(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104365056 B
(45)授权公告日 2017.11.24

(21)申请号 201380018278.5
(22)申请日 2013.04.03
(65)同一申请的已公布的文献号
申请公布号 CN 104365056 A
(43)申请公布日 2015.02.18
(30)优先权数据
20120110 2012.04.05 FI
(85)PCT国际申请进入国家阶段日
2014.09.30
(86)PCT国际申请的申请数据
PCT/FI2013/050362 2013.04.03
(87)PCT国际申请的公布数据
WO2013/150186 EN 2013.10.10

(73)专利权人 托西博克斯有限公司
地址 芬兰奥卢
(72)发明人 V.伊里马蒂莫 M.科卡洛
J.朱奥佩里
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张凌苗 陈岚

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 12/28(2006.01)
H04L 12/46(2006.01)
H04L 29/06(2006.01)
G06F 21/33(2006.01)

审查员 亓晓旭

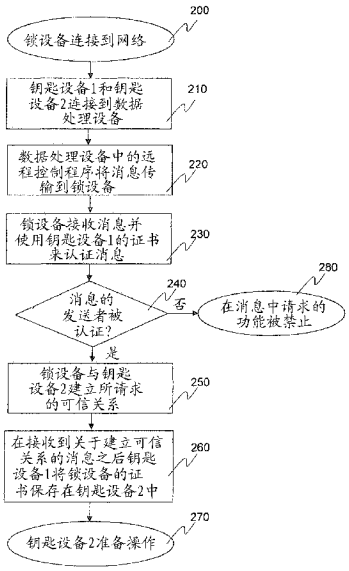
权利要求书2页 说明书8页 附图4页

(54)发明名称

用于操作权的远程授予的安全方法和设备

(57)摘要

在建立可信关系的方法和系统中，首先在钥匙设备和至少一个锁设备之间建立虚拟专用网。之后，为了建立可信关系，钥匙设备将使用其私有密码密钥加密的消息发送到至少一个锁设备。该消息包括可信钥匙设备的证书和某个其它设备的证书，接收该消息的锁设备应与所述其它设备建立新可信关系。通过使用所建立的可信关系，在锁设备和新钥匙设备之间的可信关系或在两个或更多锁设备之间的可信关系被建立，由此，可在锁设备之间建立虚拟专用网。



CN 104365056 B

1.一种用于在资产的致动器的远程控制系统(1)中的虚拟专用网(41)中利用的可信钥匙设备(34)和/或锁设备(61)之间建立新可信关系的方法,在所述方法中:

- 可信钥匙设备(34)电连接(210、310)到数据处理设备(32),所述数据处理设备(32)与因特网(2)连接,

- 所述可信钥匙设备(34)确定它到因特网(2)的网络路径并将它的网络路径保存在连接到因特网(2)的服务器(21)中,

- 所述可信钥匙设备(34)接收至少一个锁设备(61)的网络路径信息,以及

- 所述可信钥匙设备(34)与至少一个锁设备(61)形成虚拟专用网(41),

其特征在于,

- 所述可信钥匙设备(34)将使用所述可信钥匙设备(34)的私有加密密钥加密的消息传输(220)到至少一个锁设备(61),所述消息包括所述可信钥匙设备的证书和至少一个其它设备的证书,进行接收的锁设备(61)应与所述至少一个其它设备建立可信关系,

- 锁设备(61)使用已知的所述可信钥匙设备(34)的公共加密密钥来打开并确认(230、330)它所接收的消息的发送者的真实性,

- 所述锁设备将与由所识别的设备发送的消息有关的设备的证书保存在其存储器中,

- 所述锁设备(61)与在所述消息中声明的至少一个其它设备建立可信关系(250、350)。

2.如权利要求1所述的建立新可信关系的方法,其特征在于,另一钥匙设备电连接(210)到所述数据处理设备(32),所述证书由所述可信钥匙设备(34)包括在被发送到至少一个锁设备(61)的消息中。

3.如权利要求2所述的建立新可信关系的方法,其特征在于,所述可信钥匙设备(34)从至少一个锁设备(61)接收建立可信关系的确认消息,以及所述可信钥匙设备(34)将从其接收了确认所述可信关系的建立的消息的锁设备(61)的证书保存在其它钥匙设备的存储器中。

4.如权利要求1所述的建立新可信关系的方法,其特征在于,所述可信钥匙设备(34)将单独的个别消息发送到至少两个锁设备,所述单独的个别消息包括至少一个其它锁设备的证书和在所述消息中提到的锁设备之间的功能关系的描述。

5.如权利要求1所述的建立新可信关系的方法,其特征在于,至少两个锁设备在它们本身之间通过利用从所述可信钥匙设备(34)接收的证书建立虚拟专用网,在所述专用网中一个锁设备用作服务器设备,以及至少一个其他锁设备用作所述服务器的客户端设备。

6.一种资产的远程控制系统的致动器的可信钥匙设备(34),包括:

- 网络连接接口元件,其包括用于将所述可信钥匙设备连接到数据处理设备(32)的输入/输出装置(343),所述数据处理设备(32)连接到因特网,

- 密码处理器(341),以及

- 存储器(342),其包含计算机程序代码,

其特征在于,所述网络连接接口元件配置成:

- 将使用可信钥匙设备(34)的私有加密密钥加密的消息从所述可信钥匙设备(34)传输(220)到至少一个锁设备(61),所述消息包括所述可信钥匙设备的证书和至少一个其它设备的证书,进行接收的锁设备应与所述至少一个其它设备建立可信关系,

- 从至少一个锁设备(61)接收建立所述可信关系的确认消息并将所述确认消息保存在其存储器中。

7.如权利要求6所述的资产的远程控制系统的致动器的钥匙设备，其特征在于，所述密码处理器、所述存储器和保存在其中的所述计算机程序代码配置成在被发送到至少一个锁设备(61)的消息中包括电连接(210)到数据处理设备的另一钥匙设备的证书。

