[19] 中华人民共和国国家知识产权局

[12] 发明专利申请公布说明书

[21] 申请号 200910118237.9

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)
H04L 9/08 (2006.01)
G06K 19/073 (2006.01)

[43] 公开日 2009 年 9 月 9 日

[11] 公开号 CN 101527723A

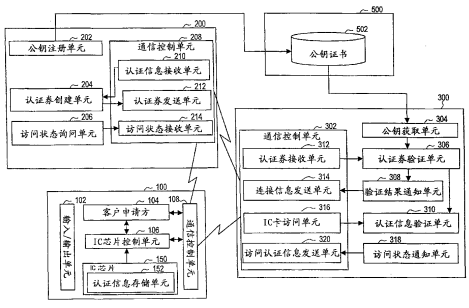
[22] 申请日 2009.3.3
[21] 申请号 200910118237.9
[30] 优先权
[32] 2008. 3. 3 [33] JP [31] 2008 - 052729
[71] 申请人 飞力凯网路股份有限公司
地址 日本东京
[72] 发明人 畑冈纯 疋田智治
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 秦 晨
权利要求书 9 页 说明书 32 页 附图 17 页

[54] 发明名称

卡发行系统、卡发行服务器、卡发行方法和程序

[57] 摘要

本发明提供卡发行系统、卡发行服务器、卡发行方法和程序。 本发明提供一种服务提供服务器，该服务提供服务器包括：认证券创建单元，用于对访问认证信息加密并创建认证券；以及认证券发送单元，用于将认证券发送至卡发行服务器，其中卡发行服务器包括：认证券验证单元，用于将认证券解密，并验证该认证券；验证结果通知单元，用于将认证券的验证结果通知给服务提供服务器；连接信息发送单元，用于将与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至服务提供服务器；以及认证信息验证单元，用于比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。



1.一种卡发行系统，包括信息处理终端、服务提供服务器和卡发行服务器，其中，信息处理终端配备有 IC 芯片，服务提供服务器和卡发行服务器可通过网络与信息处理终端相连接，

其中，服务提供服务器包括：

认证券创建单元，被配置为对用于认证信息处理终端的访问的访问认证信息加密，并创建认证券，以及

认证券发送单元，被配置为将由认证券创建单元创建的认证券发送至卡发行服务器，

其中，卡发行服务器包括：

认证券验证单元，被配置为将由认证券发送单元发送的认证券解密，并验证该认证券，

验证结果通知单元，被配置为将由认证券验证单元验证的认证券的验证结果通知给服务提供服务器，

连接信息发送单元，被配置为将用于与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至服务提供服务器，以及

认证信息验证单元，被配置为比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息，并且

其中，信息处理终端包括：

连接单元，被配置为基于连接信息与卡发行服务器相连接，以及

认证信息存储单元，被配置为存储访问认证信息，该认证信息存储单元被设置在 IC 芯片中。

2.一种可通过网络与配备有 IC 芯片的信息处理终端和服务提供服务器相连接的卡发行服务器，其中，服务提供服务器对用于认证信息处理终端的访问的访问认证信息加密，并创建认证券，

该卡发行服务器包括：

认证券接收单元，被配置为接收由服务提供服务器创建的认证券；

认证券验证单元，被配置为将由认证券接收单元接收的认证券解密，并验证该认证券；

验证结果通知单元，被配置为将由认证券验证单元验证的认证券的验证结果通知给服务提供服务器；

连接信息发送单元，被配置为将用于与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至服务提供服务器；以及

认证信息验证单元，被配置为比较并验证认证券的访问认证信息和存储在信息处理终端的IC芯片中的访问认证信息。

3.根据权利要求2所述的卡发行服务器，其中

服务提供服务器使用认证私钥向访问认证信息添加电子签名，并且创建认证券，以及

认证券验证单元使用对应于认证私钥的认证公钥来验证被添加到认证券的电子签名。

4.根据权利要求2所述的卡发行服务器，

其中，卡发行服务器通过网络与服务代理服务器相连接，该服务代理服务器被配置为代理服务提供服务器，

其中，服务提供服务器对许可给服务代理服务器的服务的信息进行加密，并且创建认证许可，并且服务代理服务器将用于认证信息处理终端的访问的访问认证信息添加到认证许可中，并进行加密，从而创建认证券，

所述卡发行服务器包括：

认证许可获取单元，被配置为解密认证券，并获取认证许可；以及

认证券验证单元，被配置为将由认证许可获取单元获取的认证许可解密，并验证该认证许可，并且

其中，认证券验证单元基于由认证许可验证单元验证的认证许可来验证认证券。

5.根据权利要求4所述的卡发行服务器，其中

服务提供服务器使用第一认证私钥来向用户认证信息添加第一

电子签名，从而创建认证许可，并且服务代理服务器向认证许可添加访问认证信息，并且还使用第二认证私钥来添加第二电子签名，从而创建认证券，

认证许可验证单元使用对应于第一认证私钥的第一认证公钥来验证被添加到认证许可的第一电子签名，以及

认证券验证单元使用对应于第二认证私钥的第二认证公钥来验证被添加到认证券的第二电子签名，该第二认证私钥包含在由认证许可验证单元验证的认证许可中。

6.根据权利要求 2 所述的卡发行服务器，其中，访问认证信息至少包括被信息处理终端所使用的处理信息、IC 芯片的识别信息、和 IC 芯片的发行源信息。

7.根据权利要求 2 所述的卡发行服务器，其中

访问认证信息包括用于判断是否有可能向 IC 芯片写入的写入判断信息，并且

认证信息验证单元基于写入判断信息来确定对 IC 芯片的写入。

8.根据权利要求 2 所述的卡发行服务器，其中，访问认证信息包括允许向 IC 芯片写入数据或使用写入到 IC 芯片的数据的装置的控制信息。

9.根据权利要求 2 所述的卡发行服务器，该卡发行服务器包括被配置为通过质询响应认证来认证服务提供服务器的质询响应认证单元。

10.根据权利要求 9 所述的卡发行服务器，其中，所述质询响应认证单元通过质询响应认证来认证服务代理服务器。

11.根据权利要求 2 所述的卡发行服务器，该卡发行服务器包括：访问状态通知单元，被配置为响应于服务提供服务器的请求通知对信息处理终端的 IC 芯片的访问状态。

12.根据权利要求 11 所述的卡发行服务器，其中，访问状态通知单元包括：访问认证信息发送单元，被配置为响应于服务提供服务器的请求，将在 IC 芯片中存储的访问认证信息发送至服务提供服务器。

13.一种卡发行系统，包括信息处理终端、服务提供服务器和卡发行服务器，其中，信息处理终端配备有 IC 芯片，服务提供服务器和卡发行服务器可通过网络与信息处理终端相连接，

其中，服务提供服务器包括:

认证券创建单元，被配置为对用于认证信息处理终端的访问的访问认证信息加密，并创建认证券，以及

认证券发送单元，被配置为将由认证券创建单元创建的认证券发送至信息处理终端，

其中，信息处理终端包括:

认证券发送单元，被配置为将由在服务提供服务器中包含的认证券发送单元所发送的认证券发送至卡发行服务器，并且

其中，卡发行服务器包括

认证券验证单元，被配置为将由在信息处理终端中包含的认证券发送单元发送的认证券解密,并验证该认证券，

验证结果通知单元，被配置为将由认证券验证单元验证的认证券的验证结果通知给信息处理终端，

连接信息发送单元，被配置为将用于与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至信息处理终端，以及

认证信息验证单元，被配置为比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。

14. 一种可通过网络与配备有 IC 芯片的信息处理终端和服务提供服务器相连接的卡发行服务器，

其中，服务提供服务器对用于认证信息处理终端的访问的访问认证信息加密，并创建认证券，

该卡发行服务器包括:

认证券接收单元，被配置为通过信息处理终端接收由服务提供服务器创建的认证券;

认证券验证单元，被配置为将由认证券接收单元接收的认证券解密,并验证该认证券;

验证结果通知单元，将由认证券验证单元验证的认证券的验证结果通知给信息处理终端；以及

认证信息验证单元，被配置为比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。

15.一种卡发行系统，包括信息处理终端、服务提供服务器、服务代理服务器和卡发行服务器，其中，信息处理终端配备有 IC 芯片，服务提供服务器、服务代理服务器和卡发行服务器可通过网络与信息处理终端相连接，

其中，服务提供服务器包括：

认证许可创建单元，被配置为对服务提供服务器许可给服务代理服务器的服务的信息加密，并创建认证许可，以及

认证许可发送单元，被配置为将由认证许可创建单元创建的认证许可发送至服务代理服务器，

其中，服务代理服务器包括：

认证券创建单元，被配置为将用于认证信息处理终端的访问的访问认证信息添加到由认证许可发送单元发送的认证许可中，并进行加密，从而创建认证券，以及

认证券发送单元，被配置为将由认证券创建单元创建的认证券发送至卡发行服务器，并且

其中，卡发行服务器包括：

认证许可获取单元，被配置为将由认证券发送单元发送的认证券解密，并获取该认证许可，

认证许可验证单元，被配置为将由认证许可获取单元获取的认证许可解密，并验证该认证许可，以及

认证券验证单元，被配置为基于由认证许可验证单元验证的认证许可来验证认证券。

16.一种卡发行方法，该方法是使用信息处理终端、服务提供服务器和卡发行服务器来实现的，其中，信息处理终端配备有 IC 芯片，服务提供服务器和卡发行服务器可通过网络与信息处理终端相连接，

该方法包括下述步骤:

通过服务提供服务器,

对用于认证信息处理终端的访问的访问认证信息加密,并且创建认证券;

将认证券发送至卡发行服务器;

通过卡发行服务器,

对由服务提供服务器发送的认证券进行解密,并且验证该认证券;

将已验证的认证券的验证结果通知给服务提供服务器;

将用于与卡发行服务器相连接的连接信息与认证券的验证结果一起发送至服务提供服务器;

比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息;以及

通过信息处理终端,

基于连接信息与卡发行服务器相连接。

17.一种卡发行方法,该方法是使用信息处理终端、服务提供服务器和卡发行服务器来实现的,其中,信息处理终端配备有 IC 芯片,服务提供服务器和卡发行服务器可通过网络与信息处理终端相连接,该方法包括下述步骤:

通过服务提供服务器,

对用于认证信息处理终端的访问的访问认证信息加密,并且创建认证券;

将认证券发送至信息处理终端;

通过信息处理终端,

将由服务提供服务器发送的认证券发送至卡发行服务器;

通过卡发行服务器,

对发送的认证券进行解密,并且验证该认证券;

将已验证的认证券的验证结果通知给信息处理终端;

将用于与卡发行服务器相连接的连接信息与认证券的验证结果

一起发送至信息处理终端；以及

比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。

18.一种卡发行方法，该方法是使用配备有 IC 芯片的信息处理终端、以及可通过网络与信息处理终端相连接的服务提供服务器、服务代理服务器、和卡发行服务器来实现的，该方法包括下述步骤：

通过服务提供服务器，

对服务提供服务器许可给服务代理服务器的服务的信息进行加密，并且创建认证许可；

将认证许可发送至服务代理服务器；

通过服务代理服务器，

将用于认证信息处理终端的访问的访问认证信息添加至发送的认证许可中，并且进行加密，从而创建认证券；

将认证券发送至卡发行服务器；

通过卡发行服务器，

对认证券进行解密，并且获取该认许可；

对获取的认证许可进行解密，并且验证该认证许可；以及

基于验证的认证许可来验证认证券。

19.一种使计算机作为卡发行服务器运行的程序，该卡发行服务器可通过网络与安装有 IC 芯片的信息处理终端和服务提供服务器相连接，

其中，服务提供服务器对用于认证信息处理终端的访问的访问认证信息加密，并创建认证券，

其中，卡发行服务器包括：

认证券接收单元，被配置为接收由服务提供服务器创建的认证券，

认证券验证单元，被配置为将由认证券接收单元接收的认证券解密，并验证该认证券，

验证结果通知单元，被配置为将由认证券验证单元验证的认证券

的验证结果通知给服务提供服务器，

连接信息发送单元，被配置为将用于与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至服务提供服务器，以及

认证信息验证单元，被配置为比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。

20.根据权利要求 19 所述的程序，

其中，卡发行服务器通过网络与服务代理服务器相连接，该服务代理服务器被配置为代理服务提供服务器，

其中，服务提供服务器对许可给服务代理服务器的服务的信息进行加密，并且创建认证许可，并且服务代理服务器将用于认证信息处理终端的访问的访问认证信息添加到认证许可中，并进行加密，从而创建认证券，

其中，卡发行服务器包括：

认证许可获取单元，被配置为解密认证券，并获取认证许可，以及

认证许可验证单元，被配置为将由认证许可获取单元获取的认证许可解密，并验证该认证许可，并且

其中，认证券验证单元基于由认证许可验证单元验证的认证许可来验证认证券。

21.一种使计算机作为卡发行服务器运行的程序，该卡发行服务器可通过网络与配备有 IC 芯片的信息处理终端和服务提供服务器相连接，

其中，服务提供服务器对用于认证信息处理终端的访问的访问认证信息加密，并创建认证券，

其中，卡发行服务器包括：

认证券接收单元，被配置为通过信息处理终端来接收由服务提供服务器创建的认证券，

认证券验证单元，被配置为将由认证券接收单元接收的认证券解密，并验证该认证券，

验证结果通知单元，用于将由认证券验证单元验证的认证券的验证结果通知给信息处理终端，以及

认证信息验证单元，被配置为比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。

卡发行系统、卡发行服务器、卡发行方法和程序

相关申请的交叉引用

本申请包含与于2008年3月3日在日本专利局提交的日本专利申请JP 2008-052729相关的主题，该专利申请的全部内容通过引用而并入本文。

技术领域

本发明涉及卡发行系统、卡发行服务器、卡发行方法和程序，具体地讲，涉及能够有效地防止对IC芯片的未授权访问的卡发行系统、卡发行服务器、卡发行方法和程序。

背景技术

近年来，实现了这样的技术：向安装在便携式电话等内的IC芯片写入由诸如金融机构的服务提供方发行的卡的卡号、可以由相关卡使用的服务类型等，从而允许安装有该IC芯片的便携式电话与该服务提供方发行的卡相似地使用。通常，IC芯片具有防篡改（tamper-proof）特性，并且写在IC芯片上的数据都被安全地保持。为了访问保持安全信息的IC芯片或向该IC芯片写入数据，需要建立用于访问IC芯片的系统，或需要公开用于访问IC芯片的信息。为此，卡发行代理方基于服务提供方的请求访问IC芯片或向IC芯片写入数据。

当通过网络访问安装在便携式电话等上的IC芯片时，需要来自控制该IC芯片的客户申请方的请求。因此，为了访问IC芯片并发行卡，需要卡发行代理方、服务提供方和客户申请方三方间的相互认证。可以使用一次口令等实现三方间之间的认证。使用一次口令的认证包括下述方法。

首先，在执行了便携式电话的客户申请方和服务提供方的服务器

之间的认证之后，执行服务提供方的服务器（在下文中被称作服务提供服务器）和卡发行代理方的服务器（在下文中被称作卡发行服务器）之间的相互认证。卡发行服务器通过服务提供服务器将用于认证来自客户申请方的请求的一次口令（权标（token））通知给便携式电话的客户申请方。然后，卡发行服务器可以指定安装有要对其写入卡信息的 IC 芯片的便携式电话的客户申请方。在将请求发送至卡发行服务器的同时，便携式电话的客户申请方将通知的权标通知给卡发行服务器，并且卡发行服务器通过验证通知的权标来执行对便携式电话的客户申请方的认证。

在上述方法中，可以在发送来自客户申请方的请求的同时，仅执行对客户申请方的认证。权标可以预先离线获取，但在该情况下，卡发行服务器中的权标的保持时间段变长，从而增加了系统上的负荷。为了解决这个问题，公开了一种使用基于从客户申请方发送的个人化信息（individualizing information）而产生的认证许可来实现三方间的相互认证的技术（例如专利文献 1）。在日本专利申请公开 No.2006－246015 中，从客户申请方对其发送个人化信息的服务提供服务器产生认证许可，并且将产生的认证许可从客户申请方发送至卡发行服务器。卡发行服务器验证发送的认证许可，以便执行对客户申请方、便携式终端和服务提供服务器的认证。

[专利文献 1] 日本专利申请公开 No.2006－246015

发明内容

当卡发行服务器通过诸如因特网的网络访问安装在便携式电话上的 IC 芯片时，需要预先验证 IC 芯片的合法性。然而，尽管客户申请方、服务提供服务器和卡发行服务器三方间的相互认证可以在日本专利申请公开 No.2006－246015 中实现，但卡发行服务器可以不预先验证 IC 芯片，或检测存储在 IC 芯片上的卡信息等。服务提供服务器不能有效地检查卡发行服务器执行的处理结果。

本发明解决了上述问题和其它问题，其中，需要提供一种新的和

改进的卡发行系统、卡发行服务器、卡发行方法和程序，所述卡发行系统能够在访问存储在IC芯片上的卡信息之前获取IC芯片的个体信息（individual information），预先验证 IC 芯片，并有效地防止对IC芯片的未授权访问。

根据本发明的实施例，提供有一种卡发行系统，该卡发行系统包括：安装有 IC 芯片的信息处理终端；以及可通过网络与信息处理终端相连接的服务提供服务器和卡发行服务器。服务提供服务器包括：认证券创建单元，用于对用于认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券（authertication ticket）；以及认证券发送单元，用于将由认证券创建单元创建的认证券发送至卡发行服务器。

卡发行服务器包括：认证券验证单元，用于对由认证券发送单元发送的认证券进行解密,并验证该认证券；验证结果通知单元，用于将由认证券验证单元验证的认证券的验证结果通知给服务提供服务器；连接信息发送单元，用于将用于与卡发行服务器相连接的连接信息与认证券的验证结果一起发送至服务提供服务器；以及认证信息验证单元，用于比较并验证认证券的访问认证信息、和存储在信息处理终端的 IC 芯片中的访问认证信息。信息处理终端包括用于基于连接信息与卡发行服务器相连接的连接单元；以及设置在 IC 芯片中的、用于存储访问认证信息的认证信息存储单元。

根据这样的配置，服务提供服务器对用于认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券，并且该认证券被发送至卡发行服务器。卡发行服务器验证该认证券，并将验证结果通知给服务提供服务器，并且发送用于与卡发行服务器相连接的连接信息。然后，通过服务提供服务器对其发送连接信息的信息处理终端与卡发行服务器相连接，从而卡发行服务器可以访问该信息处理终端的 IC 芯片。

