[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06K 17/00 (2006.01)
G06K 19/00 (2006.01)
H04L 9/10 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480043663.6

[45] 授权公告日 2008 年 12 月 31 日

[11] 授权公告号 CN 100447764C

[22] 申请日 2004.8.20
[21] 申请号 200480043663.6
[86] 国际申请 PCT/JP2004/011964 2004.8.20
[87] 国际公布 WO2006/018890 日 2006.2.23
[85] 进入国家阶段日期 2007.1.23
[73] 专利权人 三菱电机株式会社
地址 日本东京
[72] 发明人 米田健
[56] 参考文献
CN1316087A 2001.10.3
JP9 - 282393A 1997.10.31
JP2003 - 108952A 2003.4.11
WO2004/055680A1 2004.7.1
CN1472699A 2004.2.4
JP2004 - 38270A 2004.2.5
JP11 - 203439A 1999.7.30
审查员 张 文
[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 王以平

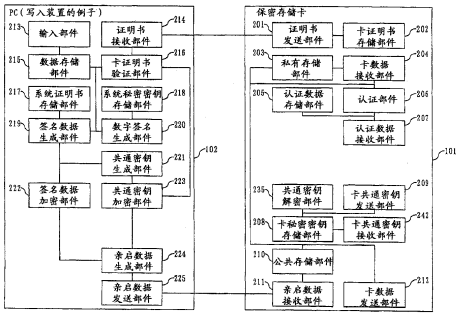
权利要求书 12 页 说明书 25 页 附图 10 页

[54] 发明名称

存储卡、数据交换系统和数据交换方法

[57] 摘要

本发明的存储卡即使不输入 PIN 也能够将只有 IC 卡的拥有者能够读取的信息写入到 IC 卡中，并且实现写入的信息的作成者的认证和篡改的防止，由此保证只有 IC 卡的拥有者能够读出写入到 IC 卡中的数据，能够确定写入的数据的作者，不篡改写入的数据。 保密存储卡(101)包括：存储秘密密钥的卡秘密密钥存储部件(208)；存储与该秘密密钥成对的公开密钥的证明书的卡证明书存储部件(202)；将该证明书发送到 PC(102)的证明书发送部件(201)；只在输入了正确的 PIN 的情况下能够从外部读写的私有存储部件(203)；不进行 PIN 对照也能够从外部读写的公共存储部件(210)；从 PC(102)接收亲启数据的亲启数据接收部件(211)等。



1. 一种存储卡，从写入装置接收数据，存储接收到的数据，将存储的数据发送到读取装置，其特征在于包括：

从所述写入装置接收由所述写入装置对数据进行加密而生成的亲启数据的亲启数据接收部件；

存储由所述亲启数据接收部件接收到的亲启数据的公共存储部件；

接收由所述读取装置发送的认证数据的认证数据接收部件；

存储正规的认证数据的认证数据存储部件；

将由所述认证数据接收部件接收到的认证数据与存储在所述认证数据存储部件中的正规的认证数据进行对照而进行认证的认证部件；

在所述认证部件进行的认证成功了的情况下，存储对存储在所述公共存储部件中的亲启数据进行解密而得到的数据的私有存储部件；

在所述认证部件进行的认证成功了的情况下，将存储在所述私有存储部件中的数据发送到所述读取装置的卡数据发送部件。

2. 根据权利要求 1 所述的存储卡，其特征在于：

所述卡数据发送部件将存储在所述公共存储部件中的亲启数据发送到所述读取装置，

所述存储卡还具备：从所述读取装置接收由所述读取装置对由所述卡数据发送部件发送的亲启数据进行解密而取得的数据的卡数据接收部件，

所述私有存储部件在所述认证部件进行的认证成功了的情况下，存储由所述卡数据接收部件接收到的数据。

3. 根据权利要求 2 所述的存储卡，其特征在于还包括：

存储包含第一公开密钥的证明书的卡证明书存储部件；

将存储在所述卡证明书存储部件中的证明书发送到所述写入装置的证明书发送部件；

存储与所述第一公开密钥成对的第一秘密密钥的卡秘密密钥存储

部件；

接收所述读取装置发送的加密了的共通密钥的卡共通密钥接收部件；

使用存储在所述卡秘密密钥存储部件中的第一秘密密钥对所述卡共通密钥接收部件接收到的共通密钥进行解密的共通密钥解密部件；

将所述共通密钥解密部件解密了的共通密钥发送到所述读取装置的卡共通密钥发送部件。

4. 根据权利要求 3 所述的存储卡，其特征在于：

作为正规的认证数据，所述认证数据存储部件存储密码号即 PIN。

5. 根据权利要求 1 所述的存储卡，其特征在于还包括：

取得对存储在所述公共存储部件中的亲启数据进行解密而得到的数据的数据取得部件，其中

在所述认证部件进行的认证成功了的情况下，所述私有存储部件存储所述数据取得部件取得的数据。

6. 根据权利要求 5 所述的存储卡，其特征在于还包括：

存储包含第一公开密钥的证明书的卡证明书存储部件；

将存储在所述卡证明书存储部件中的证明书发送到所述写入装置的证明书发送部件；

存储与所述第一公开密钥成对的第一秘密密钥的卡秘密密钥存储部件；

从存储在所述公共存储部件中的亲启数据取得加密了的签名数据的签名数据取得部件；

从存储在所述公共存储部件中的亲启数据取得加密了的共通密钥的共通密钥取得部件；

使用存储在所述卡秘密密钥存储部件中的第一秘密密钥对所述共通密钥取得部件取得的共通密钥进行解密的共通密钥解密部件；

使用所述共通密钥解密部件解密了的共通密钥对所述签名数据取得部件取得的签名数据进行解密的签名数据解密部件；

从所述签名数据解密部件解密了的签名数据取得数字签名的数字签名取得部件；

从所述签名数据解密部件解密了的签名数据取得包含第二公开密钥的证明书的证明书取得部件；

对所述证明书取得部件取得的证明书进行验证，取得包含在该证明书中的第二公开密钥的系统证明书验证部件；

使用所述数据取得部件取得的数据和所述系统证明书验证部件取得的第二公开密钥，对所述数字签名取得部件取得的数字签名进行验证的数字签名验证部件，其中

所述数据取得部件从所述签名数据解密部件解密了的签名数据取得数据。

7. 根据权利要求 6 所述的存储卡，其特征在于还包括：

从发行证明书的认证局即 CA 取得证明书的认证局通信部件，其中

所述系统证明书验证部件根据所述认证局通信部件取得的证明书，对所述证明书取得部件取得的证明书进行验证。

8. 根据权利要求 7 所述的存储卡，其特征在于：

作为正规的认证数据，所述认证数据存储部件存储密码号即 PIN。

9. 一种数据交换系统，具备：写入数据的写入装置；读取数据的读取装置；从所述写入装置接收数据，存储接收到的数据，将存储的数据发送到所述读取装置的存储卡，该数据交换系统的特征在于：

所述存储卡是权利要求 2 记载的存储卡，

所述写入装置具备：

输入数据的输入部件；

存储所述输入部件输入的数据的数据存储部件；

对存储在所述数据存储部件中的数据进行加密，生成亲启数据的亲启数据生成部件；

将所述亲启数据生成部件生成的亲启数据发送到所述亲启数据接

收部件的亲启数据发送部件，

所述读取装置具备：

接收所述卡数据发送部件发送的亲启数据的读取装置数据接收部件；

取得对所述读取装置数据接收部件接收到的亲启数据进行解密而得到的数据的数据取得部件；

输出所述数据取得部件取得的数据的输出部件；

将所述数据取得部件取得的数据发送到所述卡数据接收部件的读取装置数据发送部件；

输入认证数据的操作部件；

将所述操作部件输入的认证数据发送到所述认证数据接收部件的认证数据发送部件。

10. 一种数据交换系统，具备写入数据的写入装置；读取数据的读取装置；从所述写入装置接收数据，存储接收到的数据，将存储的数据发送到所述读取装置的存储卡，该数据交换系统的特征在于包括：

所述存储卡是权利要求 3 记载的存储卡，

所述写入装置具备：

输入数据的输入部件；

存储所述输入部件输入的数据的数据存储部件；

接收所述证明书发送部件发送的证明书的证明书接收部件；

对所述证明书接收部件接收到的证明书进行验证，取得包含在该证明书中的第一公开密钥的卡证明书验证部件；

存储第二秘密密钥的系统秘密密钥存储部件；

使用存储在所述数据存储部件中的数据和存储在所述系统秘密密钥存储部件中的第二秘密密钥，生成数字签名的数字签名生成部件；

存储包含与所述第二秘密密钥成对的第二公开密钥的证明书的系统证明书存储部件；

使用存储在所述数据存储部件中的数据、所述数字签名生成部件

生成的数字签名、存储在所述系统证明书存储部件中的证明书，生成签名数据的签名数据生成部件；

生成共通密钥的共通密钥生成部件；

使用所述共通密钥生成部件生成的共通密钥，对所述签名数据生成的签名数据进行加密的签名数据加密部件；

使用所述卡证明书验证部件取得的第一公开密钥，对所述共通密钥生成部件生成的共通密钥进行加密的共通密钥加密部件；

使用所述签名数据加密部件加密了的签名数据和所述共通密钥加密部件加密了的共通密钥，生成亲启数据的亲启数据生成部件；

将所述亲启数据生成部件生成的亲启数据发送到所述亲启数据接收部件的亲启数据发送部件，

所述读取装置具备：

接收所述卡数据发送部件发送的亲启数据的读取装置数据接收部件；

从所述读取装置数据接收部件接收到的亲启数据取得加密了的签名数据的签名数据取得部件；

从所述读取装置数据接收部件接收到的亲启数据取得加密了的共通密钥的共通密钥取得部件；

将所述共通密钥取得部件取得的加密了的共通密钥发送到所述卡共通密钥接收部件的读取装置共通密钥发送部件；

接收所述卡共通密钥发送部件发送的解密了的共通密钥的读取装置共通密钥接收部件；

使用所述读取装置共通密钥接收部件接收到的共通密钥，对所述签名数据取得部件取得的签名数据进行解密的签名数据解密部件；

从所述签名数据解密部件解密了的签名数据取得数据的数据取得部件；

从所述签名数据解密部件解密了的签名数据取得数字签名的数字签名取得部件；

从所述签名数据解密部件解密了的签名数据取得证明书的证明书

取得部件；

对所述证明书取得部件取得的证明书进行验证，取得包含在该证明书中的第二公开密钥的系统证明书验证部件；

使用所述数据取得部件取得的数据和所述系统证明书验证部件取得的第二公开密钥，对所述数字签名取得部件取得的数字签名进行验证的数字签名验证部件；

根据所述数字签名验证部件进行了的验证的结果，输出所述数据取得部件取得的数据的输出部件；

将所述数据取得部件取得的数据发送到所述卡数据接收部件的读取装置数据发送部件；

输入认证数据的操作部件；

将所述操作部件输入的认证数据发送到认证数据接收部件的认证数据发送部件。

11. 一种数据交换系统，具备：写入数据的写入装置；读取数据的读取装置；从所述写入装置接收数据，存储接收到的数据，将存储的数据发送到所述读取装置的存储卡，该数据交换系统的特征在于包括：

所述存储卡是权利要求 5 记载的存储卡，

所述写入装置具备：

输入数据的输入部件；

存储所述输入部件输入的数据的数据存储部件；

对存储在所述数据存储部件中的数据进行加密，生成亲启数据的亲启数据生成部件；

将所述亲启数据生成部件生成的亲启数据发送到所述亲启数据接收部件的亲启数据发送部件，

所述读取装置具备：

输入认证数据的操作部件；

将所述操作部件输入的认证数据发送到所述认证数据接收部件的认证数据发送部件；

接收所述卡数据发送部件发送的数据的读取装置数据接收部件；

输出所述读取装置数据接收部件接收到的数据的输出部件。

12. 一种数据交换系统，具备：写入数据的写入装置；读取数据的读取装置；从所述写入装置接收数据，存储接收到的数据，将存储的数据发送到所述读取装置的存储卡，该数据交换系统的特征在于包括：

