(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 108573551 A
(43)申请公布日 2018.09.25

(21)申请号 201810187762.5

(22)申请日 2018.03.07

(30)优先权数据
2017-045103 2017.03.09 JP

(71)申请人 丰田自动车株式会社
地址 日本爱知县丰田市

(72)发明人 藤原靖久 辻村宽子 春名雄一郎 前川觉

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 唐京桥 董娟

(51)Int.Cl.
G07C 9/00(2006.01)

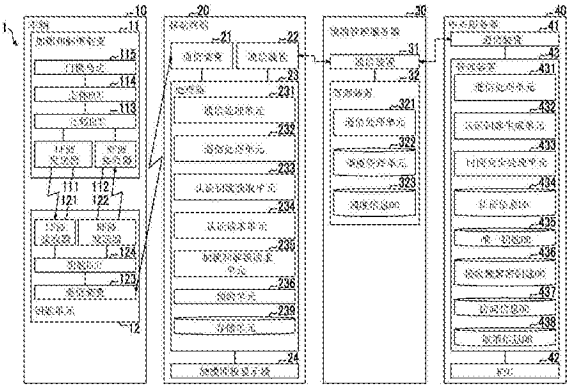
权利要求书3页 说明书25页 附图10页

(54)发明名称

加锁和解锁系统、钥匙单元和服务器

(57)摘要

本发明公开了一种加锁和解锁系统、钥匙单元和服务器，所述加锁和解锁系统包括服务器、移动终端和设置在车辆等中的钥匙单元。所述服务器将对于车辆等的取消信息发送至钥匙单元。所述移动终端将认证信息和用于请求车辆等的门的加锁和解锁的请求信号发送至钥匙单元。所述钥匙单元包括：第一接收单元，其从服务器接收取消信息；第二接收单元，其从移动终端接收认证信息和请求信号；认证单元，其当已经接收到认证信息时基于所述认证信息来认证所述移动终端；以及加锁和解锁处理单元，其当认证已经成功并且已经接收到请求信号时加锁和解锁车辆等。当接收到的取消信息指示已经取消了车辆等的预约时，加锁和解锁处理单元禁止车辆等的解锁。



CN 108573551 A

1.一种加锁和解锁系统，其特征在于包括：

服务器，其被配置成存储关于车辆或设施的预约的信息；

移动终端，其被配置成与所述服务器进行通信；以及

钥匙单元，其被配置成对所述车辆或设施的门解锁或加锁，所述钥匙单元设置在所述车辆或设施中，

其中，所述服务器包括服务器发送单元，所述服务器发送单元被配置成将指示所述车辆或设施的预约是否已被取消的取消信息发送至所述钥匙单元，

其中，所述移动终端包括终端发送单元，所述终端发送单元被配置成将与所述车辆或设施的预约相关的第一认证信息和用于请求所述车辆或设施的门的解锁或加锁的第一请求信号发送至所述钥匙单元，

其中，所述钥匙单元包括：

钥匙单元第一接收单元，其被配置成从所述服务器接收所述取消信息；

钥匙单元第二接收单元，其被配置成从所述移动终端接收所述第一认证信息和所述第一请求信号；

第一认证单元，其被配置成当所述钥匙单元第二接收单元已经接收到所述第一认证信息时基于所述第一认证信息来认证所述移动终端；以及

加锁和解锁处理单元，其被配置成当所述第一认证单元对所述移动终端的认证已经成功并且所述钥匙单元第二接收单元已经接收到所述第一请求信号时，执行对所述车辆或设施的门解锁或加锁的过程，以及

其中，所述加锁和解锁处理单元被配置成：当所述第一认证单元对所述移动终端的认证已经成功并且由所述钥匙单元第一接收单元接收到的取消信息指示已经取消了与用于所述第一认证单元对所述移动终端的认证的第一认证信息相对应的所述车辆或设施的预约时，禁止基于从所述移动终端发送的用于请求解锁所述车辆或设施的门的第一请求信号来对所述车辆或设施的门进行解锁。

2.根据权利要求1所述的加锁和解锁系统，其特征在于，所述钥匙单元包括钥匙单元发送单元，所述钥匙单元发送单元被配置成：当所述第一认证单元对所述移动终端的认证已经成功时，将第二请求信号发送至所述服务器，所述第二请求信号包括针对与用于所述第一认证单元对所述移动终端的认证的第一认证信息相对应的取消信息的请求，

其中，所述服务器包括服务器接收单元，所述服务器接收单元被配置成接收从所述钥匙单元发送的所述第二请求信号，以及

其中，所述服务器发送单元被配置成：当所述服务器接收单元已经接收到所述第二请求信号时，将包括所述取消信息的响应信号发送至所述钥匙单元。

3.根据权利要求2所述的加锁和解锁系统，其特征在于，所述钥匙单元包括被配置成执行计时的钥匙单元计时器，

其中，所述服务器包括服务器计时器，所述服务器计时器被配置成以比所述钥匙单元计时器更高的精度来执行计时；

其中，所述移动终端包括中继单元，所述中继单元被配置成接收从所述服务器和所述钥匙单元中的一个向所述服务器和所述钥匙单元中的另一个发送的信号，并且将所接收到的信号发送至所述服务器和所述钥匙单元中的所述另一个，

其中，所述钥匙单元发送单元被配置成将包括向所述服务器的对所述取消信息的请求和对所述服务器计时器的时间的请求的第二请求信号发送至所述移动终端，

其中，所述中继单元被配置成从所述钥匙单元接收所述第二请求信号并且将所述第二请求信号发送至所述服务器，

其中，所述服务器接收单元被配置成从所述移动终端接收所述第二请求信号，

其中，所述服务器发送单元被配置成：当所述服务器接收单元已经接收到所述第二请求信号时，将包括所述取消信息和所述服务器计时器的时间的对所述钥匙单元的响应信号发送至所述移动终端，

其中，所述中继单元被配置成从所述服务器接收所述响应信号并且将所述响应信号发送至所述钥匙单元，

其中，所述钥匙单元第一接收单元被配置成从所述移动终端接收所述响应信号，以及

其中，所述钥匙单元计时器被配置成基于包括在所述钥匙单元第一接收单元接收的响应信号中的所述服务器计时器的时间来与所述服务器计时器同步。

4.根据权利要求1至3中任一项所述的加锁和解锁系统，其特征在于，还包括安装在所述车辆或设施中的加锁和解锁装置，

其中，所述钥匙单元包括存储单元，所述存储单元被配置成存储与所述车辆或设施相关的第二认证信息。

其中，所述加锁和解锁装置包括：

加锁和解锁装置接收单元，其被配置成从所述钥匙单元接收包括所述第二认证信息的第三请求信号；

第二认证单元，其被配置成当所述加锁和解锁装置接收单元已经接收到所述第三请求信号时基于包括在所述第三请求信号中的第二认证信息来认证所述钥匙单元；以及

加锁和解锁控制单元，其被配置成当所述第二认证单元进行的认证已经成功时对所述车辆或设施的门解锁或加锁，以及

其中，所述加锁和解锁处理单元被配置成在对所述车辆或设施的门解锁或加锁的过程中将包括所述第二认证信息的第三请求信号发送至所述加锁和解锁装置。

5.一种钥匙单元，其被配置成响应于从移动终端发送的用于请求车辆或设施的解锁或加锁的第一请求信号来解锁或加锁所述车辆或设施的门，所述钥匙单元设置在所述车辆或设施中，所述钥匙单元的特征在于包括：

钥匙单元第一接收单元，其被配置成从用于存储关于所述车辆或设施的预约的信息的服务器接收指示所述车辆或设施的预约是否已经被取消的取消信息；

钥匙单元第二接收单元，其被配置成从所述移动终端接收与所述车辆或设施的预约相关的第一认证信息和用于请求解锁或加锁所述车辆或设施的门的第一请求信号；

第一认证单元，其被配置成当所述钥匙单元第二接收单元已经接收到所述第一认证信息时基于所述第一认证信息来认证所述移动终端；以及

加锁和解锁处理单元，其被配置成：当所述第一认证单元对所述移动终端的认证已经成功并且所述钥匙单元第二接收单元已经接收到所述第一请求信号时，执行解锁或加锁所述车辆或设施的门的过程，

其中，所述加锁和解锁处理单元被配置成：当所述第一认证单元对所述移动终端的认

证已经成功并且由所述钥匙单元第一接收单元接收到的取消信息指示已经取消了与用于所述第一认证单元对所述移动终端的认证的第一认证信息相对应的所述车辆或设施的预约时，禁止基于从所述移动终端发送的用于请求解锁所述车辆或设施的门的第一请求信号来对所述车辆或设施的门进行解锁。

6.一种服务器，所述服务器被配置成与钥匙单元进行通信并且存储关于车辆或设施的预约的信息，所述钥匙单元被配置成响应于从移动终端发送的用于请求所述车辆或设施的解锁或加锁的第一请求信号来对所述车辆或设施的门进行解锁或加锁，所述钥匙单元设置在所述车辆或设施中，所述服务器的特征在于包括：

服务器发送单元，其被配置成将指示所述车辆或设施的预约是否已经被取消的取消信息发送至所述钥匙单元。

加锁和解锁系统、钥匙单元和服务器

技术领域

[0001] 本发明涉及一种加锁和解锁系统、钥匙单元和服务器。

背景技术

[0002] 已经公开了一种钥匙管理系统，该系统通过移动终端经由网络从服务器接收用于解锁车辆的钥匙信息(即，用于确定车辆侧是否允许解锁的认证信息)并且该移动终端可以被用作电子钥匙(例如，参见日本未审查专利申请公开第2006-118122号(JP2006-118122A)等)。

[0003] 例如，当多个用户在不同时区共享和使用特定车辆(例如租用车、共享车或公司车)时，通过采用这种配置，可以解决交付电子钥匙等的问题，并且改善了用户的便利性。

[0004] 相同的技术可以用于对由多个用户在不同时间段使用的相同设施(诸如会议室、度假屋或体育馆的设施)执行加锁和解锁，并且通过使用移动终端作为安装在设施中的加锁和解锁装置的电子钥匙来改善用户的便利性。

发明内容

[0005] 可构想的是，即使在移动终端不能访问通信网络来访问服务器的情况下，也可采用预先从服务器或预定终端获可以取认证信息以解锁车辆或设施的配置。

[0006] 然而，在允许预先获得认证信息的情况下，即使移动终端被盗或移动终端被用户丢失然后取消了车辆或设施的预约，已经获得存储了预先获取的认证信息的移动终端的恶意第三方也有可能不适当地使用车辆或设施。

[0007] 因此，本发明提供一种加锁和解锁系统，即使在可以预先获取认证信息的情况下，该系统也可以防止已经获得存储了预先获取的认证信息的移动终端的恶意第三方不适当地使用车辆或设施。

[0008] 根据本发明的第一方面，提供了一种加锁和解锁系统，包括：服务器，其被配置成存储关于车辆或设施的预约的信息；移动终端，其被配置成与服务器进行通信；以及钥匙单元，其被配置成解锁或加锁车辆或设施的门，所述钥匙单元设置在车辆或设施中，其中，所述服务器包括服务器发送单元，所述服务器发送单元被配置成将指示是否已经取消所述车辆或设施的预约的取消信息发送至钥匙单元，所述移动终端包括终端发送单元，所述终端发送单元被配置成将与车辆或设施的预约相关的第一认证信息和用于请求车辆或设施的门的解锁或加锁的第一请求信号发送至钥匙单元，所述钥匙单元包括：钥匙单元第一接收单元，其被配置成从服务器接收取消信息；钥匙单元第二接收单元，其被配置成从移动终端接收第一认证信息和第一请求信号；第一认证单元，其被配置成当钥匙单元第二接收单元已经接收到第一认证信息时基于第一认证信息来认证移动终端；以及加锁和解锁处理单元，其被配置成当第一认证单元对移动终端的认证已经成功并且钥匙单元第二接收单元已经接收到第一请求信号时执行解锁或加锁车辆或设施的门的过程，以及所述加锁和解锁处理单元被配置成：当第一认证单元对移动终端的认证已经成功并且钥匙单元第一接收单元

接收到的取消信息指示已经取消了与用于第一认证单元对移动终端的认证的第一认证信息相对应的车辆或设施的预约时，禁止基于从移动终端发送的用于请求门的解锁的第一请求信号来进行车辆或设施的门的解锁。

[0009] 根据该方面，服务器将车辆或设施的预约的取消信息发送至钥匙单元，并且钥匙单元基于从服务器收到的取消信息来确认是否已经取消与用于认证的第一认证信息相对应的车辆或设施的预约。当已经取消了与用于移动终端的认证的第一认证信息相对应的预约时，钥匙单元(加锁和解锁处理单元)禁止车辆或设施的解锁。因此，即使当恶意第三方已经获得了其中预先获取并存储了第一认证信息的移动终端时，也禁止例如通过使移动终端的用户使用任何方法取消车辆或设施的预约而使移动终端对车辆或设施进行解锁。因此，可以防止恶意第三方不适当地使用车辆或设施。

[0010] 在该方面中，钥匙单元可以包括钥匙单元发送单元，所述钥匙单元发送单元被配置成：当由第一认证单元对移动终端的认证已经成功时，将包括对与用于第一认证单元对移动终端的认证的第一认证信息相对应的取消信息的请求的第二请求信号发送至服务器，所述服务器可以包括服务器接收单元，所述服务器接收单元被配置成接收从钥匙单元发送的第二请求信号，以及所述服务器发送单元可以被配置成当服务器接收单元已经接收到第二请求信号时将包括取消信息的响应信号发送至钥匙单元。

[0011] 根据该方面，当基于从移动终端发送的第一认证信息的认证已经成功时，钥匙单元可以将与第一认证信息相对应的用于请求关于车辆或设施的预约的取消信息的第二请求信号发送至服务器，并从服务器获取取消信息。因此，即使当已经获得了其中存储了预先获取的第一认证信息的移动终端的恶意第三方成功认证移动终端时，也会在认证成功作为触发的情况下将第二请求信号从钥匙单元立即发送至服务器，并且响应于第二请求信号可以禁止基于从服务器发送的取消信息来使用移动终端解锁车辆或设施。因此，可以防止恶意第三方不适当地使用车辆或设施。

[0012] 在该方面中，所述钥匙单元可以包括被配置成执行计时的钥匙单元计时器，所述服务器可以包括服务器计时器，所述服务器计时器被配置成以比钥匙单元计时器的精度高的精度执行计时，所述移动终端可以包括中继单元，所述中继单元被配置成接收从服务器和钥匙单元中的一者发送至另一者的信号，并且将所接收到的信号发送至所述另一者，所述钥匙单元发送单元被配置成将包括向所述服务器的对所述取消信息的请求和对所述服务器计时器的时间的请求的第二请求信号发送至所述移动终端，中继单元可以被配置成从钥匙单元接收第二请求信号并将第二请求信号发送至服务器，服务器接收单元可以被配置成从移动终端接收第二请求信号，服务器发送单元可以被配置成当服务器接收单元已经接收到第二请求信号时将包括取消信息和服务器计时器的时间的对钥匙单元的响应信号发送至移动终端，中继单元可以被配置成从服务器接收响应信号并且将响应信号发送至钥匙单元，所述钥匙单元第一接收单元可以被配置成从移动终端接收响应信号，以及钥匙单元计时器可以被配置成基于包括在由钥匙单元第一接收单元所接收的响应信号中的服务器计时器的时间来与服务器计时器同步。

[0013] 根据该方面，钥匙单元基于从服务器发送的服务器计时器的时间使具有相对低精度的钥匙单元计时器的时间与服务器计时器同步。在钥匙单元与服务器之间的通信经由移动终端来执行。钥匙单元将包括对取消信息的请求和对服务器计时器的时间的请求的第二

请求信号经由移动终端发送至服务器，并且服务器响应于第二请求信号的接收将包括取消信息和服务器计时器的时间的响应信号经由移动终端发送至钥匙单元。因此，钥匙单元需要在其可以与移动终端进行通信的状态下执行具有相对低精度的钥匙单元计时器的时间的同步。在这种情况下，可以通过采用如下配置来实现服务器、移动终端和钥匙单元之间的通信效率的提高：在该配置中，在可以与移动终端进行通信的状态下执行的移动终端的认证成功作为触发的情况下，发送包括发送到服务器的对取消信息的获取请求和对服务器(服务器计时器)的时间的获取请求的第二请求信号，并且取消信息和时间信息同时从服务器获取。

[0014] 在该方面中，加锁和解锁系统还可以包括安装在车辆或设施中的加锁和解锁装置，所述钥匙单元可以包括存储单元，所述存储单元被配置成存储与车辆或设施相关的第二认证信息，所述加锁和解锁装置可以包括：加锁和解锁装置接收单元，其被配置成接收来自钥匙单元的包括第二认证信息的第三请求信号；第二认证单元，其被配置成当加锁和解锁装置接收单元已经接收到第三请求信号时，基于第三请求信号中包括的第二认证信息来认证钥匙单元；以及加锁和解锁控制单元，其被配置成当由第二认证单元的认证已经成功时解锁或加锁车辆或设施的门，以及加锁和解锁处理单元可以被配置成在解锁或加锁车辆或设施的门的过程中将包括第二认证信息的第三请求信号发送至加锁和解锁装置。

