(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102611552 B
(45)授权公告日 2016.10.12

(21)申请号 201110025553.9

(22)申请日 2011.01.24

(65)同一申请的已公布的文献号
申请公布号 CN 102611552 A

(43)申请公布日 2012.07.25

(73)专利权人 必拓电子商务有限公司
地址 301712 天津市武清区京滨工业园晋元道22号

(72)发明人 张贵宝 柯玉亮

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 宋焰琴

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 29/06(2006.01)

(56)对比文件
EP 0114368 B1,1991.04.24,
CN 101807994 A,2010.08.18,
CN 1538657 A,2004.10.20,

审查员 夏礼

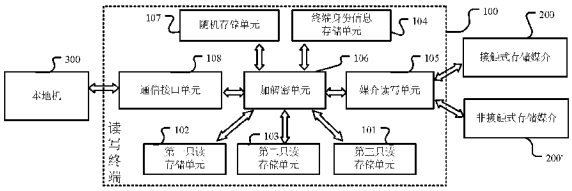
权利要求书2页 说明书8页 附图6页

(54)发明名称

有价信息存储媒介的读写终端、系统

(57)摘要

本发明公开了一种有价信息存储媒介的读写终端、系统。该读写终端实现了有价信息存储媒介、系统服务器和网银服务器三个方向的相对独立的数据交换加解密，加解密的方式由本地机转移到了读写终端，从而方便了用户使用。



CN 102611552 B

1.一种有价信息存储媒介的读写终端，其特征在于，该读写终端独立于本地机，不具有显示功能和输入键盘；包括终端身份信息存储单元、第一只读存储单元、加解密单元、媒介读写单元、第二只读存储单元和通信接口单元，其中：

所述终端身份信息存储单元，用于存储所述读写终端的身份信息；

所述媒介读写单元，与有价信息存储媒介相连接，用于从所述有价信息存储媒介中读取媒介持有人信息；

所述第一只读存储单元，用于存储所述读写终端和系统服务器进行数据安全传输的第一加密程序、第一加密密钥；

所述第二只读存储单元，用于存储所述读写终端和有价信息存储媒介进行数据安全传输的第二解密程序、第二解密密钥；

所述加解密单元，

与所述终端身份信息存储单元和所述第一只读存储单元相连接，用于根据所述第一加密程序和第一加密密钥对所述读写终端的身份信息进行加密；

与所述媒介读写单元和所述第二只读存储单元相连接，用于根据所述第二解密程序和第二解密密钥对所述有价信息存储媒介持有人信息进行解密，并将所述解密后的有价信息存储媒介持有人信息利用所述第一加密程序和第一加密密钥进行加密；

所述通信接口单元，

与所述加解密单元和本地机相连，用于通过所述本地机将所述加密后的读写终端身份信息发送至系统服务器，以供系统服务器对所述读写终端的身份进行认证；还用于将所述加密后的数据发送至所述系统服务器，以供所述系统服务器对所述有价信息存储媒介的身份进行认证。

2.根据权利要求1所述的读写终端，其特征在于，

所述第一只读存储单元，还用于存储所述读写终端和系统服务器进行数据安全传输的第一解密程序和第一解密密钥；

所述加解密单元，还用于根据所述第一加密程序和第一加密密钥对所述读写终端向系统服务器发送的数据进行加密；并根据第一解密程序和第一解密密钥对所述系统服务器下发的数据进行解密；

所述通信接口单元，还用于通过本地机将所述进行加密数据发送至系统服务器；接收所述系统服务器下发的经过加密的数据。

3.根据权利要求2所述的读写终端，其特征在于，所述第一加密程序和第一解密程序均为非对称加解密程序，所述第一加密密钥和所述第一解密密钥为所述非对称加解密程序对应的公、私密钥。

4.根据权利要求3所述的读写终端，其特征在于，所述非对称加解密程序为RSA加解密算法。

5.根据权利要求2所述的读写终端，其特征在于，

所述第二只读存储单元，还用于存储所述读写终端和有价信息存储媒介进行数据安全传输的第二加密程序、第二加密密钥；

所述加解密单元，还用于根据所述第一解密程序和第一解密密钥对从所述系统服务器下发的经加密的有价信息存储媒介的写指令进行解密；并根据所述第二加密程序和第二加

密密钥对经过解密的写指令进行加密；

所述媒介读写单元，还用于根据经过所述加密的写指令，对所述有价信息存储媒介进行写操作。

6.根据权利要求5所述的读写终端，其特征在于，第二加密程序和第二解密程序均为对称加解密程序，所述第二加密密钥和所述第二解密密钥为所述对称加解密程序对应的密钥。

7.根据权利要求6所述的读写终端，其特征在于，所述对称加密密程序为3DES加解密算法。

8.根据权利要求1所述的读写终端，其特征在于，还包括第三只读存储单元，其中：

所述第三只读存储单元，还用于存储所述读写终端与网银服务器进行数据传输的第三加解密程序和第三加解密密钥；

所述加解密单元，通过所述通信接口单元、本地机与网银服务器相连接，用于根据所述第三加解密程序和第三加解密密钥对有价信息存储媒介持有人的身份信息和/或账户变更信息进行加密，供网银服务器对有价信息存储媒介持有人的身份进行认证，和/或对有价信息存储媒介持有人的账户信息进行更新。

9.根据权利要求8所述的读写终端，其特征在于，还包括：

随机存储单元，与所述加解密单元相连接，用于存储所述读写终端、有价信息存储媒介、系统服务器和所述网银服务器的加、解密后的数据。

10.根据权利要求1～8中任一项所述的读写终端，其特征在于：所述媒介读写单元为接触式媒介读写单元或非接触式媒介读写单元；所述通信接口单元为USB接口单元或RS232接口单元。

11.根据权利要求1～8中任一项所述的读写终端，其特征在于，所述一个读写终端对应一个或多个所述有价信息存储媒介。

12.一种有价信息存储媒介的读写系统，其特征在于，包括：权利要求1～8中任一项所述的有价信息存储媒介的读写终端、本地机和系统服务器，其中，所述读写终端与所述有价信息存储媒介相连，所述本地机与所述读写终端相连，所述系统服务器与所述本地机相连。