所述存储卡是权利要求 6 记载的存储卡，

所述写入装置具备：

输入数据的输入部件；

存储所述输入部件输入的数据的数据存储部件；

接收所述证明书发送部件发送的证明书的证明书接收部件；

对所述证明书接收部件接收到的证明书进行验证，取得包含在该证明书中的第一公开密钥的卡证明书验证部件；

存储第二秘密密钥的系统秘密密钥存储部件；

使用存储在所述数据存储部件中的数据和存储在所述系统秘密密钥存储部件中的第二秘密密钥，生成数字签名的数字签名生成部件；

存储包含与所述第二秘密密钥成对的第二公开密钥的证明书的系统证明书存储部件；

使用存储在所述数据存储部件中的数据、所述数字签名生成部件生成的数字签名、存储在所述系统证明书存储部件中的证明书，生成签名数据的签名数据生成部件；

生成共通密钥的共通密钥生成部件；

使用所述共通密钥生成部件生成的共通密钥，对所述签名数据生成部件生成的签名数据进行加密的签名数据加密部件；

使用所述卡证明书验证部件取得的第一公开密钥，对所述共通密钥生成部件生成的共通密钥进行加密的共通密钥加密部件；

使用所述签名数据加密部件加密了的签名数据和所述共通密钥加密部件加密了的共通密钥，生成亲启数据的亲启数据生成部件；

将所述亲启数据生成部件生成的亲启数据发送到所述亲启数据接

收部件的亲启数据发送部件，

所述读取装置具备：

输入认证数据的操作部件；

将所述操作部件输入的认证数据发送到所述认证数据接收部件的认证数据发送部件；

接收所述卡数据发送部件发送的数据的读取装置数据接收部件；

输出所述读取装置数据接收部件接收到的数据的输出部件。

13. 一种数据交换方法，其中存储卡从写入装置接收数据，存储接收到的数据，将存储的数据发送到读取装置，该数据交换方法的特征在于：

在所述写入装置中，

输入数据，

并存储输入的数据，

对存储的数据进行加密而生成亲启数据，

将生成的亲启数据发送到所述存储卡，

在所述存储卡中，

从所述写入装置接收所述写入装置对数据进行加密而生成的亲启数据，

存储接收到的亲启数据到公共存储部件中，

将存储的亲启数据发送到所述读取装置，

在所述读取装置中，

接收所述存储卡发送的亲启数据，

取得对接收到的亲启数据进行解密而得到的数据，

输出取得的数据，

将取得的数据发送到所述存储卡，

在所述存储卡中，

从所述读取装置接收所述读取装置对发送的亲启数据进行解密而取得的数据，

在所述读取装置中，

输入认证数据，

将输入的认证数据发送到所述存储卡，

在所述存储卡中，

接收所述读取装置发送的认证数据，

存储正规的认证数据，

将接收到的认证数据与存储的正规的认证数据进行对照，进行认证，

在认证成功了的情况下，存储从所述读取装置接收到的解密而得到的数据到私有存储部件，

在认证成功了的情况下，将存储的数据发送到所述读取装置。

14. 根据权利要求 13 所述的数据交换方法，其特征在于还包括：

在所述存储卡中，

存储包含第一公开密钥的证明书，

将存储的证明书发送到所述写入装置，

存储与所述第一公开密钥成对的第一秘密密钥，

在所述写入装置中，

接收所述存储卡发送的证明书，

对接收到的证明书进行验证，取得包含在该证明书中的第一公开密钥，

存储第二秘密密钥，

使用存储的数据和第二秘密密钥，生成数字签名，

存储包含与所述第二秘密密钥成对的第二公开密钥的证明书，

使用存储的数据、生成的数字签名、包含所存储的第二公开密钥的证明书，生成签名数据，

生成共通密钥，

使用生成的共通密钥，对生成的签名数据进行加密，

使用取得的第一公开密钥，对生成的共通密钥进行加密，

使用加密了的签名数据和共通密钥，生成亲启数据，

在所述读取装置中，

从接收到的亲启数据取得加密了的签名数据，

从接收到的亲启数据取得加密了的共通密钥，

将取得的加密了的共通密钥发送到所述存储卡，

在所述存储卡中，

接收所述读取装置发送的加密了的共通密钥，

使用存储的第一秘密密钥，对接收到的共通密钥进行解密，

将解密了的共通密钥发送到所述读取装置，

在所述读取装置中，

接收所述存储卡发送的解密了的共通密钥，

使用接收到的共通密钥，对取得的签名数据进行解密，

从解密了的签名数据取得数据，

从解密了的签名数据取得数字签名，

从解密了的签名数据取得证明书，

对取得的证明书进行验证，取得包含在该证明书中的第二公开密钥，

使用取得的数据和第二公开密钥，对取得的数字签名进行验证，

根据验证的结果，输出取得的数据。

15. 一种数据交换方法，其中存储卡从写入装置接收数据，存储接收到的数据，将存储的数据发送到读取装置，该数据交换方法的特征在于：

在所述写入装置中，

输入数据，

存储输入的数据，

对存储的数据进行加密而生成亲启数据，

将生成的亲启数据发送到所述存储卡，

在所述存储卡中，

从所述写入装置接收所述写入装置对数据进行加密而生成的亲启数据，

存储接收到的亲启数据到公有存储部件，

取得对存储的亲启数据进行解密而得到的数据并验证签名数据，

在验证成功的情况下，存储所取得的数据到私有存储部件中，

在所述读取装置中，

输入认证数据，

将输入的认证数据发送到所述存储卡，

在所述存储卡中，

接收所述读取装置发送的认证数据，

存储正规的认证数据，

将接收到的认证数据与存储的正规的认证数据进行对照，进行认证，

在认证成功了的情况下，将私有存储部件中存储的数据发送到所述读取装置，

在所述读取装置中，

接收所述存储卡发送的数据，

输出接收到的数据。

16. 根据权利要求 15 所述的数据交换方法，其特征在于还包括：

在所述存储卡中，

存储包含第一公开密钥的证明书，

将存储的证明书发送到所述写入装置，

存储与所述第一公开密钥成对的第一秘密密钥，

从解密了的签名数据取得数据，

在所述写入装置中，

输入数据，

存储所输入的数据，

接收所述存储卡发送的证明书，

对接收到的证明书进行验证，取得包含在该证明书中的第一公开密钥，

存储第二秘密密钥，

使用存储的数据和第二秘密密钥，生成数字签名，

存储包含与所述第二秘密密钥成对的第二公开密钥的证明书，

使用存储的数据、生成的数字签名、包含存储的第二公开密钥的证明书，生成签名数据，

生成共通密钥，

使用生成的共通密钥，对生成的签名数据进行加密，

使用取得的第一公开密钥，对生成的共通密钥进行加密，

使用加密了的签名数据和共通密钥，生成亲启数据，

将生成的亲启数据发送到所述存储卡，

在所述读取装置中，

输入认证数据，

将输入的认证数据发送到所述存储卡，

在所述存储卡中，

从存储的亲启数据取得加密了的签名数据，

从存储的亲启数据取得加密了的共通密钥，

使用存储的第一秘密密钥，对取得的共通密钥进行解密，

使用解密了的共通密钥，对取得的签名数据进行解密，

从解密了的签名数据取得数字签名，

从解密了的签名数据取得包含第二公开密钥的证明书，

对取得的证明书进行验证，取得包含在该证明书中的第二公开密钥，

使用取得的数据和第二公开密钥，对取得的数字签名进行验证，

在所述读取装置中，

接收所述存储卡发送的数据，

输出接收到的数据。

存储卡、数据交换系统和数据交换方法

技术领域

本发明涉及用于进行安全的数据交换的存储卡、数据交换系统和数据交换方法。

背景技术

对于身份证明书、会员卷、诊断卷，可以利用 IC 卡。IC 可以具有能够读出和写入的区域。某机构向 IC 卡中写入信息，IC 卡拥有者或其他机构从 IC 读出该信息，从而能够收发或共有信息。在专利文献 1 中，提示了如果某医疗机构向患者的 IC 卡写入医疗信息，则其他医疗机构能够参考该医疗信息的方法。

专利文献 1：特开 2000－285189 公报

为了验证 IC 卡的使用者是该 IC 卡的正当拥有者，在使用 IC 卡的系统中，一般如现金自动出纳机（ATM，Automated Teller Machine）那样，使得输入只有 IC 卡的拥有者知道的 PIN（Personal Identification Number）。但是，在该情况下，插入 IC 卡的系统必须是不能不正当地存储和利用使用者输入的 PIN 信息的可以信任的系统。因此，在使用必须输入 PIN 的 IC 卡的系统中，一般在 IC 卡和插入 IC 卡的系统之间进行相互认证。为了进行相互认证，必须安全地共有共通密钥密码方式的密钥信息，或安全地持有公开密钥密码方式的公开密钥、秘密密钥的对。

另外，在使用必须输入 PIN 的 IC 卡的系统中，在将 IC 卡交给某机构，在该机构中对 IC 卡进行需要 PIN 的处理的情况下，只有机构内的操作者是不能够进行处理的，还必须由 IC 卡的拥有者输入 PIN。其结果是有以下的限制，即 IC 卡拥有者为了输入 PIN，必须等在机构的系统旁边。

发明内容

本发明的目的在于：实现即使不进行 PIN 的输入，也能够向 IC 卡写入只有 IC 卡的拥有者能够读出的信息，并且对写入的信息的作成者进行认证，防止篡改，由此能够保证只有 IC 卡的拥有者能够读出写入到 IC 卡中的数据，能够确定写入了的数据的作者，写入的数据不被篡改。

本发明的存储卡的特征在于包括：

从上述写入装置接收由上述写入装置对数据进行加密而生成的亲启数据的亲启数据接收部件；

存储由上述亲启数据接收部件接收到的亲启数据的公共（public）存储部件；

接收由上述读取装置发送的认证数据的认证数据接收部件；

存储正规的认证数据的认证数据存储部件；

将由上述认证数据接收部件接收到的认证数据与存储在上述认证数据存储部件中的正规的认证数据进行对照而进行认证的认证部件；

在上述认证部件进行的认证成功了的情况下，存储对存储在上述公共存储部件中的亲启数据进行解密而得到的数据的私有（private）存储部件；

在上述认证部件进行的认证成功了的情况下，将存储在上述私有存储部件中的数据发送到上述读取装置的卡数据发送部件。

另外，其特征在于：

上述卡数据发送部件将存储在上述公共存储部件中的亲启数据发送到上述读取装置，

上述存储卡还具备：从上述读取装置接收由上述读取装置对由上述卡数据发送部件发送的亲启数据进行解密而取得的数据的卡数据接收部件，

上述私有存储部件在上述认证部件进行的认证成功了的情况下，存储由上述卡数据接收部件接收到的数据。

另外，上述存储卡的特征在于还包括：

存储包含第一公开密钥的证明书的卡证明书存储部件；

将存储在上述卡证明书存储部件中的证明书发送到上述写入装置的证明书发送部件；

存储与上述第一公开密钥成对的第一秘密密钥的卡秘密密钥存储部件；

接收上述读取装置发送的加密了的共通密钥的卡共通密钥接收部件；

使用存储在上述卡秘密密钥存储部件中的第一秘密密钥对上述卡共通密钥接收部件接收到的共通密钥进行解密的共通密钥解密部件；

将上述共通密钥解密部件解密了的共通密钥发送到上述读取装置的卡共通密钥发送部件。

另外，其特征在于：

作为正规的认证数据，上述认证数据存储部件存储密码号（PIN，Personal Identification Number）。

另外，上述存储卡的特征在于还包括：

取得对存储在上述公共存储部件中的亲启数据进行解密而得到的数据的数据取得部件，其中

上述私有存储部件存储上述数据取得部件取得的数据。

另外，上述存储卡的特征在于还包括：

存储包含第一公开密钥的证明书的卡证明书存储部件；

将存储在上述卡证明书存储部件中的证明书发送到上述写入装置的证明书发送部件；

存储与上述第一公开密钥成对的第一秘密密钥的卡秘密密钥存储部件；

从存储在上述公共存储部件中的亲启数据取得加密了的签名数据的签名数据取得部件；

从存储在上述公共存储部件中的亲启数据取得加密了的共通密钥的共通密钥取得部件；

使用存储在上述卡秘密密钥存储部件中的第一秘密密钥对上述共通密钥取得部件取得的共通密钥进行解密的共通密钥解密部件；

使用上述共通密钥解密部件解密了的共通密钥对上述签名数据取得部件取得的签名数据进行解密的签名数据解密部件；

从上述签名数据解密部件解密了的签名数据取得数字签名的数字签名取得部件；

从上述签名数据解密部件解密了的签名数据取得包含第二公开密钥的证明书的证明书取得部件；

对上述证明书取得部件取得的证明书进行验证，取得包含在该证明书中的第二公开密钥的系统证明书验证部件；

使用上述数据取得部件取得的数据和上述系统证明书验证部件取得的第二公开密钥，对上述数字签名取得部件取得的数字签名进行验证的数字签名验证部件，其中

上述数据取得部件从上述签名数据解密部件解密了的签名数据取得数据。

另外，上述存储卡的特征在于还包括：

从发行证明书的认证局（CA，Certificate Authority）取得证明书的认证局通信部件，其中

上述系统证明书验证部件根据上述认证局通信部件取得的证明书，对上述证明书取得部件取得的证明书进行验证。

另外，其特征在于：作为正规的认证数据，上述认证数据存储部件存储密码号（PIN，Personal Identification Number）。

本发明的数据交换系统的特征在于包括：

写入数据的写入装置；读取数据的读取装置；从上述写入装置接收数据，存储接收到的数据，将存储的数据发送到上述读取装置的存储卡，

上述存储卡是以上说明的存储卡，

上述写入装置具备：

输入数据的输入部件；

存储上述输入部件输入的数据的数据存储部件;