[0015] 根据该方面，钥匙单元可以通过将第二请求信号发送至设置在车辆等中的加锁和解锁装置来解锁车辆或设施。因此，例如，加锁和解锁系统可以被实施为其中钥匙单元被添加到已经安装在车辆或设施中的加锁和解锁装置的配置。

[0016] 根据本发明的第二方面，提供了一种钥匙单元，所述钥匙单元被配置成响应于从移动终端发送的用于请求车辆或设施的解锁或加锁的第一请求信号来解锁或加锁车辆或设施的门，所述钥匙单元设置在车辆或设施中，所述钥匙单元包括：钥匙单元第一接收单元，其被配置成从存储关于车辆或设施的预约的信息的服务器接收指示是否已经取消车辆或设施的预约的取消信息；钥匙单元第二接收单元，其被配置成从移动终端接收与车辆或设施的预约相关的第一认证信息和用于请求解锁或加锁车辆或设施的门的第一请求信号；第一认证单元，其被配置成当钥匙单元第二接收单元已经接收到第一认证信息时基于第一认证信息来认证移动终端；以及加锁和解锁处理单元，其被配置成当第一认证单元对移动终端的认证已经成功并且钥匙单元第二接收单元已经接收到第一请求信号时执行解锁或加锁车辆或设施的门的过程，其中，所述加锁和解锁处理单元被配置成：当第一认证单元对移动终端的认证已经成功并且由钥匙单元第一接收单元接收到的取消信息指示已经取消了与用于第一认证单元对移动终端的认证的第一认证信息相对应的车辆或设施的预约时，禁止基于从移动终端发送的用于请求解锁门的第一请求信号来进行车辆或设施的门的解锁。

[0017] 根据本发明的第三方面，提供了一种服务器，所述服务器被配置成与钥匙单元进行通信并且存储关于车辆或设施的预约的信息，所述钥匙单元被配置成响应于从移动终端发送的用于请求解锁或加锁车辆或设施的第一请求信号来解锁或加锁车辆或设施的门，所述钥匙单元设置在车辆或设施中，所述服务器包括：服务器发送单元，其被配置成将指示是否已经取消车辆或设施的预约的取消信息发送至钥匙单元。

[0018] 根据这些方面，可以提供一种加锁和解锁系统，即使在可以预先获取认证信息的

情况下，也可以防止已经获得存储了预先获取的认证信息的移动终端的恶意第三方不适当地使用车辆或设施。

附图说明

[0019] 下面将参照附图来描述本发明的示例性实施方式的特征、优点以及技术和工业意义，在附图中相同的附图标记表示相同的元件，并且其中：

[0020] 图1是示意性地示出根据本发明的一个方面的加锁和解锁系统的配置的示例的框图；

[0021] 图2是示意性地示出根据本发明的一个方面的加锁和解锁装置以及钥匙单元的配置的示例的框图；

[0022] 图3是示意性地示出根据本发明的一个方面的加锁和解锁系统中从车辆的预约到由移动终端获取认证钥匙的操作的示例的顺序图；

[0023] 图4是示意性地示出根据本发明的一个方面的由移动终端的处理器所执行的开始加锁和解锁功能的过程(加锁和解锁功能开始过程)的示例的流程图；

[0024] 图5是示意性地示出根据本发明的一个方面的由钥匙单元的钥匙ECU执行的移动终端认证过程的示例的流程图；

[0025] 图6是示意性地示出根据本发明的一个方面的加锁和解锁系统的与由移动终端执行的加锁和解锁功能开始过程和由钥匙单元执行的移动终端认证过程相对应的操作的示例的顺序图；

[0026] 图7是示意性地示出根据本发明的一个方面的由钥匙单元的钥匙ECU执行的时间更新过程的示例的流程图；

[0027] 图8是示意性地示出本发明的一个方面的由中央服务器的管理装置执行的时间更新过程的示例的流程图；

[0028] 图9是示意性地示出根据本发明的一个方面的由钥匙单元的钥匙ECU执行的解锁过程的示例的流程图；以及

[0029] 图10是示意性地示出在根据本发明的一个方面的加锁和解锁系统中由钥匙单元和中央服务器执行的时间同步过程和由钥匙单元执行的解锁过程中的操作的示例的顺序图。

具体实施方式

[0030] 在下文中，将参照附图对本发明的实施方式进行描述。

[0031] 首先，以下将参照图1和图2来描述根据本发明的实施方式的加锁和解锁系统1的配置。

[0032] 图1是示意性地示出根据该实施方式的加锁和解锁系统1的配置的示例的框图。图2是示意性地示出在车辆10中包括的加锁和解锁装置11以及钥匙单元12的配置的示例的框图。

[0033] 加锁和解锁系统1包括车辆10、移动终端20、预约管理服务器30和中央服务器40。

[0034] 车辆10是加锁和解锁系统1中的加锁和解锁(解锁和加锁)对象。车辆10包括加锁和解锁装置11和钥匙单元12。

[0035] 根据该实施方式的车辆10的示例包括租用车、共享车(不管是由公司提供还是由个人提供)以及组织中的可以由多个用户使用的公司车。

[0036] 加锁和解锁装置11安装在车辆10中,并且响应于来自钥匙单元12的作为射频(RF)频带(例如,300MHz至3GHz)的无线电波(下文中称为"RF波")发送的加锁信号和解锁信号(两者都是第三请求信号的示例)来执行车辆10的门的解锁和加锁。加锁和解锁装置11包括低频(LF)波发送器111、RF波接收器112、比较电子控制单元(ECU)113、主体ECU 114和门锁马达115。

[0037] 加锁和解锁装置11利用从安装在车辆10中的辅助电池(未示出)供应的电力进行操作。

[0038] LF波发送器111被内置在例如车厢的门把手或中央控制台中,并且在比较ECU 113(稍后将描述的LF发送处理单元1131)的控制下发送LF频带(例如,30Hz至300kHz)的无线电波(以下称为"LF波")。

[0039] RF波接收器112被设置在例如车辆10的后备箱的装饰配件中,并且在比较ECU 113(稍后将描述的RF接收处理单元1132)的控制下接收RF波。

[0040] 比较ECU 113是电子控制单元,其响应于从钥匙单元12接收到的解锁信号和加锁信号来执行对车辆10的门的解锁和加锁的控制。比较ECU113主要例如由微型计算机构成,并通过使CPU执行存储在ROM中的程序来执行各种控制过程。比较ECU 113包括LF发送处理单元1131、RF接收处理单元1132、认证处理单元1133和加锁和解锁控制单元1134作为通过使CPU执行一个或更多个程序而实施的功能单元。比较ECU 113包括被实施为内部存储器的存储区域的存储单元1135。

[0041] LF发送处理单元1131执行经由LF波发送器111将LF波发送至车辆的内部和外部的过程。

[0042] RF接收处理单元1132(加锁和解锁装置接收单元的示例)执行经由RF波接收器112接收RF波的过程。具体地,RF接收处理单元1132接收从钥匙单元作为RF波发送的解锁信号和加锁信号。

[0043] 当RF接收处理单元1132已经接收到解锁信号或加锁信号时,认证处理单元1133(第二认证单元的示例)基于解锁信号或加锁信号中所包括的加锁和解锁钥匙信息(稍后将描述的加锁和解锁钥匙信息1250b)执行对解锁信号或加锁信号的发送源(钥匙单元12)的认证。具体地,当预先登记在存储单元1135中的加锁和解锁钥匙信息1135a与在解锁信号或加锁信号中包括的加锁和解锁钥匙信息匹配时,认证处理单元1133确定认证已成功,而确定当两条信息彼此不匹配时,认证失败。

[0044] 当由认证处理单元1133进行的认证成功时,加锁和解锁控制单元1134经由车载网络(诸如控制器局域网络(CAN))将解锁命令(当RF接收处理单元1132已接收到解锁信号时)或加锁命令(当RF接收处理单元1132已接收到加锁信号)发送至主体ECU 114。

[0045] 主体ECU 114是电子控制单元,其以可通信的方式经由一对一通信线路等控制与其连接的门锁马达115的操作。主体ECU 114根据来自比较ECU 113的解锁命令输出用于使门锁马达115执行解锁操作的控制命令。主体ECU 114根据来自比较ECU 113的加锁命令输出用于使门锁马达115执行加锁操作的控制命令。

[0046] 门锁马达115是现有电动致动器,其根据来自主体ECU 114的控制命令来解锁和加

锁车辆10的门(其包括后备箱盖、后门等)。

[0047] 钥匙单元12安装在车辆10中(在车厢内),并且响应于从移动终端20发送的解锁请求和加锁请求(两者都是第一请求信号的示例)将解锁信号和加锁信号作为RF波发送至加锁和解锁装置11。钥匙单元12包括LF波接收器121、RF波发送器122、通信装置123和钥匙ECU 124。

[0048] 钥匙单元12可以设置在从坐在车辆10的座位上的用户不可见的位置(例如,在手套箱或中央控制台箱中)。钥匙单元12可以固定到车辆10或者可以不固定到车辆10。钥匙单元12可以被配置成利用内置式纽扣电池等执行操作或者可以被配置成利用从安装在车辆10中的辅助电池供应的电力进行操作。

[0049] LF波接收器121在钥匙ECU 124(稍后将描述的LF接收处理单元1241)的控制下执行接收LF波的过程。

[0050] RF波发送器122在钥匙ECU 124(稍后将描述的RF发送处理单元1242)的控制下执行发送RF波的过程。

[0051] 通信装置123是在钥匙ECU 124的控制下根据预定的通信标准以相对短的距离(可以在车辆的内部和外部之间进行通信的距离)与移动终端20进行通信的装置。通信装置123可以是例如BLE通信模块,其根据蓝牙(注册商标)低能耗(BLE)的通信标准与移动终端20进行通信。以下描述基于如下前提:通信装置123采用的通信标准基于BLE通信。

[0052] 通信装置123可以是基于具有非常短的通信范围的短程通信标准(例如,近场通信(NFC)标准)的通信装置。在这种情况下,通信装置123可以被内置在靠近车辆10的外部的主体表面(例如,门把手)等的位置中。因此,即使当通信装置123的通信范围非常短时,钥匙单元12(钥匙ECU 124)也可以与车辆外部的移动终端20进行通信。

[0053] 钥匙ECU 124是电子控制单元,其响应于从移动终端20接收到的解锁请求和加锁请求执行向加锁和解锁装置11发送加锁信号和解锁信号的控制过程。钥匙ECU 124主要由例如微型计算机构成,并且通过使CPU执行存储在ROM中的程序来执行各种控制过程。钥匙ECU 124包括LF接收处理单元1241、RF发送处理单元1242、通信处理单元1243、计时单元1244、认证处理单元1245、时间更新处理单元1246、确定单元1247、加密钥匙生成单元1248以及加锁和解锁处理单元1249作为通过执行一个或更多个程序而实施的功能单元。钥匙ECU 124还包括例如被实施为内部存储器的存储区域的存储单元1250(第一存储单元和第二存储单元的示例)。

[0054] LF接收处理单元1241执行经由LF波接收器121接收LF波的过程。例如,LF接收处理单元1241接收从加锁和解锁装置11发送的LF波。

[0055] RF发送处理单元1242执行经由RF波发送器122发送RF波的过程。例如,RF发送处理单元1242响应于来自加锁和解锁处理单元1249的发送请求来执行发送包括稍后将描述的加锁和解锁钥匙信息1250b(第二认证信息的示例)的解锁信号(当通过通信处理单元1243接收到解锁请求时)和包括加锁和解锁钥匙信息1250b的加锁信号(当通信处理单元1243接收到加锁请求时)的过程。

[0056] 通信处理单元1243(钥匙单元第一接收单元、钥匙单元第二接收单元和钥匙单元发送单元的示例)经由通信装置123执行与移动终端20的通信过程。例如,通信处理单元1243从移动终端20接收包括稍后将描述的认证钥匙的认证请求。例如,通信处理单元1243

从移动终端20接收解锁请求和加锁请求。

[0057] 如稍后将描述的，钥匙单元12经由移动终端20与中央服务器40进行通信，但是可以被配置成直接与中央服务器40通信。例如，钥匙单元12可以被配置成经由安装在车辆10中的数据通信模块(DCM)访问预定的包括移动电话网络或因特网的通信网络并且与中央服务器40通信。

[0058] 计时单元1244(钥匙单元计时器的示例)通过软件执行计时过程，并且在钥匙单元12中生成时间。例如，计时单元1244的时间的精度比硬件的实时时钟(RTC)的精度低。如稍后将描述的，计时单元1244的时间被更新为中央服务器40的时间(具体地，稍后将描述的RTC 42的时间)。也就是说，计时单元1244的时间与中央服务器40的时间同步。

[0059] 当由通信处理单元1243从目标移动终端20接收到包括与钥匙单元12相关的认证钥匙(第一认证信息的示例)的认证请求时，认证处理单元1245(第一认证单元的示例)基于认证钥匙来执行对移动终端20的认证。当从移动终端20接收到由通信处理单元1243认证的移动终端20在钥匙单元12之间通过BLE通信请求重新访问的重新认证请求时，认证处理单元1245执行移动终端20的质询-响应认证(下文中称为“重新认证”)。稍后将描述其详细内容。

[0060] 当认证成功时，认证处理单元1245执行将存储在存储单元1250中的加锁和解锁钥匙信息1250b恢复到可用状态的过程。例如，加锁和解锁钥匙信息1250b被例如以如下状态进行存储：加锁和解锁钥匙信息不可访问、加密等，并且不能用于加锁和解锁装置11中的认证。因此，当移动终端20的认证成功时，认证处理单元1245改变访问存储单元1250的权限，以将加锁和解锁钥匙信息1250b改变为可访问状态或者基于认证钥匙对经加密的加锁和解锁钥匙信息1250b进行解密。因此，RF发送处理单元1242可以访问通常不可访问的加锁和解锁钥匙信息1250b，并将包括加锁和解锁钥匙信息1250b的解锁信号或加锁信号发送至加锁和解锁装置11，或者可以将包括经解密的加锁和解锁钥匙信息1250b的解锁信号或加锁信号发送至加锁和解锁装置11。因此，加锁和解锁装置11(具体地，认证处理单元1133)可以基于包括在解锁信号和加锁信号中的加锁和解锁钥匙信息1250b执行适当的认证。即使当恶意第三方不适当地获取钥匙单元12的情况发生时，钥匙单元12中的加锁和解锁钥匙信息1250b不可访问或被加密，并且因此可以阻止对车辆10的盗窃。

[0061] 时间更新处理单元1246向通信处理单元1243传送发送请求，并以移动终端20和预约管理服务器30的中继方式经由通信处理单元1243向中央服务器40发送用于请求获取中央服务器40的时间的时间获取请求(第二请求信号的示例)。当由通信处理单元1243经由预约管理服务器30和移动终端20接收到来自中央服务器40的时间信息时，时间更新处理单元1246利用时间信息更新计时单元1244的时间，并使该时间与中央服务器40的时间(即，稍后将描述的RTC 42的时间)同步。

[0062] 确定单元1247确定当前时间是否在与已经用于由认证处理单元1245认证的认证钥匙相对应的车辆10的预约时间内。确定单元1247确定是否已经取消针对与已经用于由认证处理单元1245认证的认证钥匙相对应的车辆10的预约。其详细内容将在后面描述。

[0063] 加密钥匙生成单元1248生成通信加密钥匙，以用于认证处理单元1245对其的认证已经成功的移动终端20(即，经认证的移动终端20)向钥匙单元12发送信号。加密钥匙生成单元1248还生成通信解密钥匙，以用于对用所生成的加密钥匙加密的数据进行解密。加密

钥匙生成单元1248生成通信加密钥匙，使得所生成的通信加密钥匙与过去生成的通信加密钥匙不同。如稍后将描述的，通信加密钥匙被发送至钥匙单元12，并且通信解密钥匙被存储在存储单元1250中。因此，通过使移动终端20使用通信加密钥匙对用于钥匙单元12的各种命令(例如，解锁请求或加锁请求)进行加密并将经加密的命令发送至钥匙单元12，认证处理单元1245在每次由通信处理单元1243接收到各种命令时不需要使用加密钥匙来执行移动终端20的认证。因此，如稍后将描述的，认证钥匙的使用可以被限制为一次，并且例如当通信处理单元1243接收到使用通信加密钥匙加密的解锁请求或加锁请求(即，可以使用通信解密钥匙解密的解锁请求或加锁请求)时，加锁和解锁处理单元1249可以确定接收到的解锁请求或接收到的加锁请求是来自经认证的移动终端20的命令，并且可以执行车辆10的门的解锁或加锁的过程。其详细内容将在稍后描述。

[0064] 当认证处理单元1245对移动终端20的认证成功并且由通信处理单元1243从移动终端20接收到解锁请求或加锁请求时，加锁和解锁处理单元1249执行车辆10的门的解锁或加锁的过程。具体地，当如上所述认证处理单元1245对移动终端20的认证成功并且从移动终端20接收到可以使用通信加密钥匙解密的解锁请求或加锁请求时，加锁和解锁处理单元1249通过向RF发送处理单元1242传送发送请求并经由RF发送处理单元1242和RF波发送器122将解锁信号或加锁信号发送至加锁和解锁装置11来执行车辆10的门的解锁或加锁的过程。其详细内容将在稍后描述。