13.根据权利要求12所述的读写系统，其特征在于：所述本地机为能够连接到所述系统服务器的台式机、便携机或嵌入式装置。

14.根据权利要求12所述的读写系统，其特征在于，还包括网银服务器，其中：

该网银服务器，与所述本地机相连接，用于完成网上支付的功能。

有价信息存储媒介的读写终端、系统

技术领域

[0001] 本发明涉及电子信息行业信息安全领域，尤其涉及一种有价信息存储媒介的读写终端、系统。

背景技术

[0002] 当今，居住城市化的人群比例在不断扩大，而城市里人们的日常活动也变得越来越多样化，节奏化，这就要求城市的各种信息网络越来越健全，同时也需要越来越多、越来越灵活便捷的支付手段。城市IC卡系统从某种程度上较好地解决了人们在生活中对于日常支付和充值的问题。随着城市IC卡的更广泛应用，人们的日常生活也将享受到更多的便利。然而在日常生活中不同类型IC卡的充值一般要到指定的网点才能操作，这给使用IC卡的持有人带来了不便，而且持有人只能到营业大厅去了解最新相关信息，信息传递比较单一、缓慢和滞后。

[0003] 在实现本发明的过程中，发明人意识到现有技术存在如下技术问题：有价信息存储媒介的读写过程中，加密过程与解密过程均是在专用计算机上进行，从而造成了持卡人查询和交易的不便。

发明内容

[0004] (一)要解决的技术问题

[0005] 针对上述问题，本发明提出一种有价信息存储媒介的读写终端、系统，以将加解密功能从专用计算机转移到读写终端，方便用户的查询与交易。

[0006] (二)技术方案

[0007] 根据本发明的一个方面，提供了一种有价信息存储媒介的读写终端。该读写终端独立于本地机，包括终端身份信息存储单元、第一只读存储单元，加解密单元和通信接口单元。终端身份信息存储单元，用于存储读写终端的身份信息。第一只读存储单元，用于存储读写终端和系统服务器进行数据安全传输的第一加密程序、第一加密密钥。加解密单元，与终端身份信息存储单元和第一只读存储单元相连接，用于根据第一加密程序和第一加密密钥对读写终端的身份信息进行加密。通信接口单元，与加解密单元和本地机相连，用于通过本地机将加密后的读写终端身份信息发送至系统服务器，以供系统服务器对读写终端的身份进行认证。

[0008] 优选地，该有价信息存储媒介的读写终端中，第一只读存储单元，还用于存储读写终端和系统服务器进行数据安全传输的第一解密程序和第一解密密钥。加解密单元，还用于根据第一加密程序和第一加密密钥对读写终端向系统服务器发送的数据进行加密；并根据第一解密程序和第一解密密钥对系统服务器下发的数据进行解密。通信接口单元，还用于通过本地机将加密后的数据发送至系统服务器；接收系统服务器下发的经过加密的数据。优选地，第一加密程序和第一解密程序均为非对称加解密程序，第一加密密钥和第一解密密钥为非对称加解密程序对应的公、私密钥。最优地，非对称加解密程序为RSA加解密算

法。

[0009] 优选地，该有价信息存储媒介的读写终端中，该读写终端还包括媒介读写单元、随机存储单元和第二只读存储单元。媒介读写单元，与有价信息存储媒介相连接，用于从有价信息存储媒介中读取媒介持有人信息。随机存储单元，与加解密单元和媒介读写单元相连接，用于随机存储通过媒介读写单元从有价信息存储媒介中读取的媒介用户的信息。第二只读存储单元，用于存储读写终端和有价信息存储媒介进行数据安全传输的第二加密程序、第二加密密钥。加解密单元，还与媒介读写单元、随机存储单元和第二只读存储单元相连接，用于将随机存储单元中存储的媒介持有人的信息利用第一加密程序和第一加密密钥进行加密。通信接口单元，还用于将加密后的数据发送至系统服务器，以供系统服务器对有价信息存储媒介的身份进行认证，并存储有价信息存储媒介的其它信息。

[0010] 优选地，该有价信息存储媒介的读写终端中，第二只读存储单元，还用于存储读写终端和有价信息存储媒介进行数据安全传输的第二解密程序、第二解密密钥。加解密单元，还用于根据第一解密程序和第一解密密钥对从系统服务器下发的经加密的对有价信息存储媒介的写指令进行解密，随机储存到随机存储单元；并将随机储存到随机存储单元的写指令根据第二加密程序和第二加密密钥进行加密。媒介读写单元，还用于根据经过加密的写指令，对有价信息存储媒介进行写操作。最优地，该第二加密程序和第二解密程序均为对称加解密程序，第二加密密钥和第二解密密钥为对称加解密程序对应的密钥。最优地，对称加密密程序为3DES加解密算法。

[0011] 优选地，该有价信息存储媒介的读写终端还包括第三只读存储单元。第三只读存储单元，用于存储读写终端与银行服务器进行数据传输的第三加解密程序和第三密钥。加解密单元，通过通信接口单元、本地机与网银服务器相连接，用于根据第三加解密程序和第三密钥对用户的身份信息进行加密，供银行服务器对用户的身份进行认证，并进行数据交换。

[0012] 根据本发明的另一个方面，还提供了一种有价信息存储媒介的读写系统。该系统包括：上述读写终端、本地机和系统服务器。其中，所述读写终端与所述有价信息存储媒介相连，所述本地机与所述读写终端相连，所述系统服务器与所述本地机相连。本地机为能够连接到系统服务器的台式机、便携机或嵌入式装置。此外，该读写系统还包括：网银服务器，与本地机相连接，用于完成网上支付的功能。

[0013] (三)有益效果

[0014] 本发明的有价信息存储媒介的读写终端、系统，实现了有价信息存储媒介、系统服务器和网银服务器三个方向的相对独立的数据交换加解密，加解密的方式由本地机转移到了读写终端，从而方便持有人使用。此外，由于读写终端不具有显示功能和输入输出键盘，解决了系统的安全问题，并且本读写终端兼有网银UKEY的功能。

附图说明

[0015] 图1为本发明有价信息存储媒介的读写终端的示意图；

[0016] 图2为本发明有价信息存储媒介的读写系统的示意图；

[0017] 图3为本发明读写系统对读写终端进行认证的流程图；

[0018] 图4为本发明读写系统对有价信息存储媒介进行认证的流程图；

[0019] 图5为本发明读写系统中，有价信息存储媒介持有人通过网银服务器进行付款交易的流程图；

[0020] 图6为本发明读写系统中，对有价信息存储媒介进行写数据的流程图；

[0021] 图7为本发明实施例读写终端与系统服务器进行数据安全传输的示意图。

具体实施方式

[0022] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

[0023] 图1为本发明有价信息存储媒介的读写终端的示意图。如图1所示，在本发明的一个示例性实施例中，有价信息存储媒介的读写终端100独立于本地机300，包括：终端身份信息存储单元104、第一只读存储单元102，加解密单元106和通信接口单元108。终端身份信息存储单元104，用于存储读写终端的身份信息。第一只读存储单元102，用于存储读写终端100和系统服务器进行数据安全传输的第一加密程序、第一加密密钥。加解密单元106，与终端身份信息存储单元104和第一只读存储单元102相连接，用于根据第一加密程序和第一加密密钥对读写终端的身份信息进行加密。通信接口单元108，与加解密单元106和本地机300相连，用于通过本地机300将加密后的读写终端身份信息发送至系统服务器，以供系统服务器对读写终端的身份进行认证。