对存储在上述数据存储部件中的数据进行加密，生成亲启数据的亲启数据生成部件;

将上述亲启数据生成部件生成的亲启数据发送到上述亲启数据接收部件的亲启数据发送部件，

上述读取装置具备:

接收上述卡数据发送部件发送的亲启数据的读取装置数据接收部件;

取得对上述读取装置数据接收部件接收到的亲启数据进行解密而得到的数据的数据取得部件;

输出上述数据取得部件取得的数据的输出部件;

将上述数据取得部件取得的数据发送到上述卡数据接收部件的读取装置数据发送部件;

输入认证数据的操作部件;

将上述操作部件输入的认证数据发送到上述认证数据接收部件的认证数据发送部件。

本发明的数据交换系统的特征在于包括:

写入数据的写入装置；读取数据的读取装置；从上述写入装置接收数据，存储接收到的数据，将存储的数据发送到上述读取装置的存储卡，

上述存储卡是以上说明的存储卡，

上述写入装置具备:

输入数据的输入部件;

存储上述输入部件输入的数据的数据存储部件;

接收上述证明书发送部件发送的证明书的证明书接收部件;

对上述证明书接收部件接收到的证明书进行验证，取得包含在该证明书中的第一公开密钥的卡证明书验证部件;

存储第二秘密密钥的系统秘密密钥存储部件;

使用存储在上述数据存储部件中的数据和存储在上述系统秘密密

钥存储部件中的第二秘密密钥，生成数字签名的数字签名生成部件；

存储包含与上述第二秘密密钥成对的第二公开密钥的证明书的系统证明书存储部件；

使用存储在上述数据存储部件中的数据、上述数字签名生成部件生成的数字签名、存储在上述系统证明书存储部件中的证明书，生成签名数据的签名数据生成部件；

生成共通密钥的共通密钥生成部件；

使用上述共通密钥生成部件生成的共通密钥，对上述签名数据生成的签名数据进行加密的签名数据加密部件；

使用上述卡证明书验证部件取得的第一公开密钥，对上述共通密钥生成部件生成的共通密钥进行加密的共通密钥加密部件；

使用上述签名数据加密部件加密了的签名数据和上述共通密钥加密部件加密了的共通密钥，生成亲启数据的亲启数据生成部件；

将上述亲启数据生成部件生成的亲启数据发送到上述亲启数据接收部件的亲启数据发送部件，

上述读取装置具备：

接收上述卡数据发送部件发送的亲启数据的读取装置数据接收部件；

从上述读取装置数据接收部件接收到的亲启数据取得加密了的签名数据的签名数据取得部件；

从上述读取装置数据接收部件接收到的亲启数据取得加密了的共通密钥的共通密钥取得部件；

将上述共通密钥取得部件取得的加密了的共通密钥发送到上述卡共通密钥接收部件的读取装置共通密钥发送部件；

接收上述卡共通密钥发送部件发送的解密了的共通密钥的读取装置共通密钥接收部件；

使用上述读取装置共通密钥接收部件接收到的共通密钥，对上述签名数据取得部件取得的签名数据进行解密的签名数据解密部件；

从上述签名数据解密部件解密了的签名数据取得数据的数据取得

部件；

从上述签名数据解密部件解密了的签名数据取得数字签名的数字签名取得部件；

从上述签名数据解密部件解密了的签名数据取得证明书的证明书取得部件；

对上述证明书取得部件取得的证明书进行验证，取得包含在该证明书中的第二公开密钥的系统证明书验证部件；

使用上述数据取得部件取得的数据和上述系统证明书验证部件取得的第二公开密钥，对上述数字签名取得部件取得的数字签名进行验证的数字签名验证部件；

根据上述数字签名验证部件进行了的验证的结果，输出上述数据取得部件取得的数据的输出部件；

将上述数据取得部件取得的数据发送到上述卡数据接收部件的读取装置数据发送部件；

输入认证数据的操作部件；

将上述操作部件输入的认证数据发送到认证数据接收部件的认证数据发送部件。

本发明的数据交换系统的特征在于包括：

写入数据的写入装置；读取数据的读取装置；从上述写入装置接收数据，存储接收到的数据，将存储的数据发送到上述读取装置的存储卡，

上述存储卡是以上说明的存储卡，

上述写入装置具备：

输入数据的输入部件；

存储上述输入部件输入的数据的数据存储部件；

对存储在上述数据存储部件中的数据进行加密，生成亲启数据的亲启数据生成部件；

将上述亲启数据生成部件生成的亲启数据发送到上述亲启数据接收部件的亲启数据发送部件，

上述读取装置具备:

输入认证数据的操作部件;

将上述操作部件输入的认证数据发送到上述认证数据接收部件的认证数据发送部件;

接收上述卡数据发送部件发送的数据的读取装置数据接收部件;

输出上述读取装置数据接收部件接收到的数据的输出部件。

本发明的数据交换系统的特征在于包括:

写入数据的写入装置;读取数据的读取装置;从上述写入装置接收数据,存储接收到的数据,将存储的数据发送到上述读取装置的存储卡,

上述存储卡是以上说明的存储卡,

上述写入装置具备:

输入数据的输入部件;

存储上述输入部件输入的数据的数据存储部件;

接收上述证明书发送部件发送的证明书的证明书接收部件;

对上述证明书接收部件接收到的证明书进行验证,取得包含在该证明书中的第一公开密钥的卡证明书验证部件;

存储第二秘密密钥的系统秘密密钥存储部件;

使用存储在上述数据存储部件中的数据和存储在上述系统秘密密钥存储部件中的第二秘密密钥,生成数字签名的数字签名生成部件;

存储包含与上述第二秘密密钥成对的第二公开密钥的证明书的系统证明书存储部件;

使用存储在上述数据存储部件中的数据、上述数字签名生成部件生成的数字签名、存储在上述系统证明书存储部件中的证明书,生成签名数据的签名数据生成部件;

生成共通密钥的共通密钥生成部件;

使用上述共通密钥生成部件生成的共通密钥,对上述签名数据生成的签名数据进行加密的签名数据加密部件;

使用上述卡证明书验证部件取得的第一公开密钥,对上述共通密

钥生成部件生成的共通密钥进行加密的共通密钥加密部件;

使用上述签名数据加密部件加密了的签名数据和上述共通密钥加密部件加密了的共通密钥，生成亲启数据的亲启数据生成部件;

将上述亲启数据生成部件生成的亲启数据发送到上述亲启数据接收部件的亲启数据发送部件，

上述读取装置具备:

输入认证数据的操作部件;

将上述操作部件输入的认证数据发送到上述认证数据接收部件的认证数据发送部件;

接收上述卡数据发送部件发送的数据的读取装置数据接收部件;

输出上述读取装置数据接收部件接收到的数据的输出部件。

在本发明的数据交换方法中，其特征在于:

在上述存储卡中，

从上述写入装置接收上述写入装置对数据进行加密而生成的亲启数据，

存储接收到的亲启数据，

将存储的亲启数据发送到上述读取装置，

从上述读取装置接收上述读取装置对发送的亲启数据进行解密而取得的数据，

接收上述读取装置发送的认证数据，

存储正规的认证数据，

将接收到的认证数据与存储的正规的认证数据进行对照，进行认证，

在认证成功了的情况下，存储从上述读取装置接收到的数据，

在认证成功了的情况下，将存储的数据发送到上述读取装置，

在上述写入装置中，

输入数据，

存储输入的数据，

对存储的数据进行加密而生成亲启数据，

将生成的亲启数据发送到上述存储卡，

在上述读取装置中，

接收上述存储卡发送的亲启数据，

取得对接收到的亲启数据进行解密而得到的数据，

输出取得的数据，

将取得的数据发送到上述存储卡，

输入认证数据，

将输入的认证数据发送到上述存储卡。

另外，其特征在于：

上述存储卡还包括：

存储包含第一公开密钥的证明书，

将存储的证明书发送到上述写入装置，

存储与上述第一公开密钥成对的第一秘密密钥，

接收上述读取装置发送的加密了的共通密钥，

使用存储的第一秘密密钥，对接收到的共通密钥进行解密，

将解密了的共通密钥发送到上述读取装置，

上述写入装置还包括：

接收上述存储卡发送的证明书，

对接收到的证明书进行验证，取得包含在该证明书中的第一公开密钥，

存储第二秘密密钥，

使用存储的数据和第二秘密密钥，生成数字签名，

存储包含与上述第二秘密密钥成对的第二公开密钥的证明书，

使用存储的数据、生成的数字签名、包含所存储的第二公开密钥的证明书，生成签名数据，

生成共通密钥，

使用生成的共通密钥，对生成的签名数据进行加密，

使用取得的第一公开密钥，对生成的共通密钥进行加密的共通密钥加密部件；

使用加密了的签名数据和共通密钥，生成亲启数据，

在上述读取装置中，

从接收到的亲启数据取得加密了的签名数据，

从接收到的亲启数据取得加密了的共通密钥，

将取得的加密了的共通密钥发送到上述存储卡，

接收上述存储卡发送的解密了的共通密钥，

使用接收到的共通密钥，对取得的签名数据进行解密，

从解密了的签名数据取得数据，

从解密了的签名数据取得数字签名，

从解密了的签名数据取得证明书，

对取得的证明书进行验证，取得包含在该证明书中的第二公开密钥，

使用取得的数据和第二公开密钥，对取得的数字签名进行验证，

根据验证的结果，输出取得的数据。

在本发明的数据交换方法中，

在上述存储卡中，

从上述写入装置接收上述写入装置对数据进行加密而生成的亲启数据，

存储接收到的亲启数据，

取得对存储的亲启数据进行解密而得到的数据，

存储所取得的数据，

接收上述读取装置发送的认证数据，

存储正规的认证数据，

将接收到的认证数据与存储的正规的认证数据进行对照，进行认证，

在认证成功了的情况下，将存储的数据发送到上述读取装置，

在上述写入装置中，

输入数据，

存储输入的数据，

对存储的数据进行加密而生成亲启数据，

将生成的亲启数据发送到上述存储卡，

在上述读取装置中，

输入认证数据，

将输入的认证数据发送到上述存储卡，

接收上述存储卡发送的数据，

输出接收到的数据。

另外，其特征在于：

上述存储卡还包括：

存储包含第一公开密钥的证明书，

将存储的证明书发送到上述写入装置，

存储与上述第一公开密钥成对的第一秘密密钥，

从解密了的签名数据取得数据，

从存储的亲启数据取得加密了的签名数据，

从存储的亲启数据取得加密了的共通密钥，

使用存储的第一秘密密钥，对取得的共通密钥进行解密，

使用解密了的共通密钥，对取得的签名数据进行解密，

从解密了的签名数据取得数字签名，

从解密了的签名数据取得包含第二公开密钥的证明书，

对取得的证明书进行验证，取得包含在该证明书中的第二公开密钥，

使用取得的数据和第二公开密钥，对取得的数字签名进行验证，

在上述写入装置中，

输入数据，

存储所输入的数据，

接收上述存储卡发送的证明书，

对接收到的证明书进行验证，取得包含在该证明书中的第一公开密钥，

存储第二秘密密钥，

使用存储的数据和第二秘密密钥，生成数字签名，

存储包含与上述第二秘密密钥成对的第二公开密钥的证明书，

使用存储的数据、生成的数字签名、包含存储的第二公开密钥的证明书，生成签名数据，

生成共通密钥，

使用生成的共通密钥，对生成的签名数据进行加密，

使用取得的第一公开密钥，对生成的共通密钥进行加密，

使用加密了的签名数据和共通密钥，生成亲启数据，

将生成的亲启数据发送到上述存储卡，

在上述读取装置中，

输入认证数据，

将输入的认证数据发送到上述存储卡，

接收上述存储卡发送的数据，

输出接收到的数据。

根据本发明，即使不输入 PIN，也能够将只有 IC 卡的拥有者能够读出的信息写入到 IC 卡中，并且能够实现对写入的信息的作成者进行认证和防止篡改。另外，能够保证只有 IC 卡的拥有者能够读出写入到 IC 卡中的数据，能够确定写入的数据的作者，防止篡改写入的数据。

