(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 102118745 A
(43)申请公布日 2011.07.06

(21)申请号 201110008673.8

(22)申请日 2011.01.14

(71)申请人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号

(72)发明人 石磊 杨秀芬 张黎清 王禹 王玉生

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 任默闻

(51)Int.Cl.
H04W 12/02(2009.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

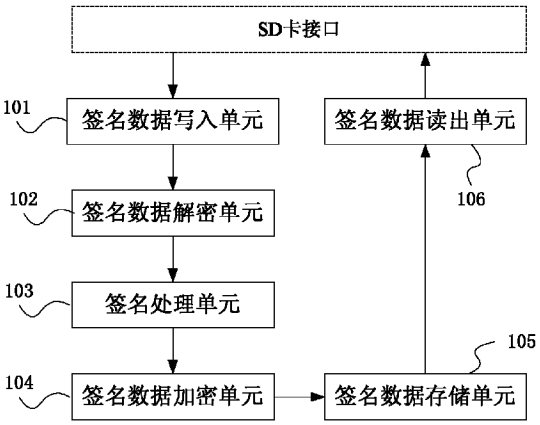
权利要求书 2 页 说明书 8 页 附图 9 页

(54)发明名称

一种移动支付数据安全加密方法、装置及手机

(57)摘要

本发明提供一种移动支付数据安全加密方法、装置及手机，该装置包括：签名数据写入单元，根据写文件指令将移动通信设备传来的已加密的移动支付数据和证书密码数据写入虚拟输入文件；签名数据解密单元，读取移动支付数据和证书密码数据并解密；签名处理单元，对证书密码进行认证，并对移动支付数据进行签名处理；签名数据加密单元，对移动支付数据加密；签名数据存储单元，将加密后的签名的移动支付数据存储到虚拟输出文件；签名数据读出单元，从虚拟输出文件中读取加密后的签名的移动支付数据经SD卡接口传送给移动通信设备。以实现对手机银行移动支付数据的硬件签名，并提高手机签名的安全性。



CN 102118745 A

1. 一种移动支付数据安全加密方法，其特征是，所述的方法包括：

通过安全数码 SD 卡接口接收移动通信设备传来的写文件指令；

根据所述的写文件指令将所述移动通信设备经所述的 SD 卡接口传来的已加密的移动支付数据和证书密码数据写入虚拟输入文件；

从所述的虚拟输入文件中读取所述的已加密的移动支付数据和证书密码数据，并进行解密处理；

对解密后证书密码数据进行认证，认证通过后对解密后的移动支付数据进行签名处理；

对签名的移动支付数据进行加密处理；

将加密后的签名的移动支付数据存储到虚拟输出文件；

经所述的 SD 卡接口接收移动通信设备传来的读文件指令；

根据所述的读文件指令从所述的虚拟输出文件中读取加密后的签名的移动支付数据经所述的 SD 卡接口传送给所述的移动通信设备。

2. 一种移动支付数据安全加密方法，其特征是，所述的方法包括：

通过无线通信网络从银行服务器接收需要签名的移动支付数据；

通过用户界面接收用户输入的证书密码数据；

对所述的移动支付数据和证书密码数据进行加密处理；

通过安全数码 SD 卡接口将所述的已加密的移动支付数据和证书密码数据写入虚拟输入文件；

从所述的虚拟输入文件中读取所述的已加密的移动支付数据和证书密码数据，并进行解密处理；

对解密后的移动支付数据和证书密码数据进行签名处理；

对签名的移动支付数据进行加密处理；

将加密后的签名的移动支付数据存储到虚拟输出文件；

经所述的 SD 卡接口从所述的虚拟输出文件中读取加密后的签名的移动支付数据；

对所述的加密后的签名的移动支付数据进行解密处理；

将解密后的签名的移动支付数据经无线通信网络发送给所述的银行服务器。

3. 一种移动支付数据安全加密装置，其特征是，所述的装置包括：

签名数据写入单元，用于通过安全数码 SD 卡接口接收移动通信设备传来的写文件指令，根据所述的写文件指令将所述移动通信设备经所述的 SD 卡接口传来的已加密的移动支付数据和证书密码数据写入虚拟输入文件；