[0024] 本实施例中，第一只读存储单元102，还用于存储读写终端100和系统服务器进行数据安全传输的第一解密程序和第一解密密钥。加解密单元106，还用于根据第一加密程序和第一加密密钥对读写终端向系统服务器发送的数据进行加密；并根据第一解密程序和第一解密密钥对系统服务器下发的数据进行解密。通信接口单元108，还用于通过本地机将进行加密数据发送至系统服务器；接收系统服务器下发的经过加密的数据。优选地，本实施例中，第一加密程序和第一解密程序均为非对称加解密程序，第一加密密钥和第一解密密钥为非对称加解密程序对应的公、私密钥。最优地，该非对称加解密程序为RSA加解密算法。

[0025] 本实施例实现了与系统服务器方向的相对独立的数据交换加解密，加解密的方式由本地机转移到了读写终端，用户可以随时随地的进行有价信息存储媒介的信息查询和充值操作，从而不必要在专用计算机上进行，方便了用户使用。

[0026] 此外，本实施例的有价信息存储媒介读写终端中，加入了供系统服务器对读写终端的认证的功能，在对有价信息存储媒介进行读写之前，首先由系统服务器对读写终端进行身份认证。只有当该身份认证通过时，才可以由该读写终端对存储媒介进行读写，从而增强了有价信息存储媒介读写终端的安全性。

[0027] 在本发明优选实施例的有价信息存储媒介读写终端还包括：媒介读写单元105、随机存储单元107和第二只读存储单元103。媒介读写单元105，与有价信息存储媒介(200和/或200′)相连接，用于从有价信息存储媒介中读取媒介用户信息。随机存储单元107，与加解密单元106和媒介读写单元105相连接，用于随机存储通过媒介读写单元105从有价信息存储媒介(200和/或200′)中读取的媒介用户的信息。第二只读存储单元103，用于存储读写终端100和有价信息存储媒介(200和/或200′)进行数据安全传输的第二加密程序、第二加密密钥。加解密单元106，还与媒介读写单元105、随机存储单元107和第二只读存储单元103相连接，用于将随机存储单元107中存储的媒介用户的信息利用第一加密程序和第一加密密

钥进行加密。通信接口单元108，还用于将加密后的数据发送至系统服务器，以供系统服务器对有价信息存储媒介(200和/或200′)的身份进行认证，并存储有价信息存储媒介的其它信息。

[0028] 此外，本实施例中，第二只读存储单元103，还用于存储读写终端100和有价信息存储媒介(200和/或200′)进行数据安全传输的第二解密程序、第二解密密钥；加解密单元106，还用于根据第一解密程序和第一解密密钥对从系统服务器下发的经加密的对有价信息存储媒介(200和/或200′)的写指令进行解密；并根据第二加密程序和第二加密密钥对经过解密的写指令进行加密。媒介读写单元105，还用于根据经过加密的写指令，对有价信息存储媒介(200和/或200′)进行写操作。优选地，第二加密程序和第二解密程序均为对称加解密程序，第二加密密钥和第二解密密钥为对称加解密程序对应的密钥。最优地，对称加密密程序为3DES加解密算法。

[0029] 为了适应目前市场上普遍使用的接触式IC卡，如水、电、气方面，本实施例中，读写终端和有价信息存储媒介间通过对称加密方式进行信息交互。当然也可以采用前述的第一只读存储单元的加密方式。对称加密方式以3DES加解密算法为佳。相对于系统服务器和读写终端的非对称加密算法，该算法的加密效果较差，但速度快，能够满足读写终端和有价信息存储媒介间进行信息交互的要求。

[0030] 在本发明进一步的实施例中，有价信息存储媒介读写终端还包括：第三只读存储单元101。第三只读存储单元101，还用于存储读写终端100与银行服务器进行数据传输的第三加解密程序和第三密钥。加解密单元106，通过通信接口单元108、本地机300与银行服务器相连接，用于根据第三加解密程序和第三密钥对用户的身份信息进行加密，供银行服务器对读写终端的身份进行认证。简单来说，读写终端兼具有网银UKEY的功能，用户在进行网银操作的时候，不必再持有额外的认证介质，从而更加方便了用户使用。

[0031] 优选地，本实施例中，有价信息存储媒介读写终端还包括：随机存储单元107。该随机存储单元，与所述加解密单元相连接，用于存储所述读写终端、有价信息存储媒介和所述系统服务器的加、解密后的共享数据。

[0032] 通过设置随机存储单元，可以存储共享数据，从而加快读写终端的处理速度，优化整套系统的处理流程。

[0033] 与上述装置实施例相对应，本发明还提供了一种有价信息存储媒介的读写系统。图2为本发明有价信息存储媒介的读写系统的示意图。如图2所示，本实施例提供一种包含有价存储媒介200、读写终端100、本地机300、系统服务器400等组成的网络化电子信息存储及读取系统，使得金融领域有价存储媒介持有人可以自行对媒介进行信息交换。其中读写终端与有价信息存储媒介相连，本地机与读写终端相连，系统服务器与本地机相连。

[0034] 本实施例中，读写终端为上述实施例的读写终端。其中通信接口单元为USB或RS232通信接口；加解密单元为一微处理器；只读存储单元包括一个以上可单独进行电可擦可编程的只读存储器(如EEPROM、FlashMemory等)模块，分别存储加解密程序、加解密密钥等。本地机为常用的PC机，包括台式机、便携机等，甚至可以是具有上网功能的嵌入式系统装置。系统服务器存储有价存储媒介及其持有人的相关信息，此外，该系统还可以包括网银服务器，用于存储与有价存储媒介持有人相关联的网络银行信息，进行网上银行交易。

[0035] 在下文中，所有的附加技术特征均同时适用于装置实施例、系统实施例，而不再另

行说明。本发明的实现流程包括四个流程：认证流程，付款交易流程、写卡流程、读写终端升级流程和加密流程。

[0036] 一、认证流程

[0037] (1)读写终端自动识别存储媒介的类型；

[0038] (2)存储媒介持有人通过本地机登陆系统浏览器，进行系统服务器与读写终端和存储媒介的关联，并完成读写终端和存储媒介的认证。读写终端和存储媒介不是一对一的，一个读写终端可以识别多种存储媒介，但必须通过合法性验证。

