限于具有NFC接口的移动设备,但至少有一些基于NFC的访问控制的优点的电子访问控制装置和访问控制方法。

[0011] 根据本发明,这些目的是通过独立权利要求的特征实现的。另外,从属权利要求和说明书中存在另外的有利实施例。

[0012] 电子访问控制装置包括无线电通信模块,所述无线电通信模块被配置成用于通过在所述无线电通信模块与移动设备之间的直接无线通信链路与所述移动设备进行无线数据交换。

[0013] 根据本发明,上述目的特别实现为,所述电子访问控制装置进一步包括存储在电子访问控制装置中的访问确认模块。访问确认模块在移动设备的处理器上可执行,并被配置为用于控制移动设备的处理器接收来自移动设备的用户确认指令,和,响应于确认指令,向访问控制装置的无线电通信模块传输确认消息。电子访问控制装置进一步包括控制器,所述控制器连接到无线电通信模块,并且被配置成控制无线电通信模块经由直接无线通信链路将访问确认模块传输至移动设备。控制器进一步被配置为,在经由直接无线通信链路接收来自移动设备的确认消息后,生成访问控制信号。

[0014] 在一个实施例中,访问确认模块被进一步配置成用于控制移动设备的处理器将访问密钥包括在确认消息中,并且控制器被进一步配置成用于使用所述包括在确认消息中的访问密钥生成访问控制信号。

[0015] 在一个实施例中,控制器被进一步配置成用于检查移动设备的信号强度是否高于位于距访问控制装置的确定近距离内的移动设备的信号强度阈值,如果移动设备的信号强度大于信号强度阈值,则经由直接无线通信链路将访问确认模块传输至移动设备。

[0016] 在一个实施例中,控制器被进一步配置成用于控制无线电通信模块向所述移动设备传输可执行的访问确认模块,所述访问确认模块被配置成用于控制移动设备的处理器通过移动设备的指纹传感器和/或移动设备的图形用户界面,从移动设备的用户接收确认指令。

[0017] 在一个实施例中,控制器被进一步配置成用于控制无线电通信模块向移动设备传输可执行的访问确认模块,所述可执行的访问确认模块被配置成用于控制移动设备的处理器验证通过用户输入的授权信息,和/或验证通过移动设备的指纹传感器输入用户的指纹,和,在肯定的验证时,生成包括访问密钥的肯定性确认消息。

[0018] 在另一个实施例中,无线通信模块被配置成用于在第一射频频带内与移动设备进

行无线数据交换,和电子访问控制装置进一步包括接近度检测器,所述接近度检测器被配置成使用区别于第一射频频带的第二射频频带中的射频来检测在电子访问控制装置的确定接近度内的移动设备是否存在。控制器连接到接近度检测器并且被进一步配置成用于当接近度检测器在距电子访问控制装置的确定接近度内检测到移动设备时,控制无线电通信模块与移动设备建立直接无线通信链路。

[0019] 在进一步的实施例中,无线通信模块被配置成在几米、特别是距离可达十米的短距离通信链路、与移动设备进行无线数据交换,和接近度检测器被配置成用于在距电子访问控制装置几厘米、特别是在距离可达十厘米的近接近度内检测移动设备是否存在。

[0020] 在一个实施例中,接近度检测器包括RFID读取器,并被配置成用于通过发射电磁场脉冲检测移动设备是否存在,检测在电磁场脉冲发射过程中的返回信号,并使用该返回信号检测移动设备是否存在。

[0021] 在一个实施例中,无线电通信模块包括蓝牙收发器,并且控制器被进一步配置成用于控制蓝牙收发器通过执行蓝牙连接过程与移动设备建立直接无线通信链路。例如,无线电通信模块包括蓝牙低能收发器。

[0022] 在另一个实施例中,访问控制装置进一步包括电子锁,并且控制器连接到电子锁并且被进一步配置成用于向所述电子锁提供访问控制信号,从而控制电子锁执行解锁功能。

[0023] 除了电子访问控制装置,本发明还涉及一种移动设备,该移动设备包括无线电通信模块,所述无线电通信模块被配置成用于通过在无线电通信模块与访问控制装置之间的直接无线通信链路进行无线数据交换。所述移动设备还包括处理器,其连接到无线电通信模块,并被配置为用于控制无线电通信模块经由直接无线通信链路接收来自访问控制装置的可执行的访问确认模块,和用于执行访问确认模块。通过执行访问确认模块,移动设备的处理器接收来自移动设备的用户的确认指令,响应于该确认指令,通过直接无线通信链路向访问控制装置传输一个确认消息。该确认消息使访问控制装置能够生成访问控制信号。在一个实施例中,访问确认模块进一步被配置成用于控制移动设备的处理器在确认消息中的包括入访问密钥,使访问控制装置能够使用包括在确认消息中的访问密钥生成访问控制信号。

[0024] 除了电子访问控制装置,本发明还涉及一种访问控制方法。所述访问控制方法包括:通过电子访问控制装置的控制器控制电子访问控制装置的无线电通信模块,以建立与移动设备的用于无线数据交换的直接无线通信链路。所述访问控制方法还包括:通过直接无线通信链路向移动设备传输来自访问控制装置的可执行的访问确认模块。所述访问控制方法进一步包括:通过移动设备的处理器执行可执行的访问确认模块。可执行的访问确认模块控制移动设备的处理器,使处理器接收来自移动设备的用户的确认指令,和,响应于所述确认指令,生成确认消息。所述确认消息包括存储在移动设备中的访问密钥。可执行的访问确认模块进一步控制移动设备的处理器,从而处理器通过直接无线通信链路向访问控制装置的无线电通信模块传输所述确认消息,从而使访问控制装置能够使用访问密钥生成访问控制信号。

[0025] 在一个实施例中,所述方法进一步包括:访问确认模块控制移动设备的处理器,以使处理器在确认消息中包括入存储在移动设备中的访问密钥,使访问控制装置能够使用该