8.如权利要求7所述的资产的远程控制系统的致动器的钥匙设备，其特征在于，所述密码处理器、所述存储器和保存在其中的所述计算机程序代码配置成从至少一个锁设备(61)接收建立所述可信关系的确认消息，以及所述可信钥匙设备(34)配置成在另一钥匙设备的存储器中保存从其接收了确认所述可信关系的建立的消息的锁设备(61)的证书。

9.一种用于提供致动器的远程控制系统的钥匙设备功能或用于在至少两个锁设备之间建立可信关系的方法，所述方法包括：

- 确定从在建立可信关系时使用的可信钥匙设备(34)到因特网(2)的网络路径并将所述网络路径保存在连接到因特网(2)的远程控制网络服务器(21)中，

- 从所述远程控制网络服务器(21)接收至少一个锁设备(61)的网络路径信息，

- 借助于至少一个锁设备(61)的证书和网络路径信息与所述锁设备(61)形成虚拟专用网(41)，

其特征在于，所述方法还包括：

- 将使用所述可信钥匙设备(34)的私有加密密钥加密的消息从所述可信钥匙设备(34)传输(220)到至少一个锁设备(61)，所述消息包括所述可信钥匙设备的证书和至少一个其它钥匙设备或其它锁设备的证书，进行接收的锁设备(61)应与所述至少一个其它钥匙设备或其他锁设备建立可信关系，以及

- 从至少一个锁设备(61)接收建立所述锁设备的可信关系的确认消息和将发送所述消息的锁设备(61)的证书至少保存在所述可信钥匙设备(34)的存储器中。

用于操作权的远程授予的安全方法和设备

[0001] 本发明涉及在资产中的致动器的远程控制方法和远程控制系统中要利用的操作权的安全分配过程。

背景技术

[0002] 远程可控制的设备和系统越来越多地安装在资产和家庭中。系统的目的是固定和/或维持资产中的条件以使得它们中的人既安全又舒适。

[0003] 在市场上，在资产中的技术设备的远程控制布置和利用该远程控制布置的远程控制方法是可获得的，其中已经存在于资产和家庭中的因特网连接因此在建筑物服务和监督的远程使用中被利用。在所述远程控制布置中，利用远程使用设备对。用户携带便携式钥匙设备，且锁设备安装在资产中，资产的目的地连接因此借助于锁设备被改变为适合于远程使用。在目的地中的数据网络连接和目的地中的内联网的已经存在的功能未改变。

[0004] 在所述远程控制布置中，以固定方式安装在资产中的锁设备和由实现资产的监控的人携带的钥匙设备能够基于从属于远程控制布置的远程控制网络服务器得到的联系信息通过因特网建立安全双向虚拟专用网(VPN)。资产中的锁设备连接到资产中的数据网络接口设备/网络终端，例如连接到调制解调器，在资产中将被远程控制或远程监控的设备连接到所述锁设备。

[0005] 布置的远程控制设备对形成预定的唯一设备对或设备组，其在网络中识别彼此。由于识别方法，由用户或安装在一些数据处理设备中的计算机程序一起携带的钥匙设备只与其自己的唯一锁设备建立网络连接，且相应的连接不能与任何其它网络设备建立，其中所述计算机程序实现钥匙设备的功能。因此，钥匙设备用作资产的“网络门”的强安全钥匙。

[0006] 可结合制造或结合稍后发生的启动来建立在远程控制布置中使用的远程控制网络设备对。在这两种情况中，通过例如在钥匙设备的USB端口处使锁设备和钥匙设备彼此连接来形成设备对，由此，设备之一或二者接收彼此的识别码、设备证书。

[0007] 锁设备和钥匙设备的当前IP地址被维持在属于布置的远程控制网络服务器中，所述IP地址用于建立在所述设备之间的连接。由于所利用的连接建立方法，所述设备二者可连接到某个专用的非公共网络，且它们仍然可在它们本身当中通过因特网建立安全的数据传输连接。通过在移动钥匙设备和固定安装的锁设备之间通过因特网建立数据传输连接对于以下是足够的：在所建立的连接中的某个点处所述设备也获得公共IP地址，即使锁设备和钥匙设备同时只有非公共IP地址。远程控制网络服务器在它发送了设备可用的设备IP地址之后不参与实际数据传输连接的建立。

[0008] 在所述远程控制布置中，如果设备需要彼此配对，锁设备和钥匙设备的物理互连是要求的。在系统中，可能添加并行或从属于在使用中的钥匙设备的新钥匙设备。这可以用与第一对钥匙设备/锁设备的形成相同的方式；通过将新钥匙设备连接到锁设备的USB端口来实现。在实践中，这可涉及从正执行新钥匙到远程控制系统的连接的人行进几百千米。

[0009] 相同的钥匙设备可经由若干单独的锁设备来控制若干单独的远程控制对象。在这些锁设备之间的相互控制关系的改变是不可能的。某个锁设备不能被指派为另一锁设备的

主设备，该另一锁设备将用作充当主设备的锁设备的从锁设备。

发明内容

[0010] 本发明的目的是提供在资产的远程控制布置中利用的新钥匙设备或锁设备的操作权的新分配过程，其可通过对一个或多个锁设备的远程访问来实现。

[0011] 本发明的目的由这样的过程实现，在该过程中，钥匙设备的证书通过数据传输网络从所利用的数据处理设备传输到使用钥匙设备的有效私有PKI密钥(公钥基础设施)签名的锁设备，然后，在锁设备中接收的新钥匙设备的PKI密钥和证书二者被识别，然后，对新的识别出的钥匙设备确定的操作权的添加或改变在锁设备中实现。如果使用相同的钥匙设备控制若干单独的锁设备，则可通过给它们发送使用私有PKI密钥签名的变更的消息以相应的方式来改变在锁设备之间的相互关系。