根据本发明的另一实施例，提供有一种可通过网络与安装有 IC 芯片的信息处理终端和服务提供服务器相连接的卡发行服务器，其

中，服务提供服务器对用于认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券，并且卡发行服务器包括：认证券接收单元，用于接收由服务提供服务器创建的认证券；认证券验证单元，用于对由认证券接收单元接收的认证券进行解密,并验证该认证券；验证结果通知单元，用于将由认证券验证单元验证的认证券的验证结果通知给服务提供服务器；连接信息发送单元，用于将用于与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至服务提供服务器；以及认证信息验证单元，用于比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。

根据这样的配置，服务提供服务器对用于认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券，并且该认证券被发送至卡发行服务器。卡发行服务器验证该认证券，并将验证结果通知给服务提供服务器，并且发送用于与卡发行服务器相连接的连接信息。然后，通过服务提供服务器对其发送连接信息的信息处理终端与卡发行服务器相连接，从而卡发行服务器可以访问信息处理终端的 IC 芯片。

此外，服务提供服务器可以使用认证私钥向访问认证信息添加电子签名，从而创建认证券；并且认证券验证单元可以使用对应于认证私钥的认证公钥来验证被添加到认证券的电子签名。

此外，卡发行服务器通过网络与代理服务提供服务器的服务代理服务器（active acting server）相连接；服务提供服务器对许可给服务代理服务器的服务的信息进行加密从而创建认证许可，并且服务代理服务器将用于认证信息处理终端的访问的访问认证信息添加到认证许可中，并进行加密从而创建认证券；以及卡发行服务器包括：认证许可获取单元，用于解密认证券并获取认证许可；以及认证许可验证单元，用于解密由认证许可获取单元获取的认证许可并验证该认证许可；并且认证券验证单元可以基于由认证许可验证单元验证的认证许可来验证认证券。

根据这样的配置，服务提供服务器创建能够仅执行请求服务代理

服务器的处理的认证许可，并基于该认证许可创建认证券。通过认证券的多级配置，当服务提供服务器请求服务代理服务器可供替换的处理时，在保持安全性的同时可以限制可执行的处理。利用对于认证许可和认证券使用不同认证密钥的多级配置，即使当服务代理服务器等为服务提供服务器执行处理时，认证也变得相互可行。服务提供服务器可以使用第一认证私钥来向用户认证信息添加第一电子签名，从而创建认证许可，并且服务代理服务器可以向认证许可添加访问认证信息，并且还使用第二认证私钥来添加第二电子签名，从而创建认证券；认证许可验证单元可以使用与第一认证私钥相对应的第一认证公钥来验证被添加到认证许可的第一电子签名；并且认证券验证单元可以使用对应于第二认证私钥的第二认证公钥来验证被添加到认证券的第二电子签名，所述第二认证私钥包含在被认证许可验证单元验证的认证许可中。

根据这样的配置，利用对于认证许可和认证券使用不同认证密钥的多级配置，即使当服务代理服务器等为服务提供服务器执行处理时，认证也变得相互可行，并且可以限制要执行的处理。

访问认证信息可以至少包括被信息处理终端所使用的处理的信息、IC 芯片的识别信息和 IC 芯片的发行源信息。要被信息处理终端使用的处理的信息是与服务提供方所提供的服务相关的处理的信息。因此，可以基于认证券执行 IC 芯片的认证。

访问认证信息包括写入判断信息，用于判断是否有可能向 IC 芯片写入；并且认证信息验证单元可以基于该写入判断信息来判断对 IC 芯片的写入。因此，可以执行仅相对于特定的 IC 卡对应终端和该 IC 卡的处理。访问认证信息可以包括能够向 IC 芯片写入数据或能够使用写在 IC 芯片上的数据的设备的限制信息。

服务提供服务器可以通过质询响应式（challenge-response）认证而被认证。质询响应认证单元可以通过质询响应认证来认证服务代理服务器。因此，可以执行更高安全性的认证。

可以设置用于响应于服务提供服务器的请求来通知信息处理终

端的 IC 芯片的访问状态的访问状态通知单元。访问状态通知单元可以包括访问认证信息发送单元，用于响应于服务提供服务器的请求，将在 IC 芯片中存储的访问认证信息发送至服务提供服务器。因此，当客户申请方不可靠时，当客户申请方和服务提供服务器之间的通信路径不可靠等时，服务提供服务器可以得到关于客户申请方的准确的处理结果。

根据本发明的另一实施例，提供有一种卡发行系统，该卡发行系统包括：安装有 IC 芯片的信息处理终端；可通过网络与信息处理终端相连接的服务提供服务器和卡发行服务器。服务提供服务器包括：认证券创建单元，用于对用于认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券；以及认证券发送单元，用于将由认证券创建单元创建的认证券发送至信息处理终端。信息处理终端包括认证券发送单元，用于将由设置在服务提供服务器中的认证券发送单元所发送的认证券发送至卡发行服务器。

卡发行服务器包括：认证券验证单元，用于对由设置在信息处理终端中的认证券发送单元发送的认证券进行解密并验证该认证券；验证结果通知单元，用于将由认证券验证单元验证的认证券的验证结果通知给信息处理终端；连接信息发送单元，用于将用于与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至信息处理终端；以及认证信息验证单元，用于比较并验证认证券的访问认证信息、和存储在信息处理终端的 IC 芯片中的访问认证信息。

根据这样的配置，由服务提供服务器创建的认证券被发送至信息处理终端的客户申请方，并且客户申请方与卡发行服务器相连接并发送认证券，从而可以执行 IC 卡的认证处理。因此，服务提供服务器和卡发行服务器之间的通信被减少了，并且可以减少服务提供服务器的建立工时。

根据本发明的另一实施例，提供有一种可通过网络与安装有 IC 芯片的信息处理终端和服务提供服务器相连接的卡发行服务器，其中，服务提供服务器对用于认证信息处理终端的访问的访问认证信息

进行加密，从而创建认证券，并且卡发行服务器包括：认证券接收单元，用于通过信息处理终端接收由服务提供服务器创建的认证券；认证券验证单元，用于对由认证券接收单元接收的认证券进行解密，并验证该认证券；验证结果通知单元，用于将由认证券验证单元验证的认证券的验证结果通知给信息处理终端；以及认证信息验证单元，用于比较并验证认证券的访问认证信息、和存储在信息处理终端的 IC 芯片中的访问认证信息。

根据本发明的另一实施例，提供有一种卡发行系统，该卡发行系统包括：安装有 IC 芯片的信息处理终端；以及可通过网络与信息处理终端相连接的服务提供服务器、服务代理服务器和卡发行服务器。服务提供服务器包括：认证许可创建单元，用于对许可给服务代理服务器的服务的信息进行加密，从而创建认证许可；以及认证许可发送单元，用于将由认证许可创建单元创建的认证许可发送至服务代理服务器。服务代理服务器包括认证券创建单元，用于将用于认证信息处理终端的访问的访问认证信息添加到由认证许可发送单元发送的认证许可中，并进行加密，从而创建认证券；以及认证券发送单元，用于将由认证券创建单元创建的认证券发送至卡发行服务器。

卡发行服务器包括：认证许可获取单元，用于对由认证券发送单元发送的认证券进行解密，并获取认证许可；认证许可验证单元，用于对由认证许可获取单元获取的认证许可进行解密，并验证该认证许可；以及认证券验证单元，用于基于由认证许可验证单元验证的认证许可来验证认证券。

根据本发明的另一实施例，提供有一种卡发行方法，该方法是使用配备有 IC 芯片的信息处理终端、以及可通过网络与信息处理终端相连接的服务提供服务器、和卡发行服务器来实现的，该方法包括下述步骤：通过服务提供服务器，对用于认证信息处理终端的访问的访问认证信息加密，并且创建认证券；将认证券发送至卡发行服务器，通过卡发行服务器，对由服务提供服务器发送的认证券进行解密，并且验证该认证券；将已验证的认证券的验证结果通知给服务提供服务

器;将用于与卡发行服务器相连接的连接信息与认证券的验证结果一起发送至服务提供服务器；比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息;通过信息处理终端，基于连接信息与卡发行服务器相连接。

根据本发明的另一实施例，提供有一种卡发行方法，该方法是使用配备有 IC 芯片的信息处理终端、以及可通过网络与信息处理终端相连接的服务提供服务器和卡发行服务器来实现的，该方法包括下述步骤：通过服务提供服务器，对用于认证信息处理终端的访问的访问认证信息加密，并且创建认证券；将认证券发送至信息处理终端;通过信息处理终端，将由服务提供服务器发送的认证券发送至卡发行服务器；通过卡发行服务器，对由设置在信息处理终端中的认证卷发送单元发送的认证券进行解密，并且验证该认证券；将已验证的认证券的验证结果通知给信息处理终端;将用于与卡发行服务器相连接的连接信息与认证券的验证结果一起发送至信息处理终端；以及比较并验证认证券的访问认证信息和存储在信息处理终端的 IC 芯片中的访问认证信息。

根据本发明的另一实施例，提供有一种卡发行方法，该方法是使用配备有 IC 芯片的信息处理终端、以及可通过网络与信息处理终端相连接的服务提供服务器、服务代理服务器和卡发行服务器来实现的，该方法包括下述步骤：通过服务提供服务器，对许可给服务代理服务器的服务的信息进行加密，并且创建认证许可；将认证许可发送至服务代理服务器,通过服务代理服务器，将用于认证信息处理终端的访问的访问认证信息添加至发送的认证许可中,并且进行加密，从而创建认证券；将认证券发送至卡发行服务器；通过卡发行服务器，对认证券进行解密，并且获取该认许可；对获取的认证许可进行解密，并且验证该认证许可；以及基于验证的认证许可来验证认证券。

根据本发明的另一实施例，提供有一种使计算机作为卡发行服务器运行的程序，所述卡发行服务器可通过网络与安装有 IC 芯片的信息处理终端和服务提供服务器相连接，其中，服务提供服务器对用于

认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券；以及卡发行服务器包括：认证券接收单元，用于接收由服务提供服务器创建的认证券；认证券验证单元，用于对由认证券接收单元接收的认证券进行解密,并验证该认证券；验证结果通知单元，用于将由认证券验证单元验证的认证券的验证结果通知给服务提供服务器；连接信息发送单元，用于将用于与卡发行服务器相连接的连接信息和认证券的验证结果一起发送至服务提供服务器；以及认证信息验证单元，用于比较并验证认证券的访问认证信息、和存储在信息处理终端的 IC 芯片中的访问认证信息。

此外，这样的计算机可以作为卡发行服务器来运行，其中，所述卡发行服务器通过网络与代理服务提供服务器的服务代理服务器相连接；服务提供服务器对许可给服务代理服务器的服务的信息进行加密，从而创建认证许可，并且服务代理服务器将用于认证信息处理终端的访问的访问认证信息添加到认证许可，并进行加密从而创建认证券；卡发行服务器包括用于解密认证券并获取认证许可的认证许可获取单元和用于解密由认证许可获取单元获取的认证许可并验证该认证许可的认证许可验证单元；并且认证券验证单元可以基于由认证许可验证单元验证的认证许可来验证认证券。

根据本发明的另一实施例，提供了一种使计算机作为卡发行服务器来运行的程序，所述卡发行服务器可通过网络与安装有 IC 芯片的信息处理终端和服务提供服务器相连接，其中，服务提供服务器对用于认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券，并且卡发行服务器包括：认证券接收单元，用于通过信息处理终端接收由服务提供服务器创建的认证券；认证券验证单元，用于对由认证券接收单元接收的认证券进行解密,并验证该认证券；验证结果通知单元，用于将由认证券验证单元验证的认证券的验证结果通知给信息处理终端；以及认证信息验证单元，用于比较并验证认证券的访问认证信息、和存储在信息处理终端的 IC 芯片中的访问认证信息。

根据本发明的实施例，在访问存储在 IC 芯片中的卡信息之前获

取 IC 芯片的个体信息，以便预先验证 IC 芯片，从而可以有效地防止对 IC 芯片的未授权的访问。

附图说明

图 1 是示出了根据本发明的第一实施例的卡发行系统的配置实例的说明图；

图 2 是示出了根据实施例的信息处理终端、服务提供服务器和卡发行服务器的功能配置的框图；

图 3 是描述根据实施例的访问认证信息和认证券的内容的说明图；

图 4 是示出了根据实施例的认证券和存储在 IC 芯片中的访问认证信息的内容的说明图；

图 5 是描述根据实施例的比较数据的使用实例的说明图；

图 6 是描述根据实施例的比较数据的使用实例的说明图；

图 7 是示出了根据实施例的卡发行方法的流程的时序图；

图 8 是描述根据实施例的认证券的验证处理的说明图；

图 9 是描述根据实施例的 IC 卡的认证信息的验证处理的说明图；

图 10 是示出了根据实施例的访问信息询问处理的时序图；

图 11 是示出了根据本发明的第二实施例的信息处理终端、服务提供服务器和卡发行服务器的功能配置的框图；

图 12 是示出了根据实施例的卡发行方法的流程的时序图；

图 13 是示出了根据本发明的第三实施例的卡发行系统的配置实例的说明图；

图 14 是示出了根据实施例的信息处理终端、服务提供服务器和卡发行服务器的功能配置的框图；

图 15 是描述根据实施例的许可信息和认证许可的内容的说明图；

图 16 是描述根据实施例的访问认证信息和认证券的内容的说明

图；以及

图 17 是示出了根据实施例的卡发行方法的流程的时序图。

具体实施方式

在下文中，将参照附图详细地描述本发明的优选实施例。请注意，在本说明书和附图中，具有基本上相同的功能和结构的结构元件由相同的附图标记表示，并且省略对这些结构元件的重复说明。

（第一实施例）

首先描述根据本发明的第一实施例的卡发行系统的简要概述。图 1 是根据本实施例的卡发行系统 10 的配置实例的说明图。如图 1 所示，卡发行系统 10 被配置为包括信息处理终端 100、服务提供服务器 200、卡发行服务器 399、网络 50 等。信息处理终端 100、服务提供服务器 200 和卡发行服务器 300 通过网络 50 相连接。网络 50 被配置为包括诸如因特网、电话线网络和卫星通信网络的公用线路网络；诸如 WAN、LAN 和 IP－VPN 的专用线路网络等，并且可以是有线的或无线的。

信息处理终端 100 是安装有 IC 芯片 150 的便携式终端。下面将对安装有被应用于本发明的信息处理终端的 IC 芯片 150 的便携式电话进行说明，该便携式电话为信息处理终端 100 的一个实例，但信息处理终端 100 不限于该实例。信息处理终端 100 可以是安装有 IC 芯片的 PDA（个人数字助理）、手表、便携式音乐播放器等。IC 芯片 150 可以被并入信息处理装置 100 中，或者 IC 芯片可以通过接触或非接触通信来连接。

IC 芯片 150 是具有防篡改特性的安全存储器。IC 芯片 150 可以是接触式通信的，或者可以是非接触式通信的。信息处理终端 100 可以装载有多个 IC 芯片，或者可以根据应用来使用每一个 IC 芯片。下面主要将通过实例描述安装有一个 IC 芯片的信息处理终端 100，所述 IC 芯片能够提供由服务提供服务器 200 所提供的服务。信息处理终端 100 中的通过网络 50 的连接不仅仅是通过 HTTP、HTTPS 等的

TCP/IP 通信，而是指信息处理终端 100 的一般通信功能，并且包括红外通信、通过两维条形码、e－mail 等的通信。

服务提供服务器200对安装在信息处理终端100上的IC芯片150执行数据的写入或读取，以便使用信息处理终端100向用户提供服务。服务提供服务器 200 是诸如金融机构的服务提供方的服务器，并且可以是卡公司等的服务器。服务提供服务器 200 向卡发行服务器 300 请求诸如对 IC 芯片 150 执行的数据的写入或读取的 IC 卡发行处理。当服务提供服务器 200 向卡发行服务器 300 请求发行 IC 卡时，信息处理终端 100 需要被认证。

服务提供服务器 200 具有通过网络 50 与信息处理终端 100 相连接，并根据信息处理终端 100 的请求创建用于发行 IC 卡的认证券的功能。此处，IC 卡是指要被写入到安装在信息处理终端 100 中的 IC 芯片的卡信息，并且 IC 卡发行处理是指对 IC 芯片 150 执行的数据的写入或读取。

将在下文中详细地描述由服务提供服务器 200 创建的认证券，但认证券主要包括 IC 卡的个体信息，对 IC 卡的写入数据等。在本实施例中，一个服务提供服务器与网络相连接，但不限于这个实例，并且多个服务提供服务器可以与网络相连接。在该情况下，信息处理终端 100 可以使用从多个服务提供服务器中的每一个提供的服务。

卡发行服务器 300 具有下述功能：通过网络 50 连接到信息处理终端 100，执行诸如注册和删除应用的卡访问，并且基于来自服务提供服务器 200 的请求对信息处理终端 100 的 IC 芯片 150 写入和读取 IC 卡的卡信息。卡发行服务器 300 可以是执行卡发行的卡发行代理方的服务器。

卡发行服务器 300 保持用于认证 IC 芯片 140 的密钥信息、用于注册和删除对于多个服务提供服务器 200 的每一个都不同的应用的信息等，以便对 IC 卡进行访问。卡发行服务器 300 验证由服务提供服务器 200 创建的认证券，以便认证信息处理终端 100。在认证券被验证并且信息处理终端 100 的合法性被确认之后，由卡发行服务器 300

执行 IC 卡发行处理。

因此，由于认证券是在卡发行服务器 300 执行 IC 卡发行处理之前被验证的，所以可以获取 IC 芯片 150 的个体信息，以便验证 IC 芯片 150 的合法性，或者可以预先检查写在 IC 芯片 150 上的 IC 卡的卡信息等。

卡发行服务器 300 可以在验证认证券的同时使用一次口令等将对 IC 卡的访问结果、关于 IC 卡的信息等通知给服务提供服务器 200。诸如当卡发行服务器 300 执行 IC 卡发行处理时，或在发行处理之后，可以根据需要检查访问处理的结果，从而可以有效地防止未授权的访问。

上面已经描述了卡发行系统 10 的简要概述。现在将描述卡发行系统 10 的信息处理终端 100、服务提供服务器 200 和卡发行服务器 300 的详细配置。图 2 是示出了信息处理终端 100、服务提供服务器 200 和卡发行服务器 300 的功能配置的框图。如图 2 所示，信息处理终端 100 包括输入/输出单元 102、客户申请方 104、IC 芯片控制单元 106、通信控制单元 108、IC 芯片 150 等。