访问密钥生成访问控制信号。

[0026] 在一个实施例中,所述方法进一步包括:电子访问控制装置的控制器检查移动设备的信号强度是否高于位于距访问控制装置确定近距离内的移动设备的信号强度阈值,如果移动设备的信号强度大于信号强度阈值,则经由直线无线通信链路将访问确认模块传输至移动设备。根据该实施例和/或配置,移动设备的信号强度是在电子访问控制装置中或移动设备中被测量的。

[0027] 在另一个实施例中,所述方法进一步包括:通过电子访问控制装置的接近度检测器,使用第二射频频带内的射频,检测在电子访问控制装置确定接近度内移动设备是否存在。当通过接近度检测器13在电子访问控制装置1确定接近度P内检测到移动设备2时,所述电子访问控制装置的控制器控制电子访问控制装置的无线电通信模块,用于在区别于第二射频频带的第一射频频带内与移动设备2建立直接无线通信链路3。

附图说明

[0028] 以下更详细地通过示例参照附图讨论本发明,在附图中:

[0029] 图1示出了框图,该框图示意性地示出了具有无线电通信模块和基于无线电的接近度检测器的电子访问控制装置;

[0030] 图2示出了框图,该框图示意性地示出了具有电子访问控制装置、访问权限服务器以及移动设备的访问控制系统;

[0031] 图3示出了流程图,该流程图示出了电子访问控制的示例性步骤序列;

[0032] 图4示出了流程图,该流程图示出了在电子访问控制装置和移动设备之间建立直接无线通信链路的示例性步骤序列;

[0033] 图5示出了流程图,该流程图示出了将访问密钥从移动设备传输到电子访问控制装置的示例性步骤序列。

具体实施方式

[0034] 在图1至图5中,参考标号1指代电子访问控制装置。电子访问控制装置1包括由连接到该装置的一个或多个电池或外部电源供电的一个或多个电子电路和模块。

[0035] 如图1中的实施例示意性地所示,电子访问控制装置1包括用于锁定和解锁到访问受控区域(诸如建筑物、汽车或房间)的入口(诸如门、闸门等等)的电子锁/电动锁14。响应于访问控制信号,电子锁14驱动一个或多个门闩或门栓锁定或解锁到该访问受控区域的入口。电子锁14与电子访问控制装置1的剩余部件一起在同一个壳体或在分离的壳体内实现。本领域技术人员将理解的是取决于应用,例如控制对售货机中的物体的访问,电子访问控制装置1或电子锁14分别被相应地配置成用于阻挡或授权访问,例如在或从售货机解锁或传送物体。

[0036] 在另一个实施例中,电子访问控制装置1没有被配置锁定和解锁的入口,但被配置成通常需要一张票来控制用户访问的区域、对象或服务:如公共交通工具:例如火车、电车、船、滑雪缆车等,或事件:例如剧院表演、电影院、运动场等,或使用自动售货机提供的访问对象:例如食品、饮料或小吃分配器。因此,用户各自的访问权限是通过电子(密码)访问密钥、电子票、和/或电子转账或代金券体现的。

[0037] 如图1所示,电子访问控制装置1进一步包括无线电通信模块11、控制器12以及基于无线电的接近度检测器13。该控制器电气地连接到通信模块11和基于无线电的接近度检测器13。

[0038] 无线电通信模块11被配置成用于通过在无线电通信模块11与移动设备2之间的直接无线通信链路3与移动设备2进行无线数据交换。术语“直接”表明无线通信链路3在无线电通信模块11和移动设备2之间不包括任何中间部件,诸如路由器、中继器、网关、有线网络、基站等等。无线电通信模块11被配置成用于在若干米的短距离S、具体地在高至五米、十米或二十米的距离执行无线数据交换。在一个实施例中,无线电通信模块11包括蓝牙收发器、具体地低能蓝牙收发器。无线电通信模块11被配置成用于使用(超高频UHF)微波在从2.4到2.485GHz的频带内操作。在一个替代实施例中,无线电通信模块11包括基于IEEE 802.11标准(例如,在从2.4GHz到5GHz的频带内操作)的WLAN通信模块。

[0039] 控制器12包括具有计算机程序代码的可编程微处理器、现场可编程门阵列、特定用途集成电路、和/或被配置成用于执行各个功能的另一个电子电路,如稍后更详细所述。

[0040] 基于无线电的接近度检测器13被配置成用于检测电子访问控制装置1的确定接近度P(具体地,在高至五厘米、十厘米或十五厘米(例如,通过设置访问控制装置1内的灵敏度参数可调)的距离范围内的近接近度P)的移动设备2的存在。接近度检测器13被配置成用于通过发射电磁场脉冲10来检测移动设备2的存在,通过在发射电磁场脉冲10期间检测返回信号,并使用该返回信号来检测移动设备2的存在。本质上,接近度检测器13被配置成用于通过检测由于移动设备2的存在而导致的接近度检测器13发射的电磁场10的变化来检测移动设备2的存在。具体地,接近度检测器13在其发射确定的电磁场脉冲10的同时在天线131上测量该返回信号并且确定该返回信号中的频率衰减、放大、和/或移位,如在本申请人的专利EP 1723575或EP 2437403中所公开的,本专利的全部内容通过引用结合在此。在一个实施例中,接近度检测器13包括RFID读取器(射频标识符),例如,根据ISO 18092、ISO 21481、ISO 15693、和/或ISO 14443的RFID读取器。接近度检测器13被配置成用于使用(高频HF)无线电波在RFID系统的载频操作,例如,6.78MHz、13.56MHz、或27.12MHz(或13.56MHz的另一个倍数)。