[0065] 在存储单元1250中预先存储唯一钥匙1250a、加锁和解锁钥匙信息1250b、发送侧加密钥匙1250c等。

[0066] 唯一钥匙1250a是一组加密钥匙和解密钥匙，它们被设置为与钥匙单元12相对应，如稍后将描述的，并且具体地是用于在钥匙单元12和中央服务器40之间进行通信时在发送侧加密数据并且在接收侧对经加密的数据进行解密的加密钥匙和解密钥匙。如稍后将描述的，与唯一钥匙1250a相同的唯一钥匙也被存储在中央服务器40的唯一钥匙DB 435中。

[0067] 当由加密钥匙生成单元1248生成的通信加密钥匙从钥匙单元12被发送至移动终端20时，发送侧加密钥匙1250c用于加密通信加密钥匙。

[0068] 移动终端20的示例包括智能电话和平板终端。移动终端20可以经由预定通信网络(例如，具有多个基站作为终端的移动电话网络或因特网)与预约管理服务器30和中央服务器40进行双向通信。以下描述基于经由预约管理服务器30执行移动终端20与中央服务器40之间的信号发送和接收的前提。移动终端20包括通信装置21和22、处理器23和触摸面板显示器(下文简称为显示器)24。

[0069] 在该实施方式中，移动终端20经由预约管理服务器30与中央服务器40进行通信，但是可以被配置成经由预定的通信网络直接与中央服务器40进行双向通信。

[0070] 通信装置21是基于与通信装置123中相同的通信标准与移动终端20进行通信的装置。通信装置21是例如上述的该实施方式中的BLE通信模块。

[0071] 通信装置22是经由预定的通信网络与预约管理服务器30和中央服务器40通信的装置。

[0072] 处理器23包括CPU和辅助存储装置，并且包括通信处理单元231、通信处理单元232、认证钥匙获取单元233、认证请求单元234、加锁和解锁请求单元235和预约单元236作为通过使CPU执行一个或更多个程序而实施的功能单元。处理器23还包括被实施为辅助存

储装置中的存储区域的存储单元239(第一存储单元的示例)。

[0073] 通信处理单元231(终端发送单元的示例)使用通信装置21与钥匙单元12进行无线通信,并且发送和接收各种信号。例如,通信处理单元231响应于来自认证请求单元234的发送请求,将包括认证钥匙的认证请求和包括稍后将描述的响应的重新认证请求发送至钥匙单元12。例如,通信处理单元231响应于来自加锁和解锁请求单元235的请求,将解锁请求和加锁请求发送至钥匙单元12。例如,在该实施方式中,钥匙单元12和中央服务器40采用用于经由移动终端20执行双向通信的配置,并且通信处理单元231将应该从钥匙单元12发送至中央服务器40的信号传送至通信处理单元232,以将该信号发送至预约管理服务器30,并且发送应该从中央服务器40发送至钥匙单元12并且已经从通信处理单元232传送至钥匙单元12的信号。

[0074] 通信处理单元232使用通信装置22与基站进行无线通信,并且发送和接收各种信号,诸如数据信号和控制信号。具体地,通信处理单元232经由包括具有基站作为终端的移动电话网络或因特网的预定通信网络将各种信号发送至预约管理服务器30和中央服务器40并且接收来自预约管理服务器30和中央服务器40的各种信号。例如,在该实施方式中,通信处理单元232经由预约管理服务器30向中央服务器40发送以中央服务器40为目的地的信号。由于采用了上述配置,所以在发送侧的通信处理单元232可以将包括目的地信息的信号发送至预约管理服务器30,或者在接收侧的预约管理服务器30可以将从移动终端20发送至预约管理服务器30的多种类型的信号中的规定类型的信号自动地发送至中央服务器40。例如,在该实施方式中,如上所述,钥匙单元12和中央服务器40采用经由移动终端20执行双向通信的配置,通信处理单元232以钥匙单元12为目的地经由预约管理服务器30将从中央服务器40发送的信号传送至通信处理单元231以将该信号发送至钥匙单元12,或者以中央服务器40为目的地发送从钥匙单元12发送的信号,该信号已经被设定成从通信处理单元231至预约管理服务器30。

[0075] 也就是说,通信处理单元231和通信处理单元232是接收从中央服务器40和钥匙单元12中的一者发送至另一者的信号并且将接收到的信号发送(传送)至另一者的中继单元的示例。

[0076] 认证钥匙获取单元233在显示器24上显示GUI作为操作屏幕,并且响应于用户在显示器24的GUI上的预定操作执行从中央服务器40获取认证钥匙的过程。具体地,认证钥匙获取单元233响应于用户的预定操作向通信处理单元232传送发送请求,并经由通信处理单元232将用于请求获取认证钥匙的认证钥匙获取请求发送至中央服务器40。当由通信处理单元232接收到响应于认证钥匙获取请求而从中央服务器40返回的认证钥匙时,认证钥匙获取单元233执行将认证钥匙存储在存储单元239中的过程。在该实施方案中,用户可以预先(即在车辆10的预约的开始时间之前)获取移动终端20中的认证钥匙。其详细内容将在稍后描述。

[0077] 认证请求单元234将发送请求传送至通信处理单元231,并且经由通信处理单元231将用于请求移动终端20的认证作为用于解锁和加锁车辆10的门的远程控制器的认证请求发送至车辆10的钥匙单元12。例如,当发送请求已经被传送至通信处理单元231之后用户从车辆10等上下来使得BLE通信在经认证的移动终端20和处于访问状态的钥匙单元12之间暂时切断时,认证请求单元234经由通信处理单元231再次向车辆10的钥匙单元12发送用于

请求重新访问钥匙单元12的重新认证请求。其详细内容将在稍后描述。

[0078] 加锁-解锁请求单元235在显示器24上显示图形用户界面(GUI)作为操作屏幕。然后，加锁和解锁请求单元235响应于在GUI上的预定操作向通信处理单元231传送发送请求，并且经由通信处理单元231将包括认证钥匙的解锁请求或包括认证钥匙的加锁请求发送至钥匙单元12。具体地，加锁和解锁请求单元235将由通信处理单元231已经从移动终端20接收到并使用存储在存储单元239中的通信加密钥匙加密的解锁请求和加锁请求发送至钥匙单元12，这将在稍后描述。例如，在GUI上显示用于请求解锁车辆10的解锁按钮和用于请求加锁车辆10的加锁按钮，并且通过触摸加锁按钮来发送加锁请求，通过触摸解锁按钮来发送解锁请求。其详细内容将在稍后描述。

[0079] 将加锁请求和解锁请求发送至钥匙单元12的用户的操作可以是对操作单元的作为设置在移动终端20中的硬件的操作，而不是触摸显示器24的操作。当认证钥匙没有被存储在存储单元239中时，用于发送加锁请求和解锁请求的预定操作可能无效，或者可以在不包括认证钥匙的情况下发送加锁请求和解锁请求。

[0080] 预约单元236在显示器24上显示GUI作为操作单元，并且响应于用户在显示器24上对GUI的预定操作来对车辆10进行预约。例如，预约单元236可以经由通信处理单元232针对预约管理服务器30请求车辆10的调度信息(当前预约状态)。此时，预约单元236将包括对车辆10唯一的识别信息(例如，车辆索引号(VIN))和密码的请求发送至预约管理服务器30。存储在预约管理服务器30(具体地，将在稍后描述的调度信息DB 323)中的车辆10的调度信息包括对于车辆10的预约信息(每个预约的开始时间和结束时间、用户的识别信息等)。预约单元236在显示器24上显示经由通信处理单元232从预约管理服务器30接收到的车辆10的调度信息(当前预约状态)。因此，用户可以基于显示在显示器上的调度信息来确认空闲时间段，并在空闲时间段(尚未进行预约的时间段)对车辆10进行预约。当用户在特定时间进行预约时，预约单元236经由通信处理单元232请求更新包括新输入的预约信息(每个预约的开始时间和结束时间、用户的识别信息等)的调度信息。因此，来自移动终端20的用户的新预约被反映在调度信息DB 323中的车辆10的调度信息中。

[0081] 预约单元236响应于用户在显示器24上对GUI的预定操作取消车辆10的预约。当用户取消预约时，预约单元236请求删除包括被取消的预约信息(每个预约的开始时间和结束时间、用户的识别信息等)的调度信息。因此，从调度信息DB 323中的车辆10的调度信息中删除被取消的预约的详细内容。

[0082] 用户可以使用除了移动终端20以外的终端(具体地，固定终端(诸如台式计算机)，而非移动终端)来预约车辆10或取消预约，并且可以从其他终端执行对于车辆10的预约和取消预约

[0083] 预约管理服务器30管理车辆10的调度(预约)。预约管理服务器30包括例如云应用(未示出)，并且用户可以经由诸如移动电话网络或因特网的预定通信网络使用具有移动终端20或另一终端的云应用来来准备和更新调度信息。

[0084] 车辆10的调度表示车辆10的使用调度(预约)。

[0085] 预约管理服务器30包括通信装置31和管理装置32。

[0086] 通信装置31是经由预定的通信网络与移动终端20和中央服务器40进行通信的装置。

[0087] 管理装置32主要由一台或更多台计算机构成，并且包括通信处理单元321和调度管理单元322作为通过使CPU执行一个或更多个程序而实施的功能单元。管理装置32包括存储在辅助存储装置中的调度信息DB323，并且调度信息DB 323包括车辆10的调度信息。

[0088] 通信处理单元321使用通信装置31向移动终端20和中央服务器40发送各种信号并且接收来自移动终端20和中央服务器40的各种信号。例如，通信处理单元321接收来自移动终端20的用于请求公开车辆10的调度信息的信号，并且响应于与该信号相对应的来自调度管理单元322的请求将车辆10的调度信息(参考数据)返回到移动终端20。例如，通信处理单元321接收来自移动终端20的用于请求更新调度信息的信号，并且响应于与该信号相对应的来自调度管理单元322的请求将指示更新完成的信号返回到移动终端20。例如，通信处理单元321响应于来自调度管理单元322的请求将稍后将描述的取消通知发送至中央服务器40。在该实施方案中，如上所述，采用经由预约管理服务器30执行在移动终端20和中央服务器40之间的通信的配置，并且通信处理单元321中继并接收应该从移动终端20(或者钥匙单元12)发送至中央服务器40的信号并将该信号发送至中央服务器40，并且中继并发送应该从中央服务器40发送至移动终端20(或者钥匙单元12)的信号至移动终端。

[0089] 调度管理单元322响应于来自使用云应用的用户的各种输入来管理例如存储在调度信息DB 323中的车辆10的调度信息。当通信处理单元321从移动终端20(另一终端，当在另一终端执行车辆10的预约时)接收到用于请求公开车辆10的调度信息的信号时，调度管理单元322首先确定信号是否是基于包括在该信号中的识别信息(用户ID)和密码的授权访问。当该信号是授权访问时，调度管理单元322从调度信息DB 323中提取车辆10的调度信息，并且经由通信处理单元321将所提取的调度信息发送至移动终端20(或另一终端)。当通信处理单元321从移动终端20(或另一终端)接收到包括用于请求更新车辆10的调度信息的请求的信号时，调度管理单元322根据请求的详细内容(即，改变诸如所添加的预约信息或由于取消预约而被删除的预约信息的详细内容)更新在调度信息DB 323中车辆10的调度信息。当使用移动终端20或另一终端取消对于车辆10的预约时，调度管理单元322将发送请求传送至通信处理单元321，并经由通信处理单元321将包括被取消的车辆10的预约的预约信息(诸如每个预约的开始时间和结束时间，以及用户的识别信息)的取消通知发送至中央服务器40。

[0090] 中央服务器40管理车辆10的使用状态。中央服务器40包括通信装置41、实时时钟(RTC)42和管理装置43。

[0091] 通信装置41是经由预定的通信网络与移动终端20和预约管理服务器30进行通信的装置。

[0092] RTC 42(服务器计时器的示例)使用硬件执行计时，并且在中央服务器40中产生时间。RTC的时间的精度比使用软件的钥匙单元12的计时单元1244的精度高。

[0093] RTC 42可以设置在管理装置43中。

[0094] 管理装置43主要由一台或更多台计算机构成，并且包括通信处理单元431、认证钥匙生成单元432和时间同步处理单元433作为通过使CPU执行一个或更多个程序而实施的功能单元。管理装置43包括存储在内部辅助存储装置中的认证信息DB 434、唯一钥匙DB 435、接收侧解密钥匙DB 436、访问信息DB 437和取消信息DB 438。

[0095] 通信处理单元431(服务器发送单元和服务器接收单元的示例)使用通信装置41向

移动终端20和预约管理服务器30发送各种信号并且接收来自移动终端20和预约管理服务器30的各种信号。

[0096] 当由通信处理单元431经由预约管理服务器30从移动终端20接收到认证钥匙获取请求时，认证钥匙生成单元432生成与钥匙单元12相关的(即，对钥匙单元12唯一的)认证钥匙。认证钥匙生成单元432在生成认证钥匙时生成与所生成的认证钥匙相关的唯一识别信息(发行ID)。例如，认证钥匙包括针对钥匙单元12规定的唯一信息(钥匙单元唯一信息)。认证钥匙包括预约信息，诸如包括在认证钥匙获取请求中的车辆10的预约的开始时间和结束时间。也就是说，认证钥匙生成单元432生成与钥匙单元12相关的且与车辆10的预约详细内容相关的认证钥匙。认证钥匙生成单元432将发送请求传送至通信处理单元431，并且通过预约管理服务器30以中继方式经由通信处理单元431将包括所生成的认证钥匙的认证钥匙信息发送至移动终端20。

[0097] 时间同步处理单元433响应于由通信处理单元431经由移动终端20和预约管理服务器30从钥匙单元12接收到的时间获取请求来使钥匙单元12的时间(即，计时单元1244的时间)与中央服务器40的时间(即，RTC 42的时间)同步。当通信处理单元431接收到时间获取请求时，时间同步处理单元433使用存储在唯一钥匙DB 435中的与钥匙单元12相对应的唯一钥匙(一组加密钥匙和解密钥匙中的解密钥匙)来对该时间获取请求的数据进行解密，获取RTC 42的时间，并且生成包括所获取的时间的时间信息。此时，时间同步处理单元433生成时间信息，该时间信息包括取消标记F，其指示与包括在时间获取请求中的认证钥匙的发行ID相对应的车辆10的预约是否已经被取消，并且使用与钥匙单元12相对应的唯一钥匙(一组加密钥匙和解密钥匙中的加密钥匙)对所生成的时间信息进行加密。时间同步处理单元433将发送请求传送至通信处理单元431，并将经加密的时间信息经由通信处理单元431、预约管理服务器30和移动终端20发送至钥匙单元12。

[0098] 包括在由认证钥匙生成单元432生成的认证钥匙的一部分中的钥匙单元唯一信息被存储在与对钥匙单元12唯一的识别信息相关的认证信息DB 434中。

[0099] 与钥匙单元12相对应的唯一钥匙(一组加密钥匙和解密钥匙)被存储在与对钥匙单元12唯一的识别信息相关的唯一钥匙DB 435中。认证钥匙生成单元432使用唯一钥匙对包括所生成的认证钥匙的认证钥匙信息进行加密，然后经由通信处理单元431将认证钥匙信息发送至移动终端20。

[0100] 接收侧解密钥匙DB 436存储接收侧解密钥匙，接收侧解密钥匙与存储在钥匙单元12(存储单元1250)中的发送侧加密钥匙1250c形成一对并且用于对使用发送侧加密钥匙1250c来加密的数据进行解密。如稍后将描述的，接收侧解密钥匙在接收侧解密钥匙被包括在认证钥匙信息中的状态下被发送至移动终端20。

[0101] 访问信息DB 437存储与对钥匙单元12唯一的识别信息相关的、用于允许移动终端20以可通信的方式访问钥匙单元12的信息(BLE访问信息)。BLE访问信息包括例如钥匙单元12的通信装置123的设备ID或钥匙单元12在广告时的服务UUID。

[0102] 取消信息DB 438存储与所发行的认证钥匙的发行ID相关的、与已经发送至移动终端20的发行的认证钥匙相对应的车辆10的预约的取消信息。存储在取消信息DB 438中的取消信息是基于通过通信处理单元431从预约管理服务器30发送的取消通知而生成的。

[0103] 下面将参照图3对在加锁和解锁系统1中从车辆10的预约到由移动终端20获取认

证钥匙的操作进行描述。

[0104] 图3是示意性地示出加锁和解锁系统1中从车辆10的预约到由移动终端20获取认证钥匙的一系列操作的顺序图。

[0105] 在步骤S302中，移动终端20的预约单元236响应于在显示器24上对GUI的预定操作(例如，输入为携带移动终端20的用户预设的用户ID和密码的操作)向通信处理单元231传送发送请求，并经由通信处理单元231将包括用户ID和密码的登录请求发送至预约管理服务器30。

[0106] 在步骤S304中，预约管理服务器30的调度管理单元322基于经由通信处理单元321从移动终端20接收到的登录请求的用户ID和密码来执行该访问是否为经授权访问(即用户认证)的认证，并且当用户认证成功时，经由通信处理单元321向移动终端20发送认证响应。