附图说明

图 1 是表示实施例 1 和 2 的数据交换系统的使用者之间的交换的概念图。

图 2 是表示实施例 1 的写入装置和存储卡的结构的框图。

图 3 是表示实施例 1 的存储卡和读取装置的结构的框图。

图 4 是表示实施例 1 的写入装置和存储卡进行的处理的时序图。

图 5 是表示实施例 1 的写入装置和存储卡进行的处理的流程图。

图 6 是表示实施例 1 的存储卡和读取装置进行的处理的时序图。

图 7 是表示实施例 1 的存储卡和读取装置进行的处理的流程图。

图 8 是表示实施例 1 的存储卡和读取装置的结构的框图。

图 9 是表示实施例 1 的存储卡和读取装置进行的处理的时序图。

图 10 是表示实施例 1 的存储卡和读取装置进行的处理的流程图。

符号说明

101：保密存储卡，102：PC，103：便携电话，104：使用者，105：药店人员，201：证明书发送部件，202：卡证明书存储部件，203：私有存储部件，204：卡数据接收部件，205：认证数据存储部件，206：认证部件，207：认证数据接收部件，208：卡秘密密钥存储部件，209：卡共通密钥发送部件，210：公共存储部件，211：亲启数据接收部件，212：卡数据发送部件，213：输入部件，214：证明书接收部件，215：数据存储部件，216：卡证明书验证部件，217：系统证明书存储部件，218：系统秘密密钥存储部件，219：签名数据生成部件，220：数字签名生成部件，221：共通密钥生成部件，222：签名数据加密部件，223：共通密钥加密部件，224：亲启数据生成部件，225：亲启数据发送部件，226：读取装置数据发送部件，227：数据取得部件，228：操作部件，229：输出部件，230：认证数据发送部件，231：数字签名验证部件，232：数字签名取得部件，233：读取装置共通密钥接收部件，234：系统证明书验证部件，235：共通密钥解密部件，236：证明书取得部件，237：共通密钥取得部件，238：签名数据解密部件，239：读取装置数据接收部件，240：签名数据取得部件，241：读取装置共通密钥发送部件，242：卡共通密钥接收部件

具体实施方式

以下，根据附图说明本发明的实施例。另外，下述的实施例 1 和 2 的存储卡是具有加密认证功能的存储卡，将其称为保密存储卡。但是，也可以适用于具备与存储卡一样的功能的 IC 卡等。

另外，在下述的实施例 1 和 2 中，作为写入装置的例子，使用

PC（个人计算机）进行说明，但只要具有将数据写入到存储卡中的功能，也可以适用其他装置。同样，在下述的实施例 1 和 2 中，作为读取装置的例子，使用便携电话进行说明，但只要具有从存储卡读取数据的功能，也可以适用其他装置。

实施例 1

在本实施例中，能够利用可以不需要存储在保密存储卡中的证明书和保密存储卡的 PIN 认证地进行写入的公开存储部件，在药店中使用保密存储卡安全地向使用者提供给药指示书。

图 1 表示下述那样的使用者与药店的交换处理的概要。

（1）使用者 104 在药店的柜台，提供从医院发行的处方单和之前插入到便携电话 103 的保密存储卡 101。

（2）药店人员 105 将给药指示书写入到保密存储卡 101。

（3）使用者 104 将保密存储卡 101 安装到便携电话 103 中，查看给药指示书的内容。

使用者 104 将保密存储卡 101 安装到便携电话 103 中。如果进入药店，则在柜台交出纸的处方单和从便携电话 103 取出的保密存储卡 101。在药店内，在药店人员 105 准备好提供给使用者 104 的药后，将保密存储卡 101 安装到 PC102，使用 PC102 将该药的给药指示书写入到保密存储卡 101 中。然后，将药和保密存储卡 101 交给使用者 104。使用者 104 将保密存储卡 101 安装到便携电话 103 中，在便携电话 103 的画面上阅览给药指示书。

图 2 表示本实施例的系统的保密存储卡 101 和 PC102 的结构。另外，图 3 表示本实施例的系统的保密存储卡 101 和便携电话 103 的结构。本系统包括：保密存储卡 101；将只有拥有保密存储卡 101 的使用者 104 能够读取的信息写入到保密存储卡 101 中的 PC102；从保密存储卡 101 读出信息并显示的便携电话 103。

保密存储卡 101 包括：存储 RSA（Rivest Shamir Adleman）、椭圆密码等公开密钥加密方式的秘密密钥的卡秘密密钥存储部件 208；从便携电话 103 接收共通密钥的卡共通密钥接收部件 242；使

用存储在卡秘密密钥存储部件 208 中的秘密密钥，对该共通密钥进行解密的共通密钥解密部件 235；将解密了的共通密钥发送到便携电话 103 的卡共通密钥发送部件 209；存储与该秘密密钥成对的公开密钥的证明书，不能删除但可以不进行认证地进行读出的卡证明书存储部件 202；将该证明书发送到 PC102 的证明书发送部件 201；存储只有保密存储卡拥有者知道的 PIN 的认证数据存储部件 205；接收通过便携电话 103 输入的 PIN 的认证数据接收部件 207；进行 PIN 对照的认证部件 206；只在输入了正确的 PIN 的情况下能够从外部进行读写的私有存储部件 203；从便携电话 103 接收数据的卡数据接收部件 204；不进行 PIN 对照就能够从外部进行读写的公共存储部件 210；从 PC102 接收亲启数据的亲启数据接收部件 211；将数据发送到便携电话 103 的卡数据发送部件 212。

在此，亲启数据例如是指 RFC－2630（“Cryptographic Message Syntax”，IETF Network Working Group，R.Housley，RFC－2630，June 1999）中所揭示的 EnvelopedData，由加密对象数据和在该加密对象数据的加密中使用的加密了的共通密钥构成。在本实施例中，加密对象数据是签名数据。

签名数据例如是指 RFC-2630 中所揭示的 SignedData，由药店指示书等、PC102 的用户药向保密存储卡 101 的拥有者发送的数据、PC102 或 PC102 的用户的数字签名和证明书构成。

向保密存储卡 101 写入只有使用者 104 能够读出的数据的 PC102 包括：接受来自药店人员 105 那样的用户的输入的输入部件 213；存储输入的数据等的数据存储部件 215；从保密存储卡 101 接收证明书的证明书接收部件 214；对该证明书的正当性进行验证的卡证明书验证部件 216；存储 RSA、椭圆密码等公开密钥加密方式的秘密密钥的系统秘密密钥存储部件 218；存储与该秘密密钥成对的公开密钥的证明书的系统证明书存储部件 217；生成数字签名的数字签名生成部件 220；使用存储在数据存储部件 215 中的数据、存储在系统证明书存储部件 217 中的证明书、数字签名生成部件 220 生成的数字签名，生

成签名数据的签名数据生成部件 219；对该签名数据进行加密的签名数据加密部件 222；生成共通密钥的共通密钥生成部件 221；对该共通密钥进行加密的共通密钥加密部件 223；使用这些加密了的签名数据和共通密钥，生成亲启数据的亲启数据生成部件 224；将该亲启数据发送到保密存储卡 101 的亲启数据发送部件 225。具有加密功能的各部件进行共通密钥加密方式或公开密钥加密方式的加密、解密、哈希的计算、随机数的生成等。另外，在本实施例中，PC102 具有未图示的液晶显示器（LCD）等显示部件。

使用者 104 拥有的便携电话 103 包括：向保密存储卡 101 发送数据的读取装置数据发送部件 226；从保密存储卡 101 接收数据的读取装置数据接收部件 239；取得从保密存储卡 101 接收到的亲启数据所包含的共通密钥的共通密钥取得部件 237；向保密存储卡 101 发送该共通密钥的读取装置共通密钥发送部件 241；从保密存储卡 101 接收保密存储卡 101 解密了的共通密钥的读取装置共通密钥接收部件 233；取得从保密存储卡 101 接收到的亲启数据所包含的签名数据的签名数据取得部件 240；对该签名数据进行解密的签名数据解密部件 238；从解密了的签名数据中取得给药指示书等数据的数据取得部件 227；从解密了的签名数据中取得数字签名的数字签名取得部件 232；对该数字签名的正当性进行验证的数字签名验证部件 231；从解密了的签名数据中取得证明书的证明书取得部件 236；对该证明书的正当性进行验证的系统证明书验证部件 234；接受来自使用者 104 的输入的拨号键等操作部件 228；提供与使用者 104 的接口的液晶显示器（LCD）等输出部件 229；向保密存储卡 101 发送 PIN 的认证数据发送部件 230。具有解密功能的各部件进行共通密钥加密方式或公开密钥加密方式的加密、解密、哈希的计算、随机数的生成等。

图 4 是表示不进行 PIN 输入地由药店人员 105 使用药店中的 PC102 将只有使用者 104 能够读出的给药指示书写入到保密存储卡 101 中的处理的时序图。另外，图 5 是表示同样的处理的流程图。

在上述处理之前，药店人员 105 如果通过 PC102 确定了向使用

者 104 发行的给药指示书，则将保密存储卡 101 安装到药店中的 PC102 中。然后，药店人员从 PC102 的输入部件 213 向 PC102 进行给药指示书的发行指示。PC102 的数据存储部件 215 存储输入的给药指示书的数据。以下说明此后的处理流程。

PC102 向保密存储卡 101 发送证明书的取得请求。保密存储卡 101 的证明书发送部件 201 如果接收到证明书取得请求，则从卡证明书存储部件 202 读出使用者 104 的证明书，并发送到 PC102。PC102 的证明书接收部件 214 接收该证明书（S501）。

卡证明书验证部件 216 对得到的使用者 104 的证明书（以后称为使用者证明书）进行验证（S502）。卡证明书验证部件 216 保存可以信任的认证局（CA，Certification Authority）发行的证明书、证明书的失效列表（CRL，Certificate Revocation List），并在证明书验证中利用。在使用者证明书的验证处理中，也可以通过通信从外部得到认证局的证明书、证明书的失效列表。

在没有确认使用者证明书的正当性（验证结果是 NG）的情况下，结束处理。在确认了使用者证明书的正当性（验证结果是 OK）的情况下，在数字签名生成部件 220 中，使用存储在系统秘密密钥存储部件 218 中的秘密密钥，生成对给药指示书的数字签名。然后，在签名数据生成部件 219 中，将给药指示书、数字签名、存储在系统证明书存储部件 217 中的证明书（以后，称为药店证明书）结合在一起，生成签名数据（S503）。

接着，共通密钥生成部件 221 随机地生成共通密钥。签名数据加密部件 222 用该共通密钥对签名数据进行加密。共通密钥加密部件 223 用包含在使用者证明书中的公开密钥对该共通密钥进行加密。然后，亲启数据生成部件 224 将加密了的给药指示书和加密了的共通密钥结合起来，生成亲启数据（S504）。

亲启数据被从 PC102 的亲启数据发送部件 225 发送到保密存储卡 101 的亲启数据接收部件 211。保密存储卡 101 将接收到的亲启数据作为文件写入到公共存储部件 210 中（S505）。在文件名中附加例