[0012] 根据本发明的方法和布置的优点是新钥匙设备的操作权的分配可被执行，而不需要将新钥匙设备物理地连接到目标锁设备。

[0013] 此外，本发明的优点是从属于钥匙设备的若干锁设备的相互控制关系可通过远程访问来改变。

[0014] 此外，本发明的优点是通过借助于钥匙设备利用远程访问，虚拟专用网可在两个或更多锁设备之间建立，由此，一个锁设备用作因特网连接设备。

[0015] 根据本发明的方法特征在于：

[0016] - 可信钥匙设备将使用可信钥匙设备的私有加密密钥加密的消息传输到至少一个锁设备，所述消息包括所述可信钥匙设备的证书和至少一个其它设备的证书，接收锁设备应与所述至少一个其它设备建立可信关系，且测量的定义在建立所述可信关系时完成，

[0017] - 锁设备使用已知的所述可信钥匙设备的公共加密密钥来打开并确认它所接收的消息的发送者的真实性，

[0018] - 所述锁设备将与由所识别的设备发送的消息有关的设备的证书保存在其存储器中，

[0019] - 所述锁设备与在所述消息中声明的至少一个其它设备建立可信关系。

[0020] 根据本发明的处理器、存储器和存储在其中的计算机软件代码特征在于，钥匙设备配置成：

[0021] - 将使用可信钥匙设备的私有加密密钥加密的消息从所述可信钥匙设备传输到至少一个锁设备，所述消息包括所述可信钥匙设备的证书和至少一个其它设备的证书，接收锁设备应与所述至少一个其它设备建立可信关系，且测量的定义在建立所述可信关系时完成，

[0022] - 从至少一个锁设备接收建立可信关系的确认消息并将所述确认消息保存在其存储器中。

[0023] 根据本发明的用于提供在资产中的致动器的远程控制系统的钥匙设备功能的计算机程序特征在于它包括：

[0024] - 用于将使用可信钥匙设备的私有加密密钥加密的消息从密钥设备传输到至少一个锁设备的代码模块，所述消息包括所述可信钥匙设备的证书和至少一个其它钥匙设备或一个其它锁设备的证书，接收锁设备应与所述至少一个其它钥匙设备或一个其他锁设备

建立可信关系，且测量的定义在建立所述可信关系时完成，以及

[0025] - 用于从至少一个锁设备接收建立所述锁设备的可信关系的确认消息和用于将发送所述消息的锁设备的证书至少保存在所述可信钥匙设备的存储器中的代码模块。

[0026] 在从属权利要求中公开了本发明的一些优选实施例。

[0027] 本发明的基本思想如下：为了实现远程控制，在一些资产中，设备对、锁设备和钥匙设备存在，在该设备对中存在可基于虚拟专用网形成只与彼此的数据传输连接的至少一个锁设备和至少一个钥匙设备。

[0028] 在资产中的将被远程控制的锁设备安装在待控制的资产中的现有内联网网络或因特网网络中。它在内联网或因特网网络中建立一个子网络——控制内联网网络，在控制或管理资产时利用的各种致动器使用有线或无线数据传输连接而连接到该控制内联网网络。

[0029] 在本发明的一个有利的实施例中，单个钥匙设备或若干钥匙设备可以充当不同资产中的两个或更多锁设备的设备对。锁设备和钥匙设备的自己的识别码、证书及私有和公共PKI密钥在其制造期间保存在所述设备中。通过使用证书，锁设备和钥匙设备能够在它们之间建立双向安全数据传输连接。

[0030] 关于启动，这两个设备都确定设备的从其位置网络一直到连接到因特网的网络终端的路由信息，该路由信息是连接的建立所需要的。该路由信息存储在连接到因特网的远程控制网络服务器中。

[0031] 在根据本发明的可信关系的建立过程中，钥匙设备可连接到某个数据传输设备，该数据传输设备能够建立到因特网的数据传输连接。可能的数据传输设备例如是PC、平板计算机或智能电话。

[0032] 在本发明的一个有利的实施例中，实现钥匙设备的功能的计算机程序保存在例如USB棒的便携式数据存储装置上，将在远程控制中被利用的计算机程序在被需要时可从该便携式数据存储装置安装到适当的数据处理设备中。因而，安装在数据处理设备中的计算机程序执行钥匙设备的必要功能。

[0033] 在有利的实施例中，USB钥匙设备连接到数据传输设备，数据传输设备连接到本地网络。因而，USB钥匙设备首先确定其自己通过不同的子网络到远程控制网络服务器的路由。根据本发明，当路由被确定时，USB钥匙设备的当前路由信息被保存在远程控制网络服务器中。

[0034] 当新钥匙设备需要连接到现有的远程控制布置时，已经操作的USB钥匙设备和待引入的新USB钥匙设备二者都连接到所使用的数据传输设备。在这种情况下，由操作的USB钥匙设备控制的锁设备示出在所使用的数据处理设备的屏幕上。从该列表中，用户选择锁设备，作为将被连接到系统的新USB钥匙设备将服务于该锁设备的钥匙。在选择之后，使用已经操作的USB钥匙设备的证书确认的用于建立可信关系的请求消息被发送到所选的锁设备，该请求消息使用可信USB钥匙设备的私有PKI密钥加密。每个锁设备使用可信USB钥匙设备的公共PKI密钥打开所接收的消息。之后，每个锁设备检查到所接收的证书相应于与它配对的USB钥匙设备的证书，且该证书因此是已知的。如果识别是成功的，则与可信UEB钥匙设备的证书一起传送的新USB钥匙设备的证书以及其公共PKI密钥被保存在相应的锁设备中。关于识别的成功和可信关系的建立的消息被发送到发送消息的USB钥匙设备，该钥匙设备

基于所接收的消息来将已知锁设备的证书保存在新USB锁设备的存储器中。之后，可使用这两个USB钥匙设备来控制相应的锁设备。当对新USB钥匙设备成功地建立了所请求的新操作权(与锁设备的可信关系)时，它可与数据处理设备分离并例如通过邮件发送到有权利使用所述新钥匙设备的人。