[0039] 图3为本发明读写系统对读写终端进行认证的流程图。如图3所示，系统服务器对读写终端的认证流程包括：

[0040] 步骤S302：存储媒介持有人通过本地机300登陆系统服务器400，输入用户名和口令，确定登陆者身份的唯一性；

[0041] 步骤S304：将读写终端100通过串口与本地机300连接；

[0042] 步骤S306：系统服务器400通过本地机300读取读写终端100身份信息存储单元104中的唯一序列号；

[0043] 步骤S308：序列号经第一加密程序加密后发送至系统服务器400；

[0044] 步骤S310：系统服务器400使用其密钥进行解密；

[0045] 步骤S312：与系统服务器数据库中存储的数据进行对比认证。

[0046] 图4为本发明读写系统对有价信息存储媒介进行认证的流程图。如图4所示，系统服务器对有价信息存储媒介的认证流程包括：

[0047] 步骤S402：存储媒介持有人通过本地机300登陆系统服务器400，输入用户名和口令，确定登陆者身份的唯一性；

[0048] 步骤S404：将读写终端100通过串口与本地机300连接；

[0049] 步骤S406：有价信息存储媒介200与读写终端100连接；

[0050] 步骤S408：有价信息存储媒介200持有人请求系统服务器400验证有价信息存储媒介200合法性；

[0051] 步骤S410：系统服务器400通过本地机300和读写终端100读取有价信息存储媒介200中的唯一序列号；

[0052] 步骤S412：序列号经读写终端100第二只读存储单元103中的第二解密程序和密钥解密；

[0053] 步骤S414：再经第一只读存储单元102中的第一加密程序和密钥加密；

[0054] 步骤S416：发送加密后的唯一序列号至系统服务器400；

[0055] 步骤S418：系统服务器400使用其解密程序和密钥进行解密；

[0056] 步骤S420：与系统服务器400数据库中存储的数据进行对比认证。

[0057] 具体来说，

[0058] 1)系统服务器对读写终端通过第一只读存储单元内的第一加解密程序及密钥进行认证。

[0059] 2)读写终端通过第二只读存储单元内的第二加解密程序和密钥对其进行认证。最后，系统服务器对存储媒介通过读写终端第一只读存储单元内的第一加解密程序及密钥对其进行认证。

[0060] 综上所述，系统服务器通过读写终端第一只读存储器内的第一加解密程序及密钥联合第二只读存储器内的第二加解密程序及密钥对有价信息储存媒介进行认证。

[0061] 二、付款交易流程

[0062] (1)有价信息存储媒介持有人通过本地机、读写终端与网银服务器进行关联，并完成持有人与网银服务器的唯一对应关系；

[0063] (2)有价信息存储媒介持有人通过网银服务器完成其网银账户与系统服务器所有者的网银账户之间的转账支付。

[0064] 图5为本发明读写系统中，有价信息存储媒介持有人通过网银服务器进行付款交易的流程图。如图5所示，本流程包括：

[0065] 步骤S502：有价信息存储媒介200持有人通过本地机300登陆网银服务器500，输入用户名和口令，确定登陆者身份的唯一性；

[0066] 步骤S504：将读写终端100通过串口与本地机300连接；

[0067] 步骤S506：有价信息存储媒介200持有人请求网银服务器500验证读写终端100合法性；

[0068] 步骤S508：网银服务器500通过本地机300读取读写终端100中的唯一序列号；

[0069] 步骤S510：序列号经读写终端100第三只读存储单元101中的第三加密程序和密钥加密；

[0070] 步骤S512：发送加密后的唯一序列号至网银服务器500；

[0071] 步骤S514：网银服务器500使用其解密程序和密钥进行解密；

[0072] 步骤S516：与网银服务器500数据库中存储的数据进行对比认证；

[0073] 步骤S518：有价信息存储媒介200持有人通过本地机300和读写终端100，请求网银服务器500由其网银账户向系统服务器所有者的网银账户转账支付；

[0074] 步骤S520：包含转账支付金额数的请求指令经读写终端100第三只读存储单元101中的第三加密程序和密钥加密；

[0075] 步骤S522：发送加密后的指令至网银服务器500；

[0076] 步骤S524：网银服务器500使用相应的解密程序和密钥进行解密；

[0077] 步骤S526：网银服务器500执行请求指令从有价信息存储媒介200持有人的网银账户向系统服务器所有者的网银账户转账支付。

[0078] 步骤S528：网银服务器500向本地机300发送转账信息。转账失败，重复付款交易流程。转账成功，网银服务器500向系统服务器400发送写数指令。

[0079] 三、写数据流程

[0080] (1)交易完成后，系统服务器发出向有价信息存储媒介写数据的指令；

[0081] (2)读写终端通过本地机发出写数据成功的反馈信息。

[0082] 图6为本发明读写系统中，对有价信息存储媒介进行写数据的流程图。如图6所示，本流程包括：

[0083] 步骤S602；系统服务器400接收到网银服务器500充值指令后，使用其加密程序和密钥进行加密；

[0084] 步骤S604；系统服务器400发送加密后的充值指令，经本地机300到读写终端100；

[0085] 步骤S606；加密的充值指令经读写终端100第一只读存储单元102中的第一解密程

序和密钥解密；

[0086] 步骤S608；解密后的充值指令经读写终端100第二只读存储单元103中的第二加密程序和密钥加密；

[0087] 步骤S610；使用媒介读写单元105向存储媒介200写入加密后的充值数据；

[0088] 步骤S612；读写终端100向本地机300发送写数据信息。写数据失败，读写终端100通过本地机300向系统服务器400发送重复写数据流程。转账成功，写数据流程结束。

[0089] 四、读写终端软件功能升级流程

[0090] (1)有价信息存储媒介持有人通过本地机打开系统服务器浏览器向系统服务器发出读写终端软件功能升级申请；

[0091] (2)系统服务器完成读写终端的认证(验证读写终端的合法性)；

[0092] (3)系统服务器通过本地机发送升级软件程序至读写终端对应的电可擦可编程存储器模块；

[0093] (4)读写终端根据该升级软件程序对自身的软件进行升级；

[0094] (5)读写终端向本地机反馈信息存储成功信息。

[0095] 五、加密过程

[0096] 本发明中，读写终端的特点是独立的只读存储器(ROM)中存储了对系统服务器、有价信息存储媒介和网银服务器进行数据加解密的、相对独立的加解密程序和加解密钥匙。三方的数据只在读写终端的随机存储器(RAM)中进行数据共享。