[0041] 因此,基于无线电的接近度检测器13使用与无线电通信模块11不同的(即,更低的)频带。如图1清晰地所示,基于无线电的接近度检测器13和无线电通信模块11是访问控制装置1的两个不同的(基于无线电的通信)模块,各自具有其自身的收发器电路和其自身的天线111、131。基于无线电的接近度检测器13和无线电通信模块11是两个不同的且分离的通信单元,例如各自在不同的集成电路(芯片)中实现,并且为访问控制装置2提供两个不同的且分离的通信通道。

[0042] 移动设备2被实现为移动无线电话(即,蜂窝电话)、平板计算机或笔记本电脑、计算机化手表、或另一个移动通信设备。如图1示意性地所示,移动设备2包括无线电通信模块21和连接到其上的可编程处理器22。无线电通信模块21被配置成用于经由直接无线通信链路3与访问控制装置1的无线电通信模块11交换数据。

[0043] 如图2所示,访问控制系统100包括一个或多个电子访问控制装置1和经由通信网络4连接到电子访问控制装置1的访问权限服务器5。取决于实现方式,通信网络4包括LAN(局域网)、另一个有线网络、WLAN(无线LAN)、和/或另一个移动无线网络(诸如GSM(全球

移动通信系统)或UMTS网络(通用移动电话系统))并且可以包括互联网。

[0044] 访问权限服务器5包括具有一个或多个处理器的一个或多个可操作计算机,该一个或多个可操作计算机被配置成用于向移动设备2传输访问密钥以及用于向电子访问控制装置1传输访问密钥和/或解密密钥。在一个实施例中,访问权限服务器5或其计算机/处理器分别被进一步配置用于向移动设备2和/或电子访问控制装置1传输可执行访问确认模块23。可替代地,可执行的访问确认模块23被应用服务器7经由包括上述移动无线网络的电信网络6传输到移动设备2。

[0045] 可执行的访问确认模块23包括计算机程序代码,该计算机程序代码被配置成用于控制对应的移动设备2的处理器使得其执行各种功能,如稍后更详细描述。在一个实施例中,可执行的访问确认模块23被实现为所谓的小程序并且包括用于虚拟机的可解释计算机程序代码,例如,被配置成用于在Java虚拟机上运行的Java代码(Java是太阳微系统公司的注册商标)。

[0046] 在以下段落中,参照图3至图5描述的是由访问控制装置1、移动设备2和访问权限服务器5的功能模块执行的电子访问控制的可能步骤序列。

[0047] 在准备步骤S0,访问权限服务器5向移动设备2传送访问具有受控访问的、由访问控制装置1控制的区域的访问密钥。该访问密钥被安全地例如经由传输层安全(TLS)、安全套接层(SSL)、或用于安全数据通信的其他密码协议进行传送。在一个实施例中,该访问密钥被经由NFC接口、蓝牙接口或蓝牙信标传送到移动设备2。例如,为了将该访问密钥传输到移动设备2,NFC终端被安装在酒店前台的柜台或桌子上,或者蓝牙终端(接口)或蓝牙信标被分别安装在酒店的前台区域内。取决于实施例和配置,访问权限服务器5进一步将该访问密钥或用于验证该访问密钥的密码元素传输到对应的访问控制装置1。可替代地,在被传送到移动设备2之前,该访问密钥或密码元素分别被存在访问控制装置1中。例如,该访问密钥是加密秘密(例如,秘密访问授权码),并且访问控制装置1使用秘密解密密钥来验证该秘密。

[0048] 在一个实施例中,访问权限服务器5进一步向移动设备2传送上述可执行的访问确认模块23。在一个进一步的实施例中,该访问密钥被作为可执行的访问确认模块23的一部分传送到移动设备2。

[0049] 例如,在酒店应用的情况下,在前台办理入住期间,该访问密钥以及(如果适用的话)可执行的访问确认模块23被传输到移动设备2。

[0050] 在步骤S1中,访问控制装置1或其接近度检测器13分别在距访问控制装置1的确定(近)接近度P内检测移动设备2的存在。为此目的,移动设备2的用户物理地移动并且将移动设备2分别放置在访问控制装置2或其接近度检测器13的天线131的确定(近)接近度范围P中。

[0051] 在步骤S2中,当在距访问控制装置1或其接近度检测器13的确定(近)接近度P内分别检测到移动设备2时,访问控制装置1的控制器12控制无线电通信模块11与移动设备2建立直接无线通信链路3。

[0052] 在图4示出的实施例中,在步骤S21中,访问控制装置1或其控制器12分别控制无线电通信模块11作为主设备从而建立直接无线通信链路3。具体地,控制器12将无线电通信模块11的蓝牙收发器设置为蓝牙中心模式。

[0053] 在步骤S22中,无线电通信模块11执行连接过程;具体地,蓝牙收发器发起蓝牙连接过程并且扫描蓝牙从设备。如果成功,访问控制装置1和移动设备2或其无线电通信模块11、21分别建立直接无线通信链路3作为蓝牙连接。本领域技术人员将理解的是通过蓝牙(BT),建立连接使用先前的配对过程,而蓝牙低能(BTLE)不包括配对过程。

[0054] 否则,控制器12在步骤S23中继续控制无线电通信模块11作为从设备,从而使得移动设备2建立直接无线通信链路3。具体地,控制器12将无线电通信模块11的蓝牙收发器设置为蓝牙外围模式。

[0055] 在步骤S24中,移动设备2或其无线电通信模块21分别执行连接过程;具体地,移动设备2的蓝牙收发器发起蓝牙连接过程并且扫描蓝牙从设备。如果成功,移动设备2和访问控制装置1或其无线电通信模块11、21分别建立直接无线通信链路3作为蓝牙配对连接并且继续到步骤S3。

[0056] 否则,在步骤S25中,访问控制装置2显示错误消息,例如向用户表明在重复该过程之前应当激活移动设备2的通信模块21。在一个进一步的实施例中,在移动设备2可以与对应的访问控制装置1相关联的情况下,访问控制装置1请求访问权限服务器5向移动设备2的用户发送类似的错误消息。