客户申请方 104 是信息处理终端 100 中的程序，并且具有使用信息处理终端 100 向用户提供服务，或进行用于发行 IC 卡的认证请求的功能。客户申请方 104 也具有通过通信控制单元 108 将 IC 芯片 150 的个体信息发送至服务提供服务器 200 的功能。IC 芯片控制单元 106 具有在 IC 芯片 150 和客户申请方 104 之间交换数据，或者与通信控制单元 108 交换数据的功能。IC 芯片 150 是具有防篡改特性的安装在信息处理终端 100 上的安全存储器，并且具有与外部装置接触通信或非接触通信的功能。IC 芯片 150 可以包括 CPU（中央处理单元）、ROM（只读存储器）、RAM（随机访问存储器）、存储单元等。在本实施例中，将描述其中 IC 芯片 150 主要是存储单元，并且认证信息存储单元 152 被设置在该存储单元中的情况。

通信控制单元 108 是被配置为包括用于连接到诸如因特网的网络的通信装置等的通信接口，并且具有通过网络与服务提供服务器

200 或卡发行服务器 300 发送和接收数据的功能。

输入/输出单元 102 是设置在信息处理终端 100 中的输入和输出接口。输入接口是数字键、按钮、触摸屏等，并具有接收用户的输入的功能。输出接口是诸如显示指示或灯的显示装置、诸如扬声器的音频输出装置等。上面已经描述了信息处理终端 100 的功能配置。

现在将描述服务提供服务器 200 的功能配置。服务提供服务器 200 包括公钥注册单元 202、认证券创建单元 204、访问状态询问单元 206、通信控制单元 208 等。公钥注册单元 202 具有预先向发行公钥证书的证书授权机构注册的功能，认证公钥与认证私钥成对，从而向将要在下文中描述的访问认证信息添加电子签名。用于认证的认证密钥可以使用成对的私钥和公钥，或可以使用与卡发行服务器 300 共享的共享密钥。

可以用密钥执行加密，该密钥可以是诸如 RSA 的非对称密钥、或诸如 DES 或 ASE 的对称密钥。在对称密钥的情况下，密钥需要被秘密地分配到对方，从而不根据通信网络直接分配，而是通过诸如内容证明的邮件等的方式分配。在本实施例中，将描述使用公钥加密方法执行加密和添加电子签名的情况。

认证券创建单元 204 具有加密用于认证信息处理终端 100 的访问的访问认证信息并创建认证券的功能。可以利用认证私钥来对访问认证信息加密，或者可以将其中使用认证私钥添加电子签名的认证券作为认证券。

例如，当使用用于加密算法的带密钥的散列（hash with key）（HMAC）时，可以将利用访问认证信息作为输入数据、且利用在服务提供服务器 200 和卡发行服务器 300 之间预先被共享的密钥作为密钥来执行 HMAC 计算的结果作为访问认证信息的电子签名被添加。当使用 RSA 时，利用服务提供服务器的认证私钥以访问认证信息作为输入数据对散列值进行加密的结果可以作为访问认证信息的电子签名被添加，或者可以利用认证私钥对访问认证信息进行加密。

将参照图 3 描述访问认证信息和认证券。图 3 是示出了访问认证

信息和认证券的内容的说明图。如图 3 所示，访问认证信息 2042 包括券的使用条件、IC 卡写入数据、与 IC 读取数据进行比较的比较数据等。票的使用条件包括关于要使用的处理的信息、客户申请方的连接路径、券的 ID、券的有效期开始日期和时间、券的有效期结束日期和时间、券的可使用次数、IC 卡实体信息（solid information）、IC 卡类型信息、IC 卡发行方类型信息、客户申请方 ID、IC 卡对应终端硬件 ID、IC 卡对应终端所有者 ID 等。

券的使用条件是可由卡发行服务器 300 使用的信息。“客户申请方的连接路径”是关于连接路径的信息，客户申请方在该连接路径中连接到卡发行服务器 300。“IC 卡实体信息”是用于识别这样的 IC 卡的实体信息，在该 IC 卡上卡发行服务器 300 执行卡访问。“IC 卡写入数据”是卡发行服务器 300 写在 IC 芯片 150 上的数据。“比较数据”是用于与从 IC 芯片 150 读取的 IC 卡的数据进行比较的数据，并且是用于根据验证该比较数据的结果判断实际上是否向 IC 卡写入所述写入数据的数据。将在下文中详细地描述比较数据的使用。访问认证信息 2042 被认证私钥加密或被添加有电子签名数据，并且创建认证券 2044。

返回到图 2，访问状态询问单元 206 具有向卡发行服务器 300 询问对 IC 卡的访问状态的功能。该访问状态是由卡发行服务器 300 在 IC 卡上执行的处理的结果。因此，当客户申请方不可靠时，当客户申请方和服务提供服务器 200 之间的通信路径不可靠等时，服务提供服务器 200 可以得到关于客户申请方的准确的处理结果。

通信控制单元 208 是被配置为包括用于连接到诸如因特网的网络的通信装置等的通信接口，并且具有通过网络与信息处理终端 100 或卡发行服务器 300 发送和接收数据的功能。通信控制单元 208 包括认证信息接收单元 210、认证券发送单元 212、访问状态接收单元 214 等。认证信息接收单元 210 具有接收从信息处理终端 100 的客户申请方 104 发送的访问认证信息，并且将该访问认证信息提供至认证券创建单元 204 的功能。

认证券发送单元212具有通过网络将由认证券创建单元204创建的认证券发送至卡发行服务器300的功能。访问状态接收单元214具有从卡发行服务器300接收对IC卡的访问状态，并且将该访问状态提供至访问状态询问单元206的功能。上面已经描述了服务提供服务器200的功能配置。

现在将描述卡发行服务器300的功能配置。卡发行服务器300包括通信控制单元302、公钥获取单元304、认证券验证单元306、验证结果通知单元308、认证信息验证单元310、访问状态通知单元318等。通信控制单元302是被配置为包括用于连接到诸如因特网的网络的通信装置等的通信接口，并且具有通过网络与信息处理终端100或服务提供服务器200发送和接收数据的功能。

通信控制单元302包括认证券接收单元312、连接信息发送单元314、IC卡访问单元316、访问认证信息发送单元320等。认证券接收单元312具有接收由服务提供服务器200创建的认证券，并且将该认证券提供至认证券验证单元306的功能。连接信息发送单元314具有在验证结果通知单元308通知验证结果的同时将连接信息发送至信息处理终端100的客户申请方104的功能。IC卡访问单元316具有这样的功能：访问信息处理终端100的IC芯片150，对IC芯片150执行IC卡信息等的读取或写入，并且将IC卡的信息提供至认证信息验证单元310。访问认证信息发送单元320具有响应于服务提供服务器200的请求将访问状态通知给IC芯片150并将写在IC芯片150上的访问认证信息发送至服务提供服务器200的功能。

公钥获取单元304具有这样的功能：获取由服务提供服务器200在证书授权机构500中注册的用于认证的公钥，并且将该公钥提供至认证券验证单元306。认证券验证单元306通过使用由公钥获取单元304提供的用于认证的公钥，对由认证券接收单元312提供的认证券进行解密，或者通过验证被添加的电子签名来验证发送的认证券的合法性。

认证券验证单元306对认证券的访问认证信息执行验证。例如，

验证认证券的有效期是否合适，或者认证券的可使用次数是否已经超过了认证券实际使用的次数。根据券的 IC 卡类型信息，对于每个芯片验证可执行的处理是否被合适地选择。如果从当在 IC 芯片 150 中存储的对 IC 卡的写入等操作在客户申请方和卡发行服务器 300 之间开始时，错误发生，则由于通信中断等发生，难以理解服务提供服务器 200 中的出错的原因。对于每个芯片可以如上所述的那样验证可执行的处理是否被合适地选择，并且可以在较早的阶段检测到错误。

当对于每个 IC 芯片发行方限制注册和删除应用、数据的写入或读取等处理时，根据认证券的 IC 卡发行方类型信息，对于每个 IC 芯片发行方验证可执行的处理是否被合适地选择。与通过 IC 卡类型信息执行的验证相似，可以通过使用 IC 卡发行方类型信息来执行验证，从而在较早的阶段检测到错误。认证券验证单元 306 将认证券的验证结果提供至验证结果通知单元 308。

验证结果通知单元 308 具有将由认证券验证单元 306 提供的认证券的验证结果通知给服务提供服务器 200 的功能。验证结果通知单元 308 将使信息处理终端 100 连接到卡发行服务器 300 的连接信息与认证券的验证结果一起发送至连接信息发送单元 314。

认证信息验证单元 310 具有对由认证券验证单元 306 验证的访问认证信息、和通过 IC 卡访问单元 316 访问 IC 芯片 150 而获取的在 IC 芯片中存储的访问认证信息进行比较和验证的功能。将参照图 4 描述由认证信息验证单元 310 执行的对 IC 卡的验证。图 4 是示出了认证券 2046 和存储在 IC 芯片 150 中的访问认证信息 1522 的内容的说明图。认证信息验证单元 310 执行对连接路径的检查、对 IC 卡个体信息的检查、与从 IC 卡读取的数据进行比较的比较数据的检查等。

在对连接路径的检查中，根据在认证券的访问认证信息中包含的到卡发行服务器 300 的连接路径来验证信息处理终端 100 是否与卡发行服务器 300 相连接。该检查不仅检查连接路径，还检查连接线路、协议等。

在对 IC 卡个体信息的检查中，验证在认证券的访问认证信息中

包含的 IC 卡的 IC 卡实体信息、IC 卡类型信息、IC 卡发行方类型信息、客户申请方 ID、IC 卡对应硬件 ID 和 IC 卡对应终端所有者 ID 与在 IC 卡中存储的访问认证信息是否匹配。可以通过这样的验证来仅对特定 IC 卡对应终端或 IC 卡执行处理。

在对与从 IC 卡读取的数据进行比较的比较数据的检查时，验证在认证券的访问认证信息中包含的比较数据与从 IC 卡实际获取的数据是否匹配。可以通过比较和验证 IC 卡上的特定区域的数据来防止当认证券被盗时的重放企图等。可以根据从 IC 卡读取的值来动态地改变对 IC 卡的写入数据值。将参照图 5 和 6 详细地描述比较数据的使用实例。图 5 和 6 是描述比较数据的使用实例的说明图。

如图 5 所示，在检查与在认证券中描述的使用条件的匹配之后，卡发行服务器 300 的认证信息验证单元 310 对 IC 卡执行处理。例如，将描述其中仅当 IC 卡的数据区域 1 为“0000”时可以使用的认证券的使用条件的情况。如图 5 所示，如果 IC 卡的数据区域为“0000”，则数据可被写入。如果认证券的使用条件包括当数据区域 1 为“0000”时，同时将数据区域 1 更新为“0001”，将数据区域 2 更新为“2222”，则 IC 卡的数据区域 1 被更新为“0001”，数据区域 2 被更新为“2222”。

也考虑根据认证券的所描述的条件来动态地更新数据的情况。例如，如果认证券的使用条件包括当数据区域 1 为“0000”时，同时将数据区域 1 更新为“0001”，将数据区域 2 更新为“2222”，则当 IC 卡的数据区域 1 为“0000”时，数据区域 1 被更新为“0001”，数据区域 2 被更新为“2222”。

相似地，如果认证券的使用条件包括当数据区域 1 为“0001”时，同时将数据区域 1 更新为“0002”，将数据区域 2 更新为“3333”，则当 IC 卡的数据区域 1 为“0001”时，数据区域 1 被更新为“0002”，数据区域 2 被更新为“3333”。此外，如果认证券的使用条件包括当数据区域 1 为“0002”时，同时将数据区域 1 更新为“0002”，将数据区域 3 更新为“BBBB”，则当 IC 卡的数据区域 1 为“0002”时，数据区域 1 被更新为“0002”，数据区域 3 被更新为“BBBB”。图 6 是描述当存在认证券

的多个使用条件时数据区域的更新的说明图。如图 6 所示，由于 IC 卡的数据区域 1 是“0001”，所以基于“当数据区域 1 为“0001”时”的券使用条件来更新数据。具体地讲，如图 6 所示，当券使用条件的数据区域 1 为“0001”时将数据区域 1 更新为“0002”，同时将数据区域 2 更新为“3333”，从而数据区域 1 被更新为“0002”，并且数据区域 2 被同时更新为“3333”。上文是对比较数据的使用实例的解释。

返回到图 2，访问状态通知单元 318 具有响应于服务提供服务器 200 的请求来将访问状态通知给 IC 芯片 150 的功能。例如，如果在访问 IC 卡之前，由服务提供服务器 200 进行访问状态的询问，则可以验证与 IC 卡的通信是否开始了。此外，如果在访问 IC 卡之后，在对 IC 卡执行处理期间，由服务提供服务器 200 进行访问状态的询问，则可以通知与 IC 卡的处理状态。此外，当终止对 IC 卡的处理时可以通知利用 IC 卡执行的处理的处理结果。因此，当客户申请方不可靠时，或者当客户申请方和服务提供服务器 200 之间的通信路径不可靠时，服务提供服务器 200 可以得到关于客户申请方的准确的处理结果。

访问认证信息发送单元 320 具有响应于服务提供服务器的请求，将存储在 IC 芯片中的访问认证信息发送至服务提供服务器 200 的功能。然后，服务提供服务器 200 可以在询问访问状态的同时获取从 IC 卡读取的数据，并且可以实现有效的顺序。上面已经描述了卡发行服务器 300 的功能配置。

现在将描述在卡发行系统 10 中执行的卡发行方法。图 7 示出了说明在卡发行系统 10 中执行的卡发行方法的流程的时序图。如图 7 所示，客户申请方 104 首先将访问认证信息发送至服务提供服务器 200（S102）。在步骤 S102 中发送的访问认证信息可以仅为 IC 卡的 IC 卡个体信息、或可以是用于服务提供服务器 200 以创建认证券的访问认证信息的一部分。

在步骤 S102 中从客户申请方 104 对其发送了访问认证信息的服务提供服务器 200 对访问认证信息进行加密或添加电子签名，从而创建认证券（S104）。服务提供服务器 200 将在步骤 S104 中创建的认

证券发送至卡发行服务器 300（S106）。

在步骤 S106 中从服务提供服务器 200 对其发送了认证券的卡发行服务器 300 验证认证券（S108）。在步骤 S108 中的对认证券的验证中，检查认证券是否可以被正确地解密、是否添加了正确的电子签名，在访问认证信息中包含的使用条件等。将在下文中详细地描述在步骤 S108 中的对认证券的验证。

在步骤 S108 中验证的认证券的验证结果被发送至服务提供服务器 200（S110）。卡发行服务器 300 将使客户申请方 104 与卡发行服务器 300 相连接的连接信息发送至服务提供服务器 200（S112）。在步骤 S112 中从卡发行服务器 300 对其发送了连接信息的服务提供服务器 200 将相关的连接信息发送至客户申请方 104（S114）。

在步骤 S114 中从服务提供服务器 200 对其发送了到卡发行服务器 300 的连接信息的客户申请方 104 基于相关的连接信息连接到卡发行服务器 300（S116）。在步骤 S116 中与客户申请方 104 相连接的卡发行服务器 300 基于来自客户申请方 104 的连接状态和客户申请方 104 的个体信息检查客户申请方 104 的合法性，然后访问 IC 芯片 150（S118）。

比较并验证在步骤 S118 中通过访问 IC 芯片 150 而获取的 IC 芯片 150 的 IC 卡的个体信息和认证券的访问认证信息。将在下文中详细地描述步骤 S120 中的对认证信息的验证。当在步骤 S120 中 IC 卡的合法性被确认为验证的结果时，执行将 IC 卡的卡信息写入到 IC 芯片 150，并更新卡信息的操作。上面描述了在卡发行系统 10 中执行的卡发行方法。

现在将基于图 8 详细地描述对认证券的验证。图 8 是描述对认证券的验证处理的说明图。如图 8 所示，首先检查认证券的格式是否合适（S202）。接下来，检查是否指定了在卡发行服务器 300 中可使用的处理（S204）。然后，检查是否指定了在卡发行服务器 300 中可使用的连接路径（S206）。

当没有指定与过去使用的认证券 ID 相同的认证券 ID 或者指定

了可使用的次数时，检查是否在认证券的可使用的次数的范围内（S208）。检查是否指定了认证券的可使用期，并且当指定了可使用期时，检查是否在可使用期内（S210）。检查对于要使用的处理的信息是否适合地选择了用 IC 卡类型信息可执行的处理（S212）。检查对于要使用的处理的信息是否合适地选择了用 IC 卡发行方类型信息可执行的处理（S214）。当认证券是加密的时，检查是否添加了正确的电子签名，或者是否正确地执行了解密（S216）。认证券的验证处理可以同时地执行所有的处理，并且处理的顺序是任意的。上面描述了认证券的验证处理。

现在将基于图 9 描述 IC 卡的认证信息的验证。图 9 是描述了 IC 卡的认证信息的验证处理的说明图。如图 9 所示，检查连接路径是否与指定的连接路径相同（S220）。在步骤 S220 中，除了检查连接路径、连接线路和协议状态之外，也可以检查芯片的连接 I/F、芯片的密钥等。然后，检查 IC 卡实体信息是否与认证券的 IC 卡实体信息相同（S222）。

检查 IC 卡类型信息是否与认证券的 IC 卡类型信息相同(S224)。此外，检查 IC 卡发行方信息是否与认证券的 IC 卡发行方信息相同（S226）。然后，检查客户申请方 ID 是否与认证券的客户申请方 ID 相同（S228）。检查 IC 卡对应终端硬件 ID 是否与认证券的 IC 卡对应终端硬件 ID 相同（S230）。检查 IC 卡对应终端所有者 ID 是否与认证券的 IC 卡对应终端所有者 ID 相同（S232）。检查 IC 卡读取数据是否与在认证券中指定的读取数据相同（S234）。IC 卡的认证信息的验证处理可以同时地执行所有的处理，并且处理的顺序是任意的。上面描述了对 IC 卡的认证信息的验证处理。

现在将基于图 10 描述卡发行系统 10 中的访问信息询问处理。图 10 示出了说明访问信息询问处理的时序图。如图 10 所示，服务提供服务器 200 向卡发行服务器 300 询问对 IC 卡的访问状态（S130）。步骤 S130 中被服务提供服务器 200 询问访问状态的卡发行服务器 300 将对 IC 卡的访问状态通知给服务提供服务器 200（S132）。在步骤