如“给药指示书 20040401”等内容、容易了解作成年月日的名字。该写入处理由于是向公共存储部件 210 的写入处理，所以不需要进行 PIN 的输入操作。

图 6 是表示使用使用者 104 所拥有的便携电话 103 阅览写入到保密存储卡 101 中的加密了的给药指示书的处理的时序图。另外，图 7 是表示同样处理的流程图。

在药店中接受了保密存储卡 101 的使用者 104 将保密存储卡 101 安装到便携电话 103 中。便携电话 103 取得保密存储卡 101 的公共存储部件 210 的文件一览（S701）。

使用者 104 通过操作部件 228 从一览中选择给药指示书。这时，可以为了使用者 104 而将该文件一览显示在输出部件 229 上。从便携电话 103 接收到选择出的文件的取得请求的保密存储卡 101 从公共存储部件 210 中取出作为亲启数据的文件（亲启文件）的给药指示书，通过卡数据发送部件 212 进行发送。便携电话 103 的读取装置数据接收部件 239 接收该亲启文件（S702）。

便携电话 103 对读出的亲启数据进行解密，在共通密钥取得部件 237 中取得加密了的共通密钥。另外，在签名数据取得部件 240 中，取得用该共通密钥加密了的给药指示书的签名数据。然后，读取装置共通密钥发送部件 241 将该加密了的共通密钥发送到保密存储卡 101。保密存储卡 101 在卡共通密钥接收部件 242 中接收该共通密钥，在共通密钥解密部件 235 中使用存储在卡秘密密钥存储部件 208 中的秘密密钥对该共通密钥进行解密。解密了的共通密钥通过卡共通密钥发送部件 209 被发送到便携电话 103。便携电话 103 在读取装置共通密钥接收部件 233 中接收该解密了的共通密钥。签名数据解密部件 238 使用该共通密钥，对加密了的给药指示书的签名数据进行解密（S703）。

解密了的签名数据被分离为给药指示书、数字签名、药店证明书，并分别被发送到数据取得部件 227、数字签名取得部件 232、证明书取得部件 236。然后，系统证明书验证部件 234 对证明书取得部

件 236 取得的药店证明书进行验证。系统证明书验证部件 234 保存可以信任的认证局发行的证明书和证明书的失效列表，并在证明书的验证中使用。在药店证明书的验证处理中，也可以通过通信从外部得到认证局的证明书和证明书的失效列表。在确认了药店证明书的正当性的情况下，在数字签名验证部件 231 中，使用给药指示书、药店证明书中包含的公开密钥、数字签名，对数字签名的正当性进行验证（S704）。

在没有确认数字签名的正当性（验证结果是 NG）的情况下，结束处理。在确认了数字签名的正当性（验证结果是 OK）的情况下，使用者 104 能够通过输出部件 229 阅览数据取得部件 227 取得的给药指示书（S705）。

如果给药指示书的阅览结束了，则便携电话 103 向保密存储卡 101 发送将给药指示书存储到私有存储部件 203 中的请求（S706）。

这样，保密存储卡 101 向便携电话 103 要求 PIN 的输入。使用者 104 使用操作部件 228 输入 PIN（S707）。这时，例如可以在输出部件 229 上显示 PIN 输入窗口，让使用者 104 在 PIN 输入窗口的规定字段中输入 PIN。输入了的 PIN 被从便携电话 103 的认证数据发送部件 230 发送到保密存储卡 101 的认证数据接收部件 207。

保密存储卡 101 的认证部件 206 通过对接收到的 PIN 和存储在认证数据存储部件 205 中的 PIN 进行比较来对 PIN 进行对照，进行认证。在认证失败了（对照结果是 NG）的情况下，结束处理。在认证成功了（对照结果是 OK）的情况下，便携电话 103 的读取装置数据发送部件 226 将给药指示书的文件发送到保密存储卡 101。保密存储卡 101 的卡数据接收部件 204 接收该文件，并存储到私有存储部件 203 中（S708）。然后，也可以删除公共存储部件 210 的加密了的给药指示书。

如上所述，在本实施例中，在药店人员 105 将给药指示书写入到保密存储卡 101 中时，不需要输入保密存储卡 101 的 PIN，因此不需要向知道该 PIN 的使用者 104 要求 PIN 的输入处理。另外，给药指

示书是附加了药店的数字签名的签名数据，能够通过便携电话 103 的签名数据的验证而不篡改给药指示书，以及确认在药店中作成了给药指示书。另外，对包含给药指示书的签名数据进行加密使得只有作为保密存储卡 101 的拥有者的使用者 104 能够进行解密，因此保密存储卡 101 的拥有者以外的人无法偷看给药指示书。另外，在希望再次阅览给药指示书的情况下，只需要进行 PIN 的输入、对照处理，而不需要解密、签名的验证等密码处理。

实施例 2

图 8 表示了本实施例的系统的结构。在本实施例中，将实施例 1 中的便携电话 103 的数据取得部件 227、数字签名验证部件 231、数字签名取得部件 232、系统证明书验证部件 234、证明书取得部件 236、共通密钥取得部件 237、签名数据解密部件 238、签名数据取得部件 240 转移到保密存储卡 101 中。将数据写入到保密存储卡 101 中的 PC102 的结构与实施例 1 一样（图 2），在图 8 中省略。

从 PC102 向保密存储卡 101 写入给药指示书时的处理的流程与实施例 1 一样（图 4 和图 5）。

图 9 是表示使用使用者 104 所拥有的便携电话 103 阅览写入到保密存储卡 101 中的加密了的给药指示书的处理的时序图。另外，图 10 是表示同样的处理的流程图。

在药店中接受了保密存储卡 101 的使用者 104 将保密存储卡 101 安装到便携电话 103 中。保密存储卡 101 确认公共存储部件 210 中是否有给药指示书的亲启文件（S1001）。

在存在亲启文件的情况下，保密存储卡 101 对公共存储部件 210 的亲启文件进行解密和验证，向便携电话 103 发送对移动到私有存储部件 203 中的情况的承诺委托。便携电话 103 将该承诺委托显示在输出部件 229 上。如果使用者 104 经由操作部件 228 表示了承诺的意思，则从便携电话 103 向保密存储卡 101 发送承诺通知。如果得到承诺通知，则保密存储卡 101 对亲启文件进行解密，在共通密钥取得部

件 237 中取得加密了的共通密钥。另外，在签名数据取得部件 240 中，取得用该共通密钥加密了的给药指示书的签名数据。另外，共通密钥解密部件 235 使用保密存储卡 101 的秘密密钥，对该共通密钥进行解密。在此，保密存储卡 101 的秘密密钥使用存储在卡秘密密钥存储部件 208 中的秘密密钥。签名数据解密部件 238 使用解密了的共通密钥，对加密了的给药指示书的签名数据进行解密（S1002）。

解密了的签名数据被分离为给药指示书、数字签名、药店证明书，并分别被发送到数据取得部件 227、数字签名取得部件 232、证明书取得部件 236。然后，系统证明书验证部件 234 对证明书取得部件 236 取得的药店证明书进行验证。系统证明书验证部件 234 保存可以信任的认证局发行的证明书和证明书的失效列表，并在证明书的验证中使用。保密存储卡 101 具有未图示的认证局通信部件，该认证局通信部件可以是在药店证明书的验证处理中，通过通信从外部得到认证局的证明书和证明书的失效列表的形式。在确认了药店证明书的正当性的情况下，在数字签名验证部件 231 中，使用给药指示书、包含在药店证明书中的公开密钥、数字签名，对数字签名的正当性进行验证（S1003）。

在没有确认数字签名的正当性（验证结果是 NG）的情况下。结束处理。在确认了数字签名的正当性（验证结果是 OK）的情况下，将数据取得部件 227 取得的给药指示书复制到私有存储部件 203 中（S1004）。

如果复制给药指示书结束，则保密存储卡 101 从公共存储部件 210 中删除给药指示书的亲启文件（S1005）。

便携电话 103 要求保密存储卡 101 的私有存储部件 203 的文件一览（S1006）。

这样，保密存储卡 101 向便携电话 103 要求 PIN 的输入。使用者 104 使用操作部件 228 输入 PIN（S1007）。这时，例如可以在输出部件 229 中显示 PIN 输入窗口，让使用者 104 在 PIN 输入窗口的规定的字段中输入 PIN。输入的 PIN 被从便携电话 103 的认证数据发

送部件 230 发送到保密存储卡 101 的认证数据接收部件 207。

保密存储卡 101 的认证部件 206 通过对接收到的 PIN 和存储在认证数据存储部件 205 中的 PIN 进行比较来对 PIN 进行对照，进行认证。在认证失败了（对照结果是 NG）的情况下，结束处理。在认证成功了（对照结果是 OK）的情况下，保密存储卡 101 的卡数据发送部件 212 将文件一览发送到便携电话 103。便携电话 103 的读取装置数据接收部件 239 接收该文件一览，并输出到输出部件 229（S1008）。

在该文件一览中包括已经从公共存储部件 210 转移到私有存储部件 203 的给药指示书的文件。如果使用者 104 通过操作部件 228 选择该文件，则保密存储卡 101 的卡数据发送部件 212 将给药指示书的文件发送到便携电话 103。便携电话 103 的读取装置数据接收部件 239 接收该文件，并输出到输出部件 229，使用者 104 能够阅览给药指示书（S1009）。

如上所述，在本实施例中，保密存储卡 101 对亲启数据进行解密，使用包含在亲启数据中的数字签名和证明书，能够确认同样包含在亲启数据中的给药指示书的数据的正当性。因此，不需要预先将这些功能安装到便携电话 103 中。

在上述实施例 1 和 2 中，只有作为保密存储卡 101 的拥有者的使用者 104 能够阅览给药指示书的数据，但也可以多个使用者使用同一保密存储卡 101。

另外，在上述实施例 1 和 2 中，使用了药店的 PC102 将给药指示书的数据写入到保密存储卡 101 中的例子，但本发明也可以适用于在其他地方由具有同样功能的写入装置将其他种类的数据写入到保密存储卡 101 中的情况。

这样，在实施例 1 中说明了的保密存储卡系统的特征在于：

在将数据写入到存储卡和 IC 卡中，由卡拥有者阅览写入了的数据的存储卡系统中，具备安全存储卡、卡数据写入装置、卡数据阅览装置，存储卡的特征在于包括：不进行认证而写入数据的公共存储区

域；只在通过基于 PIN 的认证进行了认证的情况下能够进行读写的私有存储区域；存储有卡拥有者的证明书，不能写入但不进行认证就可以读出的证明书存储区域；存储卡使用者的秘密密钥的秘密密钥存储区域；存储只有卡使用者知道的 PIN 的 PIN 存储区域；一边访问各存储区域的信息，一边控制来自外部的对卡的处理请求、向外部的事件通知、内部处理的控制部件，卡数据写入装置的特征在于：为了生成签名数据、亲启数据而具备秘密密钥存储部件、证明书存储部件、加密格式处理部件，并具备对得到的证明书进行验证的证明书验证部件，具备具有签名数据和亲启数据的生成和证明书的验证所必需的加密功能的加密部件，卡数据阅览装置的特征在于：为了进行亲启数据的解密、签名数据的验证而具备证明书验证部件、加密格式处理部件、加密部件。

另外，在实施例 2 中说明了的保密存储卡系统中，

在将数据写入到存储卡和 IC 卡中，由卡拥有者阅览写入了的数据的存储卡系统中，具备保密存储卡、卡数据写入装置、卡数据阅览装置，存储卡的特征在于包括：不进行认证而写入数据的公共存储区域；只在通过基于 PIN 的认证进行了认证的情况下能够进行读写的私有存储区域；存储有卡拥有者的证明书，不能写入但不进行认证就可以读出的证明书存储区域；存储卡使用者的秘密密钥的秘密密钥存储区域；存储只有卡使用者知道的 PIN 的 PIN 存储区域；一边访问各存储区域的信息，一边控制在亲启数据的解密和签名数据的验证中使用的证明书存储部件、加密格式处理部件、加密部件、来自外部的对卡的处理请求、向外部的事件通知、内部处理的控制部件，卡数据写入装置的特征在于：为了生成签名数据、亲启数据而具备秘密密钥存储部件、证明书存储部件、加密格式处理部件，并具备对得到的证明书进行验证的证明书验证部件，具备具有签名数据和亲启数据的生成和证明书的验证所必需的加密功能的加密部件，卡数据阅览装置的特征在于：用于从保密存储卡读出数据并进行显示。