[0057] 在一个实施例中,为了增加多样性,当在访问控制装置1或其接近度检测器13的确定(近)接近度P内分别检测到移动设备2时,访问控制装置1的控制器12被配置成用于从在访问控制装置1内实现的不同类型的无线电通信模块选择优选的无线电通信模块与移动设备2建立直接无线通信链路3。具体地,控制器12被配置成用于选择上述蓝牙收发器或WLAN通信模块或例如在上述接近度检测器13的RFID读取器中实现的NFC接口。取决于实施例或配置,优选无线电通信模块的选择由控制器12使用存储在访问控制装置1内的偏好表执行或根据可编程选择规则执行,这些可编程选择规则定义访问控制装置1选择无线电通信模块与移动设备2建立直接无线通信链路3的优先级或顺序。

[0058] 在步骤S3中,一旦在移动设备2和访问控制装置1或其无线电通信模块11、21之间分别建立了直接无线通信链路3,移动设备2或其无线电通信模块21分别经由直接无线通信链路3向访问控制装置1传送访问密钥。具体地,访问确认模块23被执行并且控制移动设备2的处理器22将该访问密钥传送到访问控制装置1。一旦在移动设备2和访问控制装置1或其无线电通信模块11、21之间分别建立了直接无线通信链路3,就触发执行访问确认模块23。在一个实施例中,执行访问确认模块23由访问控制装置1经由直接无线通信链路3向移动设备2传输执行请求而触发。

[0059] 如图5所示,在步骤S33中,例如,在将该访问密钥传送到访问控制装置1之前或之后,移动设备2或访问确认模块23从移动设备的用户请求并且接收确认指令。取决于实施例,访问确认模块23生成并且在移动设备2的显示器上显示图形用户界面(例如,“取消”和“ok”按钮)以供用户确认对由访问控制装置1控制的区域的预期访问。在一个实施例中,用户被要求输入授权信息,诸如访问码或密码。可替代地或另外,访问确认模块23使用移动设备2的指纹传感器从用户接收肯定确认。

[0060] 在步骤S34中,如果用户已经输入所需的确认指令,例如,通过成功地按压“ok”按钮和/或指纹传感器,在一个实施例中,访问确认模块23生成包括该访问密钥的确认消息。该确认消息,以及如果包括该访问密钥,被经由直接无线通信链路3从移动设备2传送到访

访问控制装置1。在另一个实施例中,该访问密钥和确认消息被分别从彼此传送到访问控制装置1。

[0061] 在步骤S35中,访问控制装置1或其控制器12分别经由直接无线通信链路3从无线电通信模块11接收该确认消息。在访问密钥包括在确认信息中的实施例中,控制器12从于移动设备1接收的确认消息提取该访问密钥。

[0062] 步骤S30、S31、S32能够使在移动设备2中加载和安装访问确认模块23成为可能,无需在移动设备2中预加载和预安装访问确认模块23,而是在访问控制装置1的确定(近)接近度内检测到移动设备2时动态地加载和安装访问确认模块23。如图5所示,控制器12检查接收信号强度指示符(RSSI)是否表明移动设备2或其无线电通信模块21分别的信号强度,该信号强度对应于距访问控制装置1的确定近距离范围C,例如移动设备2到访问控制装置1的最大距离为半米、一米或两米,例如,通过设置访问控制装置1内的距离参数是可调的。如果RSSI值高于设定的信号强度阈值并且移动设备2因此位于距访问控制装置1的确定近距离范围C内,在步骤S31中,控制器12使用无线电通信模块11经由直接无线通信链路3向移动设备2传送访问确认模块23。本领域技术人员会明白,在移动设备2被配置为测量信号强度的情况下,控制器12可以使用由移动设备2测量的和从移动设备2上接收的信号强度值来执行步骤S30的信号强度测试。在另一个实施例中,控制器12设置无线电通信模块11为初始第一低发射功率,对应于距访问控制装置1的确定近距离范围C,在此范围内,来自访问控制装置1的传输被认为是可被移动设备2接收的。随后,如果访问控制设备1在一组响应时间内不接收任何来自移动设备2的响应,控制器12则增加传输功率至增强的第二发送功率,对应于近距离范围C的扩展。

[0063] 在步骤S32中,移动设备2的处理器22接收并执行访问确认模块23。访问确认模块23从移动设备2的用户请求确认指令,例如,通过在移动设备2的显示器上显示要求用户按压确认按钮和/或将手指放在指纹传感器上的对应请求,取决于配置和/或实施例。

[0064] 如上所述,在步骤S33中,访问确认模块23从移动设备2的用户接收该确认指令,例如,经由图形用户界面和/或指纹传感器。如果该确认是肯定的,例如,用户按压“ok”按钮或者指纹传感器读取并验证用户的指纹合法(被授权),在一个实施例中,访问确认模块23生成包括该访问密钥的肯定确认消息,例如,以如先前从访问权限服务器5接收的加密形式。

[0065] 在一个实施例中,为了确认消息将要被发送到访问控制装置1,或为了确认信息会被访问控制装置1接收,控制器12和/或访问确认模块23施加了访问确认模块23需要满足的特定条件。例如,访问确认模块23需要是一个特定的类型、制造商和/或版本号;访问确认模块23需要在移动设备2上作为前台应用被运行;和/或在访问控制装置1具有初始的连接建立后,访问确认模块23需要在一个确定的扫描时间内给访问控制装置1发送确认信息。因此,访问确认模块23被配置为在确认消息中包括入模块标识符,该模块标识符识别访问确认模块23,例如,关于其类型、制造商和/或版本号,和控制器12检查接收的模块标识符标是否识别由访问控制设备1支持的访问确认模块23,例如,接收的模块标识符是否识别访问确认模块23的支持类型、制造商、和/或版本号。为了确保访问确认模块23是目前运行在移动设备2上的前台应用,访问确认模块23检查其是否是目前运行在移动设备2上的前台应用,和其也在确认消息中包括入这个检查的结果,用于控制器12进行检查,或者如果访问确认模块23不是目前运行在移动设备2上的前台应用,则其不生成确认消息。