S132 中，由于卡发行服务器 300 甚至不与客户申请方 104 相连接，因此通知与信息处理终端 100 的非连接。

进行客户申请方 104 与卡发行服务器 300 的连接（S134）。在步骤 S134 中的连接之后，服务提供服务器 200 询问访问状态（S136），并且卡发行服务器 300 通知访问状态（S137）。在步骤 S137 中，卡发行服务器 300 通知已经进行了与客户申请方 104 的连接。

进行从卡发行服务器 300 到 IC 芯片的访问（S140）。在步骤 S140 中的访问之后，服务提供服务器 200 询问访问状态（S142），并且卡发行服务器 300 通知访问状态（S144）。在步骤 S144 中，卡发行服务器 300 通知访问状态，例如对 IC 芯片的访问结果、执行处理的地方、处理的执行结果等。即使在访问 IC 芯片的期间也可以执行访问状态的询问。

服务提供服务器 200 可以使用一次 ID 等来对卡发行服务器检查客户申请方 104 的处理状态。然后可以得到诸如客户申请方 104 是否与卡发行服务器 300 相连接、客户申请方 104 是否与卡发行服务器 300 相连接但发生错误、客户申请方 104 是否与卡发行服务器 300 相连接并且处理被正常完成等的处理状态。上面描述了在卡发行系统 10 中的访问信息询问处理。

上面已经描述了根据第一实施例的卡发行系统 10。根据卡发行系统 10，服务提供服务器 200 对用于认证信息处理终端的访问的访问认证信息进行加密，从而创建认证券，并且将认证券发送至卡发行服务器 300。卡发行服务器 300 验证该认证券，将验证结果通知给服务提供服务器，并且发送用于连接到卡发行服务器 300 的连接信息。通过服务提供服务器 200 对其发送了连接信息的信息处理终端 100 连接到卡发行服务器 300，从而卡发行服务器 300 可以访问信息处理终端 100 的 IC 芯片 150。

从服务提供服务器 200 发送的认证券包含 IC 卡实体信息等，从而可以预先验证 IC 芯片，以便在访问 IC 卡之前的早期阶段检测到不对应于 IC 卡的处理，由此可以有效地防止未授权的访问。

（第二实施例）

现在将描述根据本发明的第二实施例的卡发行系统的简要概述。根据本实施例的卡发行系统 10'包括信息处理终端 100'、服务提供服务器 200'和卡发行服务器 300'。卡发行系统 10'的配置基本上与根据第一实施例的卡发行系统 10 的配置相同，因此将省略详细的说明。本实施例与第一实施例不同在于信息处理终端 100'是可靠的客户。在信息处理终端 100'作为不是能够安装可以被容易地分组分析等的应用程序的终端而是诸如便携式终端的结合终端的可靠客户装置的情况下，或者在提及认证券的内容的情况下，在信息处理终端 100'中不会产生任何问题。

在该情况下，由服务提供服务器 200'创建的认证券被发送至信息处理终端 100'的客户申请方，并且客户申请方连接到卡发行服务器 300'并发送认证券，从而执行对 IC 卡的认证处理。于是，服务提供服务器 200'和卡发行服务器 300 之间的通信可以减少，并且可以减少服务提供服务器 200 的建立工时。在本实施例中，认证券在服务提供服务器 200'中被创建，但不限于这个实例。例如，信息处理终端 100'可以具有与服务提供服务器 200'相似的功能。具体地说，信息处理终端 100'可以保持用于创建认证券的私钥，并且创建认证券。在上文中描述了根据本实施例的卡发行系统 10'的简要概述。

下面将基于图 11 来描述卡发行系统 10'的信息处理终端 100'、服务提供服务器 200'和卡发行服务器 300'的功能配置。图 11 是示出了信息处理终端 100'、服务提供服务器 200'和卡发行服务器 300'的功能配置的框图。信息处理终端 100'具有与第一实施例的信息处理终端 100 基本上相同的功能，因此将省略详细的说明。如上所述，信息处理终端 100'是可靠的客户。与第一实施例的信息处理终端的尤其不同之处在于：由服务提供服务器 200'创建的认证券通过认证券接收单元 110 而被接收，并且认证券发送单元 112 将相关认证券发送至卡发行服务器 300'。

服务提供服务器 200'具有与第一实施例的服务提供服务器 200

基本上相似的功能，因此将省略详细的说明。服务提供服务器 200’与第一实施例的服务提供服务器 200 的尤其不同之处在于：提供有由认证券创建单元 204 创建的认证券的认证券发送单元 212’将认证券发送至信息处理终端 100’的客户申请方 104，而不是卡发行系统 300’。发送至客户申请方 104 的认证券从客户申请方 104 被发送至卡发行服务器 300’。于是服务提供服务器 200’和卡发行服务器 300’之间的通信可以减少，并且可以减少服务提供服务器 200’的建立工时。

卡发行服务器 300’具有与第一实施例的卡发行服务器 300 基本上相同的功能，因此将省略详细的说明。卡发行服务器 300’与第一实施例的卡发行服务器 300 尤其不同之处在于：认证券接收单元 312’接收从信息处理终端 100’发送的认证券，并将认证券提供至认证券验证单元 306。验证结果通知单元 308 的验证结果和与验证结果同时被发送的连接信息通过连接信息发送单元 314’被发送至信息处理终端 100’的客户申请方 104。在第一实施例中，验证结果和连接信息通过服务提供服务器 200 被发送至客户申请方 104，但在本实施例中，验证结果和连接信息被直接发送至客户申请方 104。因此，可以减少服务提供服务器 200’和卡发行服务器 300’之间的通信。上面描述了与卡发行系统 20’相关的每一个装置的功能配置。

现在将描述在卡发行系统 10’中执行的卡发行方法。在根据本实施例的卡发行方法中，将省略对与第一实施例相似的处理的详细描述。图 12 示出了说明在卡发行系统 10’中执行的卡发行方法的流程的时序图。如图 12 所示，客户申请方 104 首先将访问认证信息发送至服务提供服务器 200’（S302）。在步骤 S302 中从客户申请方 104 对其发送了访问认证信息的服务提供服务器 200’对访问认证信息进行加密或添加电子签名，从而创建认证券（S304）。在步骤 S304 中创建的认证券被发送至客户申请方 100’(S306)。

在步骤 S306 中由服务提供服务器 200’对其发送认证券的客户申请方 104 将认证券发送至卡发行服务器 300’(S308)。在步骤 S308 中从客户申请方 104 对其发送了认证券的卡发行服务器 300’验证认证券

（S310）。在步骤 S310 中的对认证券的验证中，如上所述，检查认证券是否可以被正确地解密、是否添加了正确的电子签名、在访问认证信息中包含的使用条件等。

在步骤 S310 中的对认证券的验证的验证结果被发送至客户申请方 104（S312）。卡发行服务器 300 将用于使客户申请方 104 与卡发行服务器 300 相连接的连接信息发送至客户申请方 104（S314）。在步骤 S314 中从卡发行服务器 300'对其发送了到卡发行服务器 300'的连接信息的客户申请方 104 基于相关的连接信息连接至卡发行服务器 300'（S316）。在步骤 S316 中与客户申请方 104 相连接的卡发行服务器 300'根据来自客户申请方 104 的连接状态和客户申请方 104 的个体信息来检查客户申请方 104 的合法性，然后访问 IC 芯片 150（S318）。

比较并验证在步骤 S318 中通过访问 IC 芯片 150 而获取的 IC 芯片 150 的 IC 卡的个体信息和认证券的访问认证信息（S320）。当在步骤 S320 中 IC 卡的合法性作为验证的结果被确认时，将 IC 卡的卡信息写入到 IC 芯片 150，并执行卡信息的更新（S322）。上面描述了在卡发行系统 10'中执行的卡发行方法。

上面已经描述了根据第二实施例的卡发行系统 10'。根据卡发行系统 10'，由服务提供服务器 200'创建的认证券被发送至信息处理终端 100'的客户申请方 104，并且客户申请方 104 与卡发行服务器 300'相连接并发送认证券，由此可以执行对 IC 卡的认证处理。于是服务提供服务器 200'和卡发行服务器 300'之间的通信可以减少，并且可以减少服务提供服务器 200'的建立工时。

（第三实施例）

现在将描述根据本发明的第三实施例的卡发行系统的简要概述。图 13 是根据本实施例的卡发行系统 20 的配置实例的说明图。如图 13 所示，卡发行系统 20 包括信息处理终端 101、服务提供服务器 201、卡发行服务器 301 和服务代理服务器 400。在卡发行系统 20 中，信息处理终端 101、服务提供服务器 201、卡发行服务器 301 和服务代理服务器 400 通过网络 50 相连接。本实施例与第一实施例和第二实施

例的显著不同之处在于设置了服务代理服务器 400。

服务代理服务器 400 具有基于来自服务提供服务器 201 的请求而执行卡发行服务器 301 和信息处理终端 101 的处理的功能。在该情况下，出现了这样的问题：如果如第一实施例或第二实施例中的一样认证券具有一层的配置，则由服务提供服务器 201 执行的所有处理都要对服务代理服务器 400 允许。创建了能够仅执行服务提供服务器 201 向服务代理服务器 400 请求的处理的认证许可，并且基于相关许可创建认证券。因此，当服务提供服务器 201 向服务代理服务器 400 请求可供替换的处理时，可以在维持安全性的同时，通过将认证券设为多级配置来限制可执行的处理。

在本实施例中，需要对认证许可和认证券分别加密，并添加电子签名，从而将认证券设为多级配置。例如，当使用通过诸如 RSA 的非对称密钥进行的电子签名验证时，创建许可的服务提供服务器 201 准备认证密钥对 1（Pk1/Sk1），并且创建认证券的服务代理服务器 400 准备认证密钥对 2（Pk2/Sk2）。预先用认证公钥（Pk1）注册卡发行服务器 301，或者如果设置了证书授权机构，则卡发行服务器 301 需要从证书授权机构获取认证公钥 1（Pk1）。

对使用认证密钥的多级配置的认证的简要概述如下。服务提供服务器 201 创建包括认证公钥 2（Pk2）的认证信息，所述认证公钥 2 与服务代理服务器 400 的认证私钥 2（Sk2）形成了一对，并且服务提供服务器 201 使用认证私钥 1(Sk1)创建添加有电子签名的认证许可。在下文中将具体地描述认证许可的细节。服务代理服务器 400 将 IC 卡的个体信息添加到从服务提供服务器 201 发送的认证许可中，并且使用认证私钥 2（Sk2）来创建添加有电子签名的认证券。

接收了由服务代理服务器 400 创建的认证券的卡发行服务器 301 使用预先获取的认证公钥 1（Pk1）来验证在券中包含的电子签名，并且检查在许可中包含的认证公钥 2（Pk2）的合法性。在确认了认证公钥 2（Pk2）的合法性之后，使用认证公钥 2（Pk2）来执行认证券的电子签名验证，从而验证认证券的合法性。

因此，根据对于认证许可和认证券使用不同的认证密钥的多级配置，即使当服务提供服务器 201 使服务代理服务器 400 等执行处理时，认证是相互可行的，并且也可以限制要代理的处理。在本实施例中，除了认证券具有多级配置以外的对认证券的验证和对 IC 卡的验证与第一实施例和第二实施例相似，因此将省略详细的描述。上面已经描述了卡发行系统 20 的简要概述。

现在将描述卡发行系统 20 的信息处理终端 101、服务提供服务器 201、卡发行服务器 301 和服务代理服务器 400 的详细配置。图 14 是示出了信息处理终端 101、服务提供服务器 201、卡发行服务器 301 和服务代理服务器 400 的功能配置的框图。信息处理终端 101 具有与根据第一实施例的信息处理终端 100 基本上相似的功能，因此将省略详细的说明。信息处理终端 101 与第一实施例的信息处理终端 100 的不同之处在于:IC 芯片 150 的个体信息被发送至服务代理服务器 400。

服务提供服务器 201 包括公钥注册单元 202、公钥获取单元 203、通信控制单元 209 和认证许可创建单元 220。公钥注册单元 202 具有预先在证书授权机构 500 注册认证密钥对 1 的认证公钥 1（Pk1）的功能。公钥获取单元 203 具有获取由服务代理服务器 400 在证书授权机构 500 中注册的认证公钥、以及将相关认证公钥提供至认证许可创建单元 220 的功能。认证许可创建单元 220 获取认证公钥（Pk2）。认证许可创建单元 220 具有对许可给服务代理服务器 400 的服务的信息加密以及创建认证许可的功能。在此将基于图 15 讨论许可给服务代理服务器 400 的服务的信息(下文中被称为许可信息)和认证许可。图 15 是描述许可信息 2202 和认证许可 2204 的内容的说明图。如图 15 所示，许可信息 2202 包括许可的使用条件，其中，许可的使用条件包括可使用处理的列表、可使用连接路径的列表、许可的 ID、许可的有效期开始日期和时间、许可的有效期结束日期和时间、许可的可使用次数、许可使用定义、认证公钥 2（Pk2）等。

许可使用定义是以下述条件来定义的：例如，在券信息中是否需要包含在卡发行服务器 301 中访问的 IC 卡的 IC 卡实体信息、客户申

请方 ID、IC 卡对应终端硬件 ID、IC 卡对应终端所有者 ID 和从卡发行服务器 301 发送的质询（一次 ID、口令信息等）。使用认证私钥 1（Sk1）对包括认证公钥 2（Pk2）的许可信息 2202 添加电子签名，从而创建认证许可 2204。返回到图 14，认证许可创建单元 220 将创建的认证许可提供至认证许可发送单元 222。

通信控制单元 209 是被配置为包括用于连接到诸如因特网的网络的通信装置等的通信接口，并且具有通过网络与服务提供服务器 400 发送和接收数据的功能。通信控制单元 209 包括认证许可发送单元 222 等。通过认证许可创建单元 220 提供有认证许可的认证许可发送单元 222 将相关认证许可发送至服务代理服务器 400。在本实施例中，通过网络将认证许可发送至服务代理服务器 400，但不限于这样的实例，并且认证许可可以被离线地发送至服务代理服务器 400。

服务代理服务器 400 包括认证券创建单元 402、通信控制单元 404 和公钥注册单元 410。认证券创建单元 402 具有这样的功能：根据由认证许可接收单元 406 接收的认证许可的使用条件来创建访问认证信息，并且使用认证私钥 2（Sk2）对访问认证信息加密或添加电子签名，从而创建认证券。在此将基于图 16 讨论访问认证信息 4022 和认证券 4024。图 16 是描述访问认证信息 4022 和认证券 4024 的内容的说明图。

如图 16 所示，除了添加许可以外，访问认证信息 4022 与根据第一实施例的访问认证信息基本上相同，因此将省略详细的说明。访问认证信息 4022 可以包含从卡发行服务器发送的质询（一次 ID 和口令信息）等。通过认证私钥 2（Sk2）向访问认证信息 4022 添加电子签名，从而创建认证券 4024。许可可以不是电子签名数据的目标。返回到图 14，由认证券创建单元 402 创建的认证券被提供至认证券发送单元 408。

通信控制单元 404 是被配置为包括用于连接到诸如因特网的网络的通信装置等的通信接口，并且具有通过网络与信息处理终端 101、服务提供服务器 201 和卡发行服务器 301 发送和接收数据的功能。通

信控制单元 404 包括认证许可接收单元 406、认证券发送单元 408 等。认证许可接收单元 406 具有接收由服务提供服务器 201 创建的认证许可的功能。认证券发送单元 408 具有将提供至认证券创建单元 402 的认证券发送至卡发行服务器 301 的功能。公钥注册单元 410 具有预先在证书授权机构 500 中注册与认证私钥(Sk2)成对的认证公钥 2(Pk2)的功能。

卡发行服务器 301 包括通信控制单元 303、公钥获取单元 304、认证许可验证单元 324、认证券验证单元 307、验证结果通知单元 308、认证信息验证单元 310 等。通信控制单元 303 是被配置为包括与诸如因特网的网络相连接的通信装置的通信接口，并且具有通过网络与信息处理终端 101 或服务代理服务器 400 发送和接收数据的功能。

通信控制单元 303 包括认证券接收单元 313、连接信息发送单元 315、IC 卡访问单元 316 等。认证券接收单元 313 具有接收由服务代理服务器 400 创建的认证券并将认证券提供至认证许可验证单元 324 的功能。连接信息发送单元 315 具有在验证结果通知单元 308 通知验证结果的同时,将连接信息发送至信息处理终端 100 的客户申请方 104 的功能。IC 卡访问单元 316 具有访问信息处理终端 101 的 IC 芯片 150、对 IC 芯片 150 执行 IC 卡信息等的读取或写入、以及将 IC 卡的信息提供至认证信息验证单元 310 的功能。

公钥获取单元 304 具有获取通过服务提供服务器 201 在证书授权机构 500 注册的认证公钥并将该认证公钥提供至认证券验证单元 307 的功能。在本实施例中，公钥获取单元 304 从证书授权机构获取认证公钥 1（Pk1）。

认证许可验证单元 324 具有对接收的认证许可解密并验证认证许可的功能。如果向认证许可添加电子签名，则认证许可验证单元 324 使用认证公钥（Pk1）来验证相关的电子签名，并且检查在认证许可中包含的认证公钥（Pk2）的合法性。认证券验证单元 307 具有使用认证公钥（Pk2）来对认证券执行电子签名验证并验证券的合法性的功能，所述认证公钥（Pk2）的合法性由认证许可验证单元 324 来确

认。与第一实施例的认证券验证单元 306 相似，认证券验证单元 307 对认证券的访问认证信息执行验证。认证许可验证单元 324 向验证结果通知单元 208 提供认证券的验证结果。

验证结果通知单元308具有将由认证券验证单元307提供的认证券的验证结果通知给服务提供服务器 400 的功能。验证结果通知单元 308 将使信息处理终端 101 与卡发行服务器 310 相连接的连接信息与认证券的验证结果一起提供至连接信息发送单元 315。认证信息验证单元 310 具有与根据第一实施例的卡发行服务器 300 的认证信息验证单元 310 基本上相同的功能，因此将省略详细的说明。

上面描述了卡发行系统 20 的每一个装置的功能配置。现在将描述在卡发行系统 20 中执行的卡发行方法。图 17 是示出了在卡发行系统 20 中执行的卡发行方法的流程的时序图。如图 17 所示，服务提供服务器 210 首先对包含许可服务代理服务器 400 的服务的信息的许可信息加密，从而创建认证许可（S402）。服务提供服务器 201 将在步骤 S402 中创建的认证许可发送至服务代理服务器 400（S404）。