在上述各实施例中，可以用计算机实现保密存储卡 101、

PC102、便携电话 103。

保密存储卡 101、PC102、便携电话 103 具备未图示的执行程序的 CPU（中央处理单元）。

例如，CPU 经由总线与 ROM（只读存储器）、RAM（随机存取存储器）、通信端口、显示装置、K/B（键盘）、鼠标、FDD（软盘驱动器）、CDD（CD 驱动器）、磁盘装置、光盘装置、打印机装置、扫描仪装置等连接。

RAM 是易失性存储器的一个例子。ROM、FDD、CDD、磁盘装置、光盘装置是非易失性存储器的一个例子。它们是存储装置、存储部件或保存部件的一个例子。

上述各实施例的保密存储卡 101、PC102、便携电话 103 所处理的数据和信息被保存在存储装置、存储部件或保存部件中，由保密存储卡 101、PC102、便携电话 103 的各部件进行记录和读出。

另外，通信端口例如与 LAN、因特网、或 ISDN 等 WAN（广域网）连接。

在磁盘装置中，存储有操作系统（OS）、窗口系统、程序群、文件群（数据库）。

由 CPU、OS、窗口系统执行程序群。

上述保密存储卡 101、PC102、便携电话 103 的各部件的一部分或全部也可以由能够在计算机上动作的程序构成。或者也可以由存储在 ROM 中的固件实现。或者也可以通过软件、硬件、或软件和硬件和固件的组合来实施。

在上述程序群中，存储有使 CPU 执行在实施例的说明中作为“~部件”说明了的处理的程序。例如用 C 语言、HTML、SGML、XML 等计算机语言作成这些程序。

另外，上述程序被存储在磁盘装置、FD（软盘）、光盘、CD（Compact Disk）、MD（MiniDisk）、DVD（Digital Versatile Disk）等其他存储介质中，由 CPU 读出并执行。

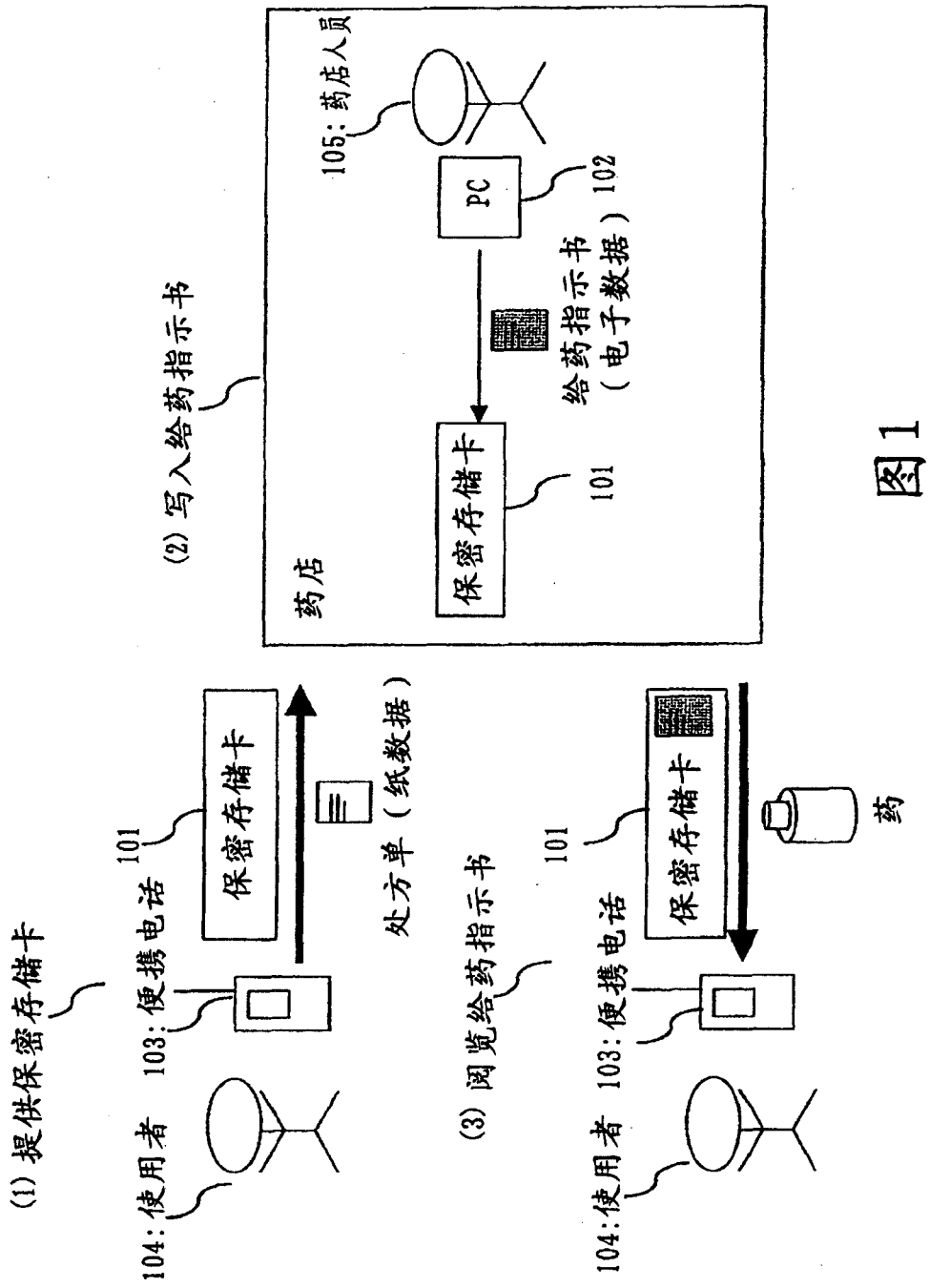

(1) 提供保密存储卡
104:使用者
103:便携电话
101
保密存储卡
处方单（纸数据）
(2) 写入给药指示书
药店
105:药店人员
PC
102
保密存储卡
101
给药指示书
（电子数据）
(3) 阅览给药指示书
药

图 1

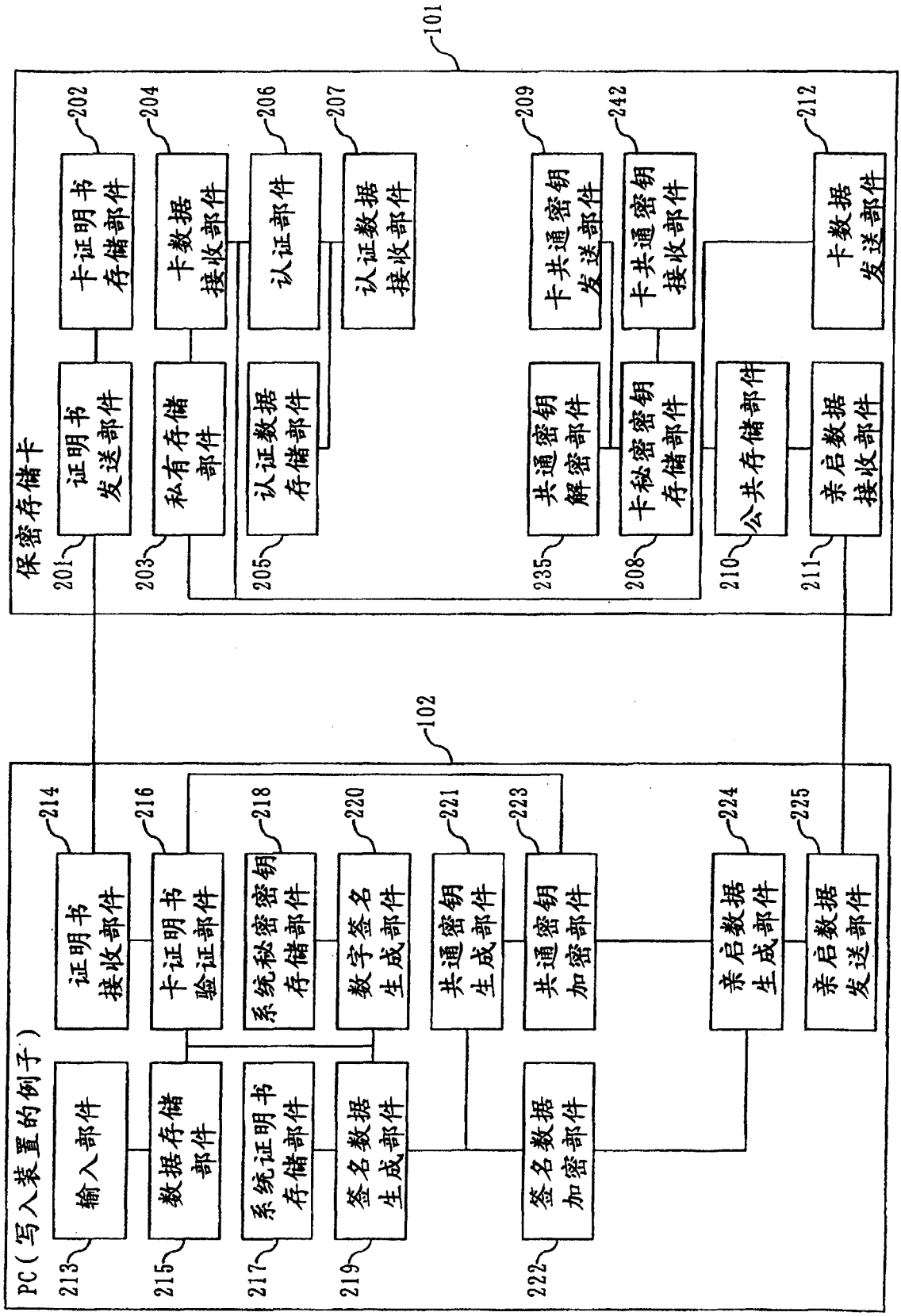

保密存储卡
101
证明书发送部件
201
卡证明书存储部件
202
私有存储部件
203
卡数据接收部件
204
认证数据存储部件
205
认证部件
206
认证数据接收部件
207
共通密钥解密部件
235
卡秘密密钥存储部件
208
卡共通密钥发送部件
209
卡共通密钥接收部件
242
公共存储部件
210
亲启数据接收部件
211
卡数据发送部件
212
PC（写入装置的例子）
102
输入部件
213
证明书接收部件
214
数据存储部件
215
卡证明书验证部件
216
系统证明书存储部件
217
系统秘密密钥存储部件
218
签名数据生成部件
219
数字签名生成部件
220
签名数据加密部件
222
共通密钥生成部件
221
共通密钥加密部件
223
亲启数据生成部件
224
亲启数据发送部件
225