[0066] 在另一个实施例中,控制器12动态地调整用于执行步骤S30的信号强度测试的固定信号强度阈值的水平。例如,如果控制器12在确定的扫描时间(如200ms的响应时间窗口)内从多于一个的移动装置2上接收到确认消息,则控制器12将固定信号强度阈值降低到一个较低的值。

[0067] 如图3所示,在步骤S4中,控制器12检查并验证从移动设备2接收的访问密钥。取决于实施例,控制器12解密所接收的访问密钥并且对经解密的访问密钥与存储在访问控制装置1中的验证密钥进行比较。本领域技术人员将理解的是存在各种密码函数和算法来验证访问密钥以及不同级别和类型的访问权限可以与具体的访问密钥相关联,例如准许访问日期和/或时间段。在任何情况下,步骤S0-S4提供访问密钥或秘密访问授权在访问权限服务器5与访问控制装置1之间的端到端加密。

[0068] 在可选步骤S41中,如果该访问密钥无法被适当地验证,控制器12使用无线电通信模块11经由直接无线通信链路3向移动设备2传送错误消息。

[0069] 在可选步骤S42中,移动设备2的处理器22接收该错误消息并且在移动设备2上渲染该错误消息,例如,通过在移动设备2的显示器显示该错误消息和/或在移动设备2上生成声音报警。

[0070] 在步骤S5中,响应于所接收的访问密钥的正确验证,控制器12生成例如处于电信号或数据值形式的访问控制信号。取决于实施例和/或配置,该访问控制信号表示与锁定命令不同的且可区分的解锁命令。

[0071] 在步骤S50中,控制器12将该访问控制信号例如经由连接到电子锁14或电子锁14可访问的电气信号线或数据寄存器应用于电子锁14。

[0072] 在步骤S51中,响应于来自控制器12的访问控制信号,电子锁14执行解锁功能,例如,其驱动门栓或门闩机械地解锁门、闸门等等,从而使得可以访问到访问受控区域(例如,建筑如或房间,诸如酒店房间)的入口。

[0073] 在可选步骤S52中,电子锁14向控制器12返回例如处于电信号或数据值形式的解锁确认或解锁状态信号。

[0074] 在步骤S6中,控制器12确定并且定义对应于并且反映该访问控制信号的访问状态。例如,该访问状态表明对应于解锁命令的“打开”状态或对应于锁定命令的“关闭”状态。在包括可选步骤S52的实施例中,控制器12使用来自电子锁14的解锁确认或解锁状态信号确定并且定义该访问状态。

[0075] 在可选步骤S61中,控制器12使用无线电通信模块11来经由直接无线通信链路3向移动设备2传送包括该访问状态的访问状态消息。

[0076] 在可选步骤S62中,移动设备2的处理器22接收该访问状态消息并且在移动设备2的显示器上显示该访问状态。

[0077] 在另一方面,另外或作为一种替代,接近度检测器13包括用于检测距电子访问控制装置1的确定接近度P内的用户存在的电容传感器130,如,在0~5厘米的确定接近度P内,如,在2-3厘米或2-5厘米。具体而言,电容传感器130被配置来检测距电子访问控制装置1的确定接近度P内的用户的手的存在。例如,电容传感器130是来自Cypress的Capsense MBR3传感器(Capsense是Cypress半导体有限公司的注册商标),例如Capsense MBR3传感器CY8CMBR3108。例如,电容传感器130电气地连接到金属门把手或连接到布置为靠近门把手

或到访问受控区域的入口的标记区域的天线。在本实施例中,控制器12分别连接到接近度检测器13或者电容传感器130,并且被进一步配置成用于当接近度检测器13在电子访问控制装置1的确定接近度P内检测到用户的存在时,控制无线电通信模块11与移动设备2建立直接无线通信链路3。作为建立直接无线通信链路3的附加第二条件,控制器12被进一步配置成用于检查并验证移动设备2的由无线电通信模块11或从移动设备2接收的测量结果表明的接收信号强度满足表明移动设备2在距访问控制装置1的确定的最大距离内的确定阈值。例如,控制器12被配置成用于仅当在电子访问控制装置1的0厘米或-5厘米的确定的附近时,并且如果无线电通信模块11所表明的移动设备2的接收信号强度为或高于表明移动设备2距访问控制装置1的0.5米或1米的最大距离的确定阈值时,控制无线电通信模块11与移动设备2建立直接无线通信链路3。

[0078] 在一个实施例中,两个或更多个访问控制装置1共享一个无线电通信模块11。例如,在酒店场景中,两个相邻酒店房间的访问控制装置1连接到安装在这两个访问控制装置1外部(被安装在门侧面)的同一个无线电通信模块11,例如,在距这两个访问控制装置1基本上相等或至少类似距离的天花板内(在天花板侧壳体中)。外部无线电通信模块11通过无线连接而分别连接到访问控制装置1或其控制器12。如上参照步骤S2所述,当接近度检测器13在电子访问控制装置1中的一个设备的确定的附近P检测到移动设备2时,该电子访问控制装置1的对应的控制器12控制外部无线电通信模块11与移动设备2建立直接无线通信链路3。为此目的,控制器12向外部无线电通信模块11传输检测信号。可替代地,外部无线电通信模块11与移动设备2建立直接无线通信链路3,而不管来自访问控制装置1的检测信号,同时该检测信号使得外部无线电通信模块11能够标识在确定接近度P有效地检测到移动设备1的具体访问控制装置1。接下来,操作在以上参照图3和图5所述的步骤S3中继续。在可替代场景和配置中,外部无线电通信模块11通过有线连接而连接到具有两个或多个天线131的一个访问控制装置1,其中,每个天线131分别于不同的门或其电子锁14相关联。在此替代配置中,控制器12确定将基于天线131打开电子锁14,通过该天线在电子访问控制装置1或具体的天线131确定接近度P分别由接近度检测器13检测移动设备2。外部无线电通信模块11和移动设备之间的通信如上述那样发生。