客户申请方 104 将访问认证信息发送至服务代理服务器 400（S406）。对于在步骤 S406 中由客户申请方 104 进行的访问认证信息的发送，可以在从服务提供服务器 201 发送认证许可之后执行发送，或者可以预先执行发送。在步骤 S404 中从服务提供服务器 201 对其发送了认证许可、且在步骤 S406 中从客户申请方 104 对其发送了访问认证信息的服务代理服务器基于认证许可和访问认证信息来创建认证券（S408）。服务代理服务器 400 将在步骤 S408 中创建的认证券发送至卡发行服务器 301（S410）。

在步骤 S410 中从服务代理服务器 400 对其发送了认证券的卡发行服务器 301 对在认证券中包含的认证许可解密并验证该认证许可（S414）。如上所述，如果向认证券和认证许可添加了电子签名，则使用认证公钥 1（Pk1）来验证在认证券中包含的电子签名，并且可以确认在认证许可中包含的认证公钥 2（Pk2）的合法性。在步骤 S414 中验证了认证许可之后，对认证券执行验证（S416）。如上所述，如

果向认证券添加了电子签名数据，则使用在认证许可中包含的认证公钥 2（Pk2）来对认证券执行电子签名验证，从而验证认证券。在步骤 S416 中验证的认证券的验证结果被发送至服务代理服务器 400（S418）。将使客户申请方 104 与卡发行服务器 301 相连接的连接信息发送至服务代理服务器(S420)。在步骤 S420 中从卡发行服务器 301 对其发送了连接信息的服务代理服务器 400 将相关的连接信息发送至客户申请方 104（S422）。

在步骤 S422 中从服务代理服务器 400 对其发送到卡发行服务器 301 的连接信息的客户申请方 104 基于相关的连接信息与卡发送服务器 301 相连接（S424）。在步骤 S424 中与客户申请方 104 相连接的卡发行服务器 301 根据来自客户申请方 104 的连接状态和客户申请方 104 的个体信息来检查客户申请方 104 的合法性，并访问 IC 芯片 150（S426）。

比较并验证在步骤 S426 中通过访问 IC 芯片 150 而获取的 IC 芯片 150 的 IC 卡的个体信息和认证券的访问认证信息。当在步骤 S428 中 IC 卡的合法性作为验证的结果被确认时，将 IC 卡的卡信息写入到 IC 芯片 150，并执行卡信息的更新（S430）。上面描述了在卡发行系统 20 中执行的卡发行方法。

上面已经描述了根据第三实施例的卡发行系统 20。根据卡发行系统 20，创建能够仅执行服务提供服务器 201 请求服务代理服务器 400 的处理的认证许可，并且基于认证许可创建认证券。因此，当服务提供服务器 201 向服务代理服务器 400 请求可供替换的处理时，可以在维持安全性的同时，通过将认证券设为多级配置来限制可执行的处理。因此，根据对于认证许可和认证券使用不同的认证密钥的多级配置，即使当服务提供服务器 201 使服务代理服务器 400 等执行处理时，认证也是相互可行的。

本领域技术人员应理解为,只要在所附权利要求或其等同物的范围内,就可以基于设计需要和其它因素进行各种变形、组合、子组合和替换。

例如，在上述实施例中，卡发行服务器使用认证券来执行对信息处理终端的认证，但本发明不限于这样的实例。例如，在使用服务提供服务器的认证中，可以通过使用质询响应的认证方法来执行认证。因此，卡发行服务器可以将使用认证券的认证和使用质询响应的认证组合来执行认证。可以基于服务提供服务器的选择来确定使用哪种认证方法。

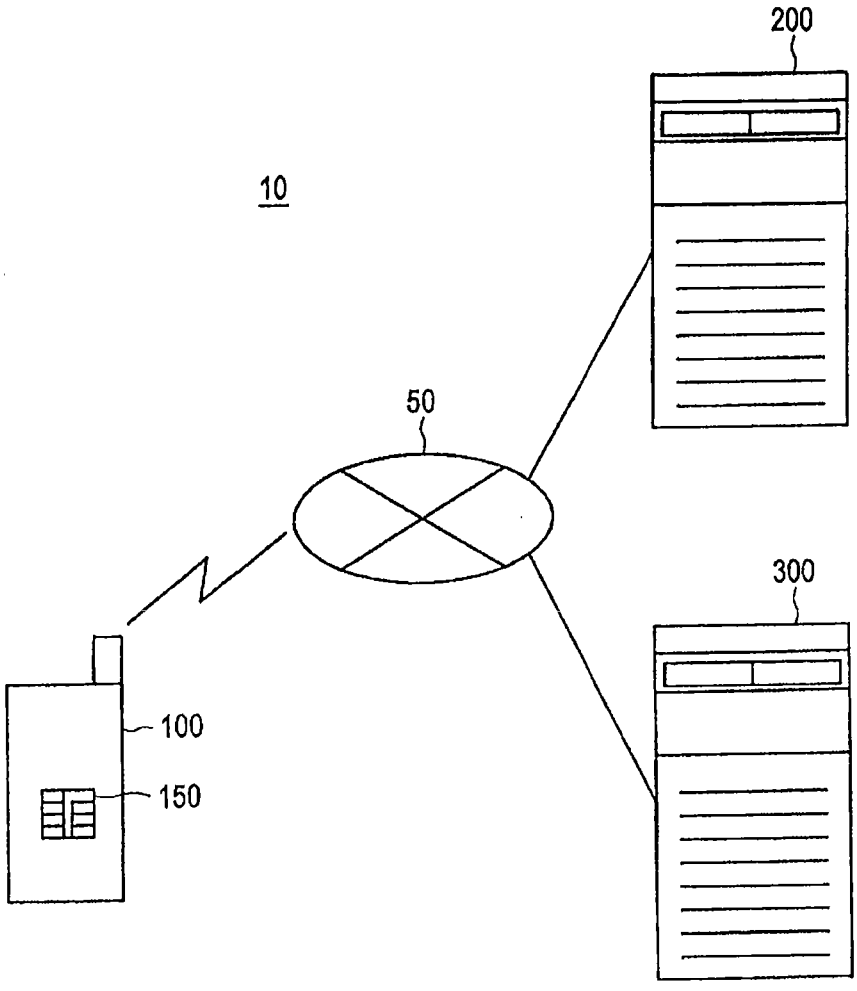


图1

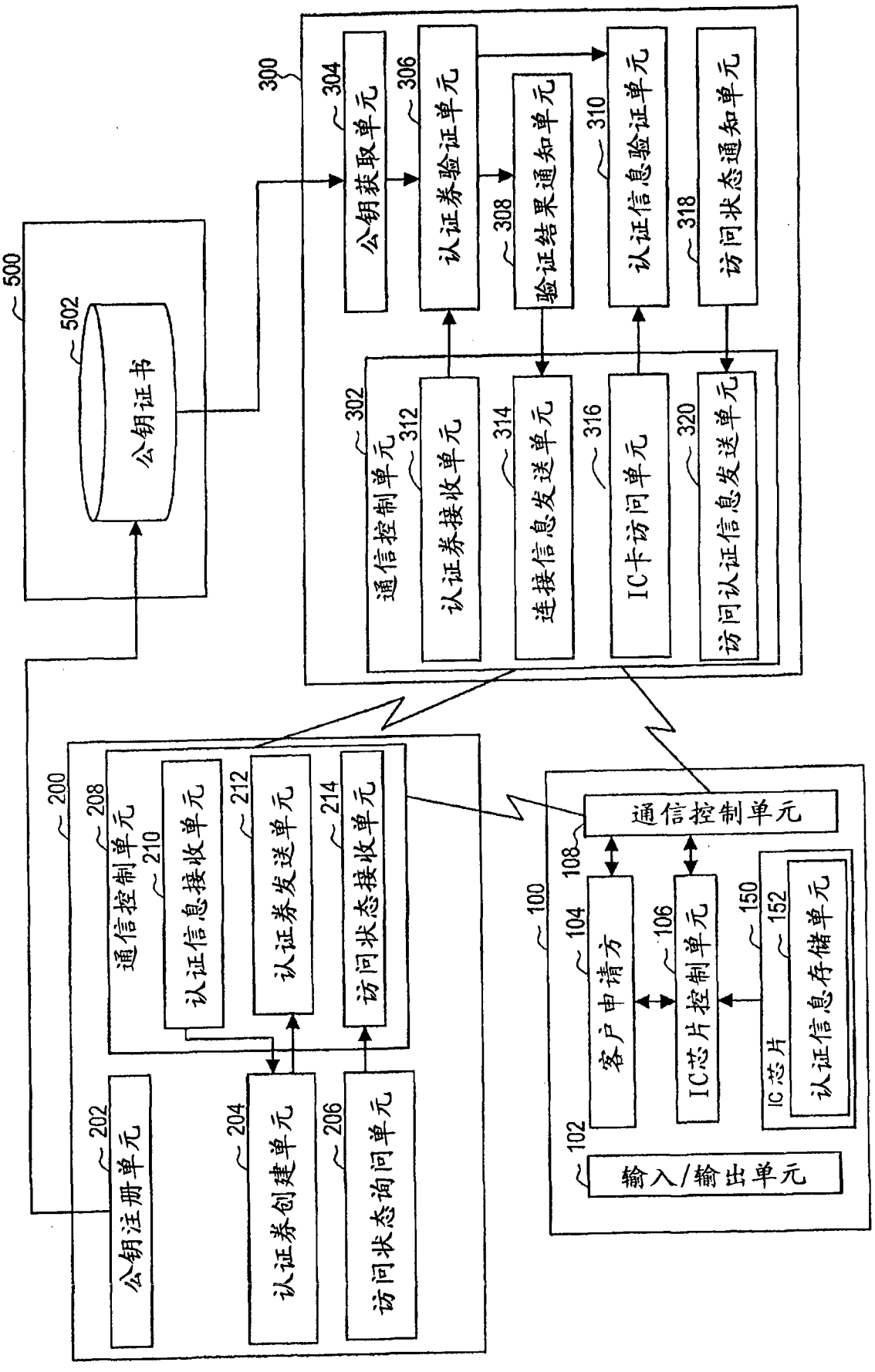

500
502
公钥证书
300
304
公钥获取单元
306
认证券验证单元
308
验证结果通知单元
310
认证信息验证单元
318
访问状态通知单元
302
通信控制单元
312
认证券接收单元
314
连接信息发送单元
316
IC卡访问单元
320
访问认证信息发送单元
200
208
通信控制单元
210
认证信息接收单元
212
认证券发送单元
214
访问状态接收单元
202
公钥注册单元
204
认证券创建单元
206
访问状态询问单元
100
108
通信控制单元
104
客户申请方
106
IC芯片控制单元
150
IC芯片
152
认证信息存储单元
102
输入/输出单元

图 2

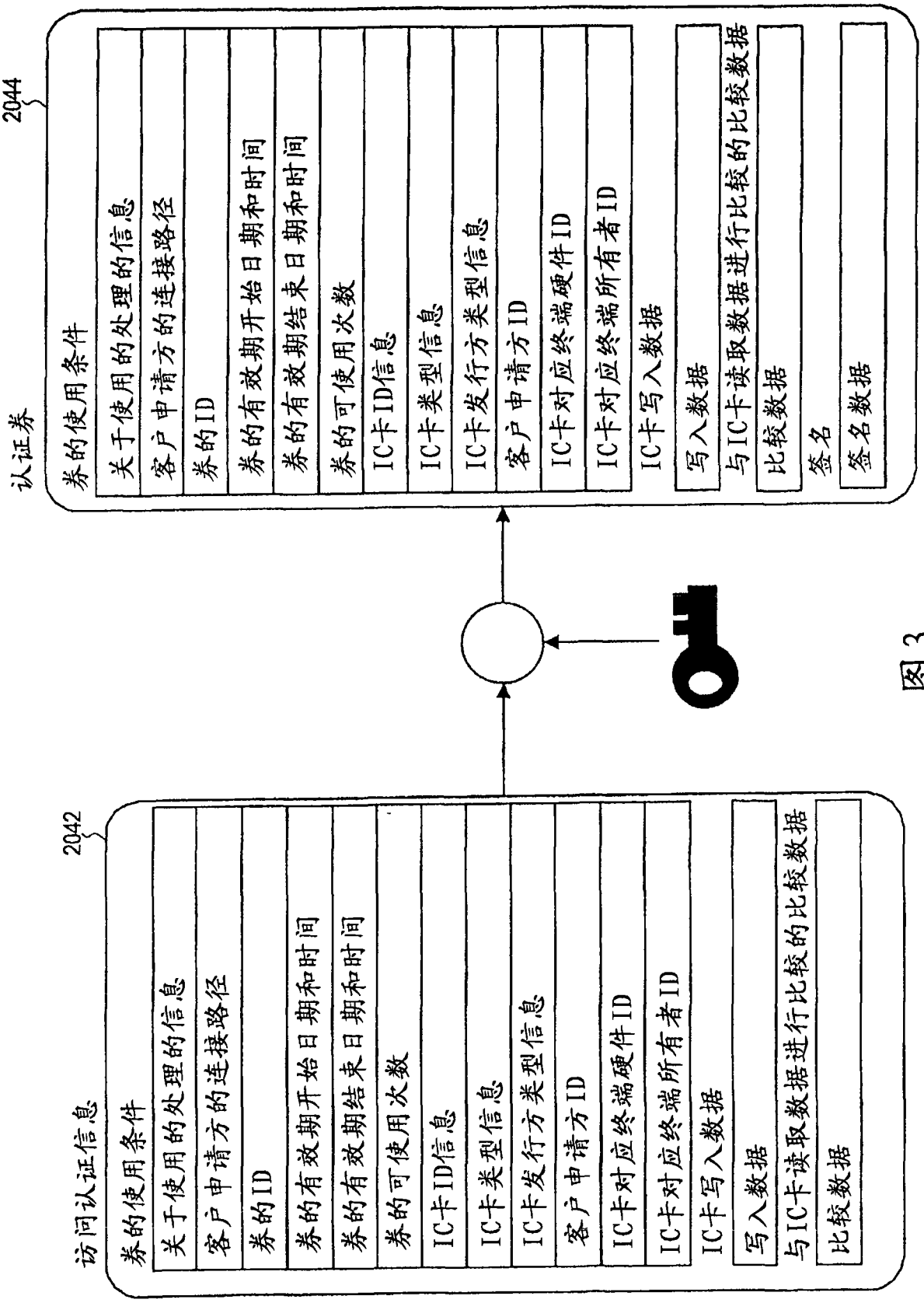

访问认证信息
2042
券的使用条件
关于使用的处理的信息
客户申请方的连接路径
券的ID
券的有效期开始日期和时间
券的有效期结束日期和时间
券的可使用次数
IC卡ID信息
IC卡类型信息
IC卡发行方类型信息
客户申请方ID
IC卡对应终端硬件ID
IC卡对应终端所有者ID
IC卡写入数据
写入数据
与IC卡读取数据进行比较的比较数据
比较数据
认证券
2044
券的使用条件
关于使用的处理的信息
客户申请方的连接路径
券的ID
券的有效期开始日期和时间
券的有效期结束日期和时间
券的可使用次数
IC卡ID信息
IC卡类型信息
IC卡发行方类型信息
客户申请方ID
IC卡对应终端硬件ID
IC卡对应终端所有者ID
IC卡写入数据
写入数据
与IC卡读取数据进行比较的比较数据
比较数据
签名
签名数据

图3

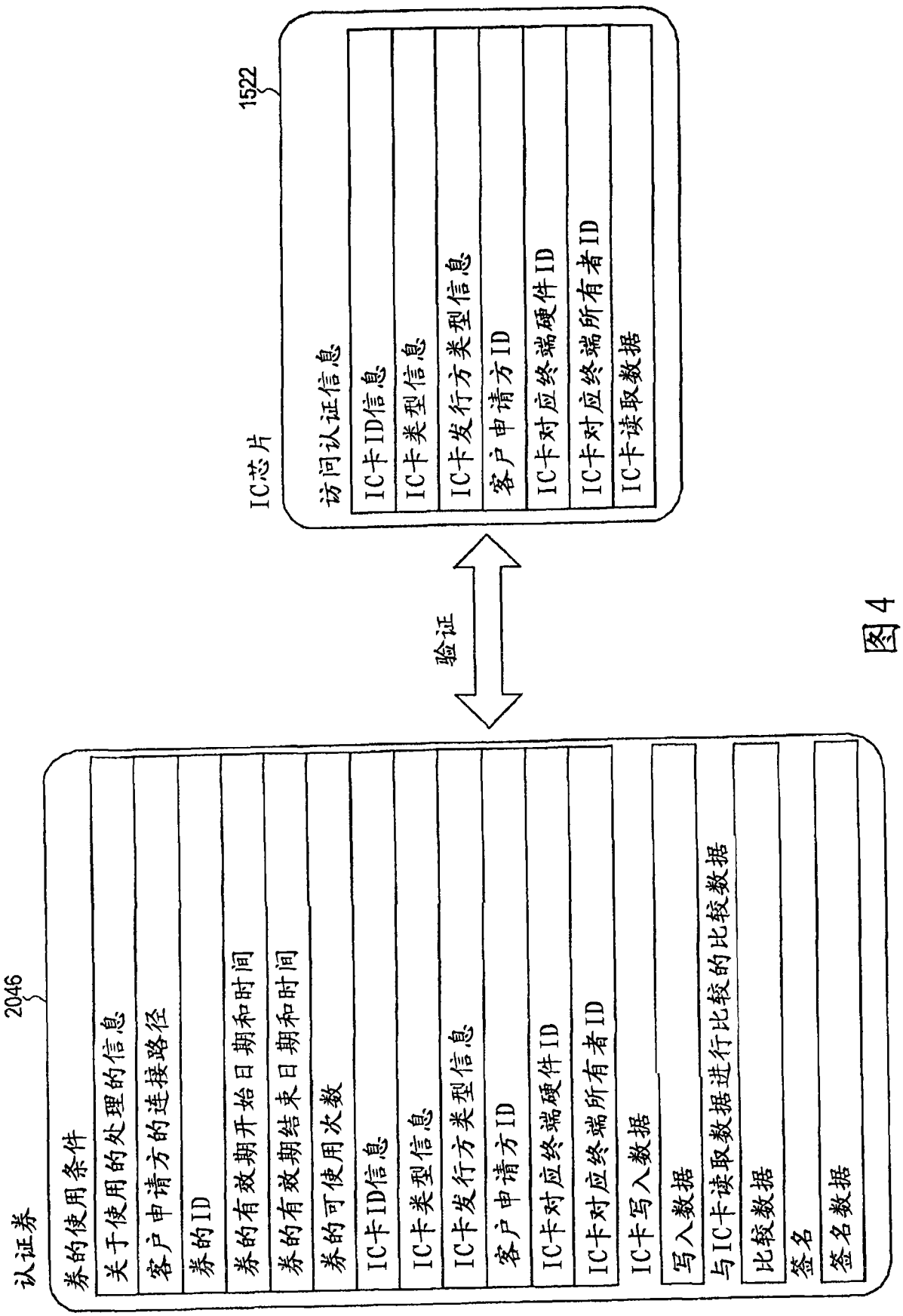

认证券
2046
券的使用条件
关于使用的处理的信息
客户申请方的连接路径
券的ID
券的有效期开始日期和时间
券的有效期结束日期和时间
券的可使用次数
IC卡ID信息
IC卡类型信息
IC卡发行方类型信息
客户申请方ID
IC卡对应终端硬件ID
IC卡对应终端所有者ID
IC卡写入数据
写入数据
与IC卡读取数据进行比较的比较数据
比较数据
签名
签名数据
验证
IC芯片
1522
访问认证信息
IC卡ID信息
IC卡类型信息
IC卡发行方类型信息
客户申请方ID
IC卡对应终端硬件ID
IC卡对应终端所有者ID
IC卡读取数据