[0097] 图7为本发明实施例读写终端与系统服务器进行数据安全传输的示意图。根据图7，本实施例读写终端与系统服务器进行数据安全传输包括以下步骤：

[0098] 步骤S702：读写终端先用Hash算法对发送信息(明文)进行运算，形成数据摘要，并用自己的私有密钥对其加密，从而形成数字签名；

[0099] 步骤S704：读写终端再把数字签名及自己的数字证书附在明文后面；

[0100] 步骤S706：读写终端随机产生的对称密钥对明文进行加密，形成密文；

[0101] 步骤S78：为了把读写终端随机产生的对称密钥安全送达系统服务器，

[0102] 使用读写终端和系统服务器的公开密钥对其进行加密，形成数字信封；

[0103] 步骤S710：读写终端最后把密文和数字信封一起发给系统服务器；

[0104] 步骤S712：系统服务器收到读写终端传来的密文和数字信封后，先用自己的私有密钥对数字信封进行解密，从而获得读写终端的对称密钥；

[0105] 步骤S714：再用该密钥对密文进行解密，继而得到明文、读写终端的数字签名及用户的数字签名。

[0106] 由上述流程可知，鉴于对称密钥和公开密钥加密技术的特点，本系统采用两种加密技术相结合，即结合使用DES(对称密钥)和RSA(公开密钥)，对网络中传输的数据用DES加密，而加密用的密钥则使用RSA加密传送，此方法既保证了数据的安全又提高了加密和解密的速度。

[0107] 具体而言，本发明的加解密过程具有如下特点：

[0108] (1)有价信息存储媒介与读写终端加密是由读写终端内的加密模块实现，加密模块的存储器里存储加密程序和加密密钥。信息交换数据加密一般采用对称加密方式(如3DES等)，用于加解密的钥匙及加解密程序分别存储于独立的电可擦可编程只读存储器块

中。

[0109] (2)读写终端与系统服务器信息交换数据加密一般采用非对称加密方式(如RSA等),用于加解密的公、私钥匙及加解密程序分别存储于独立的电可擦可编程只读存储器模块中。

[0110] (3)网银服务器与本地机之间信息交换数据加密遵循银行的数据加密规则,用于加解密的钥匙及加解密程序分别存储于读写终端中的独立的电可擦可编程只读存储器模块中。

[0111] (4)在读写终端中,由独立存储在电可擦可编程存储器中的解密程序及密钥解密后的数据受内置的操作程序控制,也就是说只读存储器中的解密程序及密钥解密后的数据都会自行地暂存于随机存储器中,可用于同系统服务器、网银服务器及有价信息存储媒介间的数据共享。

[0112] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步详细说明。所应理解的是,以上所述仅为本发明的具体实施例而已,并不用于限制本发明,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

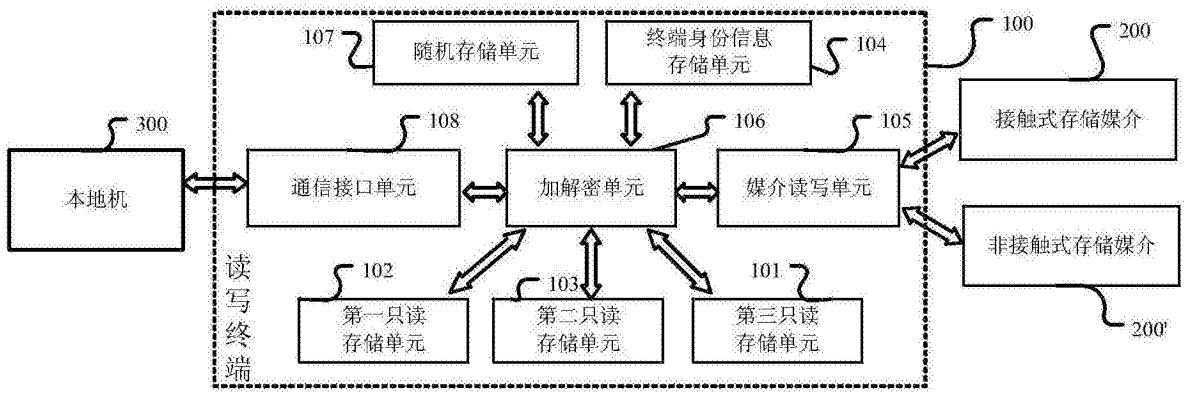

107
随机存储单元
终端身份信息
存储单元
104
100
200
接触式存储媒介
300
本地机
108
通信接口单元
加解密单元
106
媒介读写单元
105
非接触式存储媒介
200'
读写终端
102
第一只读
存储单元
103
第二只读
存储单元
101
第三只读
存储单元