签名数据解密单元，用于从所述的虚拟输入文件中读取所述的已加密的移动支付数据和证书密码数据，并进行解密处理；

签名处理单元，用于对解密后的证书密码数据进行认证，认证通过后对解密后的移动支付数据进行签名处理；

签名数据加密单元，用于对签名的移动支付数据进行加密处理；

签名数据存储单元，用于将加密后的签名的移动支付数据存储到虚拟输出文件；

签名数据读出单元，用于经所述的 SD 卡接口接收移动通信设备传来的读文件指令，根据所述的读文件指令从所述的虚拟输出文件中读取加密后的签名的移动支付数据经所述

的 SD 卡接口传送给所述的移动通信设备。

4. 一种移动支付数据安全加密手机，所述的手机包括：手机本体；其特征是，所述的手机还包括：移动支付安全数码 SD 卡；

所述的移动支付 SD 卡通过 SD 卡接口与所述的手机本体相连接；

所述的移动支付 SD 卡包括：

移动支付数据下载单元，用于通过无线通信网络从银行服务器接收需要签名的移动支付数据；

密码输入单元，用于通过用户界面接收用户输入的证书密码数据；

第一加密单元，用于对所述的移动支付数据和证书密码数据进行加密处理；

签名数据写入单元，用于通过安全数码 SD 卡接口将所述的已加密的移动支付数据和证书密码数据写入虚拟输入文件；

第二解密单元，用于从所述的虚拟输入文件中读取所述的已加密的移动支付数据和证书密码数据，并进行解密处理；

签名处理单元，用于对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理；

第二加密单元，用于对签名的移动支付数据进行加密处理；

签名数据存储单元，用于将加密后的签名的移动支付数据存储到虚拟输出文件；

签名数据读出单元，用于经所述的 SD 卡接口从所述的虚拟输出文件中读取加密后的签名的移动支付数据；

第一解密单元，用于对所述的加密后的签名的移动支付数据进行解密处理；

签名数据发送单元，用于将解密后的签名的移动支付数据经无线通信网络发送给所述的银行服务器。

一种移动支付数据安全加密方法、装置及手机

技术领域

[0001] 本发明关于硬件数字证书技术，特别是关于在手机等移动设备上使用的硬件数字证书技术，具体的讲是一种移动支付数据安全加密方法、装置及手机。

背景技术

[0002] 在现有技术中，手机银行业务签名方式有如下几种：

[0003] （一）使用存放在手机内存中的软证书签名。这种方式虽然能够实现数字签名功能，但软件层面的数字证书非常容易因系统漏洞或系统中被植入的木马、病毒等软件非法读取而失密。

[0004] （二）使用短签名技术的独立动态口令生成装置。这种方式虽然能够实现基本的签名功能，但其操作繁琐，携带不方便，生产成本较高，不利于推广。

[0005] （三）将数字证书存放到SIM卡中。这种方式虽然能够实现签名功能，但该卡片需要由电信运营商发行、密钥只有电信运营商才能够写入，且不同型号的手机读取SIM卡中数据的接口大多不相同，银行需要根据手机型号开发出多款证书读写的驱动程序，安全性较差，推广难度大。

发明内容

[0006] 本发明实施例提供了一种移动支付数据安全加密方法、装置及手机，以实现对手机银行移动支付数据的硬件签名，并提高手机签名的安全性。

[0007] 本发明的目的之一是，提供一种移动支付数据安全加密方法，该方法包括：通过安全数码SD卡接口接收移动通信设备传来的写文件指令；根据写文件指令将移动通信设备经所述的SD卡接口传来的已加密的移动支付数据和证书密码数据写入虚拟输入文件；从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理；对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理；对签名的移动支付数据进行加密处理；将加密后的签名的移动支付数据存储到虚拟输出文件；经SD卡接口接收移动通信设备传来的读文件指令；根据读文件指令从虚拟输出文件中读取加密后的签名的移动支付数据经所述的SD卡接口传送给移动通信设备。