图4

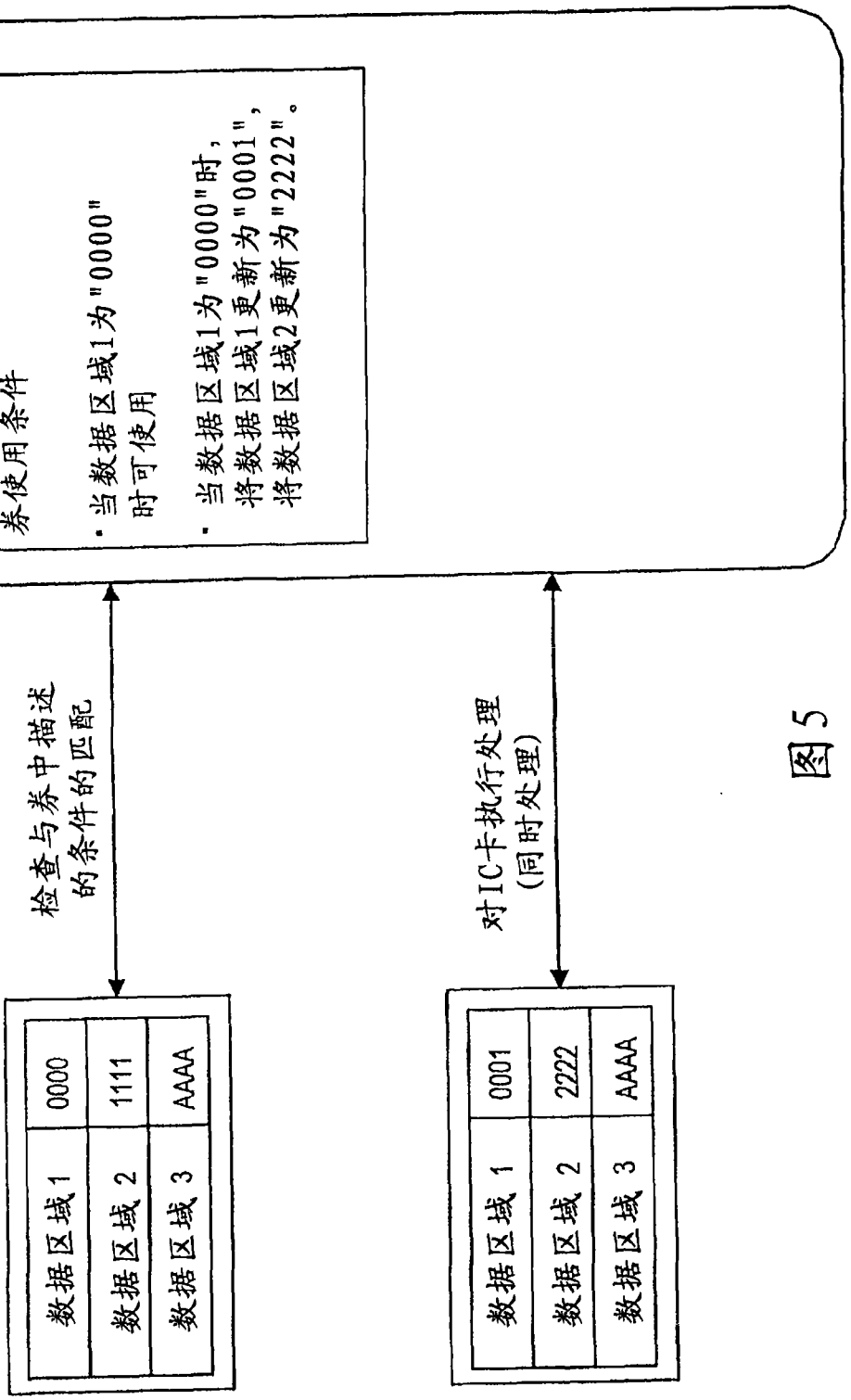

卡发行服务器
券使用条件
• 当数据区域1为"0000"时可使用
• 当数据区域1为"0000"时，将数据区域1更新为"0001"，将数据区域2更新为"2222"。
检查与券中描述的条件的匹配
对IC卡执行处理(同时处理)
数据区域 1
0000
数据区域 2
1111
数据区域 3
AAAA
数据区域 1
0001
数据区域 2
2222
数据区域 3
AAAA

图 5

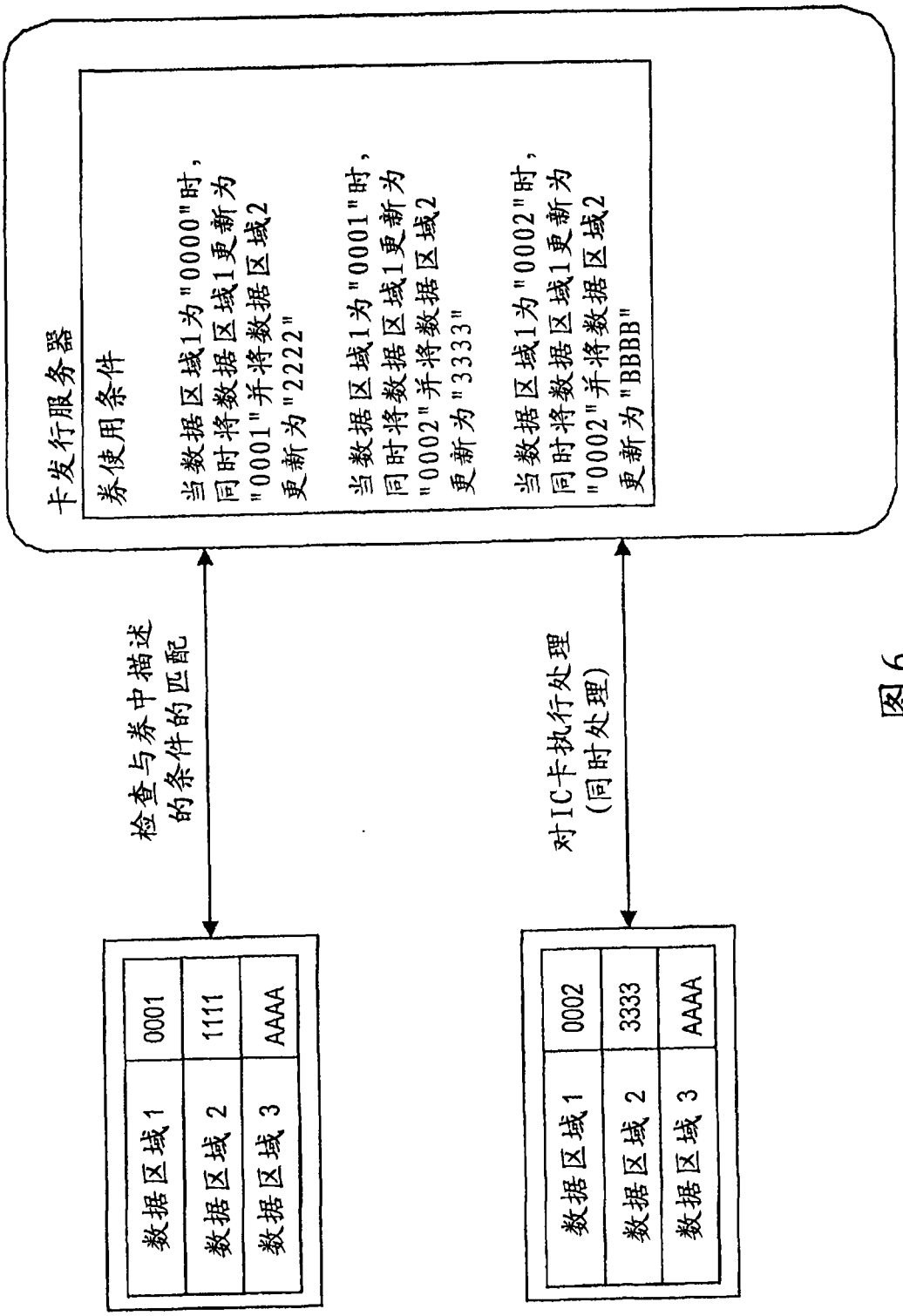

卡发行服务器
券使用条件
当数据区域1为"0000"时，同时将数据区域1更新为"0001"并将数据区域2更新为"2222"
当数据区域1为"0001"时，同时将数据区域1更新为"0002"并将数据区域2更新为"3333"
当数据区域1为"0002"时，同时将数据区域1更新为"0002"并将数据区域2更新为"BBBB"
检查与券中描述的条件的匹配
对IC卡执行处理(同时处理)
数据区域 1
数据区域 2
数据区域 3
0001
1111
AAAA
数据区域 1
数据区域 2
数据区域 3
0002
3333
AAAA

图 6

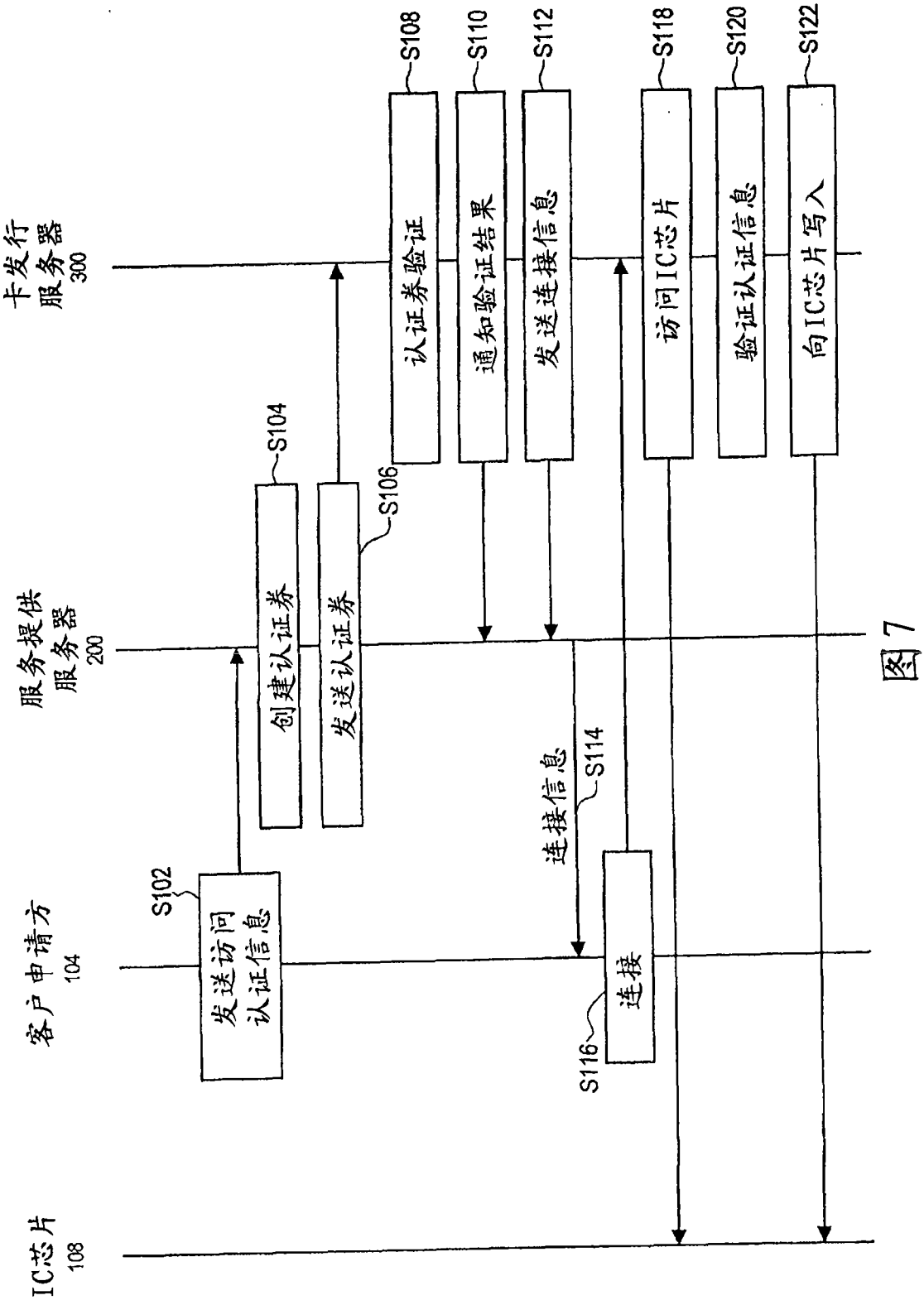

卡发行
服务器
300
服务提供
服务器
200
客户申请方
104
IC芯片
108
S102
发送访问
认证信息
S104
创建认证券
发送认证券
S106
S108
认证券验证
S110
通知验证结果
S112
发送连接信息
S114
连接信息
S116
连接
S118
访问IC芯片
S120
验证认证信息
S122
向IC芯片写入

图 7

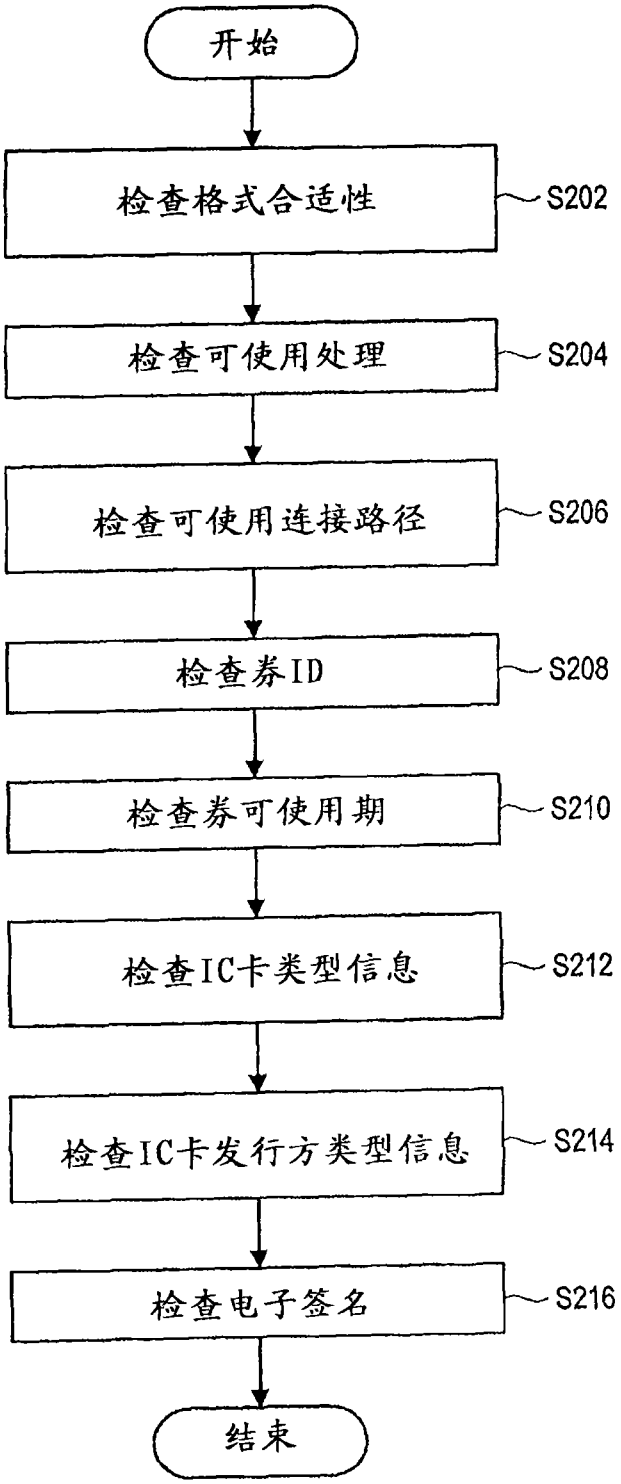

开始
检查格式合适性
S202
检查可使用处理
S204
检查可使用连接路径
S206
检查券ID
S208
检查券可使用期
S210
检查IC卡类型信息
S212
检查IC卡发行方类型信息
S214
检查电子签名
S216
结束