附图说明

[0035] 在下文中，将详细描述本发明。在该描述中，参考附图，其中：

[0036] 图1示出远程控制布置的例子，其中可在处理远程控制的客户端设备和资产的单独的控制或管理设备之间建立双向数据传输连接，

[0037] 图2示出为如何为新钥匙设备分配操作权的示例性流程图，

[0038] 图3示出为如何在两个锁设备之间建立虚拟专用网的示例性流程图，以及

[0039] 图4作为例子示出根据本发明的USB钥匙设备。

具体实施方式

[0040] 在下面的描述中的实施例仅作为例子被给出，且本领域中的技术人员也可用除了在本描述中描述的方式以外的某种其他方式来实现本发明的基本思想。虽然本描述可以指在若干位置中的某个或某些实施例，但这并不意味着参考将只指向一个所描述的实施例，或所描述的特性将只在一个所描述的实施例中是可用的。两个或更多实施例的单独特性可组合，且本发明的新实施例可因此被提供。

[0041] 图1示出远程控制系统的有利实施例1。在图1的例子中，利用数据处理设备32来与一个USB钥匙设备34建立到位于其它地方的资产中的一个锁设备61的数据传输连接。然而，USB钥匙设备34也可有利地与位于两个或更多资产中的单独锁设备(未在图1中示出)一起操作。

[0042] 在图1中，用参考数字2指代因特网。参考数字为3的某个公共网络或内联网也连接到因特网2。网络3可以是固定或无线数据传输网络。在图1中，实现远程控制的客户端设备32加入网络3。为了实现远程控制连接，USB钥匙设备34连接到客户端设备的USB端口33。

[0043] 在图1中用参考数字5指明在资产中的将被远程控制的房屋内联网。示例性数据处理设备——参考数字55和56——连接到房屋内联网网络5。此外，另一数据传输网络6——房屋控制内联网——连接到房屋内联网网络5。在资产中将被远程控制的致动器62-65使用无线数据传输连接或电缆连接而连接到家庭控制内联网6。

[0044] USB钥匙设备34和锁设备61需要通过因特网2的彼此的路由信息，以便能够在它们之间基于数据链路层或网络层来建立端到端数据传输连接，在图1的例子中是VPN数据传输连接41。所确定的实时路由信息经由连接42由USB钥匙设备34和锁设备61二者保存在因特网上的远程控制网络服务器21中。

[0045] 为了使建立数据传输连接是可能的，USB钥匙设备34和锁设备61必须确定从它们自己的网络至少一直到因特网2的其实际网络路径。可以用USB钥匙设备34和锁设备61有利地能够利用的若干种已知的方式做出该网络路径确定。

[0046] 在图1的例子中，使本地网络与因特网分离的NAT防火墙31(FW2)和51(FW1)有利地不限制外发的UDP业务(用户数据报协议)。因而，在图1的例子中，当远程控制钥匙设备34和

锁设备61知道彼此的IP地址时，在数据链路层中，以太网级连接可在它们之间建立。

[0047] 也在防火墙31和/或51至少在一些连接过程中限制外发业务的那些情况中，可通过使用适当的其它业务协议来通过防火墙，且借助于此可以在USB钥匙设备34和锁设备61之间建立数据传输连接。

[0048] 当在根据图1的远程控制系统1中期望在连接到USB钥匙设备34的数据处理设备32和锁设备61之间建立虚拟专用网(VPN)41时，则在第一步骤中，设备34和61二者都经由数据传输连接42通过对应设备从远程控制网络服务器21获取保存在其中的路由信息。在移交路由信息之前，远程控制网络服务器21检查到它实际上是被允许的USB钥匙设备-锁设备对的问题。之后，借助于所获取的路由信息，USB钥匙设备34和锁设备61在它们之间建立直接VPN连接41。当VPN连接41完成时，在数据传输网络3中的数据处理设备32可进行与在房屋控制网络6中的一个或多个设备62、63、64或65的连接。

[0049] 图2示出如何在建立并行的新USB钥匙设备的操作权——所谓的可信关系——时利用现有的USB钥匙设备的示例性流程图。在下文中，这些钥匙设备被称为USB钥匙设备1和USB钥匙设备2。也可用图1的参考数字34指代USB钥匙设备1。在可信关系的建立方法中，利用使用私有PKI密钥加密的消息(公共密码密钥方法)。设备向彼此发送使用自己的私有PKI密钥加密的消息，所述消息可由具有发送设备的已知公共PKI密钥的接收设备打开。使用与所接收的消息有关的发送者的证书来确认消息的发送者，该证书为接收设备所已知。证书、私有密码密钥和公共密码密钥一起形成在PKI方法的使用中必要的信息。

[0050] 步骤200描述远程控制布置在工作顺序中和在使用中的情形。因此，至少一个锁设备61连接到远程控制系统1。在该状态中，锁设备61不断地准备从其USB钥匙设备34(USB钥匙设备1)或从图1所示的远程控制网络服务器21接收消息。

[0051] 在步骤210中，开始建立并行于现有的钥匙设备1(在图1中的参考数字34)的新USB钥匙设备2与锁设备61的可信关系。USB钥匙设备1和2二者都具有它们可连接到在使用中的数据处理设备32的USB端口的种类。当USB钥匙设备1和USB钥匙设备2二者同时连接到数据处理设备32的两个USB端口时，可信关系的建立过程开始，需要这些钥匙设备对至少一个锁设备的操作权。之后，使用数据处理设备32激活在远程控制中利用的软件。该软件可预先安装在数据处理设备32中，或数据处理设备启动在USB钥匙设备34(USB钥匙设备1)中的所述程序的执行。

[0052] 在该步骤中，与USB钥匙设备1已配对的所有锁设备(也就是说，在它们之间有可信关系)显示在数据处理设备32的屏幕上。从该列表中选择新USB钥匙设备2需要与其配对的一个或多个锁设备。形成关于在配对中涉及的每个锁设备的选择的单独消息，该消息包括新USB钥匙设备2的证书和公共PKI密钥。使用USB钥匙设备1的私有PKI密钥签名待发送的消息。该消息可例如形成如下：

[0053] 至：锁61

[0054] 自：钥匙1

[0055] 消息：允许从钥匙2连接

[0056] 配对许可：否

[0057] 设置模式：锁

[0058] 证书：<钥匙2证书>

[0059] 签名:<钥匙1签名>。

[0060] 在步骤220中,在数据处理设备32中操作的远程控制软件将消息发送到在步骤210中形成的锁设备61,该消息的签名使用USB钥匙设备1的私有密码密钥被加密。