[0107] 在步骤S306中，移动终端20的预约单元236响应于显示器24的GUI的用户的预定操作经由通信处理单元231将包括车辆10的识别信息(VIN)和预约的开始时间和结束时间的预约请求发送至预约管理服务器30。

[0108] 在步骤S308中，预约管理服务器30的调度管理单元322取决于通信处理单元321接收到的预约请求的详细内容来更新存储在调度信息DB323中的车辆10的调度信息，并且完成车辆10的预约。

[0109] 在步骤S310中，预约管理服务器30的调度管理单元322经由通信处理单元321将预约完成通知发送至移动终端20。

[0110] 如上所述，通过步骤S302至S310完成车辆10的预约。

[0111] 此后，在步骤S312中，移动终端20的认证钥匙获取单元233接收显示器24的GUI的用户认证钥匙获取操作。

[0112] 在步骤S314中，移动终端20的认证钥匙获取单元233确定是否能够获取认证钥匙。具体地，认证钥匙获取单元233确定是否已满足与认证钥匙的初步获取相关的时间限制的要求，即当前时间是否已达到车辆10的预约的开始时间之前的预定时间(例如10分钟)。在当前时间达到车辆10的预约的开始时间之前的预定时间时，认证钥匙获取单元233执行步骤S316。另一方面，在当前时间尚未达到车辆10的预约的开始时间之前的预定时间时，认证钥匙获取单元233使用户的认证钥匙获取操作无效并且不发送认证钥匙获取请求。因此，通过在车辆10的预约的开始时间之前能够初步获取认证钥匙，可以解锁车辆10并开始使用车辆10，例如，即使在移动终端20位于在开始使用车辆10时的预定的通信网络的覆盖范围之外。另一方面，通过提供用于获取认证钥匙的时间限制(即，仅在车辆10的预约的开始时间之前的预定时间的时间点之后可以获取认证钥匙)，例如，可以使用由用户初步获取的认证钥匙来禁止在车辆10的预约的开始时间之前未经授权使用车辆10的机会，以防止未经授权使用车辆10。

[0113] 在步骤S316中，认证钥匙获取单元233经由通信处理单元231将包括对移动终端20唯一的识别信息(例如，终端ID)、作为预约对象的车辆10的识别信息VIN以及预约的开始时间和结束时间的认证钥匙获取请求发送至预约管理服务器30。

[0114] 在步骤S318中，当从移动终端20接收到认证钥匙获取请求时，预约管理服务器30的通信处理单元321将认证钥匙获取请求发送至中央服务器40。

[0115] 在步骤S320中，如上所述中央服务器40的认证钥匙生成单元432响应于由通信处

理单元431接收到认证钥匙获取请求来生成与钥匙单元12相关的认证钥匙和车辆10的预约细节，即包括钥匙单元唯一信息的认证钥匙和车辆10的预约的开始时间和结束时间。然后，如上所述，认证钥匙生成单元432使用存储在唯一钥匙DB 435中的与钥匙单元12相对应的唯一钥匙来加密认证钥匙。

[0116] 在步骤S322中，中央服务器40的认证钥匙生成单元432除了加密的认证钥匙以外还经由通信处理单元431将包括认证钥匙的发行ID、接收侧解密钥匙和BLE访问信息的认证钥匙信息发送至预约管理服务器30。

[0117] 在步骤S324中，当从中央服务器40接收到认证钥匙信息时，预约管理服务器30的通信处理单元321将认证钥匙信息发送至移动终端20。

[0118] 在步骤S326中，移动终端20的认证钥匙获取单元233将在由通信处理单元231接收到的认证钥匙信息中包括的认证钥匙、发行ID、接收侧解密钥匙和BLE访问信息存储在存储单元239中。

[0119] 如上所述，通过步骤S312至S326完成移动终端20对认证钥匙的获取。

[0120] 下面将参照图4至图6对在加锁和解锁系统1中认证移动终端20的操作进行描述。

[0121] 首先，图4是示意性地示出在移动终端20的处理器23中开始加锁和解锁功能的过程(加锁和解锁功能开始过程)的示例的流程图。以预定时间间隔(例如，在获取认证钥匙之后直到车辆10的预约的结束时间为止)执行该流程图中的过程。

[0122] 在步骤S402中，通信处理单元231基于已经从中央服务器获取并且存储在存储单元239中的BLE访问信息(设备ID、服务UUID等)从移动终端20周围的通信装置21的通信区域搜索与预约车辆10相对应的钥匙单元12，其中，BLE访问信息包括在认证钥匙信息中。

[0123] 在步骤S404中，通信处理单元231确定是否已检测到与预约车辆10相对应的钥匙单元12(通信装置123)。通信处理单元231在已检测到与预约车辆10相对应的钥匙单元12时执行步骤S406，否则结束该过程。

[0124] 在步骤S406中，通信处理单元231发送包括移动终端20的识别信息(例如，通信装置21的终端ID或设备ID)的访问请求。

[0125] 在步骤S408中，通信处理单元231确定是否已从钥匙单元12接收到访问响应。当在发送访问请求之后的预定时间(例如，足够长于从移动终端20到钥匙单元12的通信时间假设的最大时间的时间)内已经从钥匙单元12接收到访问响应时，通信处理单元231执行步骤S410，并且在发送访问请求之后的预定时间内没有从钥匙单元12接收到访问响应时结束该过程。

[0126] 在步骤S410中，认证请求单元234确定是否已经由通信处理单元231从钥匙单元12接收到认证钥匙请求。认证请求单元234在由通信处理单元231接收到访问响应之后的预定时间内由通信处理单元231从钥匙单元12已接收到认证钥匙请求时执行步骤S412，否则执行步骤S414。

[0127] 在步骤S412中，认证请求单元234经由通信处理单元231将包括由中央服务器40加密并存储在存储单元239中的认证钥匙(参见图3中的步骤S326)和认证钥匙的发行ID的认证请求发送至钥匙单元12，并且然后执行步骤S420。

[0128] 另一方面，在步骤S414中，认证请求单元234确定是否已经由通信处理单元231从钥匙单元12接收到用于重新认证移动终端20的询问。认证请求单元234当在由通信处理单

元231接收到访问响应之后的预定时间内由通信处理单元231已从钥匙单元12接收到询问时执行步骤S416，否则结束该过程。

[0129] 在步骤S416中，认证请求单元234基于由通信处理单元231所接收到的询问来产生响应。具体地，认证请求单元234使用在先前认证或重新认证时由通信处理单元231所接收到的通信加密钥匙来加密询问。

[0130] 在步骤S418中，认证请求单元234将包括所生成的响应的重新认证请求发送至钥匙单元12，并且然后执行步骤S420。

[0131] 在步骤S420中，认证请求单元234确定是否已经由通信处理单元231从钥匙单元12接收到通信加密钥匙。当在由通信处理单元231发送认证请求或重新认证请求之后的预定时间内已经由通信处理单元231从钥匙单元12接收到通信加密钥匙时，认证请求单元234执行步骤S422，否则结束该过程。

[0132] 在步骤S422中，认证请求单元234使用存储在存储单元239中的接收侧解密钥匙(参见图3中的步骤S324和S326)对由通信处理单元231接收到的通信加密钥匙进行解密。

[0133] 在步骤S424中，认证请求单元234确定对由通信处理单元231接收到的通信加密钥匙的解密是否已成功。当对接收到的通信加密钥匙的解密已成功时，认证请求单元234执行步骤S426，否则结束该过程。因此，例如，即使当利用发送侧加密钥匙1250c加密的并从钥匙单元12发送至移动终端20的通信加密钥匙已经被恶意第三方窃听时，在不使用由移动终端20获取的接收侧解密钥匙连同来自中央服务器40的认证钥匙的情况下也无法解密通信加密钥匙，因而可以防止由于通信加密钥匙的窃听而引起的车辆10的未经授权使用。

[0134] 经解密的通信加密钥匙被存储在存储单元239中。

[0135] 在步骤S426中，认证请求单元234经由通信处理单元231将已经使用通信加密钥匙加密的加锁和解锁功能ON请求发送至钥匙单元12，并且结束该过程。

[0136] 图5是示意性地示出由钥匙单元12的钥匙ECU 124执行的对移动终端20进行认证的过程的示例的流程图。例如，在不存在以可通信的方式连接至钥匙单元12的移动终端20的状态下，重复执行该流程图中的过程。

[0137] 在步骤S502中，通信处理单元1243控制通信装置123并且将广告信息(例如，服务UUID或设备ID)发送至车辆10的附近(具体地，在来自通信装置123的BLE通信无线电波的可到达的距离内)

[0138] 在步骤S504中，通信处理单元1243确定是否已经从移动终端20接收到访问请求。当已经从移动终端20接收到访问请求时，通信处理单元1243执行步骤S506，否则结束该过程。

[0139] 在步骤S506中，通信处理单元1243建立与移动终端20的BLE访问的会话，并向移动终端20发送指示完成BLE访问的访问响应。

[0140] 在步骤S508中，认证处理单元1245基于包括在访问请求中的移动终端20的识别信息来确定是否已经使用认证钥匙认证了其中已经通过通信处理单元1243建立了BLE访问的会话的移动终端20。当移动终端20没有被认证时，认证处理单元1245执行步骤S510，当移动终端已经被认证时执行步骤S518。

[0141] 在步骤S510中，认证处理单元1245经由通信处理单元1243向移动终端20发送认证钥匙请求。

[0142] 在步骤S512中，认证处理单元1245确定是否已经由通信处理单元1243从移动终端20接收到包括认证钥匙的认证请求。当在已经从通信处理单元1243发送了认证钥匙请求之后的预定时间内已经由通信处理单元1243从移动终端20接收到认证请求时，认证处理单元1245执行步骤S514，否则结束该过程。

[0143] 在步骤S514中，认证处理单元1245使用唯一钥匙1250a对由中央服务器40加密并且包括在认证请求中的认证钥匙进行解密，并且提取包括在认证钥匙中的钥匙单元唯一信息和预约信息(车辆10的预约的开始时间和结束时间)。

[0144] 在步骤S516中，认证处理单元1245基于所提取的钥匙单元唯一信息和所提取的预约信息来认证移动终端20。例如，认证处理单元1245基于所提取的钥匙单元唯一信息是否与预先存储在钥匙单元12的存储单元1250中的钥匙单元唯一信息相匹配、所提取的当前认证钥匙的预约信息(开始时间和结束时间)与用于先前认证的认证钥匙的预约信息(开始时间和结束时间)是否重叠等来认证移动终端20。因此，认证处理单元1245除了基于对钥匙单元12唯一的钥匙单元唯一信息的验证之外，还执行预约信息是否重叠的验证，并且可以使得没有终端能够重用用于一次性认证的认证钥匙，无论它是应该使用该认证钥匙来认证的移动终端20还是其他终端。因此，例如，当从移动终端20向钥匙单元12发送包括认证钥匙的认证请求时，认证钥匙被恶意的第三方窃听时，认证无法被重用，因此可以防止恶意第三方对车辆10的未经授权使用。

[0145] 另一方面，在步骤S518中，认证处理单元1245基于指定的计算式等来生成询问，并经由通信处理单元1243将询问发送至移动终端20。

[0146] 在步骤S520中，认证处理单元1245确定是否已经由通信处理单元1243从移动终端20接收到包括响应的重新认证请求。当在从通信处理单元1243发送询问之后的预定时间内已经由通信处理单元1243从移动终端20接收到重新认证请求时，认证处理单元1245执行步骤S522，否则结束该过程。

[0147] 在步骤S522中，认证处理单元1245使用已经在经认证的移动终端20与钥匙单元12之间的BLE通信的先前会话中使用的通信加密钥匙来认证询问响应。具体地，认证处理单元1245取决于已经使用先前的通信加密钥匙被加密的询问是否与由通信处理单元1243从移动终端20接收到的响应相匹配来执行移动终端20的重新认证

[0148] 在步骤S524中，认证处理单元1245确定在步骤S516或S522中的认证是否成功。认证处理单元1245在认证已成功时执行步骤S526，并且在认证失败时结束该过程。

[0149] 在步骤S526中，加密钥匙生成单元1248生成通信加密钥匙，并使用发送侧加密钥匙1250c执行加密。

[0150] 在步骤S528中，认证处理单元1245经由通信处理单元1243将由加密钥匙生成单元1248生成的通信加密钥匙发送至移动终端20，并结束该过程。因此，当移动终端20与钥匙单元12之间的通信失败状态转变为通信成功状态时，更新用于当加锁请求或解锁请求从移动终端20发送至钥匙单元12时加密的通信加密钥匙。因此，例如，即使由于身份盗用等导致通信加密钥匙泄漏，也无法使用通信加密钥匙来访问钥匙单元12，因而可以防止恶意第三方对车辆10的未经授权使用。

[0151] 图6是示意性地示出加锁和解锁系统1的与由移动终端20执行的加锁和解锁功能开始过程和由钥匙单元12执行的移动终端20的认证过程相对应的操作的示例的顺序图。

[0152] 在该示例中，描述基于以下前提：携带移动终端20的用户在车辆10的预约的开始时间到达车辆10的附近。

[0153] 在步骤S602中，移动终端20的通信处理单元231检测车辆10的预约的开始时间。

[0154] 在步骤S604中，移动终端20的通信处理单元231基于存储在存储单元239中的BLE访问信息来搜索与预约车辆10相对应的钥匙单元12(图4中的步骤S402)。

[0155] 另一方面，在步骤S606中，钥匙单元12的通信处理单元1243经由通信装置123将广告信息发送至钥匙单元12的附近(即车辆10的附近)的预定通信区域(图5中的步骤S502)。

[0156] 在步骤S608中，移动终端20的通信处理单元231通过从钥匙单元12接收广告信息来检测钥匙单元12，并且响应于来自认证请求单元234的发送请求而向钥匙单元12发送访问请求(图4中的步骤S404中的“是”和步骤S406)。

[0157] 在步骤S610中，钥匙单元12的通信处理单元1243响应于从移动终端20接收到的访问请求与移动终端20建立BLE通信会话，并向移动终端20发送访问响应(在图5中的步骤S504中的“是”和步骤S506)。

[0158] 在步骤S612中，当已经建立了BLE通信会话的移动终端20未被认证时，钥匙单元12的认证处理单元1245经由通信处理单元1243向移动终端20发送认证钥匙请求(图5中的步骤S508中的“否”和步骤S510)。

[0159] 在S614中，移动终端20的认证请求单元234响应于由通信处理单元231接收到的认证钥匙请求经由通信处理单元231将包括由中央服务器40加密的认证钥匙或认证钥匙的发行ID的认证请求发送至钥匙单元12(图4中的步骤S410中的“是”和步骤S412)。

[0160] 在步骤S616中，钥匙单元12的认证处理单元1245使用唯一钥匙1250a对在由通信处理单元1243从移动终端20接收到的认证钥匙请求中包括的经加密的认证钥匙进行解密，并且提取在认证钥匙中包括的钥匙单元唯一信息或车辆10的预约信息(图5的步骤S514)。

[0161] 在步骤S618中，钥匙单元12的认证处理单元1245基于认证钥匙来执行移动终端20的认证，即，基于从认证钥匙中提取的钥匙单元唯一信息或预约信息的移动终端20的认证(图5中的步骤S516)。

[0162] 在步骤S620中，当移动终端20的认证已成功时，钥匙单元12的加密钥匙生成单元1248生成通信加密钥匙，并使用发送侧加密钥匙1250c对通信加密钥匙进行加密(步骤图5中的S526)。

[0163] 在步骤S622中，钥匙单元12的认证处理单元1245将由加密钥匙生成单元1248生成的通信加密钥匙发送至移动终端20(图5中的步骤S528)。

[0164] 在步骤S624中，移动终端20的认证请求单元234使用存储在存储单元239中的接收侧解密钥匙对由通信处理单元231接收到的通信加密钥匙进行解密(图4中的步骤S422)。

[0165] 在步骤S626中，当通信加密钥匙已经被成功解密时，认证请求单元234经由通信处理单元231将使用通信加密钥匙加密的加锁和解锁功能ON通知发送至钥匙单元12。

[0166] 如上所述，通过步骤S602至S626完成了对移动终端20的认证。

[0167] 下面将参照图7至图10对在加锁和解锁系统1中与使用移动终端20的车辆10的门的解锁相关的操作进行描述。

[0168] 图7是示意性地示出由钥匙单元12的钥匙ECU 124执行的时间更新过程的示例的流程图。例如，当移动终端20的认证或重新认证已经成功并且由通信处理单元1243从移动

终端20接收到加锁和解锁功能ON请求时，执行该流程图中的过程。在移动终端20的认证或重新认证已成功之后保持已经建立了钥匙单元12与移动终端20之间的BLE通信访问会话的状态的情况下，周期性地(例如，每30分钟)执行从流程图中已除去了稍后将描述的步骤S722和S724的过程。

[0169] 在步骤S702中，时间更新处理单元1246使用唯一钥匙1250a来对用于认证经认证的移动终端20的认证钥匙的发行ID进行加密。

[0170] 在步骤S704中，时间更新处理单元1246经由通信处理单元1243和移动终端20将包括加密的发行ID的时间获取请求发送至中央服务器40。

[0171] 在步骤S706中，时间更新处理单元1246确定是否已经由通信处理单元1243经由移动终端20从中央服务器40接收到时间信息。当在从通信处理单元1243发送时间获取请求之后的预定时间内通信处理单元1243已经接收到时间信息时，时间更新处理单元1246执行步骤S708，否则执行步骤S718。