图8

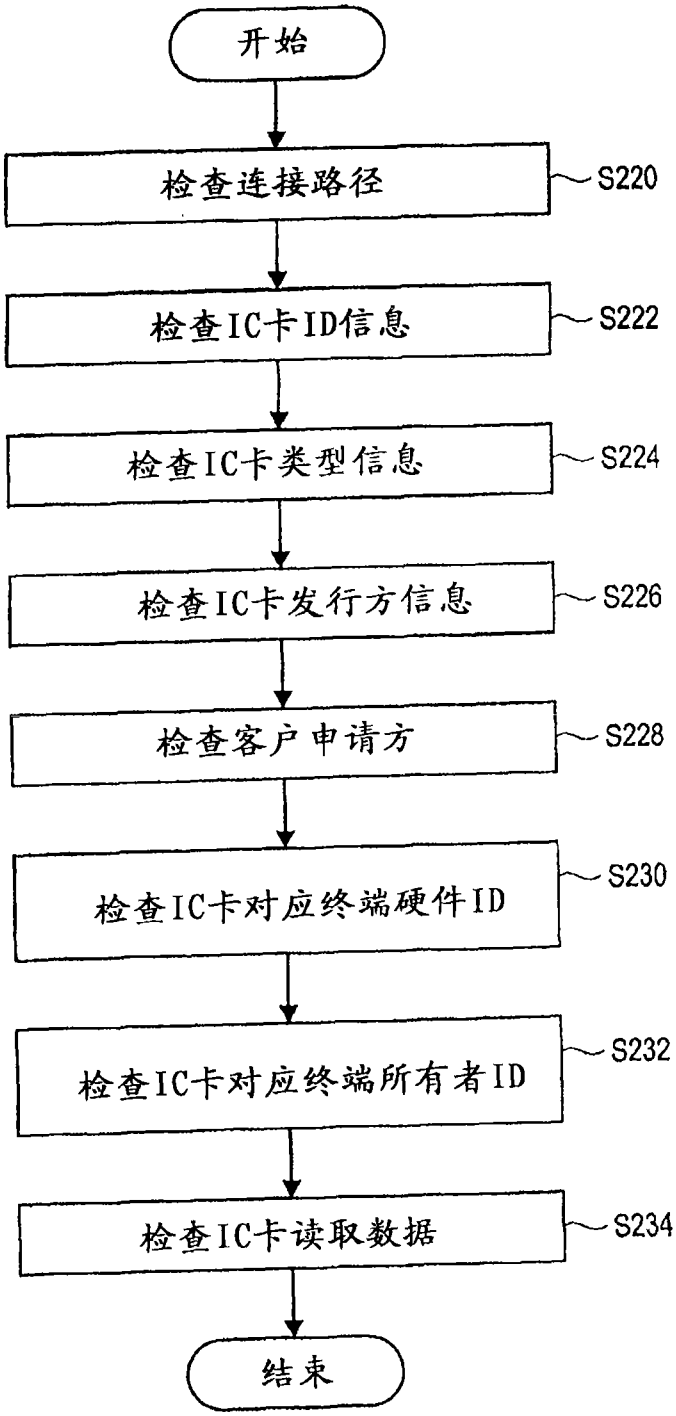

开始
检查连接路径
S220
检查IC卡ID信息
S222
检查IC卡类型信息
S224
检查IC卡发行方信息
S226
检查客户申请方
S228
检查IC卡对应终端硬件ID
S230
检查IC卡对应终端所有者ID
S232
检查IC卡读取数据
S234
结束

图9

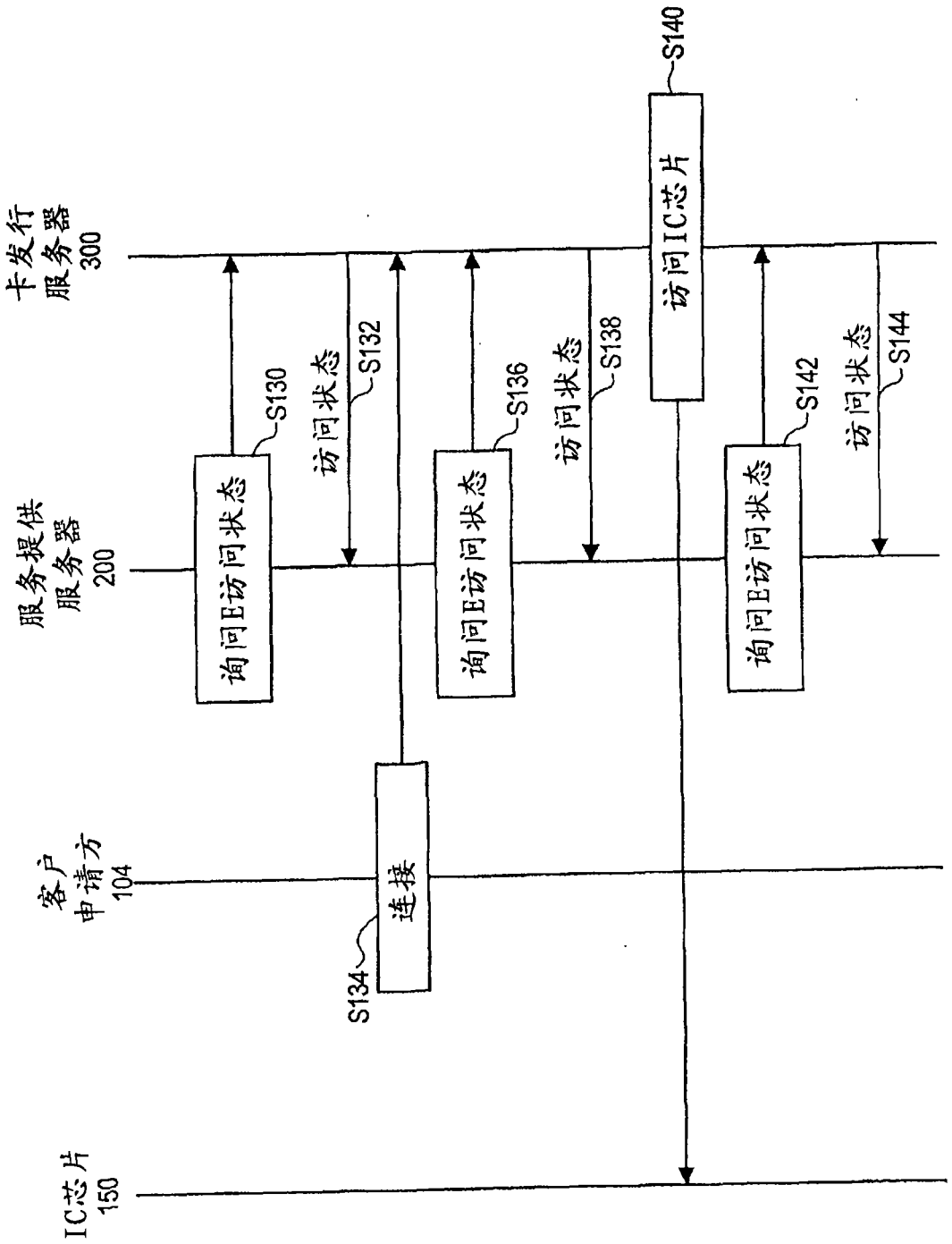

卡发行
服务器
300
服务提供
服务器
200
客户
申请方
104
IC芯片
150
询问B访问状态
S130
访问状态
S132
连接
S134
询问B访问状态
S136
访问状态
S138
访问IC芯片
S140
询问B访问状态
S142
访问状态
S144

图10

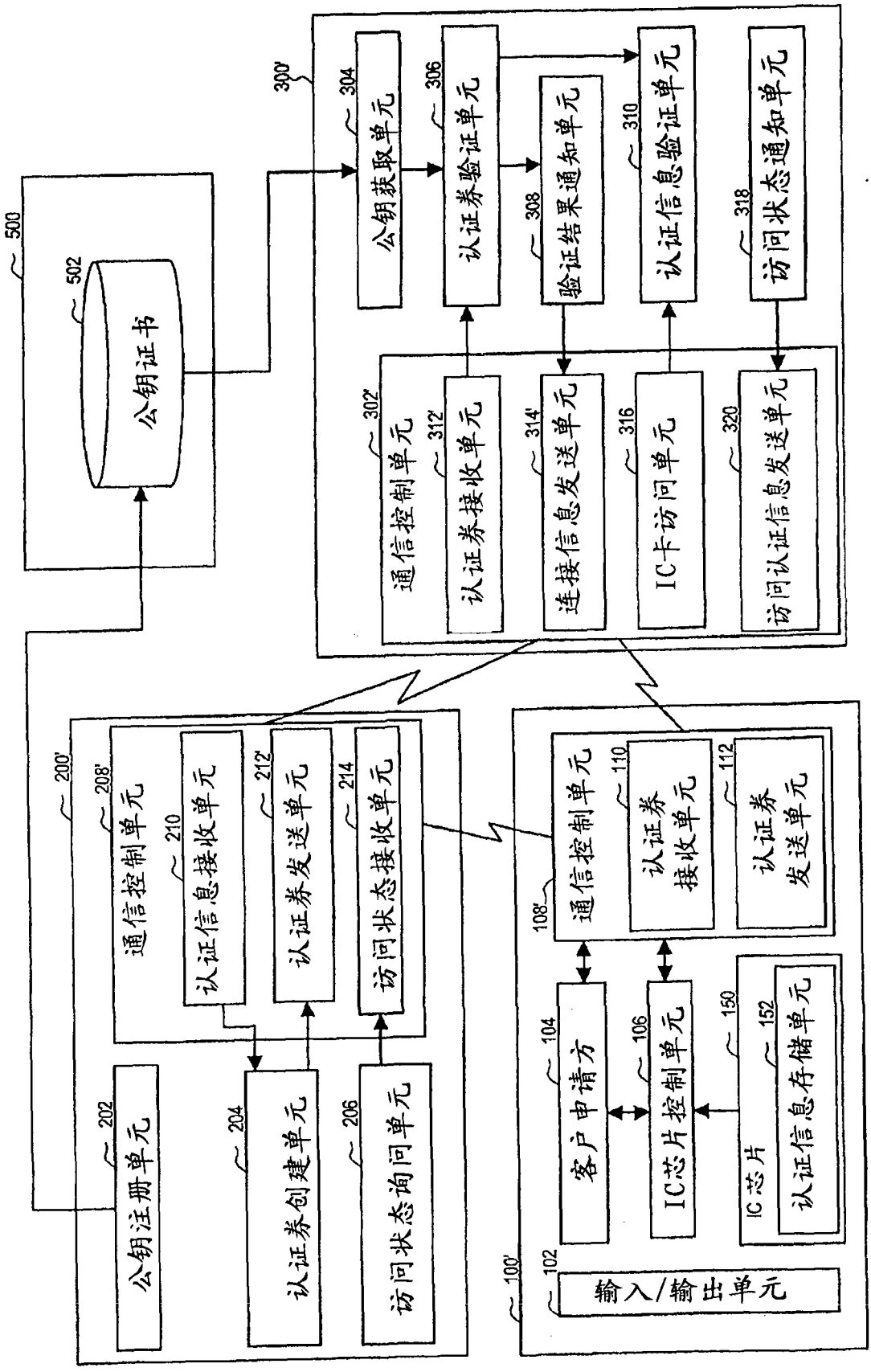

500
502
公钥证书
300'
304
公钥获取单元
306
认证券验证单元
308
验证结果通知单元
310
认证信息验证单元
318
访问状态通知单元
302'
通信控制单元
312'
认证券接收单元
314'
连接信息发送单元
316
IC卡访问单元
320
访问认证信息发送单元
200'
208'
通信控制单元
210
认证信息接收单元
212'
认证券发送单元
214
访问状态接收单元
202
公钥注册单元
204
认证券创建单元
206
访问状态询问单元
100'
102
输入/输出单元
104
客户申请方
106
IC芯片控制单元
150
IC芯片
152
认证信息存储单元
108'
通信控制单元
110
认证券接收单元
112
认证券发送单元

图 11

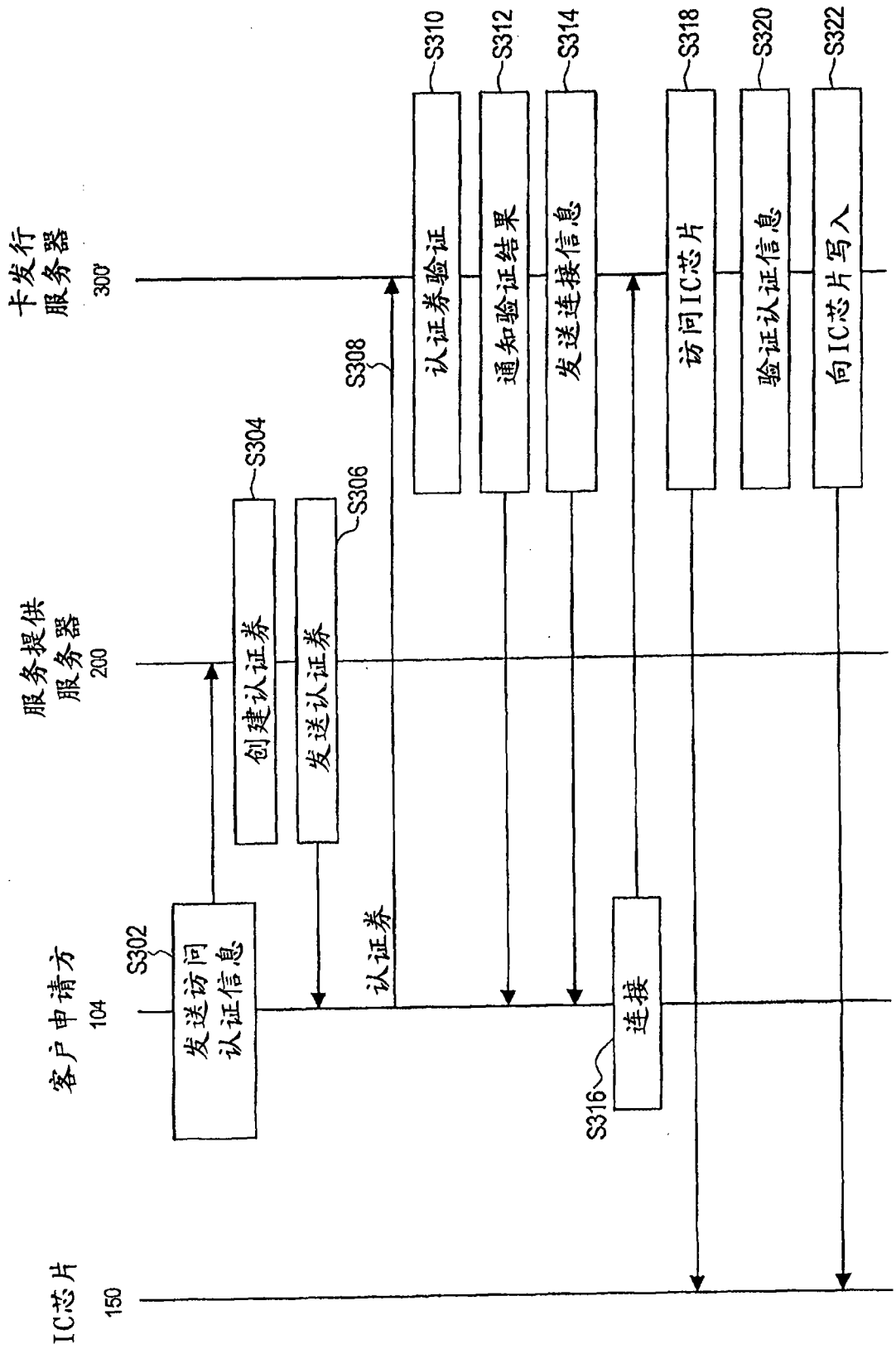

卡发行
服务器
300
服务提供
服务器
200
客户申请方
104
IC芯片
150
S302
发送访问
认证信息
S304
创建认证券
S306
发送认证券
S308
认证券
S310
认证券验证
S312
通知验证结果
S314
发送连接信息
S316
连接
S318
访问IC芯片
S320
验证认证信息
S322
向IC芯片写入