[0061] 在步骤230中,锁设备61首先从USB钥匙设备1接收消息。接着,使用USB钥匙设备1的已知公共PKI密钥,它打开消息和相关钥匙设备1的签名。之后,锁设备61也读取包括在消息中的其它USB钥匙设备2的证书。

[0062] 在步骤240中,锁设备61比较与USB钥匙设备1的所接收的签名有关的证书与保存在其自己的存储器中的USB钥匙设备1的证书。如果在比较中没有匹配,则过程在步骤280结束。

[0063] 如果在步骤240中的比较的结果示出消息由USB钥匙设备1发送,则过程继续到步骤250。

[0064] 在步骤250中,锁设备61建立与新USB钥匙设备2的所请求的可信关系,并因此将USB钥匙设备2的证书保存在其存储器中。之后,锁设备61将所形成的可信关系的确认发送到USB钥匙设备1。

[0065] 在步骤260中,USB钥匙设备1首先接收由锁设备61发送的关于建立可信关系的消息,且在那之后将已知锁设备61的证书保存在USB钥匙设备2的存储器中。

[0066] 在此之后,USB钥匙设备2可用作锁设备61的钥匙设备(步骤270)。

[0067] 图3示出为当建立在两个单独的锁设备之间的可信关系时如何利用现有的USB钥匙设备的示例性流程图,所述锁设备具有与同一USB钥匙设备的现有可信关系。在下文中,钥匙设备被称为USB钥匙设备,且锁设备被称为锁设备1和锁设备2。也可使用图1的参考数字34指代USB钥匙设备。可信关系的建立方法基于私有和公共PKI密钥的使用(公共密码密钥方法)。钥匙设备和锁设备1和2都向彼此发送使用它们的私有PKI密钥签名的消息,接收设备能够使用发送设备的相应已知公共PKI密钥打开。接收设备使用与消息有关的发送设备的证书来验证消息真正由签名的可信设备发送。

[0068] 步骤300描述远程控制布置在工作顺序中和在使用中的情形。因此,至少锁设备1和2连接到远程控制系统1。在该状态中,锁设备1和2不断地准备从其USB钥匙设备34(USB钥匙设备)或从图1所示的远程控制网络服务器21接收消息。

[0069] 在步骤310中,在锁设备1和2之间开始可信关系的建立。当USB钥匙设备连接到数据处理设备32的USB端口时,开始可信关系的建立过程,通过使用该钥匙设备,期望建立在锁设备1和2之间的可信关系。之后,使用数据处理设备32来激活在锁设备的远程控制中利用的软件。该软件可预先安装在数据处理设备32中,或数据处理设备启动在USB钥匙设备中的所述程序的执行。

[0070] 在该步骤中,与相应的USB钥匙设备已配对的所有锁设备(即,在它们之间有可信关系)显示在数据处理设备32的屏幕上。在图3的例子中,从该列表中选择需要在其之间建立可信关系的锁设备1和锁设备2。同时,确定可信关系的特性,即,锁设备将稍后与彼此建立网络的方式。在图3的例子中,建立可信关系的目的是在锁设备1和2之间建立VPN数据传输连接。在选择锁设备之后,创建两个锁设备的单独消息,所述消息包括待建立的可信关系的特性。使用USB钥匙设备的私有PKI密钥来签名待发送的消息,且发送USB钥匙设备的证书包括在该消息中。

[0071] 在步骤320中，使用在数据处理设备32中操作的远程控制软件，创建在可信关系的建立中必要的到锁设备1和2的消息。

[0072] 稍后用作服务器的锁设备1的消息可优选地被形成如下：

[0073] 至：锁1

[0074] 自：钥匙

[0075] 命令：允许从锁2连接

[0076] 配对许可：否

[0077] 设置模式：锁

[0078] 证书：<锁2证书>

[0079] 签名：<钥匙签名>。

[0080] 充当稍后用作服务器的锁设备1的客户端设备(从设备)的锁设备2的消息可优选地被形成如下：

[0081] 至：锁2

[0082] 自：钥匙

[0083] 命令：允许从锁1连接

[0084] 配对许可：否

[0085] 设置模式：子锁

[0086] 证书：<锁1证书>

[0087] 签名：<钥匙签名>。

[0088] 在步骤320结束时，在数据处理设备32中操作的远程控制软件向锁设备1和2发送关于建立可信关系的形成的消息，所述消息使用USB钥匙设备的私有PKI密钥被加密。在传输消息时，有利地使用所谓的媒介(Matchmaking)服务。

[0089] 在步骤330中，锁设备1和2首先接收由USB钥匙设备发送到相应的锁设备的关于建立可信关系的消息。接着，它使用已知的USB钥匙设备的公共PKI密钥打开消息。锁设备检查到发送USB钥匙设备的签名相应于在它们的存储器中的USB钥匙设备的签名。在这之后，锁设备也读取包括在消息中的其它锁设备的证书。

[0090] 在步骤340中，锁设备1和2将所接收的与USB钥匙设备的签名有关的USB钥匙设备的证书与保存在它自己的存储器中的USB钥匙设备的证书进行比较。如果在比较中没有匹配，则过程在步骤380结束。

[0091] 如果在步骤340中的比较的结果示出消息由USB钥匙设备发送，则过程在锁设备1和2二者中继续到步骤350。

[0092] 在步骤350中，锁设备1和2在它们本身之间建立所需的可信关系，并因此将彼此的证书保存在其自己的存储器中。之后，锁设备也将所形成的可信关系的确认发送到USB钥匙设备。

[0093] 在步骤360中，锁设备1和锁设备2在它们本身之间借助于对应方的已知证书形成VPN网络，其中锁设备1用作服务器设备(主设备)。在两个锁设备之间的VPN专用网络的建立过程类似于结合图1公开的内容，其中VPN专用网络在一个USB钥匙设备和一个锁设备之间建立。