[0172] 在步骤S708中，时间更新处理单元1246确定从通信处理单元1243发送时间获取请求到接收时间信息所经过时间(通信延迟时间Td)是否等于或小于预定阈值Td_th。预定阈值Td_th被预先设定为可以确定在中继来自中央服务器40的时间信息的移动终端20中是否存在有意的通信延迟的时间。当通信延迟时间Td等于或小于预定阈值Td_th时，时间更新处理单元1246确定在移动终端20等中不存在有意的通信延迟，并且执行步骤S710。当通信延迟时间Td不等于或不小于预定阈值Td_th时，时间更新处理单元1246确定在移动终端20等中存在有意的通信延迟，并且执行步骤S726。

[0173] 在步骤S710中，时间更新处理单元1246使用唯一钥匙1250a对由通信处理单元1243接收到的时间信息进行解密。

[0174] 在步骤S712中，时间更新处理单元1246通过将计时单元1244的时间更新为在经解密的时间信息中包括的中央服务器40(RTC 42)的时间来使计时单元1244的时间与中央服务器40的时间同步。

[0175] 在步骤S714中，确定单元1247基于包括在经解密的时间信息中的取消标记F来确定是否可以取消与用于由认证处理单元1245对经认证的移动终端20进行认证的认证钥匙相对应的车辆10的预约。当在经解密的时间信息中包括的取消标记F为“1”时，确定单元1247确定与用于认证经认证的移动终端20的认证钥匙相对应的车辆10的预约已经被取消，当取消标记F为“0”时确定车辆10的预约没有被取消。当与用于由认证处理单元1245对经认证的移动终端20进行认证的认证钥匙相对应的车辆10的预约没有被取消时，确定单元1247执行步骤S716，当预约已经被取消时执行步骤S726。

[0176] 在步骤S716中，确定单元1247确定当前时间是否在车辆10的预约时间内。具体地，确定单元1247确定计时单元1244的更新时间是否包括在由认证处理单元1245对移动终端20进行认证时从认证钥匙中提取的预约的开始时间和结束时间之间。当确定当前时间在车辆10的预约时间内时，确定单元1247执行步骤S722，当确定当前时间不在预约时间内时，执行步骤S726。

[0177] 另一方面，在步骤S718中，时间更新处理单元1246确定是否由通信处理单元1243从移动终端20接收到通信失败通知。通信失败通知从移动终端20发送至钥匙单元12，并且是指示以下内容的通知：例如由于移动终端20在移动电话网络之外或通过移动电话网络的

通信功能被关闭的原因，而不能向预约管理服务器30和中央服务器40发送移动终端20的信号并且不能从预约管理服务器30和中央服务器40接收移动终端20的信号。当在从通信处理单元1243发送时间获取请求之后的预定时间内已经由通信处理单元1243从移动终端20接收到通信失败通知时，时间更新处理单元1246无法从中央服务器40获取时间信息，因而不更新计时单元1244的时间，并且执行步骤S720。否则，这个过程结束。

[0178] 在步骤S720中，确定单元1247确定当前时间是否在车辆10的预约时间内。此处，由于移动终端20和预约管理服务器30之间的通信是不可能的，并且计时单元1244的时间与中央服务器40的时间不同步，因此执行简单的确定。具体地，基于存储在存储单元1250中的用于认证移动终端20的认证钥匙的历史中包括的车辆10的预约信息的历史(预约的开始时间和结束时间)，当与用于认证当前认证的移动终端20的当前认证钥匙相对应的车辆10的预约的开始时间晚于用于认证先前认证的移动终端20的认证钥匙相对应的车辆10的预约的结束时间时，确定单元1247确定当前时间在车辆10的预约时间内，否则确定当前时间不在车辆10的预约时间内。当确定单元1247确定当前时间在车辆10的预约时间内时执行步骤S722，当确定当前时间不在车辆10的预约时间内时执行步骤S726。

[0179] 在步骤S722中，加锁和解锁处理单元1249打开加锁和解锁功能。

[0180] 当钥匙单元12的加锁和解锁功能关闭时，具有非常小的功耗的通信处理单元1243、计时单元1244、认证处理单元1245、时间更新处理单元1246、确定单元1247、加密钥匙生成单元1248、加锁和解锁处理单元1249等的功能是可用的。当钥匙单元12的加锁和解锁功能被从OFF状态切换到ON状态时，例如，具有大功耗的LF波接收器121、RF波发送器122等是可用的。

[0181] 在步骤S724中，认证处理单元1245经由通信处理单元1243将指示加锁和解锁功能打开的加锁和解锁功能ON通知发送至移动终端20，并且结束该过程。

[0182] 另一方面，在步骤S726中，加锁和解锁处理单元1249强行切断通过通信处理单元1243建立的钥匙单元12和移动终端20之间的BLE通信的通信会话，并且禁止随后的移动终端20的重新访问。也就是说，禁止通过移动终端20解锁车辆10。因此，当通过步骤S708的过程确定在从中央服务器40向钥匙单元12发送时间信息的过程中在移动终端20中存在有意的通信延迟时，在移动终端20与钥匙单元12之间的通信被切断并且禁止重新访问。因此，例如，即使恶意的第三方使用移动终端20有意操作钥匙单元12的时间并意图在预定时间之外进行未经授权使用时，可以防止未经授权使用。当通过步骤S714的过程确定与用于认证经认证的移动终端20的认证钥匙相对应的车辆10的预约已经被取消时，移动终端20和钥匙单元12之间的通信被切断并禁止重新访问。因此，例如，即使当存储有先前获取的认证钥匙的移动终端20被移交给恶意的第三方时，移动终端20的授权用户也可以使用另一个终端、电话等取消车辆10的预约，以禁止恶意第三方使用车辆10来防止车辆10的未经授权使用。当通过步骤S716的过程确定当前时间不在车辆10的预约时间内时，移动终端20和钥匙单元12之间的通信被切断并且重新访问被禁止。因此，例如，在使用预先获取的认证钥匙的车辆10的预约的开始时间之前，不能使用车辆10，因而可以防止车辆10的未经授权使用。当通过步骤S720的过程确定当前时间不在车辆10的预约时间内时，移动终端20和钥匙单元12之间的通信被切断并且重新访问被禁止。因此，例如，即使当由于移动终端20在移动电话网络等之外的原因而无法更新计时单元1244的时间时，也可以防止车辆10在至少紧接先前预约的结

束时间之前被使用。

[0183] 图8是示意性地示出由中央服务器40的管理装置43执行的时间更新过程的示例的流程图。例如，当由通信处理单元431经由预约管理服务器30从钥匙单元12已接收到时间获取请求时，执行流程图中的过程。

[0184] 在步骤S802中，时间同步处理单元433使用存储在唯一钥匙DB 435中的与作为发送源的钥匙单元12相对应的唯一钥匙对由通信处理单元431接收到的时间获取请求的数据进行解密。

[0185] 在步骤S804中，时间同步处理单元433参照取消信息DB 438确定是否已经取消与在经解密的时间获取请求中包括的认证钥匙的发行ID相对应的车辆10的预约。在已经取消与在时间获取请求中包括的认证钥匙的发行ID相对应的车辆10的预约时，时间同步处理单元433执行步骤S806，在没有取消预约时执行步骤S808。

[0186] 在步骤S806中，时间同步处理单元433将指示车辆10的预约已经被取消的取消标记F设定为“1”，然后执行步骤S810。

[0187] 另一方面，在步骤S808中，时间同步处理单元433将指示车辆10的预约还没有被取消的取消标记F设定为“0”，然后执行步骤S810。

[0188] 在步骤S810中，时间同步处理单元433获取中央服务器40的时间，即，RTC 42的时间。

[0189] 在步骤S812中，时间同步处理单元433生成包括所获取的中央服务器40的时间和取消标记F的时间信息，并使用存储在唯一钥匙DB 435中的与作为时间获取请求的发送源的钥匙单元12相对应的唯一钥匙对时间信息进行加密。

[0190] 在步骤S814中，时间同步处理单元433经由通信处理单元431、预约管理服务器30和移动终端20将经加密的时间信息发送至钥匙单元12，并且结束该过程。因此，每当在移动终端20和钥匙单元12之间可以通信的状态下经由移动终端20和预约管理服务器30从钥匙单元12向中央服务器40发送时间获取请求时，取消标记F连同时间一起从中央服务器40发送，因而钥匙单元12侧可以掌握对车辆10的预约是否已经取消。

[0191] 图9是示意性地示出由钥匙单元12的钥匙ECU 124执行的解锁过程的示例的流程图。例如，在加锁和解锁功能打开的状态下以预定的时间间隔重复执行流程图中的过程。

[0192] 在步骤S902中，加锁和解锁处理单元1249确定是否已经由通信处理单元1243从移动终端20接收到使用通信加密钥匙加密的解锁请求。当由通信处理单元1243已经从移动终端20接收到使用通信加密钥匙加密的解锁请求时，加锁和解锁处理单元1249执行步骤S904，否则结束该过程。

[0193] 在步骤S904中，加锁和解锁处理单元1249确定是否已经响应于最新的时间获取请求而更新了计时单元1244的时间。当计时单元1244的时间已经响应于最新的时间获取请求而被更新时，过程转变到步骤S906，当计时单元1244的时间没有响应于最新的时间获取请求而被更新时，过程转变到步骤S908。

[0194] 在步骤S906中，确定单元1247确定当前时间是否在与用于认证移动终端20的认证钥匙相对应的车辆10的预约时间内。具体地，确定单元1247确定计时单元1244的时间是否包括在认证钥匙中包括的预约信息的开始时间和结束时间之间。在当前时间在与用于认证移动终端20的认证钥匙相对应的车辆10的预约时间内时，确定单元1247执行步骤S912，在

当前时间不在预约时间内时执行步骤S914。

[0195] 另一方面，在步骤S908中，加锁和解锁处理单元1249确定计时单元1244的时间未被更新的时间(未更新时间)Tnu是否等于或小于预定阈值Tnu_th。当计时单元1244的未更新时间Tnu等于或小于预定阈值Tnu_th时，加锁和解锁处理单元1249执行步骤S910，当计时单元1244的未更新时间Tnu不等于或不小于预定阈值Tnu_th时，执行步骤S914。

[0196] 在步骤S910中，确定单元1247确定当前时间是否在车辆10的预约时间内。此处，由于移动终端20和预约管理服务器30之间不可以进行通信并且计时单元1244的时间与中央服务器40的时间不同步，因此执行简单的确定。具体地，基于存储在存储单元1250中的用于认证移动终端20的认证钥匙的历史中包括的车辆10的预约信息的历史(预约的开始时间和结束时间)，当与用于认证当前认证的移动终端20的当前认证钥匙相对应的车辆10的预约的开始时间晚于用于认证先前认证的移动终端20的认证钥匙相对应的车辆10的预约的结束时间时，确定单元1247确定当前时间在车辆10的预约时间内，否则确定当前时间不在车辆10的预约时间内。当确定单元1247确定当前时间在车辆10的预约时间内时执行步骤S912，当确定当前时间不在车辆10的预约时间内时执行步骤S914。

[0197] 在步骤S912中，加锁和解锁处理单元1249执行解锁车辆10的门的过程，即，经由RF发送处理单元1242将解锁信号发送至加锁和解锁装置11，并解锁车辆10的门。

[0198] 另一方面，在步骤S914中，通信处理单元1243强行切断钥匙单元12与移动终端20之间的BLE通信的通信会话，并禁止随后的移动终端20的重新访问。也就是说，禁止使用移动终端20解锁车辆10。因此，获得了与图7中的步骤S726的过程相同的操作和优点。也就是说，例如在使用已预先获取的认证钥匙对车辆10的预约的开始时间之前，不能使用车辆10，并且可以防止车辆10的未经授权使用。例如，即使当由于移动终端20在移动电话网络等之外的原因而无法更新计时单元1244的时间时，也可以防止在至少紧接先前预约的预约结束时间之前车辆10被使用。此外，在该示例中，当通过步骤S908的过程钥匙单元12(计时单元1244)的未更新时间Tnu大于预定阈值Tnu_th时，移动终端20和钥匙单元12之间的通信被切断并且禁止重新访问。因此，例如即使当用户有意地关闭移动终端20的通信处理单元232的通信功能并且继续在钥匙单元12的时间与中央服务器40的时间不同步的状态下使用车辆10时，也可以通过将预定阈值Tnu_th设置为未更新时间Tnu的限制时间来防止车辆10的未经授权使用。

[0199] 当由通信处理单元1243已经从移动终端20接收到加锁信号时，加锁和解锁处理单元1249可以被配置成跳过图9中的步骤S904至S910和S914的过程，并且执行加锁车辆10的门的过程，即，经由RF发送处理单元1242向加锁和解锁装置11发送加锁信号。由于车辆10的加锁指的是用户走下车辆10并离开车辆10的情况，所以即使怀疑车辆10的未经授权使用，也认为优选地允许加锁。当已经由通信处理单元1243从移动终端20接收到加锁信号时，可以执行与图9中所示过程相同的过程。

[0200] 图10是示意性地示出与由加锁和解锁系统1中的钥匙单元12和中央服务器40执行的时间同步过程和由钥匙单元12执行的解锁过程相关联的操作的示例的顺序图。

[0201] 以下的描述是基于如下前提：图10所示的顺序图中的加锁和解锁系统1的操作是在图6所示的顺序图中的操作之后执行的。

[0202] 在步骤S1002中，钥匙单元12的时间更新处理单元1246对用于认证经认证的移动

终端20的认证钥匙的发行ID进行加密(图7中的步骤S702)。

[0203] 在步骤S1004中,钥匙单元12的时间更新处理单元1246经由通信处理单元1243将包括经加密的发行ID的时间获取请求发送至移动终端20(图7中的步骤S704)。

[0204] 在步骤S1006中,当从钥匙单元12接收到以中央服务器40为目的地的时间获取请求时,移动终端20的通信处理单元231将接收到的时间获取请求传送至通信处理单元232,并且通信处理单元232将时间获取请求发送至预约管理服务器30。

[0205] 在步骤S1008中,当从移动终端20接收到以中央服务器40为目的地的时间获取请求时,预约管理服务器30的通信处理单元321将接收到的时间获取请求发送至中央服务器40。

[0206] 在步骤S1010中,中央服务器40的时间同步处理单元433对由通信处理单元431接收到的时间获取请求的数据进行解密(图8中的步骤S802)。

[0207] 在步骤S1012中,中央服务器40的时间同步处理单元433将取消信息DB 438中的取消信息与包括在时间获取请求中的认证钥匙的发行ID进行比较,并设定取消标记F(图8中的步骤S804至S808)。

[0208] 在步骤S1014中,中央服务器40的时间同步处理单元433获取中央服务器40(RTC 42)的时间(图8中的步骤S810)。

[0209] 在步骤S1015中,时间同步处理单元433生成包括中央服务器40的时间和取消标记F的时间信息,并且使用唯一钥匙对所生成的时间信息进行加密(图8中的步骤S812)。

[0210] 在步骤S1016中,时间同步处理单元433经由通信处理单元431将经加密的时间信息发送至预约管理服务器30(图8中的步骤S814)。

[0211] 在步骤1018中,当从中央服务器40接收到钥匙单元12的时间信息时,预约管理服务器30的通信处理单元321将时间信息发送至移动终端20

[0212] 在步骤S1020中,当从预约管理服务器30接收到钥匙单元12的时间信息时,移动终端20的通信处理单元232将时间信息传送至通信处理单元231,并且通信处理单元231将时间信息发送至钥匙单元12。

[0213] 在步骤S1021中,当通信处理单元1243接收到时间信息时,钥匙单元12的时间更新处理单元1246确认通信延迟时间Td的限制要求(通信延迟时间Td是否等于或小于预定阈值Td_th)(图7中的步骤S708)。

[0214] 当通信延迟时间Td等于或小于预定阈值Td_th时(图7中的步骤S708中的“是”),在步骤S1022中时间更新处理单元1246使用唯一钥匙1250a对时间信息进行解密(图7中的步骤S710)。

[0215] 在步骤S1024中,钥匙单元12的时间更新处理单元1246将计时单元1244的时间更新为在经解密的时间信息中包括的中央服务器40(RTC 42)的时间(图7中的步骤S712)。

[0216] 在步骤S1026中,钥匙单元12的确定单元1247确认在经解密的时间信息中包括的取消标记F,并确定是否已经取消与经认证的移动终端20相对应的车辆10的预约(图7中的步骤S714)。

[0217] 当与经认证的移动终端20相对应的车辆10的预约没有被取消(图7中的步骤S714中的“否”)时,在步骤S1028中钥匙单元12的确定单元1247确认包括在与经认证的移动终端20相对应的认证钥匙中的预约信息(车辆10的预约的开始时间和结束时间),并且确定当前

时间是否在车辆10的预约时间内(图7中的步骤S716)。

[0218] 当当前时间在车辆10的预约时间内时(图7中的步骤S716中的“是”),在步骤S1030中加锁和解锁处理单元1249打开加锁和解锁功能(图7中的步骤S722)