图12

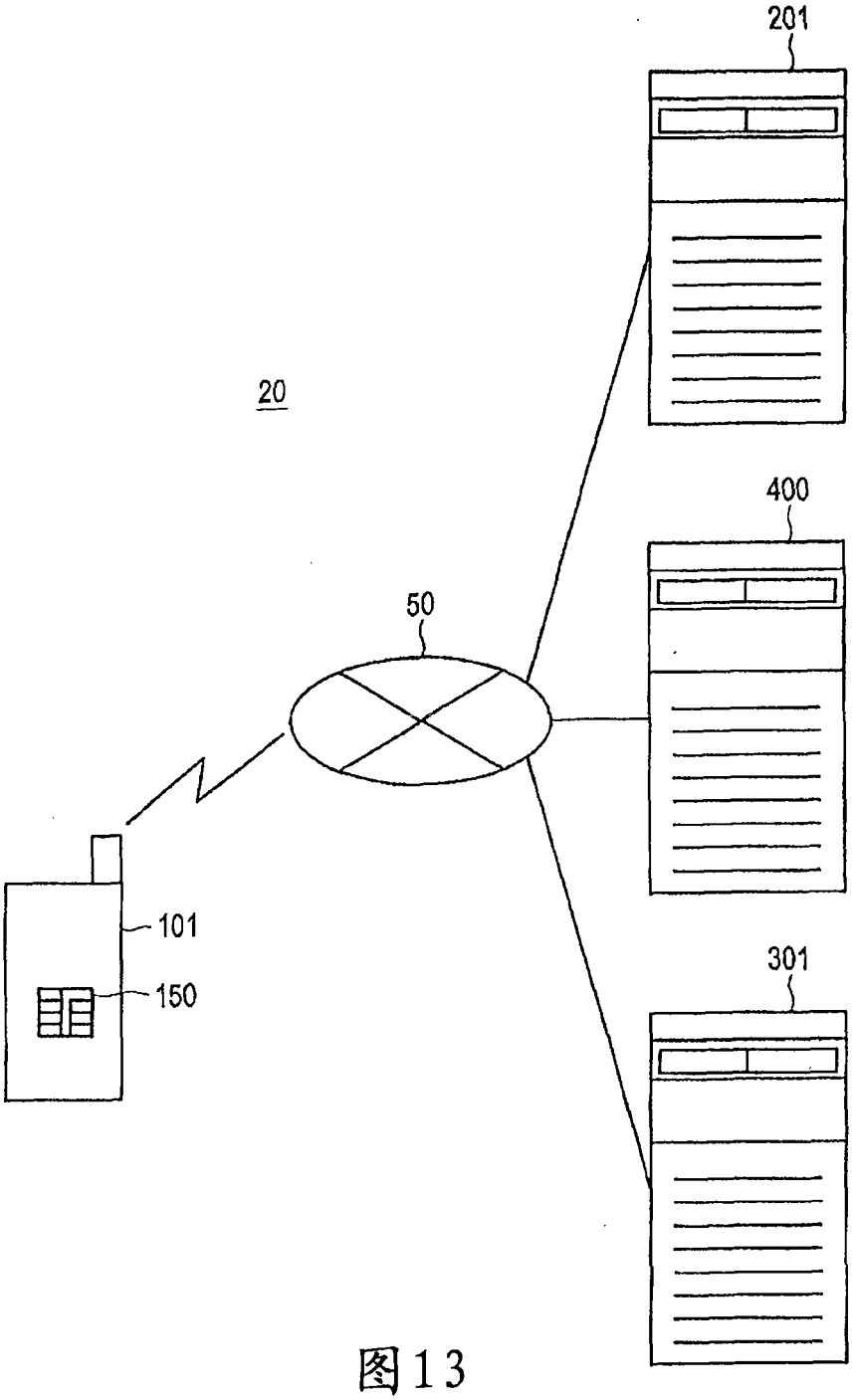


图13

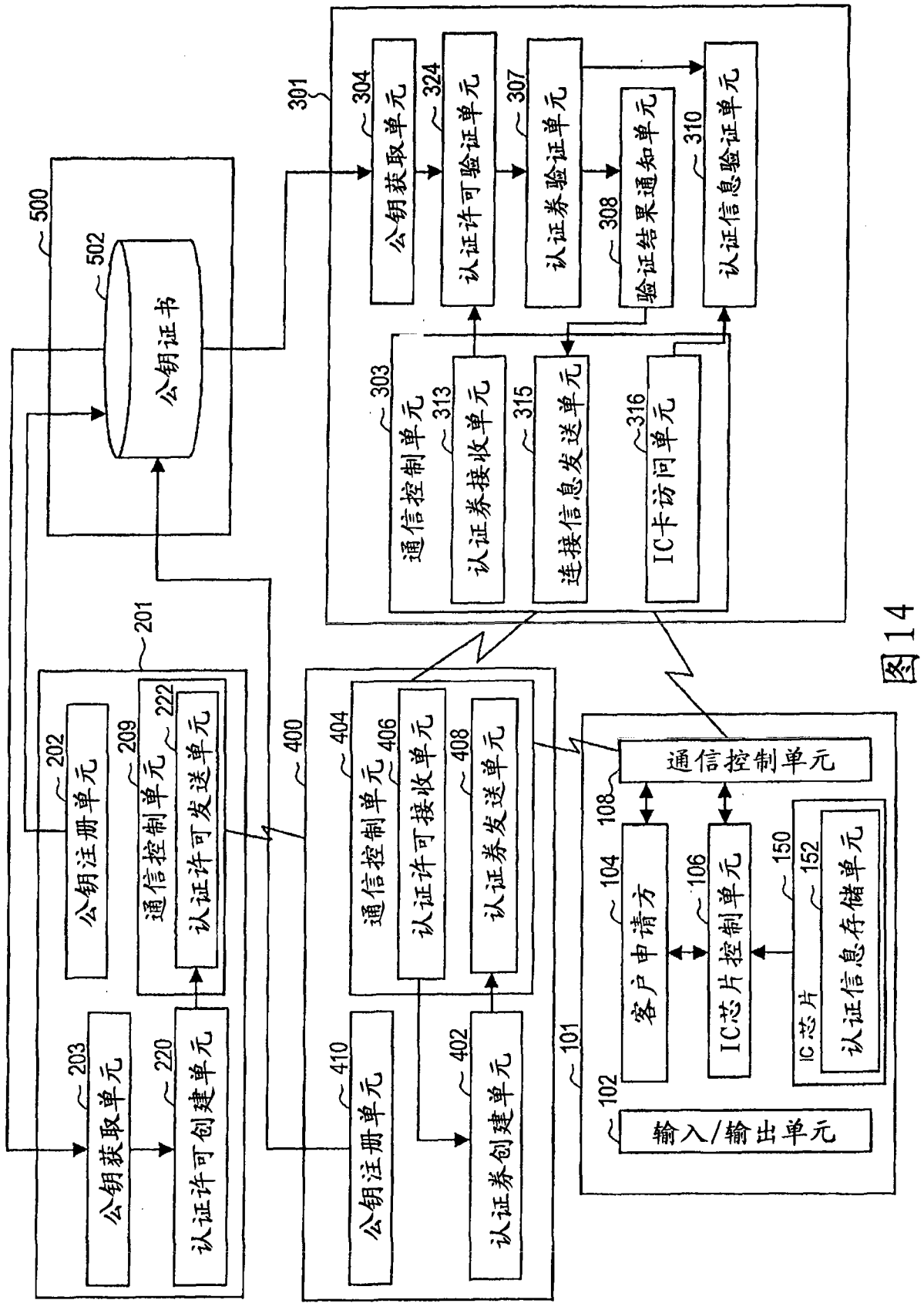

500
502
公钥证书
301
304
公钥获取单元
324
认证许可验证单元
307
认证券验证单元
308
验证结果通知单元
310
认证信息验证单元
303
通信控制单元
313
认证券接收单元
315
连接信息发送单元
316
IC卡访问单元
201
202
公钥注册单元
209
通信控制单元
222
认证许可发送单元
203
公钥获取单元
220
认证许可创建单元
400
404
通信控制单元
406
认证许可接收单元
408
认证券发送单元
410
公钥注册单元
402
认证券创建单元
101
108
通信控制单元
104
客户申请方
106
IC芯片控制单元
150
IC芯片
152
认证信息存储单元
102
输入/输出单元

图14

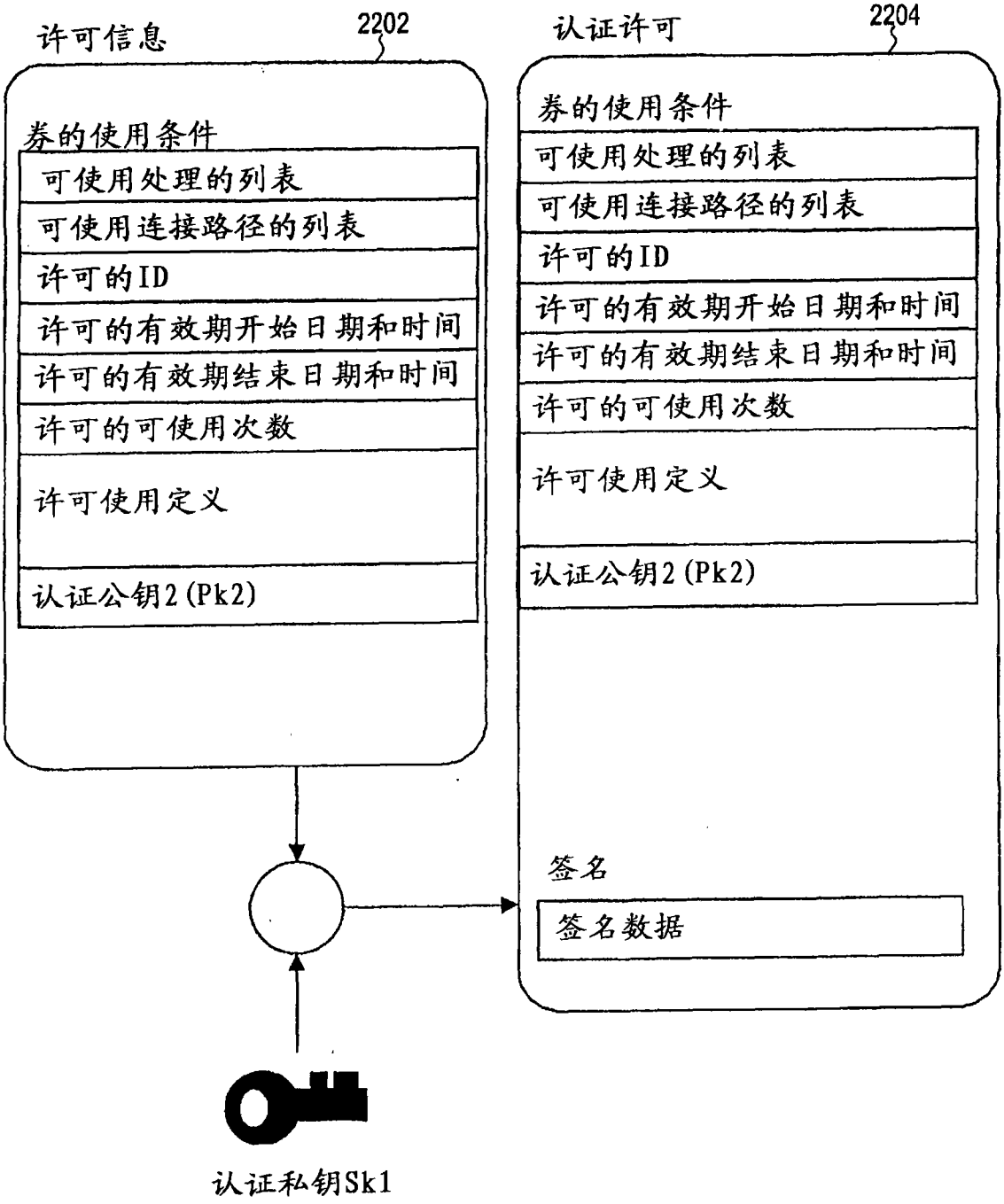

许可信息
2202
券的使用条件
可使用处理的列表
可使用连接路径的列表
许可的ID
许可的有效期开始日期和时间
许可的有效期结束日期和时间
许可的可使用次数
许可使用定义
认证公钥2(Pk2)
认证许可
2204
券的使用条件
可使用处理的列表
可使用连接路径的列表
许可的ID
许可的有效期开始日期和时间
许可的有效期结束日期和时间
许可的可使用次数
许可使用定义
认证公钥2(Pk2)
签名
签名数据
认证私钥Sk1

图15

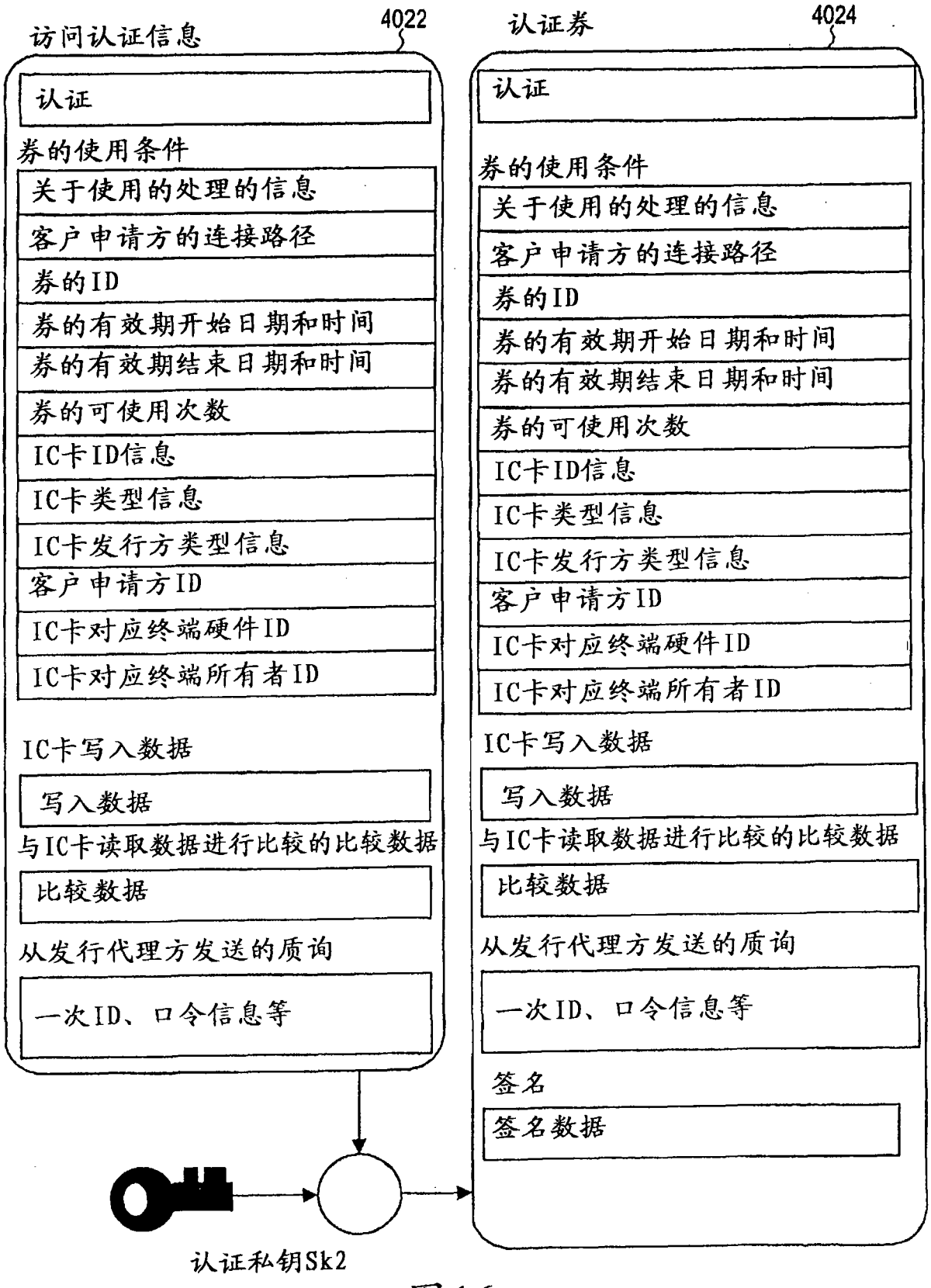

访问认证信息
4022
认证
券的使用条件
关于使用的处理的信息
客户申请方的连接路径
券的ID
券的有效期开始日期和时间
券的有效期结束日期和时间
券的可使用次数
IC卡ID信息
IC卡类型信息
IC卡发行方类型信息
客户申请方ID
IC卡对应终端硬件ID
IC卡对应终端所有者ID
IC卡写入数据
写入数据
与IC卡读取数据进行比较的比较数据
比较数据
从发行代理方发送的质询
一次ID、口令信息等
认证券
4024
认证
券的使用条件
关于使用的处理的信息
客户申请方的连接路径
券的ID
券的有效期开始日期和时间
券的有效期结束日期和时间
券的可使用次数
IC卡ID信息
IC卡类型信息
IC卡发行方类型信息
客户申请方ID
IC卡对应终端硬件ID
IC卡对应终端所有者ID
IC卡写入数据
写入数据
与IC卡读取数据进行比较的比较数据
比较数据
从发行代理方发送的质询
一次ID、口令信息等
签名
签名数据
认证私钥Sk2

图16

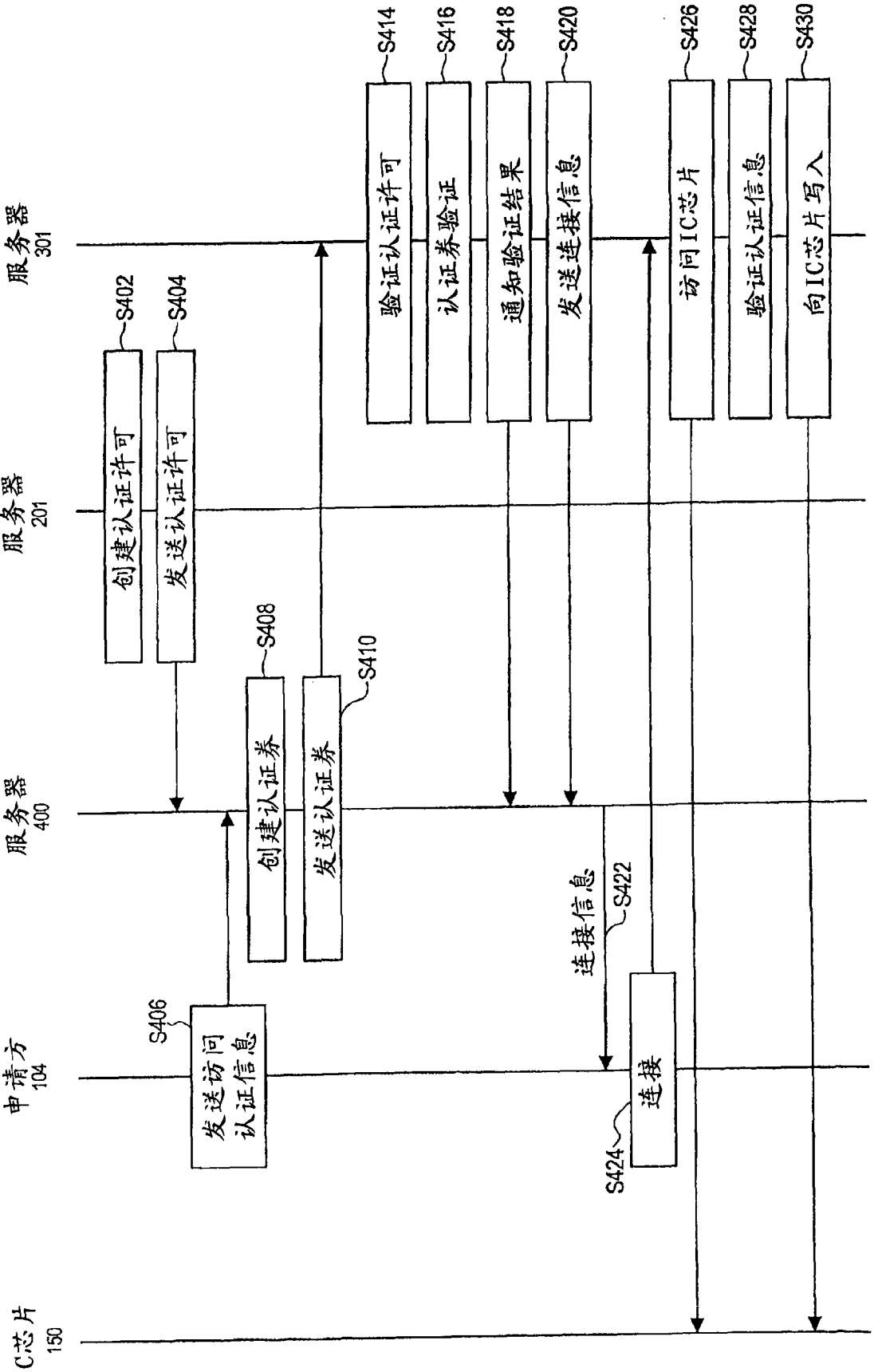

卡发行服务器 301
卡发行服务器 201
服务提供服务器 400
客户申请方 104
IC芯片 150
S402
创建认证许可
S404
发送认证许可
S406
发送访问认证信息
S408
创建认证券
S410
发送认证券
S414
验证认证许可
S416
认证券验证
S418
通知验证结果
S420
发送连接信息
连接信息
S422
S424
连接
S426
访问IC芯片
S428
验证认证信息
S430
向IC芯片写入

图17