[0094] 之后，来自USB钥匙设备的所有消息总是经由锁设备1行进到锁设备2，步骤370。

[0095] 在图2和3中所示的所有过程步骤可使用在适当的通用或专用处理器中执行的计算机程序命令来实现。计算机命令可存储在例如数据磁盘或存储器的计算机可读介质中，处理器可从所述计算机可读介质获取所述计算机程序命令并运行它们。对计算机可读介质的提及可例如也包含专用部件，例如可编程USB闪速存储器、逻辑阵列(FPLA)、专用集成电路(ASIC)和信号处理器(DSP)。

[0096] 图4示出USB钥匙设备34的功能上的主要部分。USB钥匙设备34可包括一个或几个密码处理器341。处理器或处理器装置可包括算术逻辑单元、一组不同的寄存器和控制电路。密码处理器341有利地包括内部存储器单元，单独的私有密码密钥3421存储在该内部存储器单元中。

[0097] 例如闪速存储器单元或存储器装置342的数据存储布置连接到处理器装置，在数据存储布置中可存储计算机可读信息或程序或用户信息。存储器装置342一般包含允许读和写功能二者的存储器单元(随机存取存储器，RAM)，和包含非易失性存储器的、数据只可从中读取的存储器单元(只读存储器，ROM)。USB钥匙设备34的证书、私有和公共PKI密钥、USB钥匙设备的当前网络路径信息、用作其设备对的锁设备的识别信息、证书、设备对的公共PKI密钥以及在VPN连接的建立中被利用的USB钥匙设备34的操作所必需的所有程序有利地存储在存储器装置342中。

[0098] 存储在远程控制钥匙设备34的存储器中的程序的一些例子是操作系统(例如Linux)、TCP/IP程序、VPN程序(例如OpenVPN)、DHCP客户端设备/服务器程序(例如ISC DHCP)、数据库程序(例如SQLite)、证书管理/确认程序(例如GPG)和用户接口库(例如LuCI)。

[0099] USB钥匙设备34还包括接口元件，其包括用于接收或发送信息的输入/输出或输入/输出装置343。使用输入装置接收的信息被传输以由远程控制钥匙设备34的密码处理器341处理。USB钥匙设备34的接口元件有利地用于将信息从USB钥匙设备34的存储器装置342传输到外部数据处理设备32或锁设备61(在图1的例子中)。相应地，可经由接口元件例如从数据处理设备32接收信息或命令，USB钥匙设备34连接到数据处理设备32。

[0100] 关于操作权的级别，存在上面描述的USB钥匙设备34的至少两个级别，例如管理员和基本用户级钥匙设备。较高操作权级别的用户/所有者(例如管理员)对较低级别(例如基本用户)上的远程控制钥匙设备34的用户(例如基本用户)的所有控制目标有控制权。另一方面，较低级别钥匙设备操作权级别的所有者不能访问除了他自己的目标以外的较高操作权级别的任何其它控制目标。