[0219] 在步骤S1032中,加锁和解锁处理单元1249经由通信处理单元1243将加锁和解锁功能ON通知发送至移动终端20(图7中的步骤S724)。

[0220] 在步骤S1034中,移动终端20的加锁和解锁请求单元235接收在显示器24的GUI上的用户的预定操作(解锁操作)。

[0221] 在步骤S1036中,移动终端20的加锁和解锁请求单元235响应于解锁操作经由通信处理单元231将已经使用存储在存储单元239中的通信加密钥匙加密的解锁请求发送至钥匙单元12。

[0222] 在步骤S1038中,当由通信处理单元1243接收到解锁请求时(图9中的S902中的“是”),已经执行了最新的时间更新(图9中的S904中的“是”),并且因此钥匙单元12的确定单元1247确认包括在与经认证的移动终端20相对应的认证钥匙中的预约信息(车辆10的预约的开始时间和结束时间),并确定当前时间是否在车辆10的预约时间内(图9中的步骤S906)。

[0223] 当当前时间在车辆10的预约时间内时(图9中的步骤S906中的“是”),在步骤S1040中钥匙单元12的加锁和解锁处理单元1249执行解锁车辆10的门的过程,并解锁车辆10的门。

[0224] 如上所述,通过步骤S1002至步骤S1040完成执行一系列操作:更新钥匙单元12的时间(与中央服务器40的时间同步),开始由各种限制要求的确认导致的加锁和解锁功能,并且基于解锁操作解锁车辆10的门。

[0225] 这样,在该实施方式中,中央服务器40包括通信处理单元431,通信处理单元431将指示是否已经取消车辆10的预约的取消标志F(取消信息)发送至钥匙单元12。移动终端20包括通信处理单元231,通信处理单元231将与车辆10的预约相关的认证钥匙(第一认证信息)发送至钥匙单元12,并且将用于请求解锁或加锁车辆10的门的解锁请求或加锁请求(两者都是第一请求信号)发送至钥匙单元12。钥匙单元12包括:通信处理单元1243,其从中央服务器40接收取消标记F,从移动终端20接收认证钥匙,并且从移动终端20接收解锁请求和加锁请求;认证处理单元1245,其当通信处理单元1243已经接收到认证钥匙时基于认证钥匙来认证移动终端20;以及加锁和解锁处理单元1249,其当认证处理单元1245对移动终端20的认证已经成功并且通信处理单元1243已经接收到解锁请求或加锁请求时,执行解锁或加锁车辆10的门的过程。当认证处理单元1245对移动终端20的认证已经成功并且由通信处理单元1243接收到的取消标记F指示已经取消了与用于认证处理单元1245对移动终端20的认证的认证钥匙相对应的车辆10的预约时,加锁和解锁处理单元1249禁止基于从移动终端20发送的解锁请求来解锁车辆10的门。因此,即使当恶意第三方已经获得预先获取并存储了认证钥匙(第一认证信息)的移动终端20时,也可以例如通过使移动终端20的用户使用任何方法取消车辆10的预约来禁止使用移动终端20解锁车辆10。因此,可以防止恶意第三方不适当地使用车辆10。

[0226] 在该实施方式中,钥匙单元12包括通信处理单元1243,当认证处理单元1245对移动终端20的认证已经成功时,通信处理单元1243经由移动终端20和预约管理服务器30将包

括对与用于认证处理单元1245对移动终端20的认证的认证钥匙相对应的取消标记F的请求的第二请求信号(时间获取请求)发送至中央服务器40。中央服务器40包括通信处理单元431,通信处理单元431接收从钥匙单元12发送的第二请求信号(时间获取请求)。当第二请求信号(时间获取请求)已经由通信处理单元431自身接收时,通信处理单元431将包括取消标记F的响应信号(时间信息)经由预约管理服务器30和移动终端20发送至钥匙单元12。因此,即使当已经获得其中存储了预先获取的认证钥匙的移动终端20的恶意第三方已经成功认证移动终端20时,也会在认证成功作为触发的情况下将第二请求信号从钥匙单元12立即发送至服务器40,并且响应于第二请求信号也可以禁止基于从中央服务器40发送的取消标记F来使用移动终端20解锁车辆10。因此,可以防止恶意第三方不适当地使用车辆10。

[0227] 在该实施方式中,钥匙单元12包括执行计时的计时单元1244。中央服务器40包括以比钥匙单元12的计时单元1244更高的精度来执行计时的RTC 42。移动终端20的通信处理单元231和通信处理单元232(中继单元)执行中继功能:接收从中央服务器40和钥匙单元12中的一者发送至另一者的信号,并且将信号发送(传送)至另一者。钥匙单元12的通信处理单元1243将对中央服务器40的包括对取消标记F的请求和对RTC42的时间的请求的时间获取请求发送至移动终端20,移动终端20的中继单元从钥匙单元12接收时间获取请求,并且将时间获取请求经由预约管理服务器30发送至中央服务器40,并且中央服务器40的通信处理单元431从移动终端20接收时间获取请求。当已经接收到时间获取请求时,中央服务器40的通信处理单元431将对钥匙单元12的包括取消标记F和RTC 42的时间的时间信息经由预约管理服务器30发送至移动终端20,移动终端20的中继单元从中央服务器40接收时间信息并将时间信息发送至钥匙单元12,并且钥匙单元12的通信处理单元1243从移动终端20接收时间信息。钥匙单元12的计时单元1244基于在通信处理单元1243接收到的时间信息中包括的RTC 42的时间与RTC 42同步。因此,钥匙单元12需要在与移动终端20的通信为可能的状态下以相对低的精度执行计时单元1244的时间的同步。在这种情况下,可以通过采用如下配置来实现中央服务器40、移动终端20和钥匙单元12之间的通信效率的提高:在该配置中,在可以与移动终端20进行通信的状态下执行的移动终端20的认证成功作为触发的情况下,发送包括发送至中央服务器40的对取消标记F的获取请求和对中央服务器40(RTC 42)的时间的获取请求的第二请求信号(时间获取请求),并且取消标记F和中央服务器40的时间两者是同时从中央服务器40获取的。

[0228] 可以使用与用于发送时间信息的信号不同的信号将取消标志F从中央服务器40发送至钥匙单元12。

[0229] 在该实施方式中,加锁和解锁系统1包括安装在车辆10中的加锁和解锁装置11。钥匙单元12包括存储单元1250,其存储与车辆10相关的加锁和解锁钥匙信息1250b。加锁和解锁装置11包括:RF接收处理单元1132,其接收包括来自钥匙单元12的加锁和解锁钥匙信息1250b的解锁信号和加锁信号(第三请求信号);认证处理单元1133,其在RF接收处理单元1132接收到解锁信号和加锁信号时,基于包括在解锁信号和加锁信号中的加锁和解锁钥匙信息来执行钥匙单元的认证;以及加锁和解锁控制单元1134,其在通过认证处理单元1133的认证时解锁或加锁车辆10的门。钥匙单元12的加锁和解锁处理单元1249经由RF发送处理单元1242将包括加锁和解锁钥匙信息1250b的解锁信号或加锁信号发送至加锁和解锁装置11作为解锁或加锁车辆10的门的过程。因此,钥匙单元12可以通过将解锁信号和加锁信号

发送至安装在车辆10中的加锁和解锁装置11来解锁和加锁车辆10。因此，例如，可以通过在已经安装在车辆10中的加锁和解锁装置11中另外设置钥匙单元12来对加锁和解锁系统1进行配置。

[0230] 在该实施方式中，钥匙单元12(加锁和解锁处理单元1249)被配置成经由加锁和解锁装置11的比较ECU 113来解锁和加锁车辆10的门，但是例如可以采用其中钥匙单元12直接向主体ECU 114发送控制指令以操作门锁马达115的配置。

[0231] 在该实施方式中，移动终端20(认证钥匙获取单元233)从中央服务器40获取认证钥匙，但是本发明不限于该配置。例如，认证钥匙可以以有线或无线的方式从与共享车或租用车相关联的预定存储中设置的特定终端获取。

[0232] 尽管以上已经详细描述了本发明的实施方式，但是本发明不限于具体实施方式，并且可以在不脱离所附权利要求中描述的本发明的要点的情况下以各种形式进行修改和改变。

[0233] 例如，在实施方式中，加锁和解锁和预约的对象是车辆，但是不限于车辆，只要其可以由多个用户及时共享和使用并且可以被加锁并且解锁即可。也就是说，可以利用例如诸如会议室、度假屋或体育馆等的可加锁和可解锁设施来代替作为本实施方式的加锁和解锁和预约对象的车辆。因此，如上述实施方式所提及的，可以提高使用该设施的用户的便利性，并且防止不适当地侵入设施。

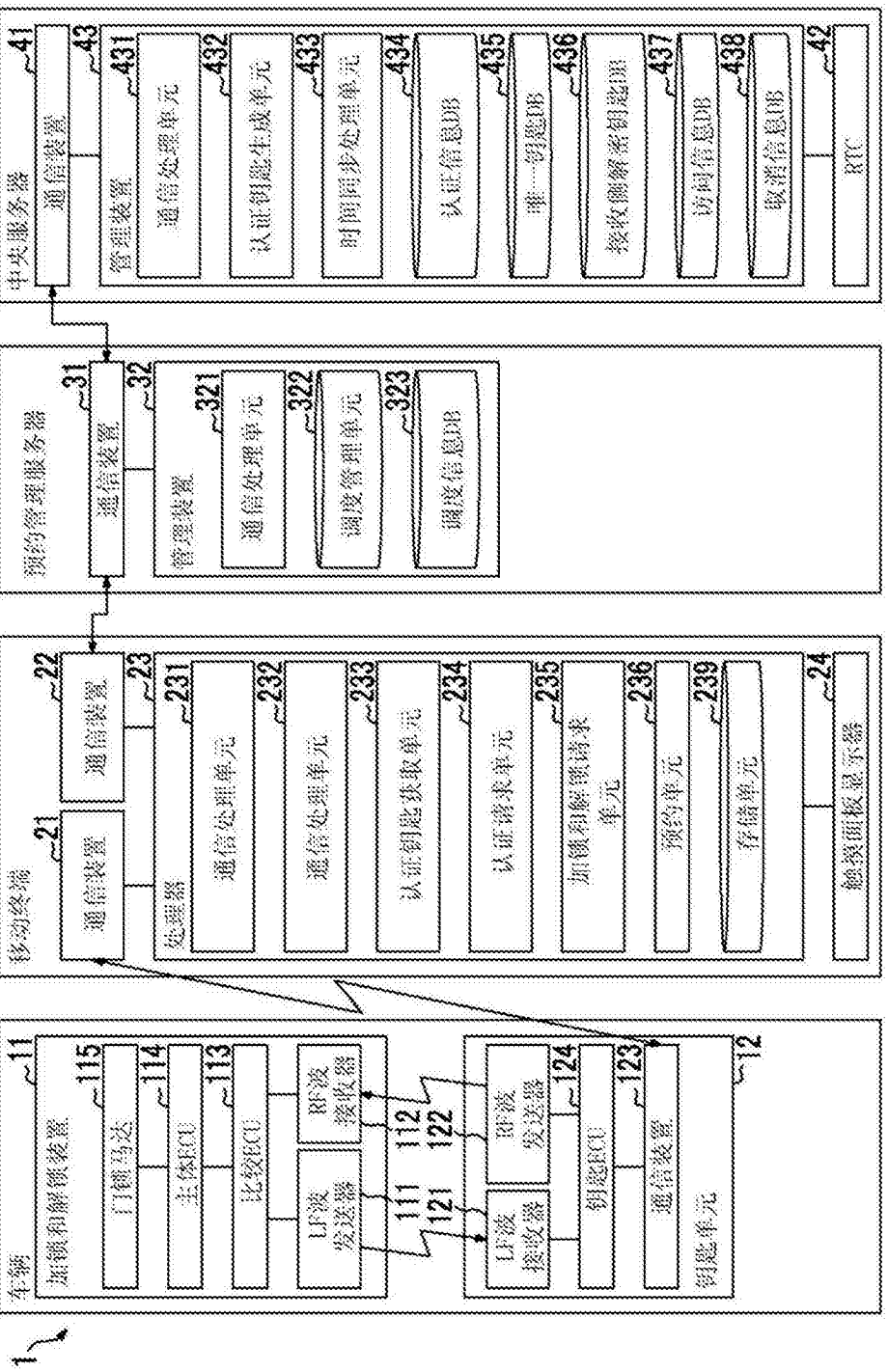

40
41
通信装置
43
管理装置
431
通信处理单元
432
认证钥匙生成单元
433
时间同步处理单元
434
认证信息DB
435
唯一钥匙DB
436
接收侧解密钥匙DB
437
访问信息DB
438
取消信息DB
42
RTC
中央服务器
30
31
通信装置
32
管理装置
321
通信处理单元
322
调度管理单元
323
调度信息DB
预约管理服务器
22
通信装置
23
处理器
231
通信处理单元
232
通信处理单元
233
认证钥匙获取单元
234
认证请求单元
235
加锁和解锁请求单元
236
预约单元
239
存储单元
24
触摸面板显示器
21
通信装置
20
移动终端
10
11
车辆
加锁和解锁装置
115
门锁马达
114
主体ECU
113
比较ECU
LF波发送器
111
121
RF波接收器
112
122
LF波接收器
RF波发送器
124
钥匙ECU
123
通信装置
12
钥匙单元
1

图1

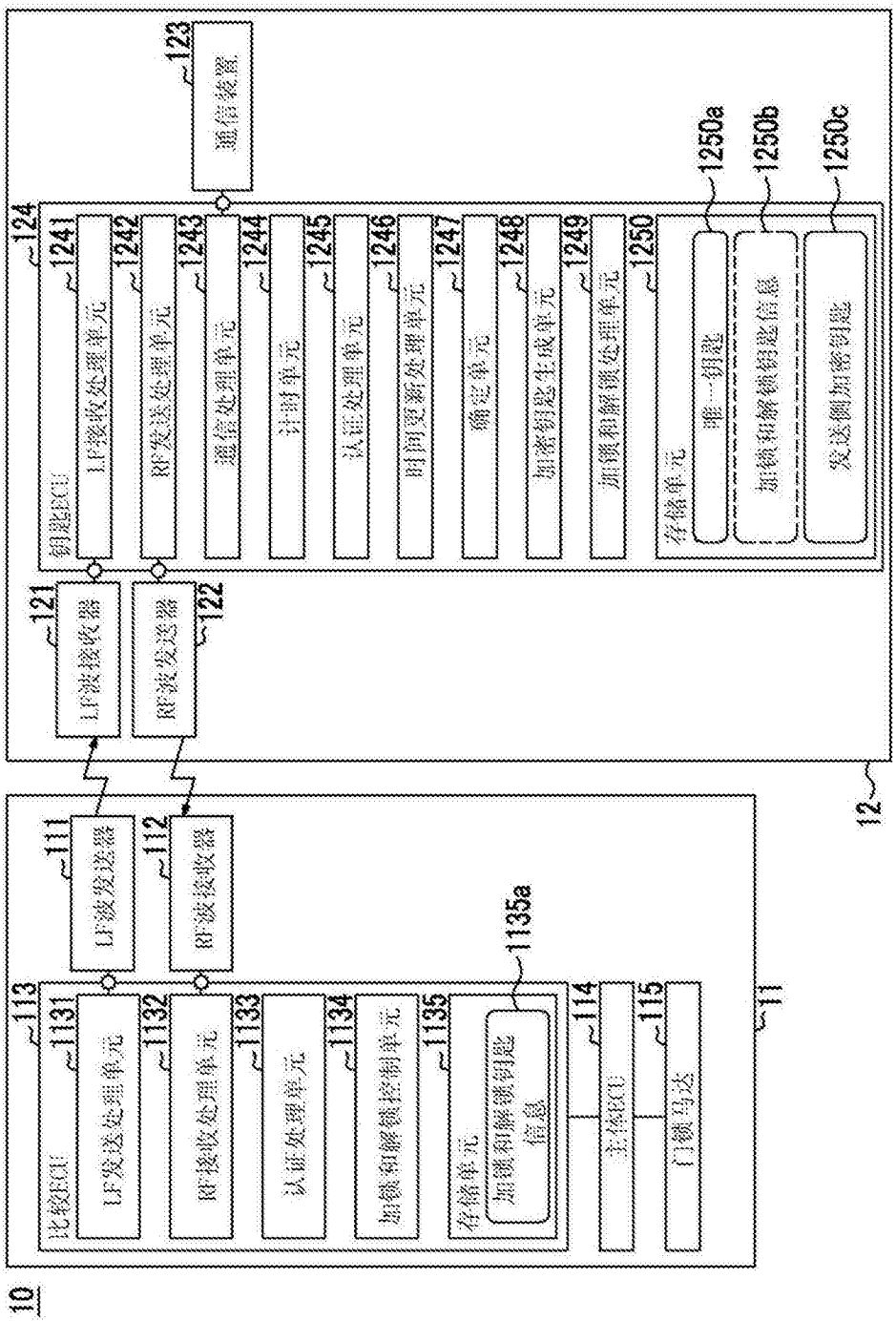

10
11
12
111
LF波发送器
112
RF波接收器
113
比较ECU
1131
LF发送处理单元
1132
RF接收处理单元
1133
认证处理单元
1134
加锁和解锁控制单元
1135
存储单元
1135a
加锁和解锁钥匙信息
114
主体ECU
115
门锁马达
121
LF波接收器
122
RF波发送器
123
通信装置
124
钥匙ECU
1241
LF接收处理单元
1242
RF发送处理单元
1243
通信处理单元
1244
计时单元
1245
认证处理单元
1246
时间更新处理单元
1247
确定单元
1248
加密钥匙生成单元
1249
加锁和解锁处理单元
1250
存储单元
1250a
唯一钥匙
1250b
加锁和解锁钥匙信息
1250c
发送侧加密钥匙