图2

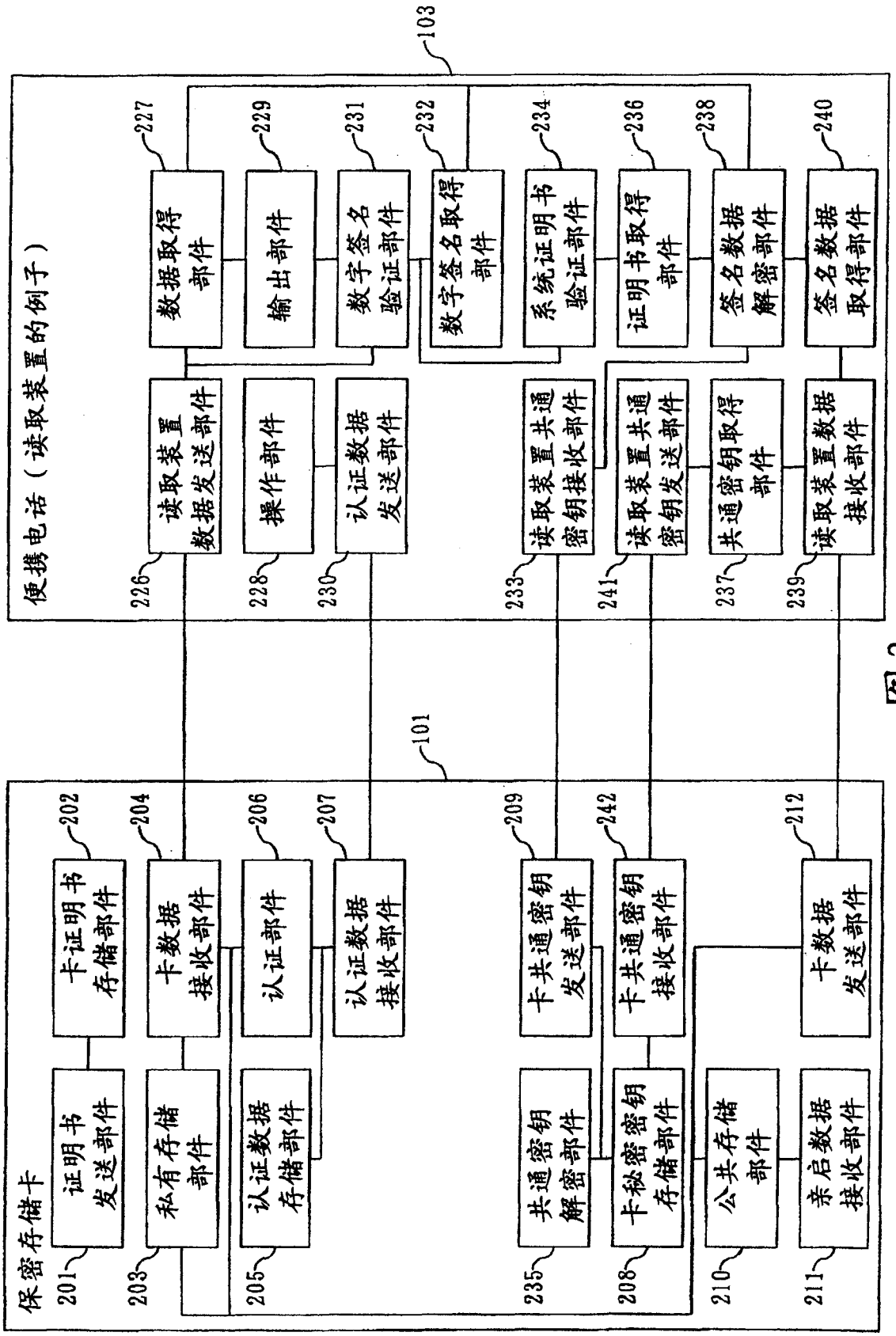

保密存储卡
证明书发送部件
卡证明书存储部件
私有存储部件
卡数据接收部件
认证数据存储部件
认证部件
认证数据接收部件
共通密钥解密部件
卡共通密钥发送部件
卡秘密密钥存储部件
卡共通密钥接收部件
公共存储部件
卡数据发送部件
亲启数据接收部件
便携电话（读取装置的例子）
读取装置数据发送部件
操作部件
认证数据发送部件
读取装置共通密钥接收部件
读取装置共通密钥发送部件
共通密钥取得部件
读取装置数据接收部件
数据取得部件
输出部件
数字签名验证部件
数字签名取得部件
系统证明书验证部件
证明书取得部件
签名数据解密部件
签名数据取得部件
101
103
201
202
203
204
205
206
207
208
209
210
211
212
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242

图 3

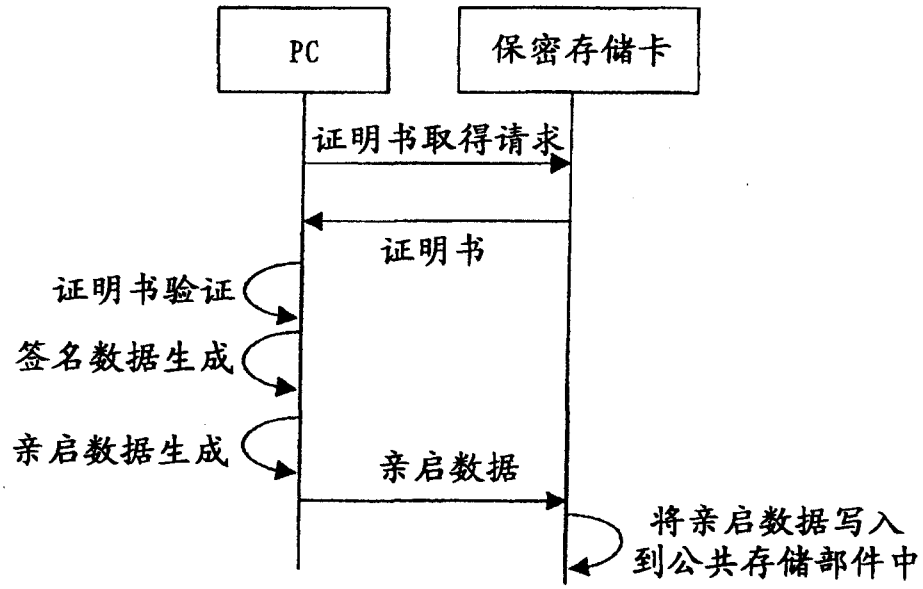

PC
保密存储卡
证明书取得请求
证明书
证明书验证
签名数据生成
亲启数据生成
亲启数据
将亲启数据写入
到公共存储部件中

图4

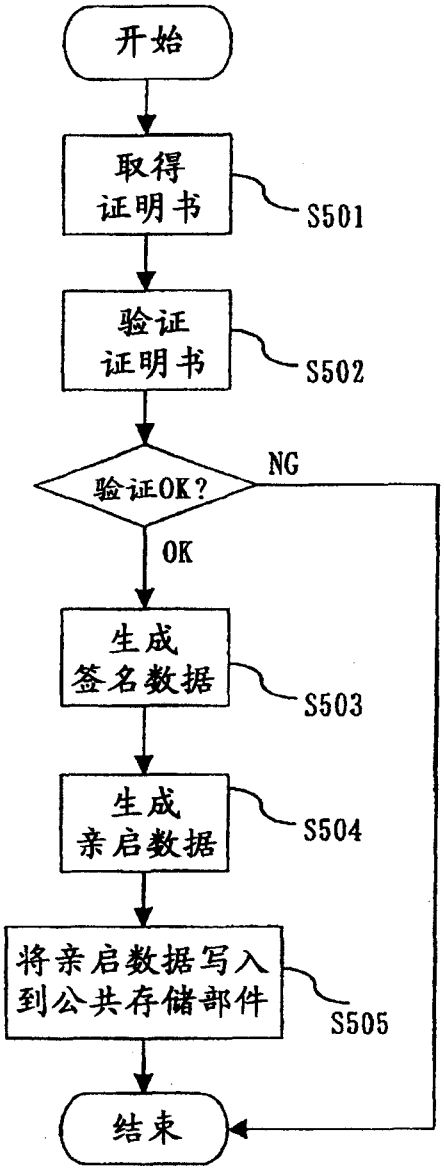

开始
取得证明书
S501
验证证明书
S502
验证OK?
NG
OK
生成签名数据
S503
生成亲启数据
S504
将亲启数据写入到公共存储部件
S505
结束

图5

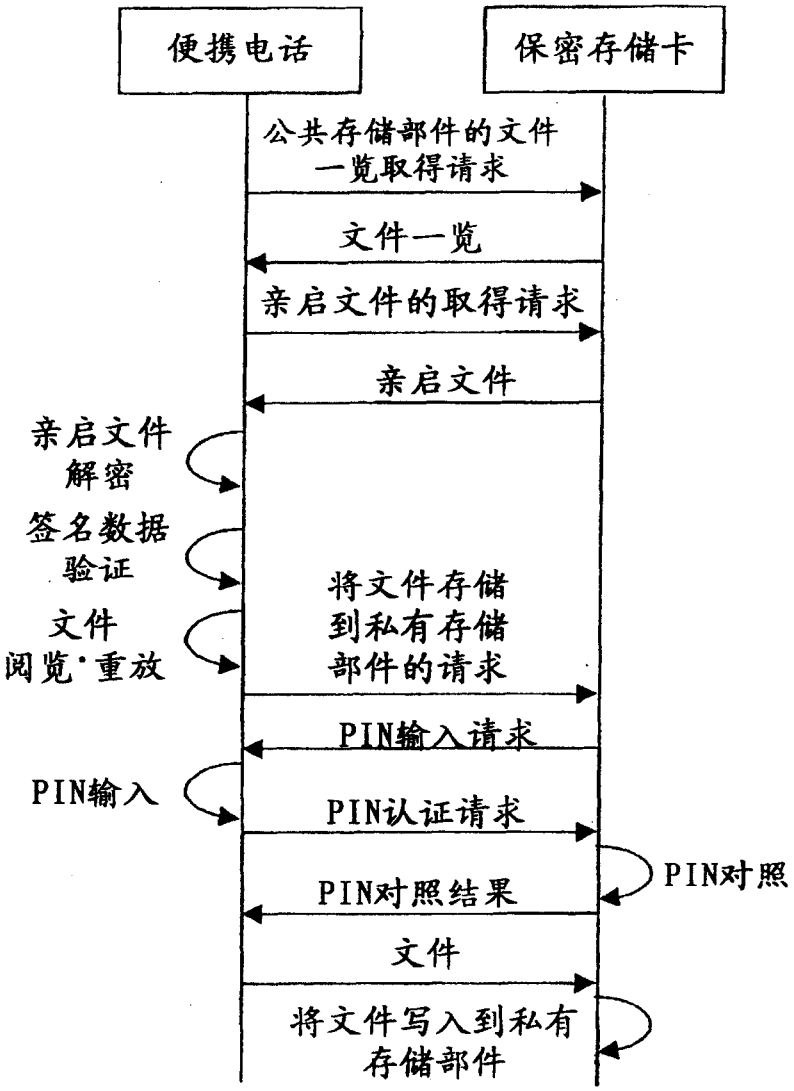

便携电话
保密存储卡
公共存储部件的文件一览取得请求
文件一览
亲启文件的取得请求
亲启文件
亲启文件解密
签名数据验证
文件阅览·重放
将文件存储到私有存储部件的请求
PIN输入请求
PIN输入
PIN认证请求
PIN对照
PIN对照结果
文件
将文件写入到私有存储部件

图6

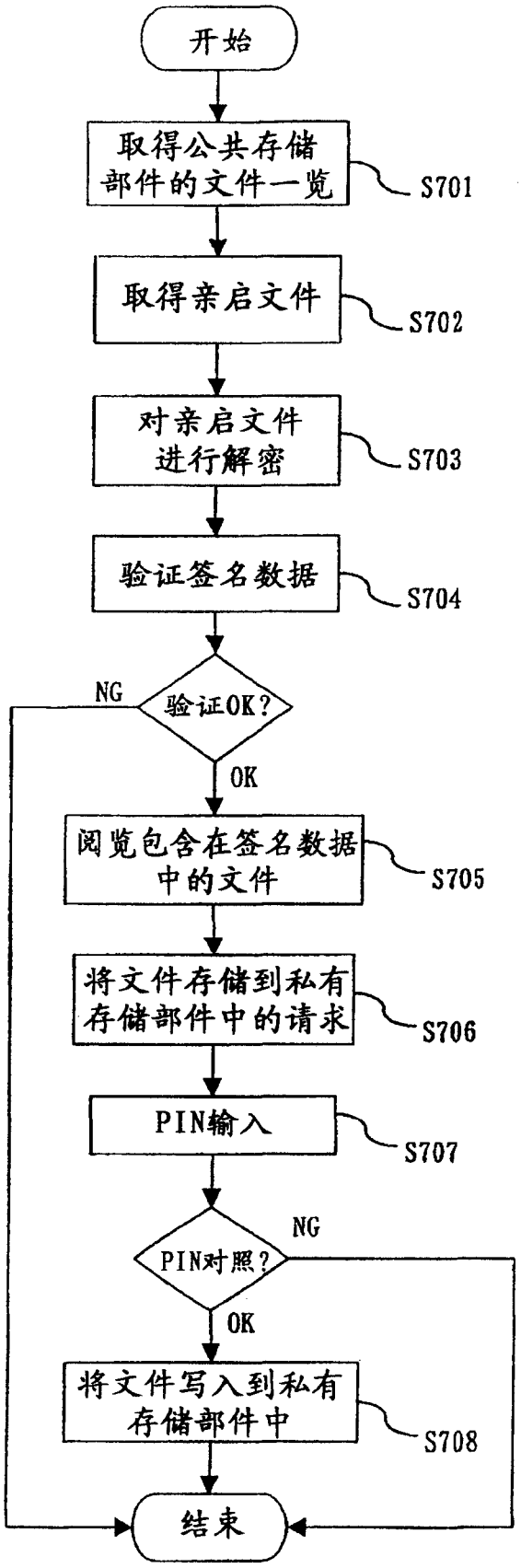

开始
取得公共存储部件的文件一览
S701
取得亲启文件
S702
对亲启文件进行解密
S703
验证签名数据
S704
NG
验证OK?
OK
阅览包含在签名数据中的文件
S705
将文件存储到私有存储部件中的请求
S706
PIN输入
S707
NG
PIN对照?
OK
将文件写入到私有存储部件中
S708
结束