[0101] 上面描述了根据本发明的方法和设备的一些有利的实施例。本发明不限于上述解决方案，而是本发明的思想可以以在权利要求的范围内的很多方式来应用。

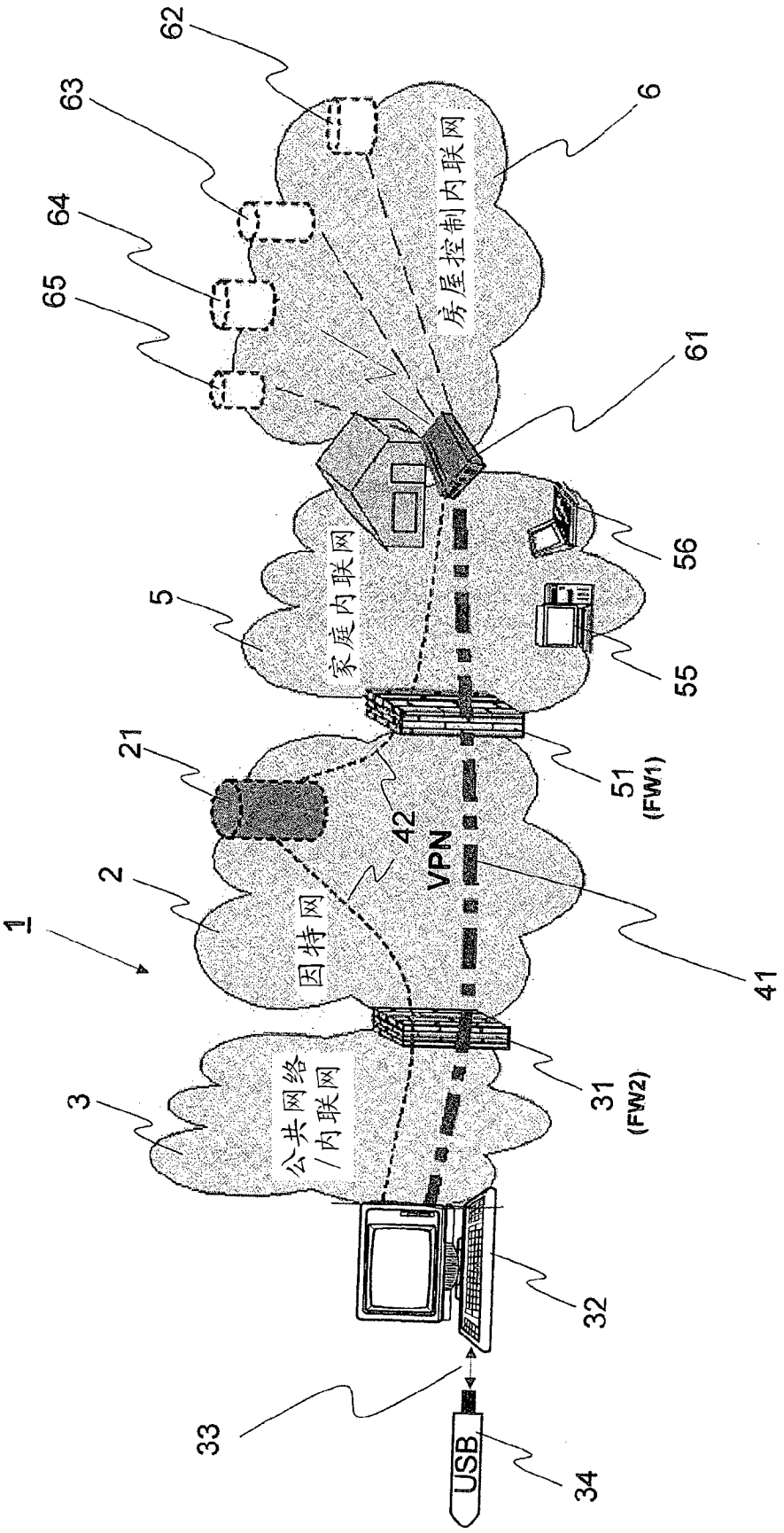

62
63
64
65
6
房屋控制内联网
61
56
55
5
家庭内联网
51
(FW1)
21
42
VPN
2
因特网
41
1
31
(FW2)
3
公共网络
/内联网
32
33
USB
34

图 1

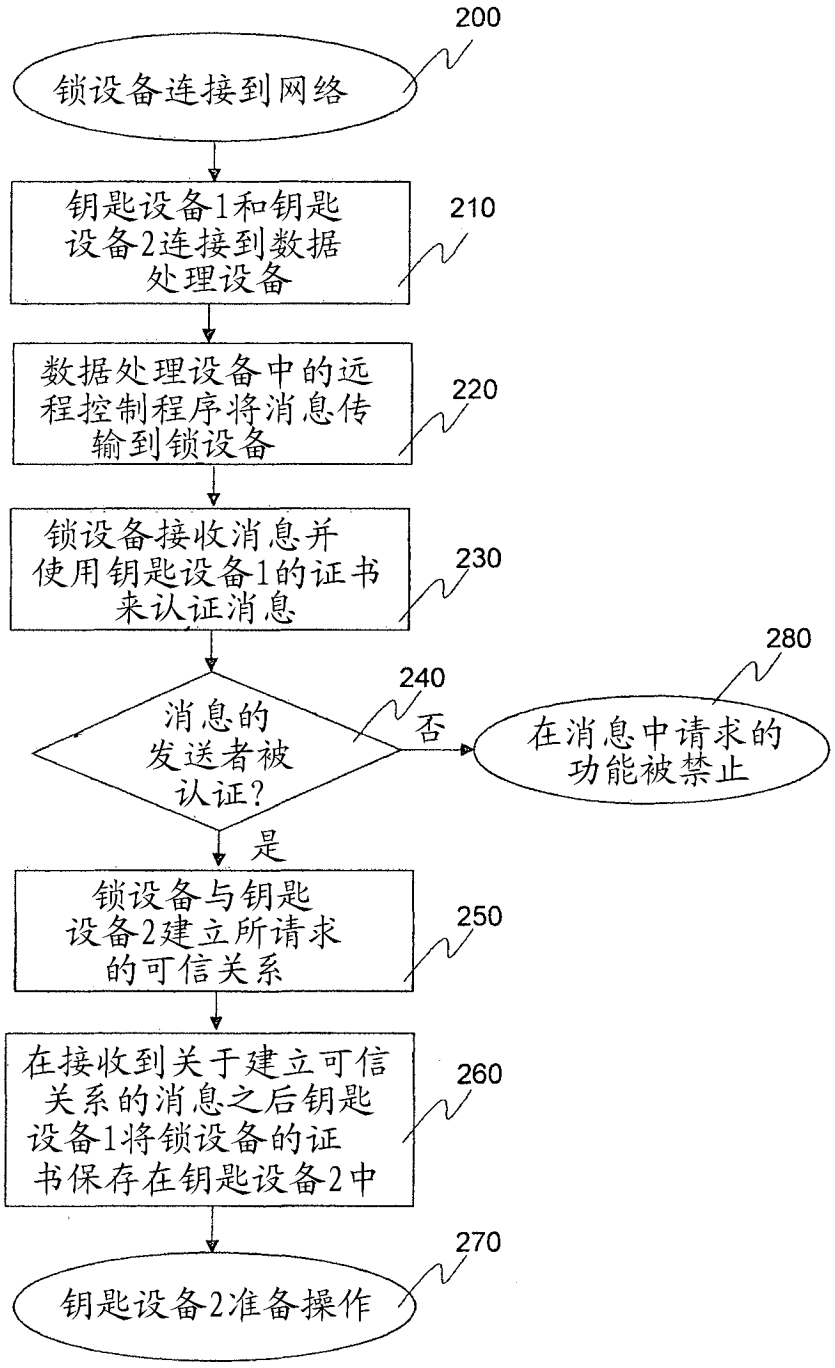

200
锁设备连接到网络
210
钥匙设备1和钥匙设备2连接到数据处理设备
220
数据处理设备中的远程控制程序将消息传输到锁设备
230
锁设备接收消息并使用钥匙设备1的证书来认证消息
240
消息的发送者被认证?
否
280
在消息中请求的功能被禁止
是
250
锁设备与钥匙设备2建立所请求的可信关系
260
在接收到关于建立可信关系的消息之后钥匙设备1将锁设备的证书保存在钥匙设备2中
270
钥匙设备2准备操作