图2

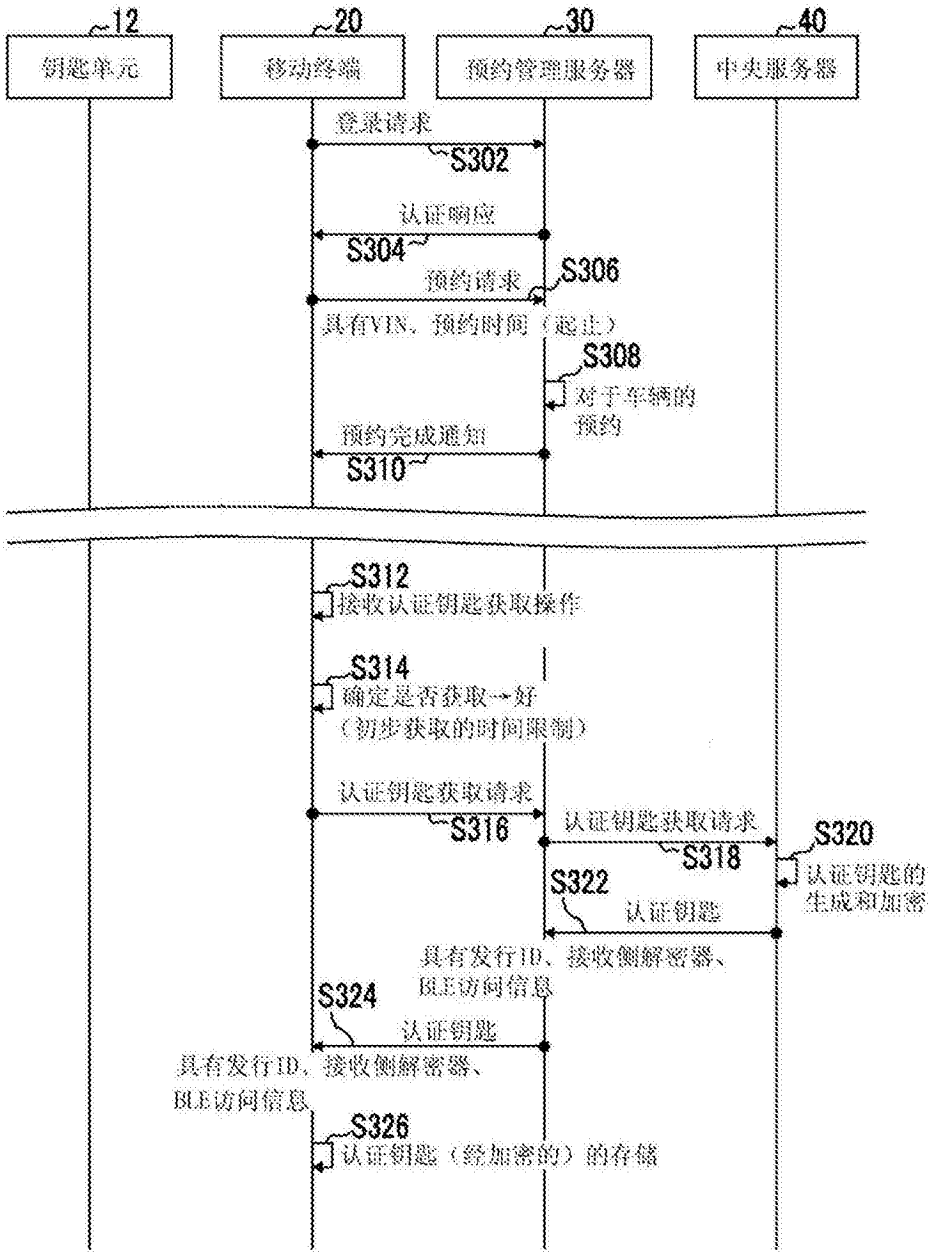

12
钥匙单元
20
移动终端
30
预约管理服务器
40
中央服务器
登录请求
S302
认证响应
S304
预约请求
S306
具有VIN、预约时间（起止）
S308
对于车辆的
预约
预约完成通知
S310
S312
接收认证钥匙获取操作
S314
确定是否获取一好
（初步获取的时间限制）
认证钥匙获取请求
S316
认证钥匙获取请求
S318
S320
认证钥匙的
生成和加密
S322
认证钥匙
具有发行ID、接收侧解密器、
BLE访问信息
S324
认证钥匙
具有发行ID、接收侧解密器、
BLE访问信息
S326
认证钥匙（经加密的）的存储

图3

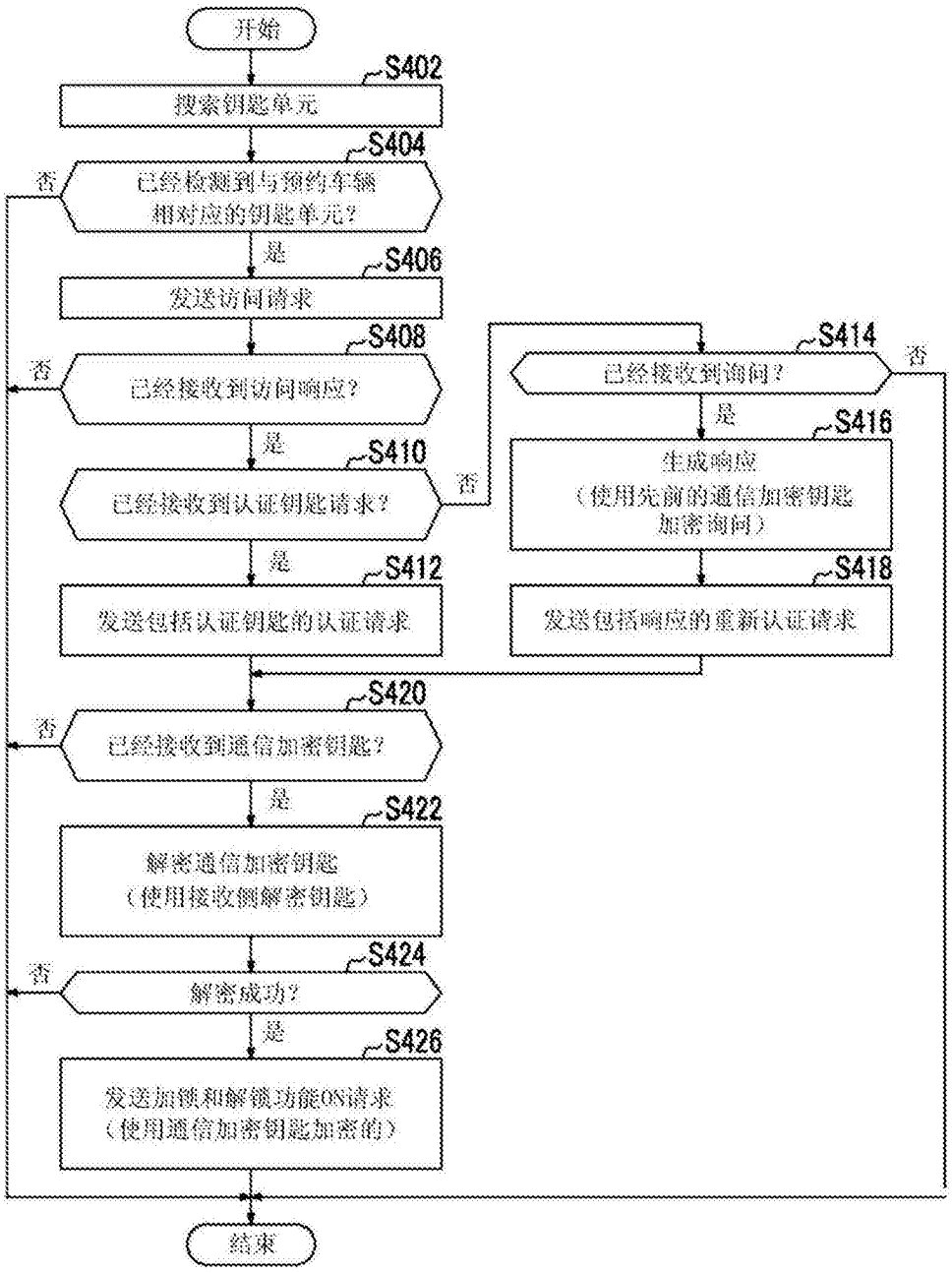

开始
S402
搜索钥匙单元
S404
已经检测到与预约车辆相对应的钥匙单元？
否
是
S406
发送访问请求
S408
已经接收到访问响应？
否
是
S410
已经接收到认证钥匙请求？
否
是
S412
发送包括认证钥匙的认证请求
S414
已经接收到询问？
否
是
S416
生成响应
（使用先前的通信加密钥匙加密询问）
S418
发送包括响应的重新认证请求
S420
已经接收到通信加密钥匙？
否
是
S422
解密通信加密钥匙
（使用接收侧解密钥匙）
S424
解密成功？
否
是
S426
发送加锁和解锁功能ON请求
（使用通信加密钥匙加密的）
结束

图4

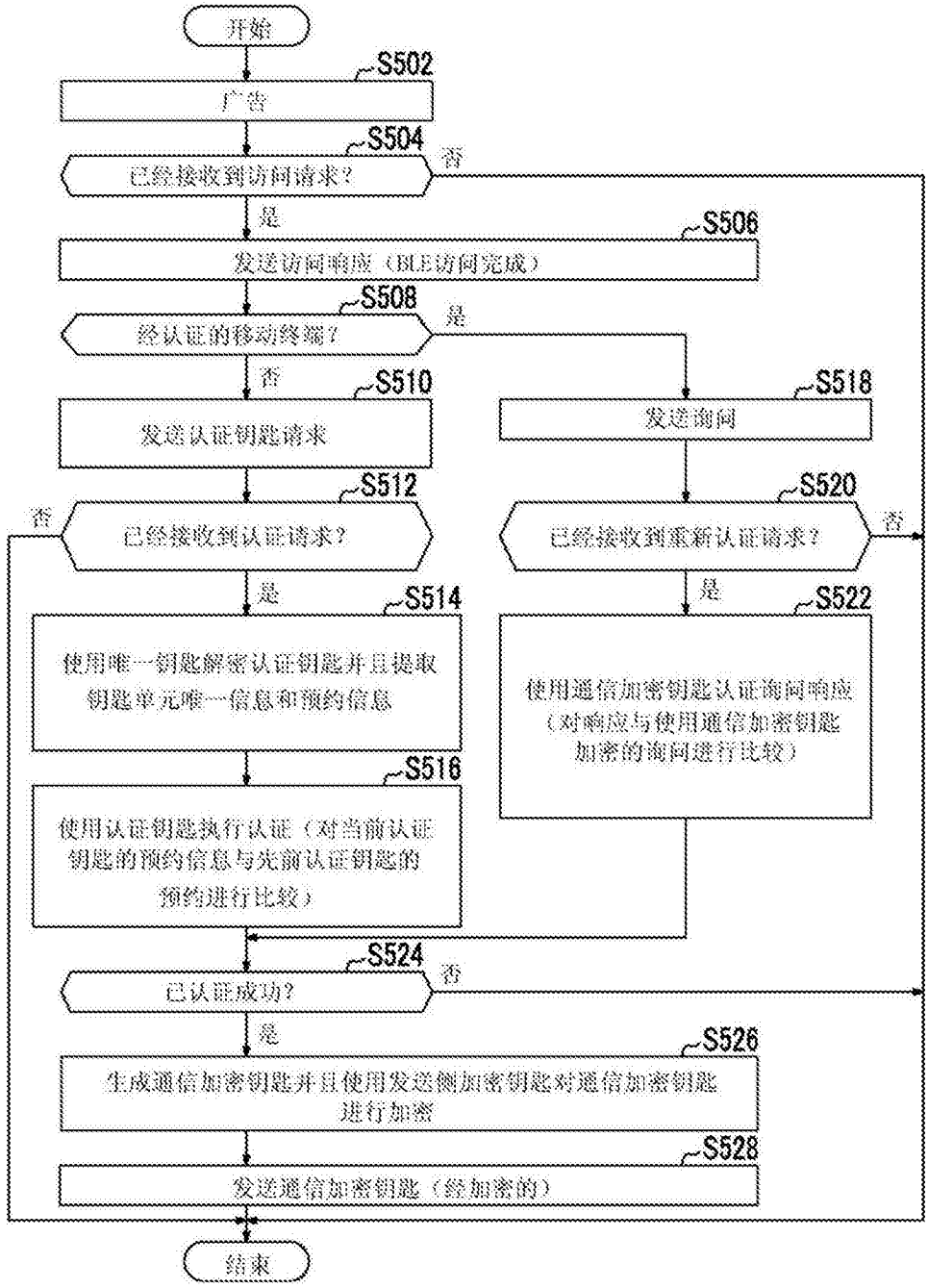

开始
S502
广告
S504
已经接收到访问请求?
否
是
S506
发送访问响应（BLE访问完成）
S508
经认证的移动终端?
是
否
S510
发送认证钥匙请求
S512
已经接收到认证请求?
否
是
S514
使用唯一钥匙解密认证钥匙并且提取钥匙单元唯一信息和预约信息
S516
使用认证钥匙执行认证（对当前认证钥匙的预约信息与先前认证钥匙的预约进行比较）
S518
发送询问
S520
已经接收到重新认证请求?
否
是
S522
使用通信加密钥匙认证询问响应（对响应与使用通信加密钥匙加密的询问进行比较）
S524
已认证成功?
否
是
S526
生成通信加密钥匙并且使用发送侧加密钥匙对通信加密钥匙进行加密
S528
发送通信加密钥匙（经加密的）
结束

图5

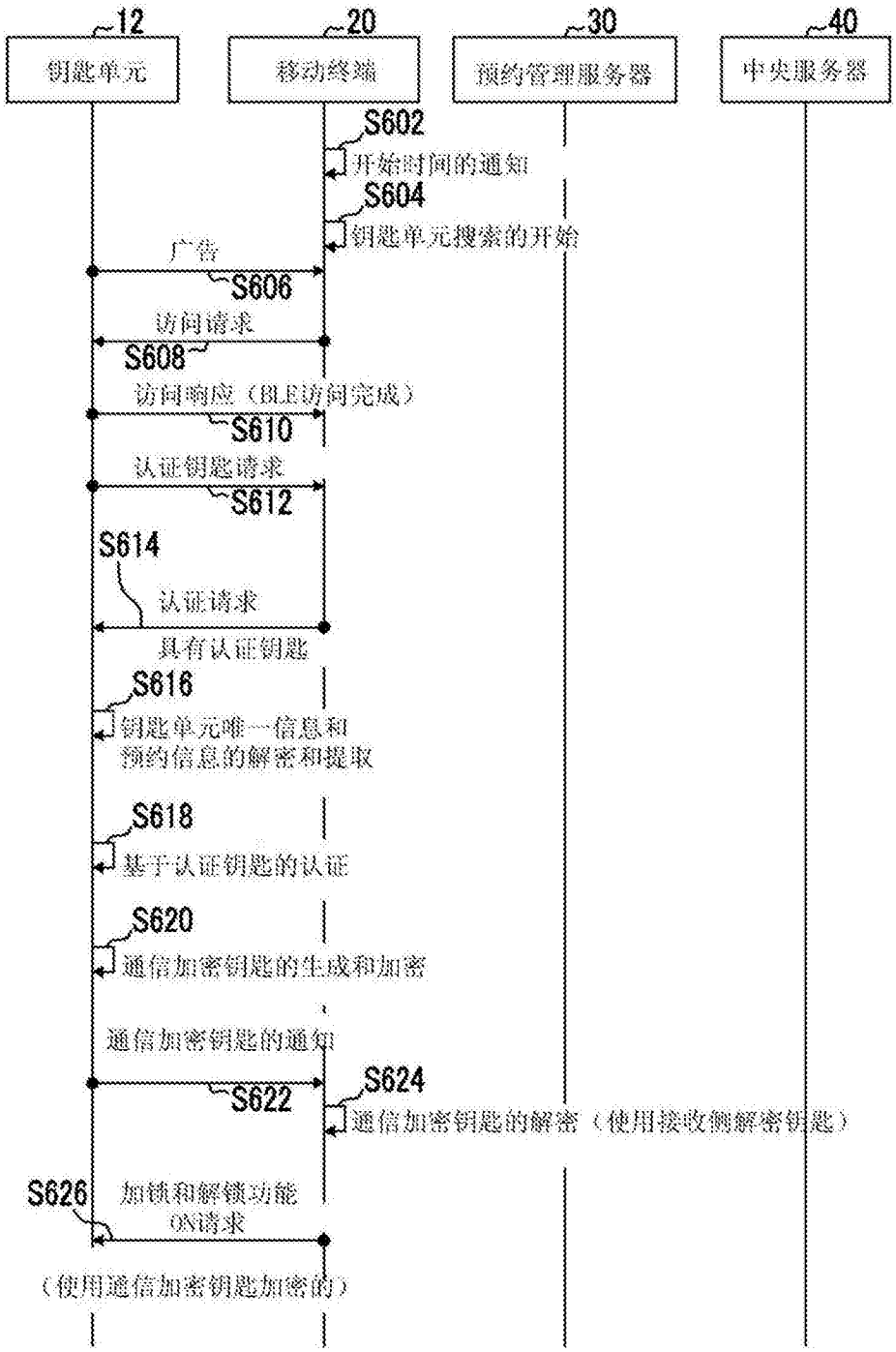

12
钥匙单元
20
移动终端
30
预约管理服务器
40
中央服务器
S602
开始时间的通知
S604
钥匙单元搜索的开始
广告
S606
访问请求
S608
访问响应（BLE访问完成）
S610
认证钥匙请求
S612
S614
认证请求
具有认证钥匙
S616
钥匙单元唯一信息和
预约信息的解密和提取
S618
基于认证钥匙的认证
S620
通信加密钥匙的生成和加密
通信加密钥匙的通知
S622
S624
通信加密钥匙的解密（使用接收侧解密钥匙）
S626
加锁和解锁功能
ON请求
（使用通信加密钥匙加密的）