[0008] 本发明的目的之一是，提供一种移动支付数据安全加密方法，该方法包括：通过无线通信网络从银行服务器接收需要签名的移动支付数据；通过用户界面接收用户输入的证书密码数据；对移动支付数据和证书密码数据进行加密处理；通过安全数码SD卡接口将已加密的移动支付数据和证书密码数据写入虚拟输入文件；从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理；对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理；对签名的移动支付数据进行加密处理；将加密后的签名的移动支付数据存储到虚拟输出文件；经SD卡接口从虚拟输出文件中读取加密后的签名的移动支付数据；对加密后的签名的移动支付数据进行解密处理；将解密后的签名的移动支付数据经无线通信网络发送给银行服务器。

[0009] 本发明的目的之一是，提供一种移动支付数据安全加密装置，该装置包括：签名数据写入单元，用于通过安全数码 SD 卡接口接收移动通信设备传来的写文件指令，根据写文件指令将移动通信设备经 SD 卡接口传来的已加密的移动支付数据和证书密码数据写入虚拟输入文件；签名数据解密单元，用于从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理；签名处理单元，用于对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理；签名数据加密单元，用于对签名的移动支付数据进行加密处理；签名数据存储单元，用于将加密后的签名的移动支付数据存储到虚拟输出文件；签名数据读出单元，用于经 SD 卡接口接收移动通信设备传来的读文件指令，根据读文件指令从虚拟输出文件中读取加密后的签名的移动支付数据经 SD 卡接口传送给移动通信设备。

[0010] 本发明的目的之一是，提供一种移动支付数据安全加密手机，该手机包括：手机本体和移动支付安全数码 SD 卡；移动支付 SD 卡通过 SD 卡接口与手机本体相连接；移动支付 SD 卡包括：移动支付数据下载单元，用于通过无线通信网络从银行服务器接收需要签名的移动支付数据；证书密码输入单元，用于通过用户界面接收用户输入的证书密码数据；第一加密单元，用于对移动支付数据和证书密码数据进行加密处理；签名数据写入单元，用于通过安全数码 SD 卡接口将已加密的移动支付数据和证书密码数据写入虚拟输入文件；第二解密单元，用于从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理；签名处理单元，用于对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理；第二加密单元，用于对签名的移动支付数据进行加密处理；签名数据存储单元，用于将加密后的签名的移动支付数据存储到虚拟输出文件；签名数据读出单元，用于经 SD 卡接口从虚拟输出文件中读取加密后的签名的移动支付数据；第一解密单元，用于对加密后的签名的移动支付数据进行解密处理；签名数据发送单元，用于将解密后的签名的移动支付数据经无线通信网络发送给银行服务器。

[0011] 本发明的有益效果在于，解决了手机银行硬件数字签名的问题，且不影响原 SD 卡的正常使用功能。且本发明实施例采用了具有个性化接口的专用浏览器，可确保客户数据安全。

附图说明

[0012] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0013] 图 1 为本发明实施例移动支付数据安全加密方法流程图；