图7

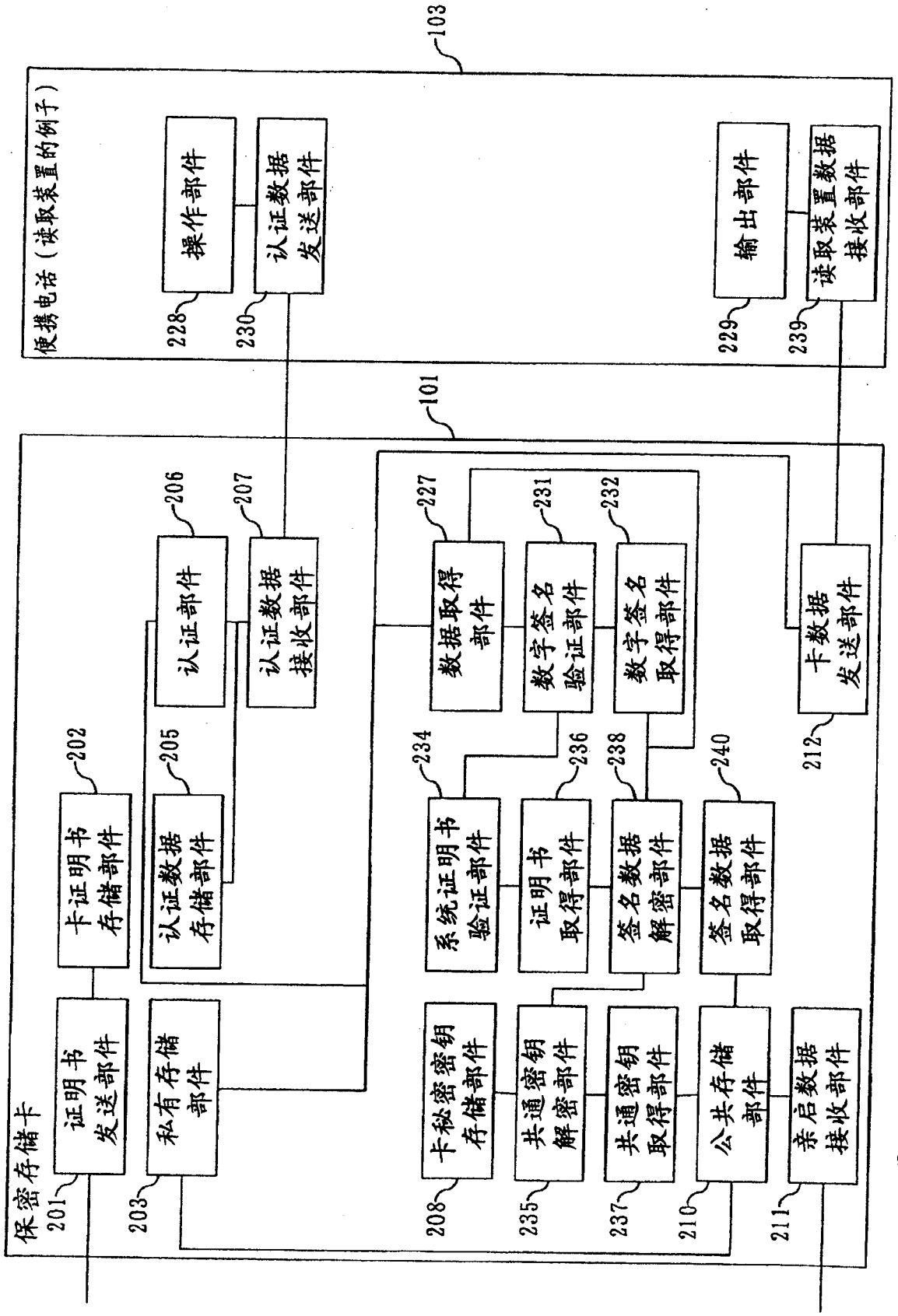

保密存储卡
便携电话（读取装置的例子）
103
101
操作部件
228
认证数据发送部件
230
输出部件
229
读取装置数据接收部件
239
卡证明书存储部件
202
证明书发送部件
201
认证部件
206
认证数据接收部件
207
认证数据存储部件
205
私有存储部件
203
数据取得部件
227
数字签名验证部件
231
数字签名取得部件
232
卡数据发送部件
212
系统证明书验证部件
234
证明书取得部件
236
签名数据解密部件
238
签名数据取得部件
240
卡秘密密钥存储部件
208
共通密钥解密部件
235
共通密钥取得部件
237
公共存储部件
210
亲启数据接收部件
211

图8

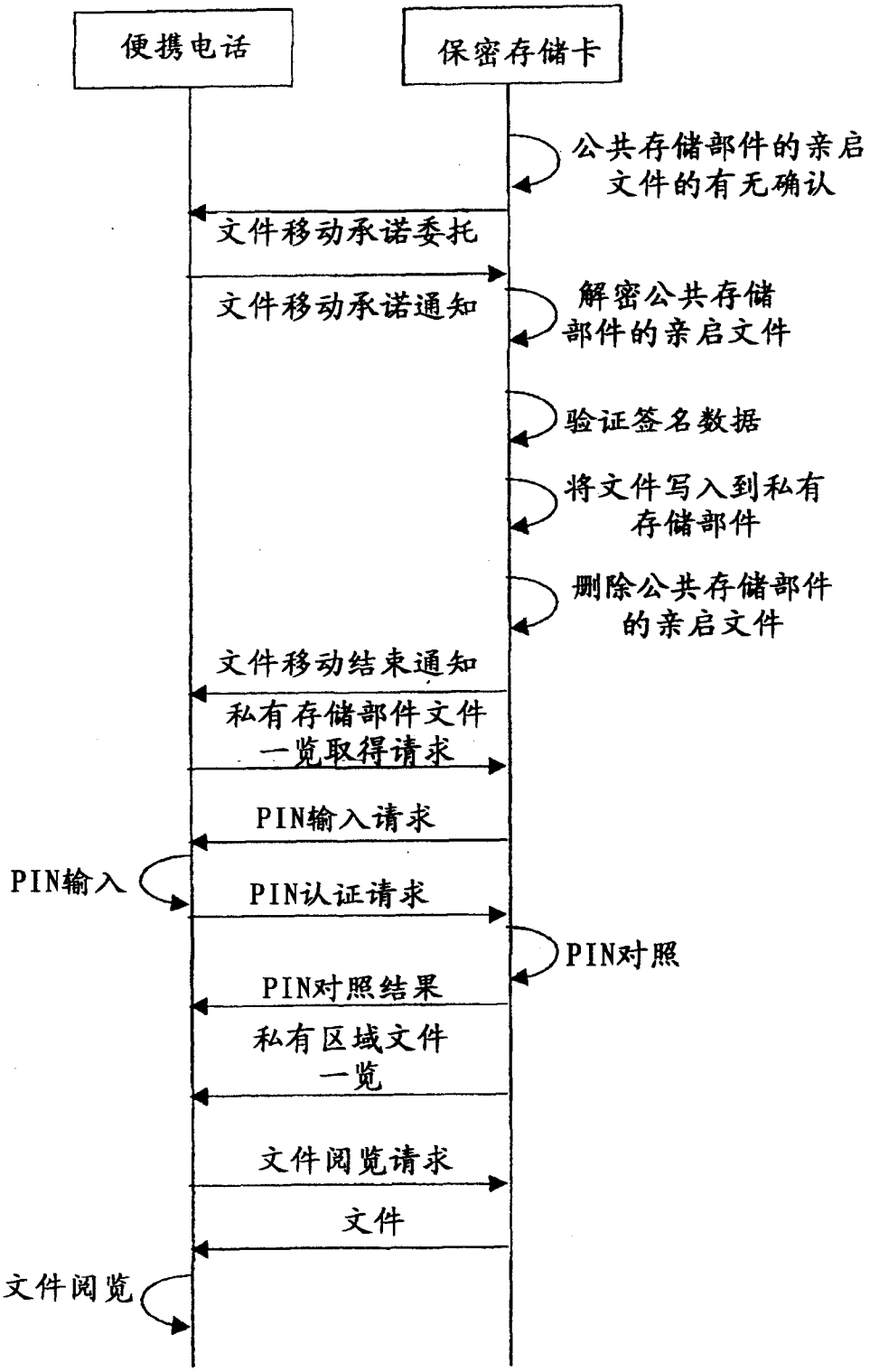

便携电话
保密存储卡
公共存储部件的亲启文件的有无确认
文件移动承诺委托
文件移动承诺通知
解密公共存储部件的亲启文件
验证签名数据
将文件写入到私有存储部件
删除公共存储部件的亲启文件
文件移动结束通知
私有存储部件文件一览取得请求
PIN输入请求
PIN输入
PIN认证请求
PIN对照
PIN对照结果
私有区域文件一览
文件阅览请求
文件
文件阅览

图9

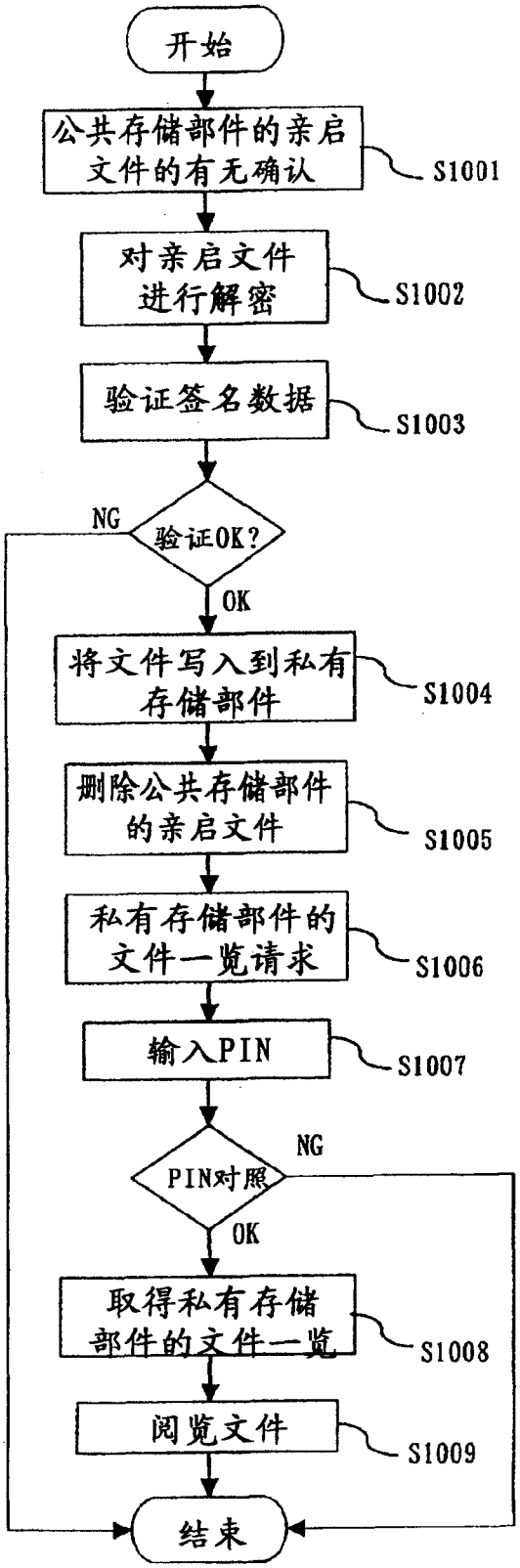

开始
公共存储部件的亲启文件的有无确认
S1001
对亲启文件进行解密
S1002
验证签名数据
S1003
NG
验证OK?
OK
将文件写入到私有存储部件
S1004
删除公共存储部件的亲启文件
S1005
私有存储部件的文件一览请求
S1006
输入PIN
S1007
NG
PIN对照
OK
取得私有存储部件的文件一览
S1008
阅览文件
S1009
结束

图10