图6

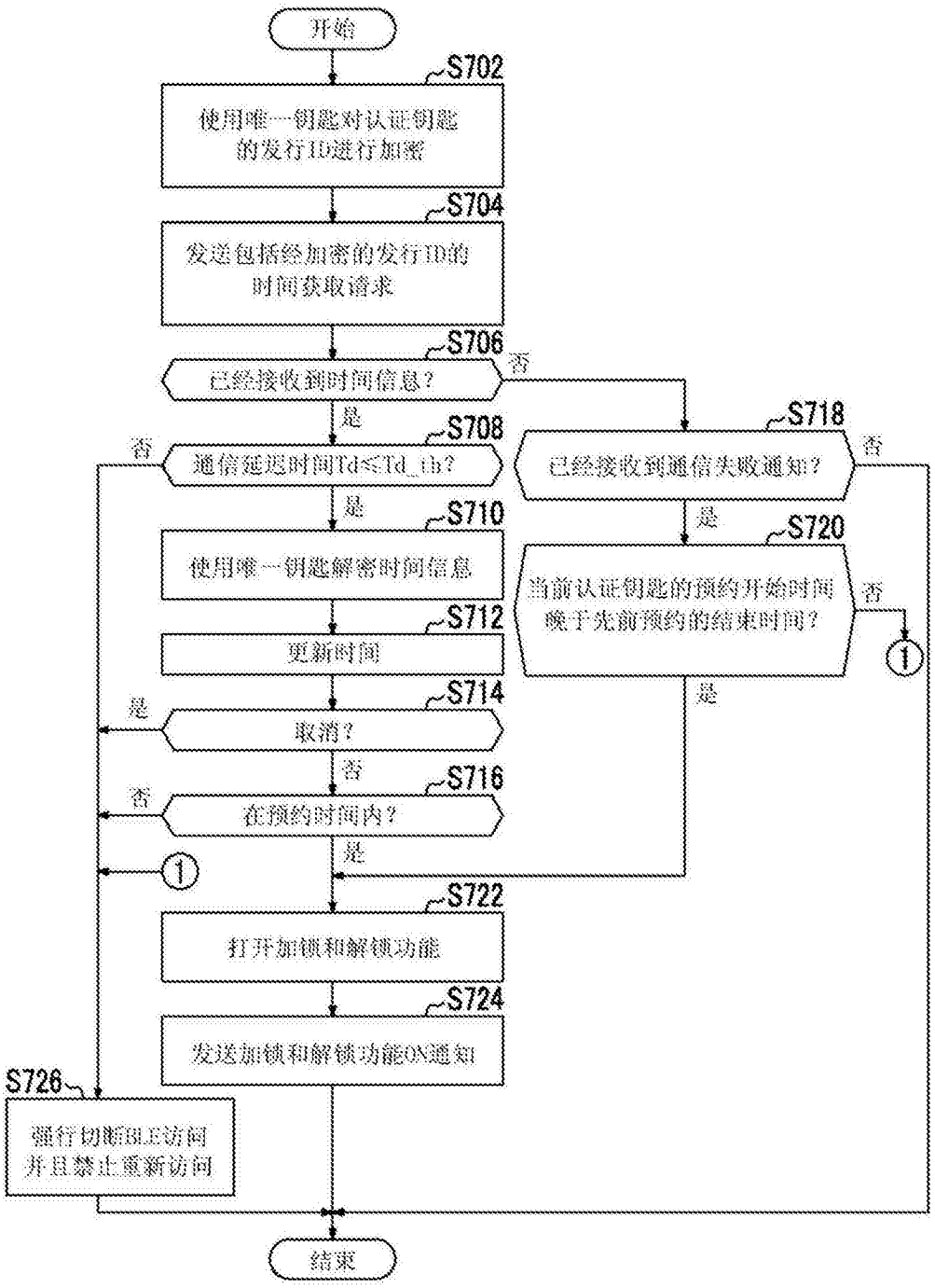

开始
S702
使用唯一钥匙对认证钥匙的发行ID进行加密
S704
发送包括经加密的发行ID的时间获取请求
S706
已经接收到时间信息？
否
是
S708
通信延迟时间Td≤Td_th？
否
是
S710
使用唯一钥匙解密时间信息
S712
更新时间
S714
取消？
是
否
S716
在预约时间内？
否
是
①
S718
已经接收到通信失败通知？
否
是
S720
当前认证钥匙的预约开始时间晚于先前预约的结束时间？
否
是
①
S722
打开加锁和解锁功能
S724
发送加锁和解锁功能ON通知
S726
强行切断BLE访问并且禁止重新访问
结束

图7

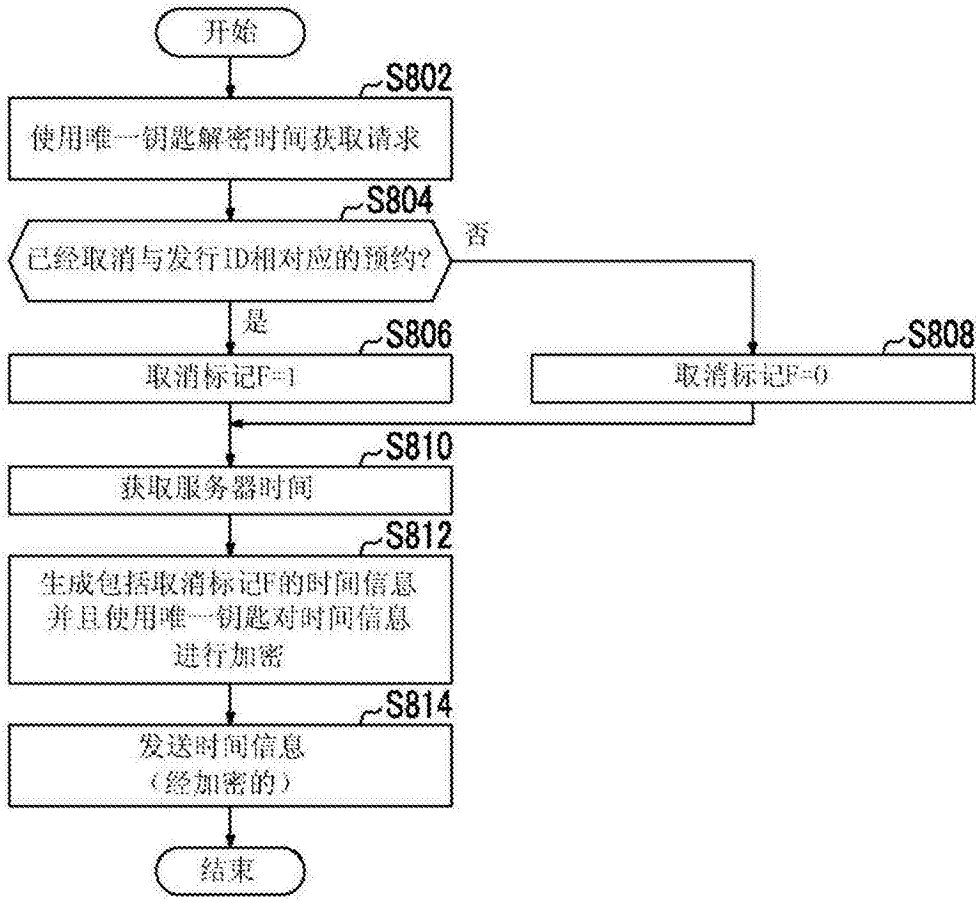

开始
S802
使用唯一钥匙解密时间获取请求
S804
已经取消与发行ID相对应的预约?
否
是
S806
取消标记F=1
S808
取消标记F=0
S810
获取服务器时间
S812
生成包括取消标记F的时间信息
并且使用唯一钥匙对时间信息
进行加密
S814
发送时间信息
（经加密的）
结束

图8

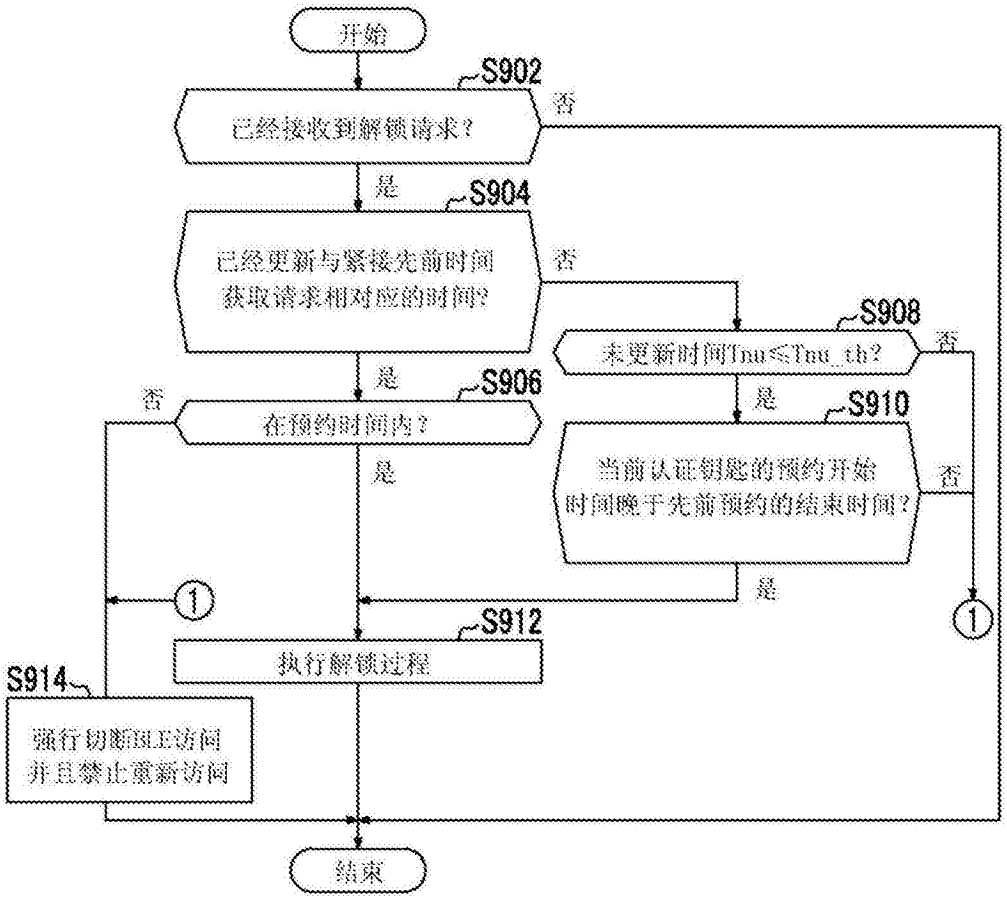

开始
S902
已经接收到解锁请求?
否
是
S904
已经更新与紧接先前时间
获取请求相对应的时间?
否
是
S906
否
在预约时间内?
是
S908
未更新时间Tnu≤Tnu_th?
否
是
S910
当前认证钥匙的预约开始
时间晚于先前预约的结束时间?
否
是
①
①
S912
执行解锁过程
S914
强行切断BLE访问
并且禁止重新访问
结束

图9

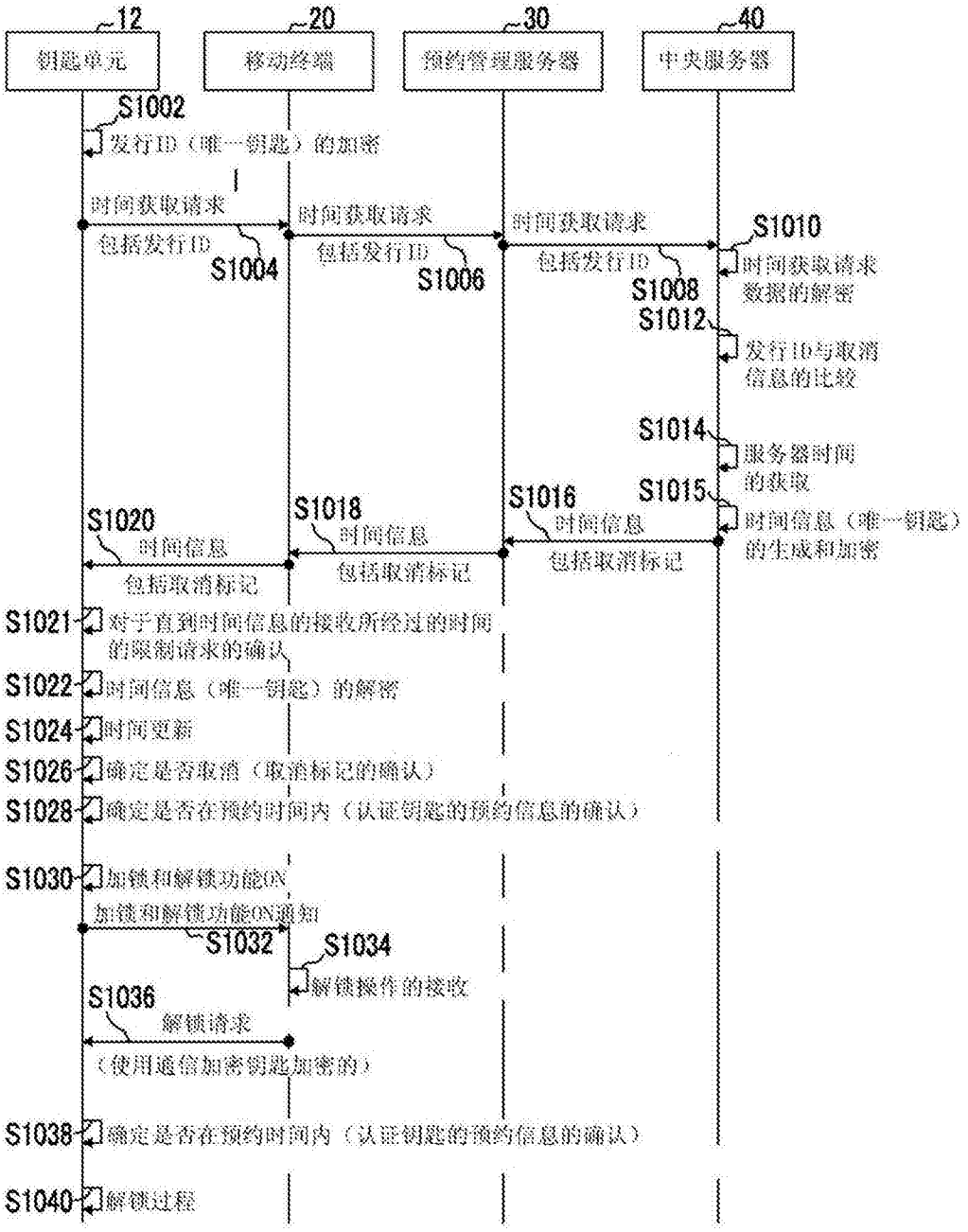

12
钥匙单元
20
移动终端
30
预约管理服务器
40
中央服务器
S1002
发行ID（唯一钥匙）的加密
时间获取请求
包括发行ID
S1004
时间获取请求
包括发行ID
S1006
时间获取请求
包括发行ID
S1008
S1010
时间获取请求数据的解密
S1012
发行ID与取消信息的比较
S1014
服务器时间的获取
S1015
时间信息（唯一钥匙）的生成和加密
S1016
时间信息
包括取消标记
S1018
时间信息
包括取消标记
S1020
时间信息
包括取消标记
S1021
对于直到时间信息的接收所经过的时间的限制请求的确认
S1022
时间信息（唯一钥匙）的解密
S1024
时间更新
S1026
确定是否取消（取消标记的确认）
S1028
确定是否在预约时间内（认证钥匙的预约信息的确认）
S1030
加锁和解锁功能ON
加锁和解锁功能ON通知
S1032
S1034
解锁操作的接收
S1036
解锁请求
（使用通信加密钥匙加密的）
S1038
确定是否在预约时间内（认证钥匙的预约信息的确认）
S1040
解锁过程

图10