[0079] 应当注意,在本描述中,计算机程序代码已经与特定的功能模块相关联,并且已经按照特定的顺序呈现步骤序列,然而,本领域技术人员将理解的是,计算机程序代码可以在结构上不同以及可以更改至少某些步骤的顺序而不背离本发明的范围。

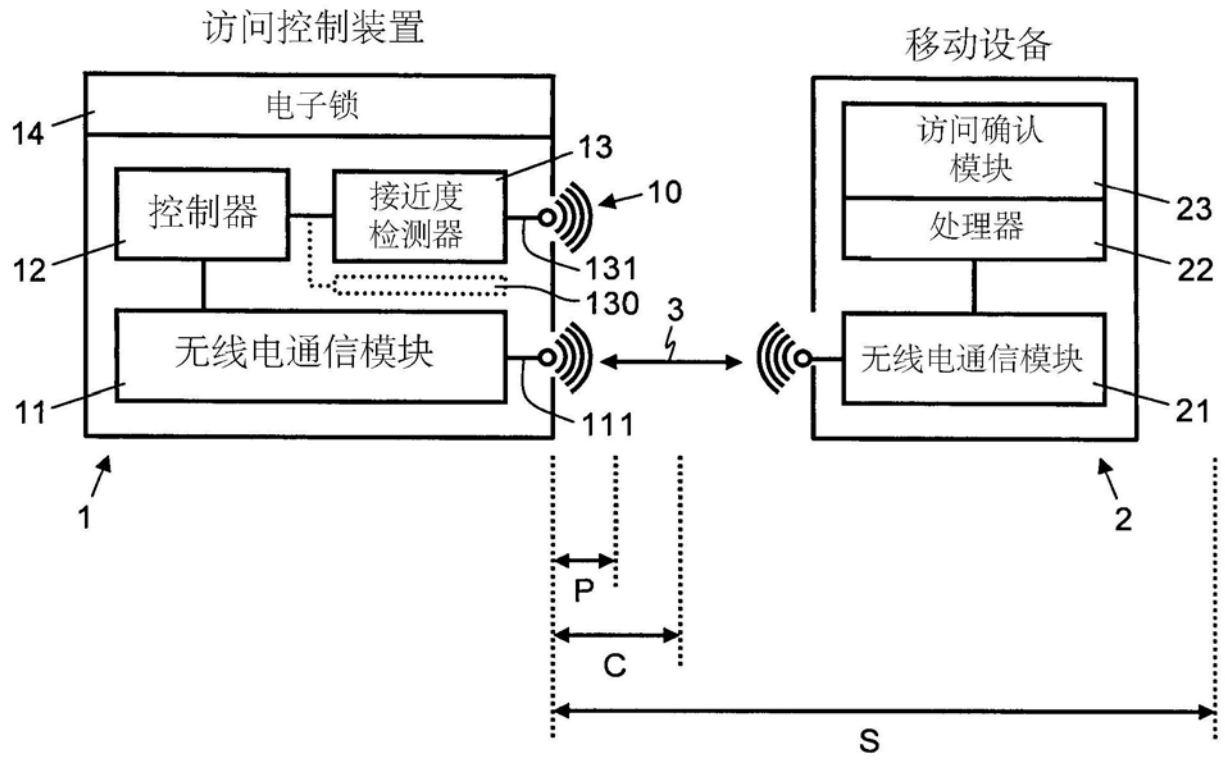


图1

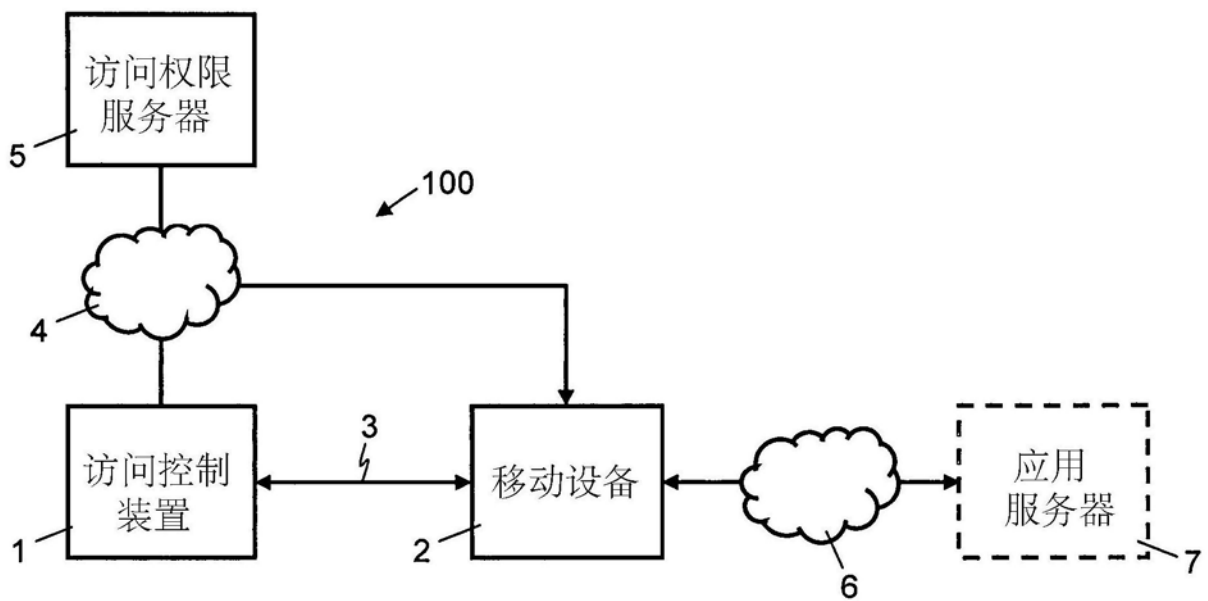


图2

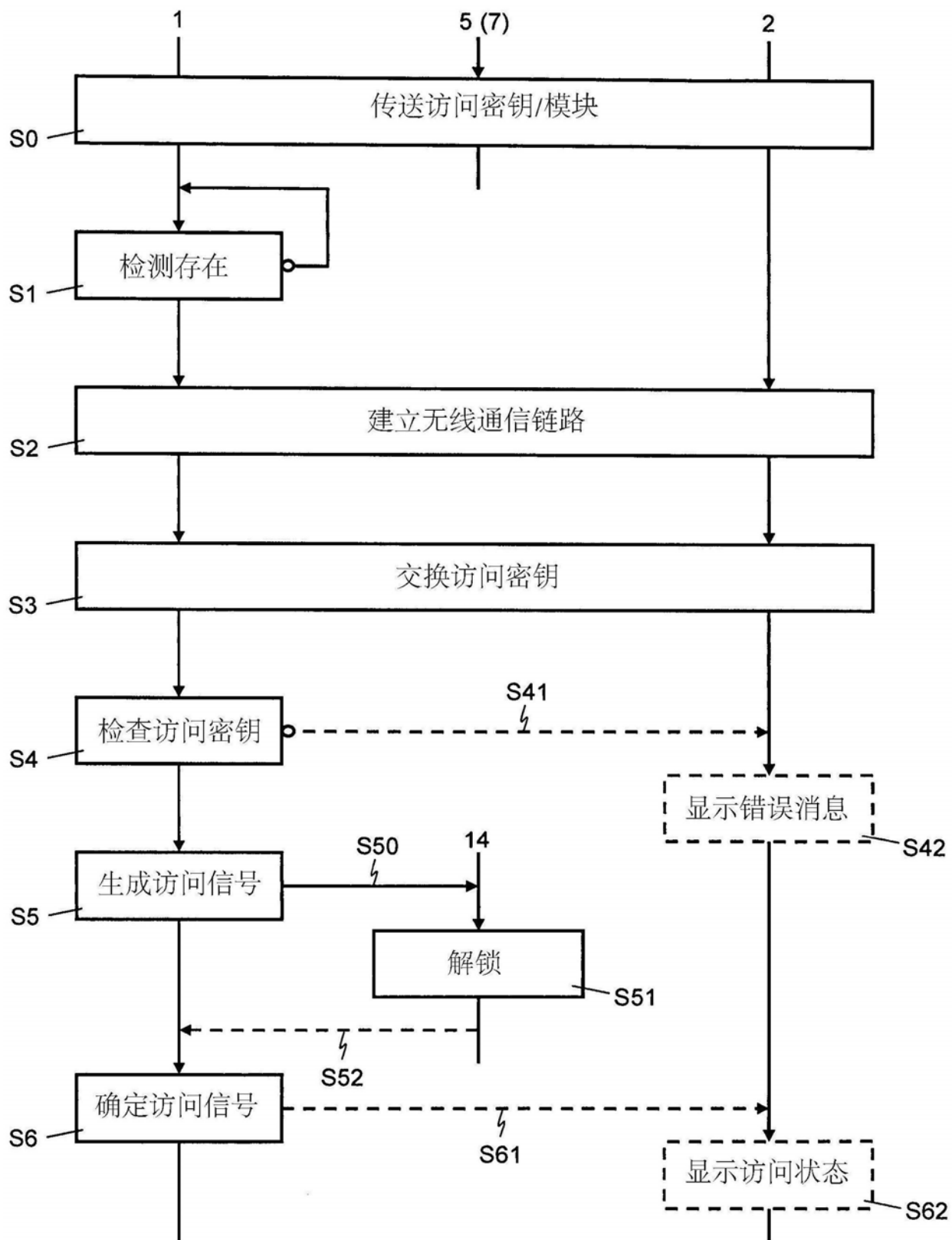