图1

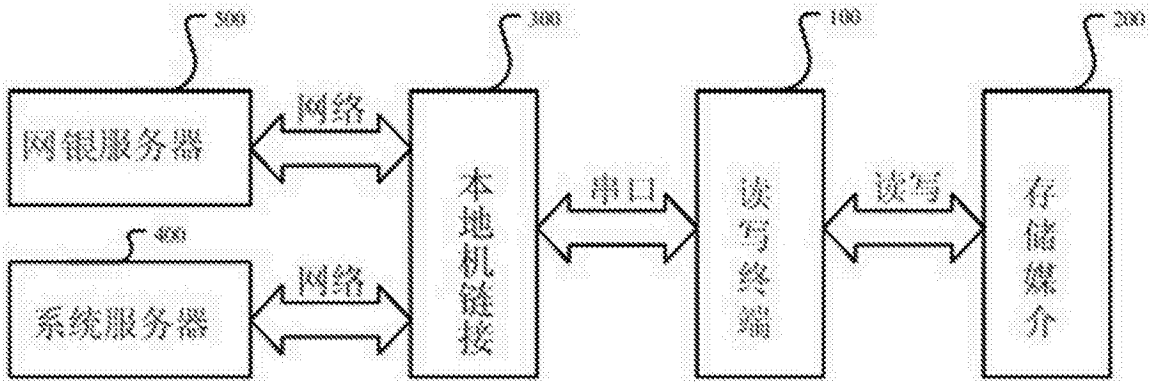

网银服务器
网络
本地机链接
串口
读写终端
读写
存储媒介
系统服务器
网络

图2

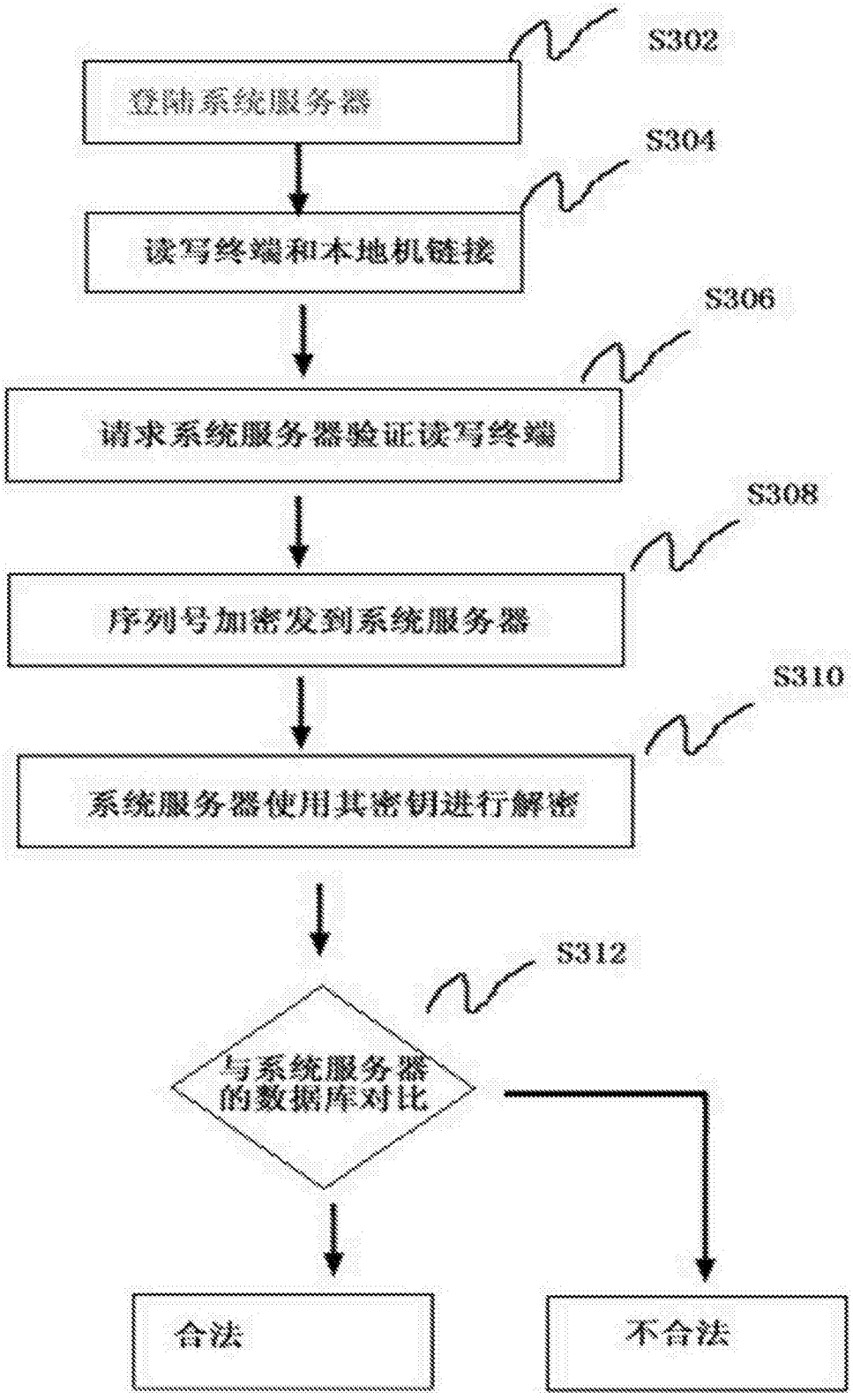

S302
登陆系统服务器
S304
读写终端和本地机链接
S306
请求系统服务器验证读写终端
S308
序列号加密发到系统服务器
S310
系统服务器使用其密钥进行解密
S312
与系统服务器的数据库对比
合法
不合法

图3

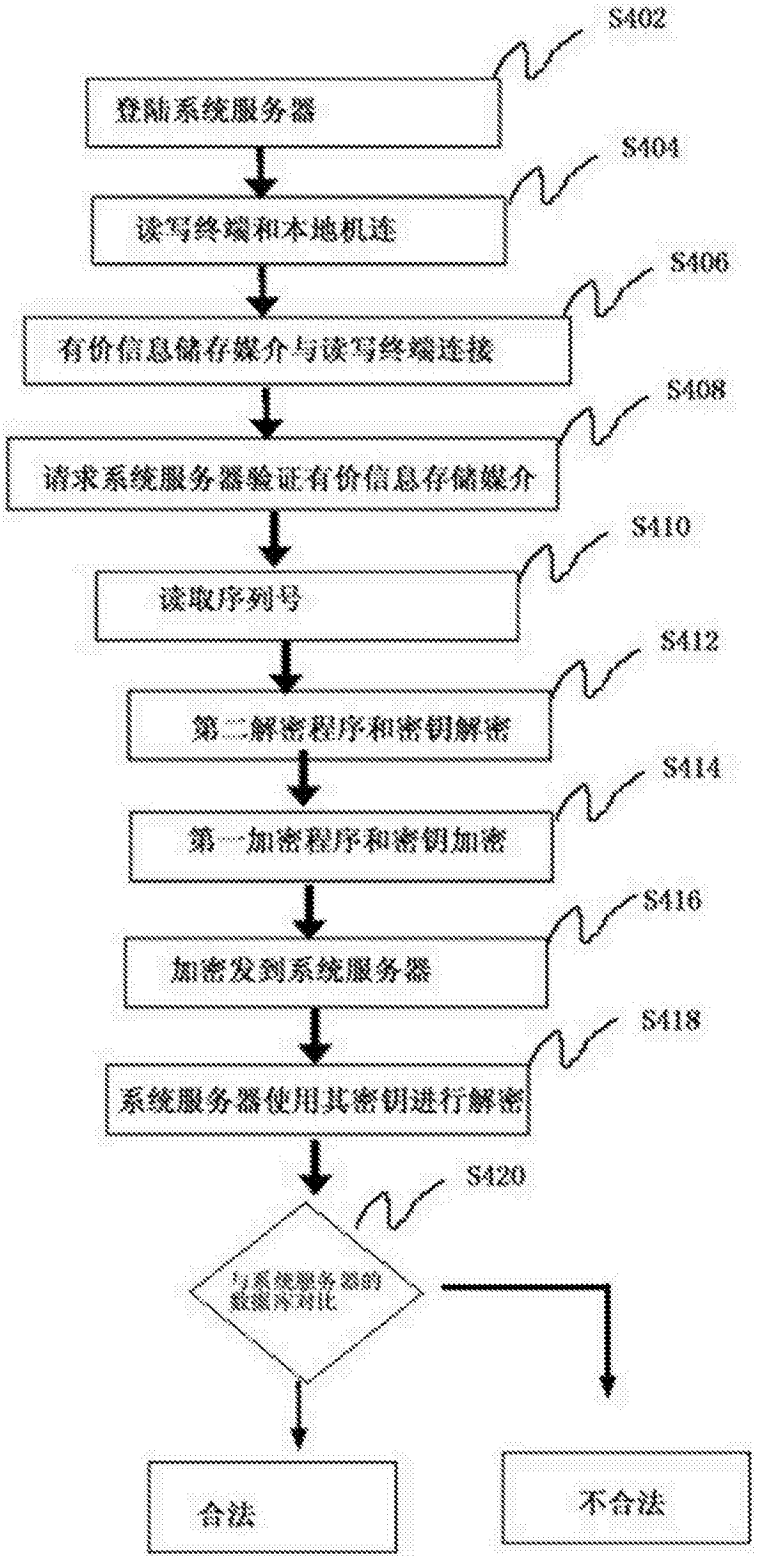

S402
登陆系统服务器
S404
读写终端和本地机连
S406
有价信息储存媒介与读写终端连接
S408
请求系统服务器验证有价信息存储媒介
S410
读取序列号
S412
第二解密程序和密钥解密
S414
第一加密程序和密钥加密
S416
加密发到系统服务器
S418
系统服务器使用其密钥进行解密
S420
合法
不合法