[0014] 图 2 为本发明实施例移动支付数据安全加密装置结构框图；

[0015] 图 3 为本发明实施例移动支付数据安全加密 SD 卡的结构图；

[0016] 图 4 为本发明实施例移动支付数据安全加密 SD 卡的工作流程图；

[0017] 图 5 为本发明实施例移动支付数据安全加密 SD 卡的电路图；

[0018] 图 6 为本发明实施例的手机移动支付数据安全加密方法流程图；

[0019] 图 7 为本发明实施例移动支付数据安全加密手机结构框图；

[0020] 图 8 为本发明实施例手机移动支付数据安全加密 SD 卡的结构图；

[0021] 图 9 为本发明实施例手机和移动支付数据安全加密 SD 卡的连接示意图；

[0022] 图 10 为本发明实施例移动支付数据安全加密手机工作流程图；

[0023] 图 11 为本发明实施例手机移动支付数据安全加密 SD 卡的浏览器结构图。

具体实施方式

[0024] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0025] 如图 1 所示，本实施例的移动支付数据安全加密方法包括：通过安全数码 (SD) 卡接口接收移动通信设备传来的写文件指令（步骤 S101）；根据写文件指令将移动通信设备经 SD 卡接口传来的已加密的移动支付数据和证书密码数据写入虚拟输入文件（步骤 S102）；从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理（步骤 S103）；对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理（步骤 S104）；对签名的移动支付数据进行加密处理（步骤 S105）；将加密后的签名的移动支付数据存储到虚拟输出文件（步骤 S106）；经 SD 卡接口接收移动通信设备传来的读文件指令（步骤 S107）；根据读文件指令从虚拟输出文件中读取加密后的签名的移动支付数据经 SD 卡接口传送给移动通信设备（步骤 S108）。

[0026] 如图 2 所示，本实施例的移动支付数据安全加密装置包括：签名数据写入单元 101，用于通过安全数码 SD 卡接口接收移动通信设备传来的写文件指令，根据写文件指令将移动通信设备经 SD 卡接口传来的已加密的移动支付数据和证书密码数据写入虚拟输入文件；签名数据解密单元 102，用于从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理；签名处理单元 103，用于对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理；签名数据加密单元 104，用于对签名的移动支付数据进行加密处理；签名数据存储单元 105，用于将加密后的签名的移动支付数据存储到虚拟输出文件；签名数据读出单元 106，用于经 SD 卡接口接收移动通信设备传来的读文件指令，根据读文件指令从虚拟输出文件中读取加密后的签名的移动支付数据经 SD 卡接口传送给移动通信设备。

[0027] 如图 3 所示，本实施例的移动支付数据安全加密装置的硬件包括一个 SD 卡接口，一个单片机，一个存储芯片，一个加解密模块，一个签名模块及其它外围元件。将所有元件集成在一块 mincro SD 卡大小的外壳内，制成本实施例的移动支付数据安全加密装置。

[0028] 移动支付数据安全加密装置内部通过单片机内部微码实现主控模块、SD 卡接口模块、装置个性化接口模块（即：加解密模块）、存储模块、签名模块等功能模块。

[0029] 如图 4 所示，主控模块功能：循环读取 SD 卡接口模块中的”读缓冲区”，根据”读缓存区”中的手机命令调度各模块。具体功能如下：

[0030] 当从 SD 卡接口模块收到的手机传来的命令为读一般 SD 卡文件时，调度存储模块将数据存储芯片中的数据读出，然后送到 SD 接口模块中；

[0031] 当从 SD 卡接口模块收到写一般 SD 卡文件时，判断该文件是否为只读文件，如果为

只读文件，则返回写保护错，如果为正常文件，则调度存储模块将数据写入到存储芯片中，然后通知 SD 接口模块操作成功。

[0032] 当从 SD 卡接口模块收到的手机传来的命令为写虚拟文件命令时，调用装置个性化接口模块对收到的数据进行解密处理，解密成功后，送签名模块对数据中的证书密码进行认证，认证通过后对数据中待签名数据进行签名，签名成功的数据经装置个性化接口模块加密后保存在已签名数据缓冲区，解密失败后，将签名的标记写入到已签名数据缓冲区，供手机读取。