图3

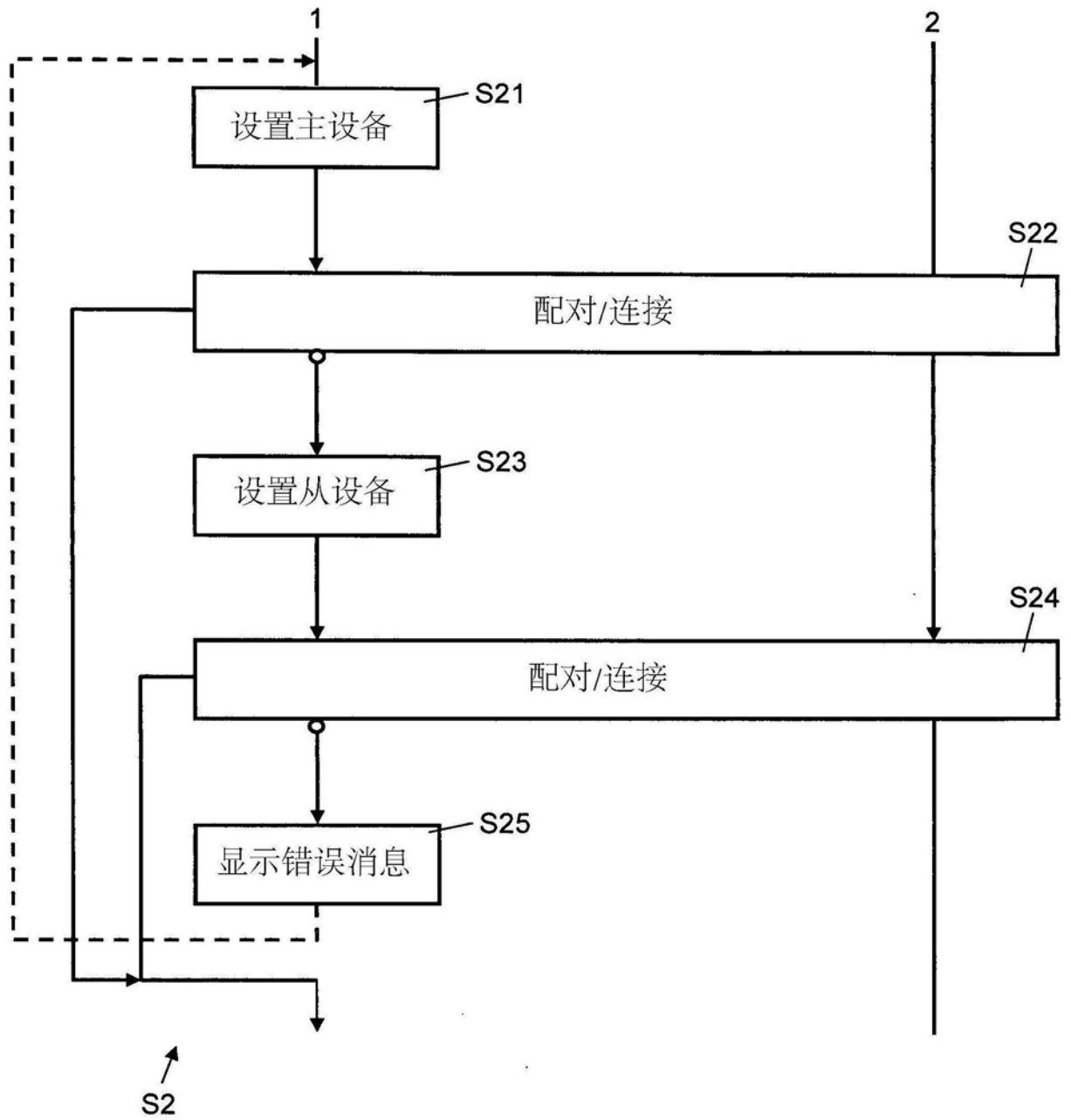


图4

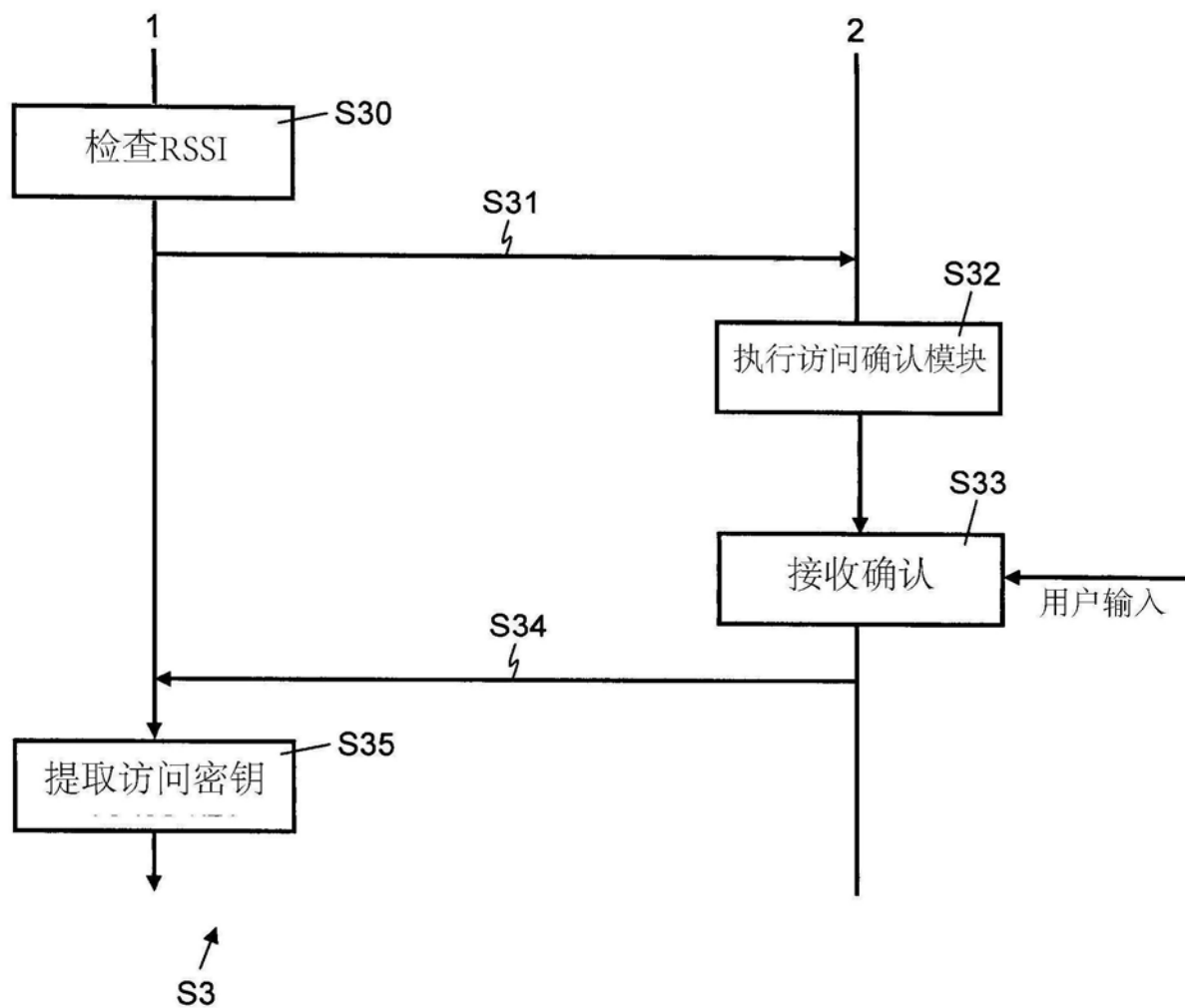


图5