图 2

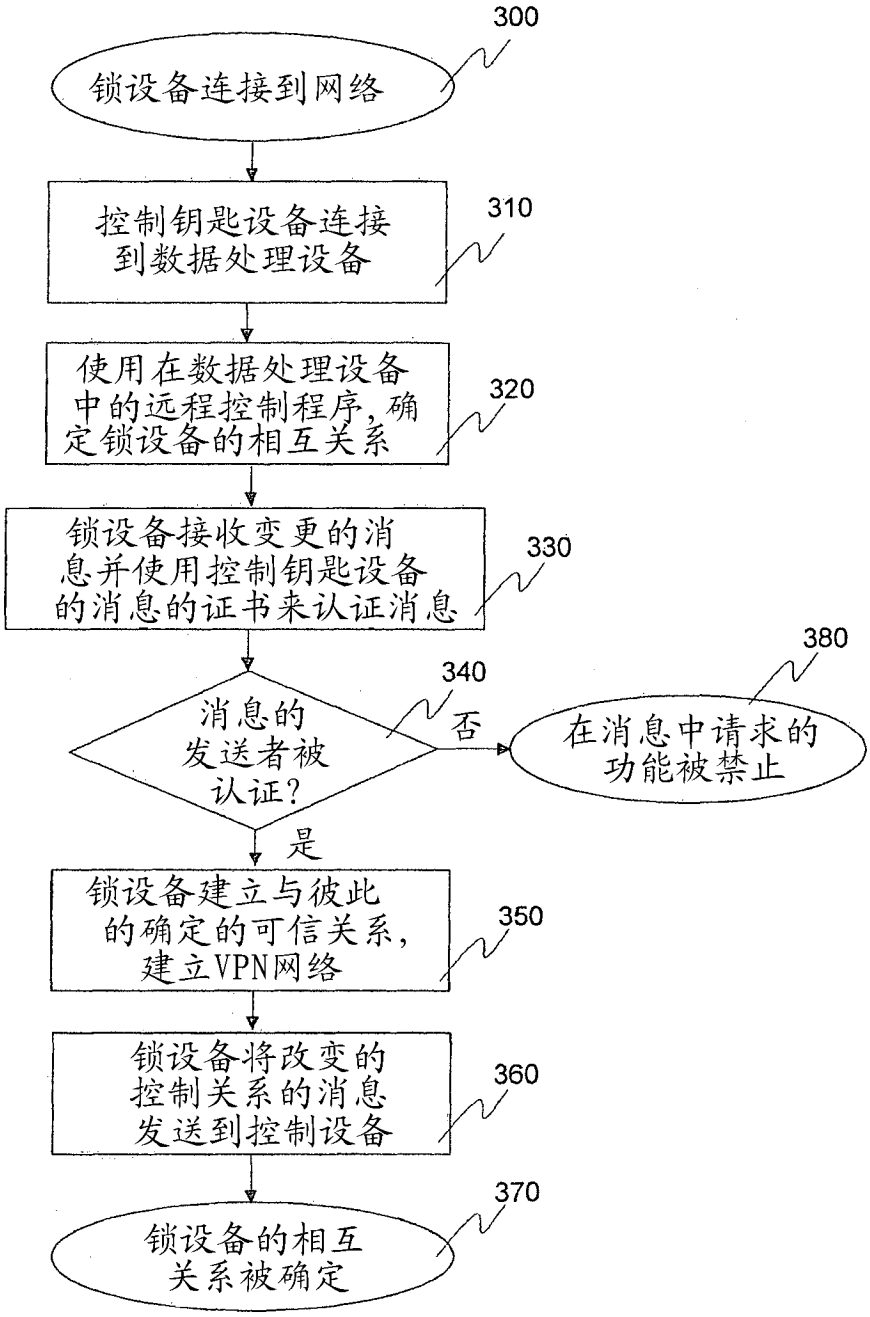

300
锁设备连接到网络
310
控制钥匙设备连接到数据处理设备
320
使用在数据处理设备中的远程控制程序，确定锁设备的相互关系
330
锁设备接收变更的消息并使用控制钥匙设备的消息的证书来认证消息
340
消息的发送者被认证？
否
380
在消息中请求的功能被禁止
是
350
锁设备建立与彼此的确定的可信关系，建立VPN网络
360
锁设备将改变的控制关系的消息发送到控制设备
370
锁设备的相互关系被确定

图 3

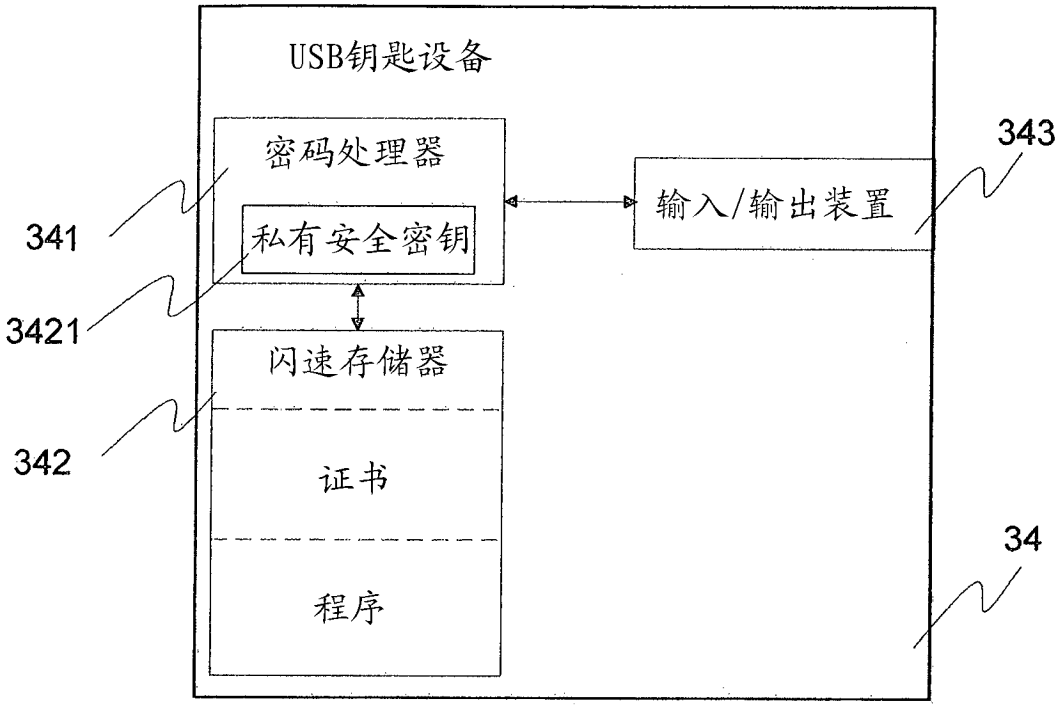


图 4