图4

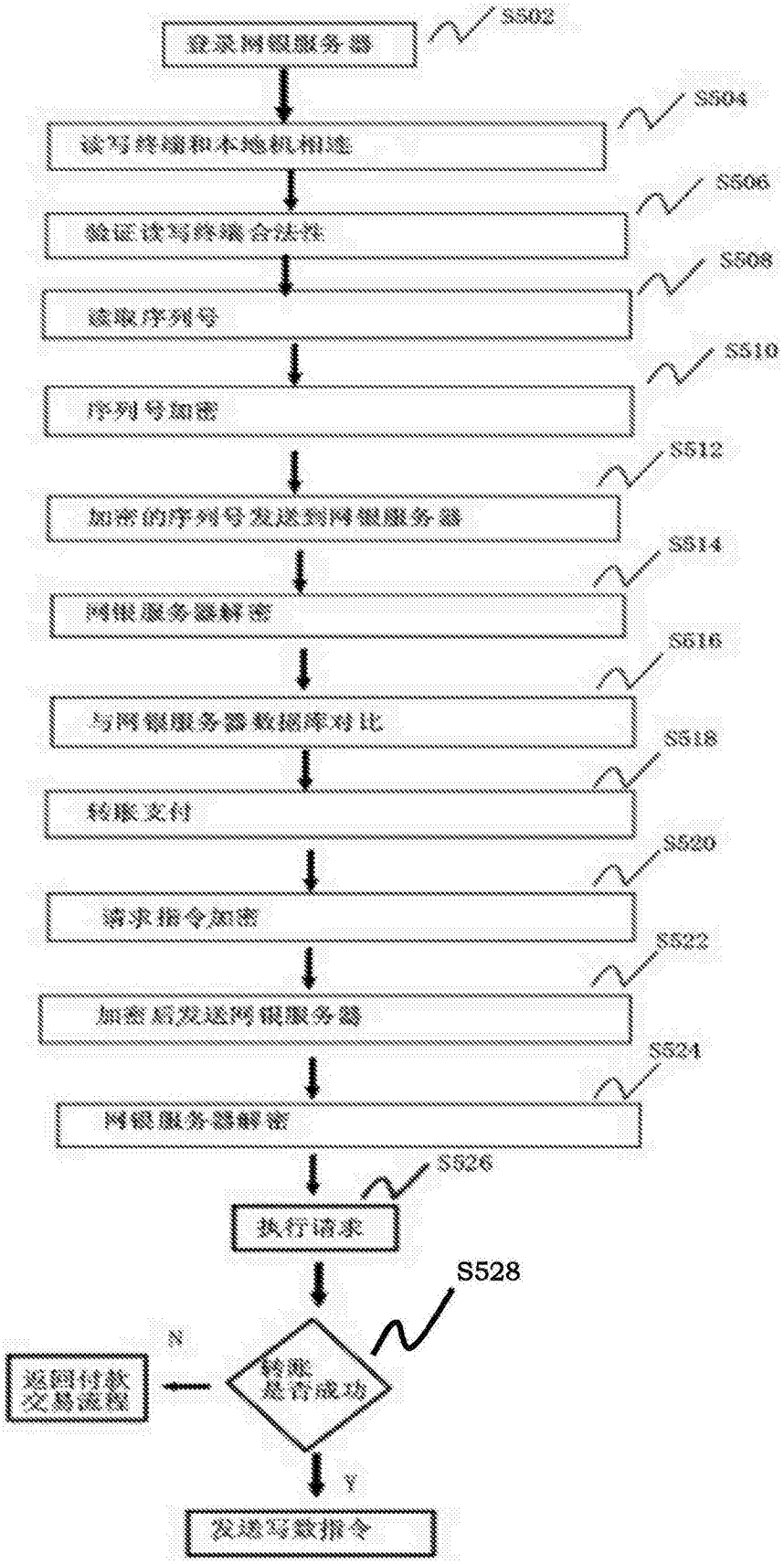

登录网银服务器
S502
读写终端和本地机相连
S504
验证读写终端合法性
S506
读取序列号
S508
序列号加密
S510
加密的序列号发送到网银服务器
S512
网银服务器解密
S514
与网银服务器数据库对比
S516
转账支付
S518
请求指令加密
S520
加密后发送网银服务器
S522
网银服务器解密
S524
执行请求
S526
转账是否成功
S528
N
返回付款交易流程
Y
发送写数指令

图5

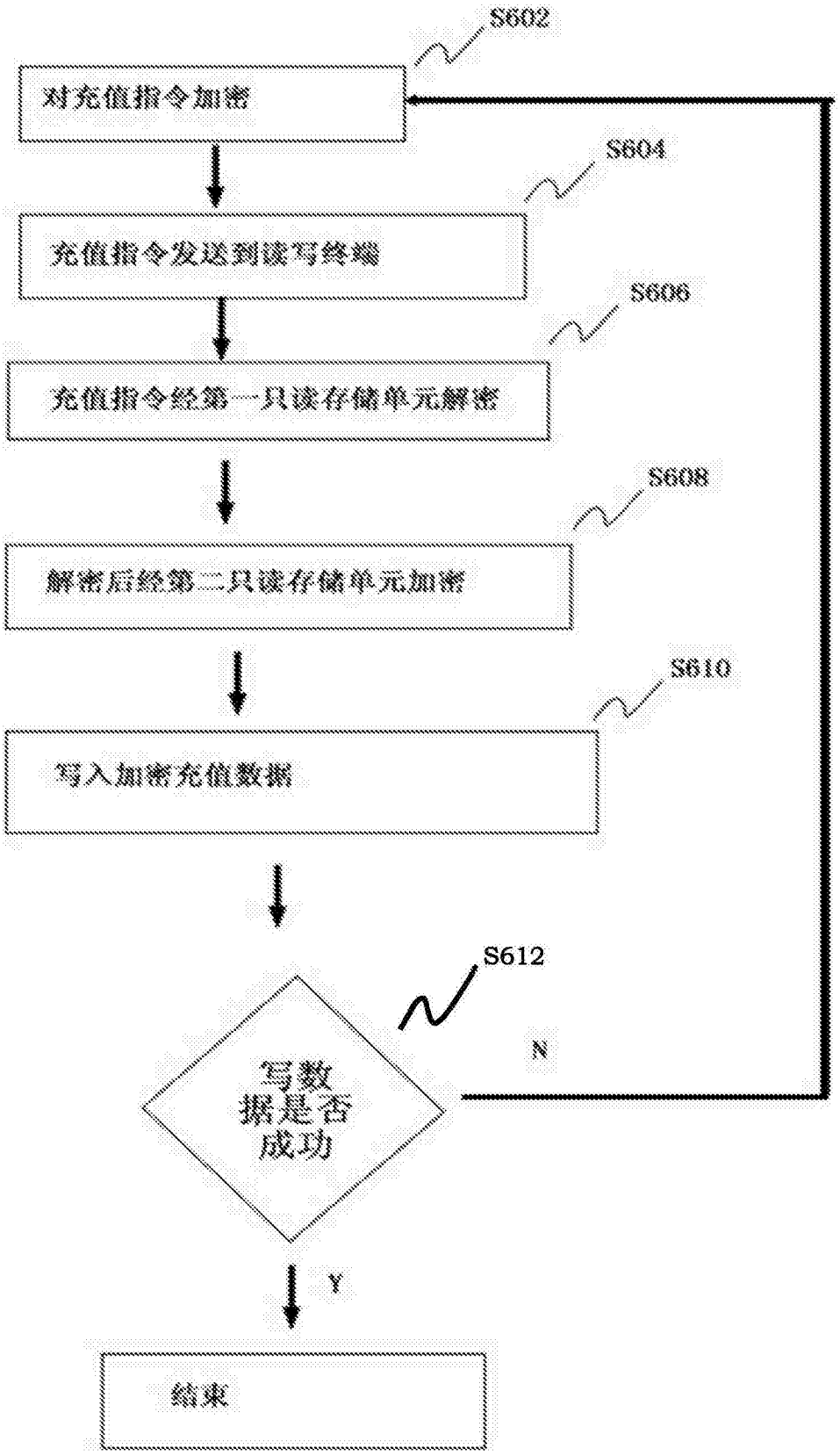

S602
对充值指令加密
S604
充值指令发送到读写终端
S606
充值指令经第一只读存储单元解密
S608
解密后经第二只读存储单元加密
S610
写入加密充值数据
S612
写数据是否成功
N
Y
结束

图6

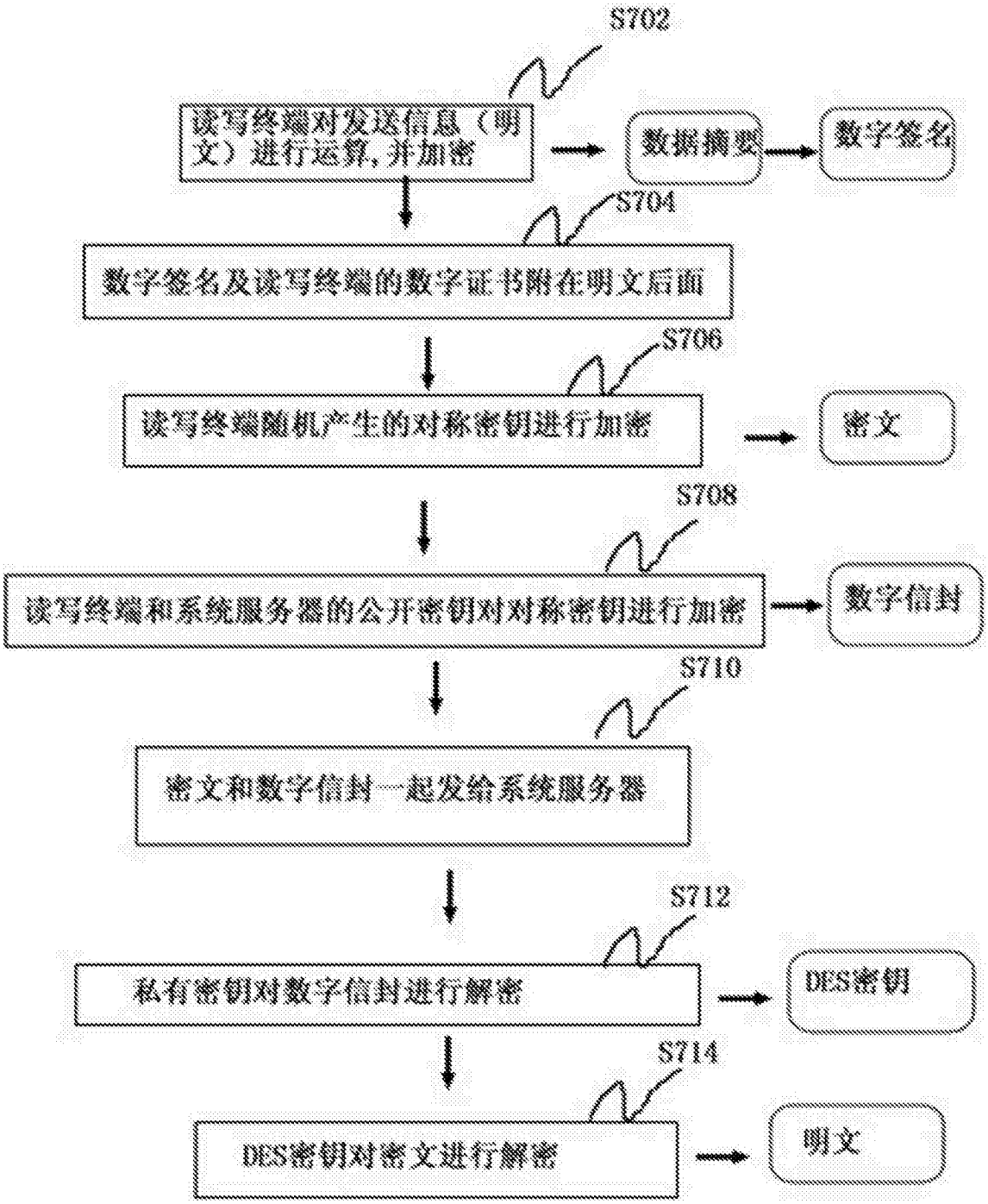

S702
读写终端对发送信息（明文）进行运算，并加密
数据摘要
数字签名
S704
数字签名及读写终端的数字证书附在明文后面
S706
读写终端随机产生的对称密钥进行加密
密文
S708
读写终端和系统服务器的公开密钥对对称密钥进行加密
数字信封
S710
密文和数字信封一起发给系统服务器
S712
私有密钥对数字信封进行解密
DES密钥
S714
DES密钥对密文进行解密
明文

图7