[0033] 当从 SD 卡接口模块收到的手机传来的命令为读虚拟文件命令时，至已签名数据缓冲区中取回已签名数据，返回给 SD 卡接口模块。

[0034] SD 卡接口模块功能：当手机需要读写 SD 卡时，将会向 SD 卡的 CLK 端口发送时钟信号，每发送一个时钟信号时由 CMD 端口向 SD 卡写入数据或由 DATA 端口从 SD 卡中读取数据。本装置在设计时，将 CLK 端口接入到单片机的中断接口 INT0，每当手机向 SD 卡发送一个时钟信号时，单片机中断会自动调本 SD 卡接口模块。根据手机发送的命令，将手机的发送来的数据保存该模块读缓存中或将写缓存中的数据发送至手机。

[0035] 存储模块功能：接收主控模块传来的读写指令及要写入的数据，根据指令读出或写入数据至存储模块。存储芯片分成三部分，分别为：读写区、只读区、内部区。其中读写区为客户存放文件的区域，该区域中的数据客户可以通过手机自由读写。只写区域为银行专用区，该区域中的数据只能由银行在生产该 SD 卡时写入，客户无法自行修改，该区域一般用来存放客户专用浏览器程序，客户可以通过手机查看或运行该区域内的程序，但如果客户要修改或删除该区域内的内容时，将会报写保护错误。内部区为本装置自己保留使用的区域，客户无法通过手机访问到该区域，该区域可以用于保存已签名数据及客户证书等数据。

[0036] 个性化接口模块功能（即：加解密模块）：接收主控模块传来的签名命令及数据。将数据采用该模块内部的个性解密程序进行解密，并将解密成功后的数据通过主控模块传送给签名模块进行签名操作。个性化解密程序由已知的多个加密算法的源代码（如 DES、3DES、RC2、RC4，IDEA、DSA、AES、BLOWFISH、ElGamal、Diffie-Hellman、TEA、RAS）中的一部分，经随机排列组合，生成的复合加密算法，并为每种算法随机生成唯一密钥。该算法排列组合方式为本装置生产过程中随机生成，并自动编译，该算法及密钥与存放在存储芯片中只读区的浏览器程序中的浏览器个性化接口模块相同。实现不同的装置的算法不同、密钥不同，保证了客户必须使用本装置上的浏览器才能访问本装置的签名模块。

[0037] 签名模块功能：与现银行使用的 USB-KEY 的签名模块功能相同。当签名模块接收到主控模块传来的待签名数据后，使用 RAS 算法，根据客户私钥对数据进行签名，签名完成后，将生成的数据返传给主控模块。

[0038] 如图 5 所示，单片机可以使用 89C51 系列单片机，SD 卡接口直接与单片机 P1 口相联，用于支持单片机与 SD 卡通讯。其中 SD 卡的 CLK 端口与单片机的 INT0 端口相联，通过从手机中接入的时钟信号，调用单片机中断，由中断程序控制 P1 口电位来达到接收或发送数据至手机的功能。单片机的 P0 口联接存储芯片的 IO 接口，P2 口联接存储芯片（FLASH 芯片）的其它端口。当单片机需要读写存储在存储芯片中的数据时，通过 P2 接口向存储芯片传送读写命令，通过 P0 读写存储芯片中的数据。单片机的 X1、X2 联接晶振电路，单片机

RESET 接复位电路。

[0039] 如图 6 所示，本实施例的移动支付数据安全加密方法包括：通过无线通信网络从银行服务器接收需要签名的移动支付数据（步骤 S201）；通过用户界面接收用户输入的证书密码数据（步骤 S202）；对移动支付数据和证书密码数据进行加密处理（步骤 S203）；通过安全数码 SD 卡接口将已加密的移动支付数据和证书密码数据写入虚拟输入文件（步骤 S204）；从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理（步骤 S205）；对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理（步骤 S206）；对签名的移动支付数据进行加密处理（步骤 S207）；将加密后的签名的移动支付数据存储到虚拟输出文件（步骤 S208）；经 SD 卡接口从虚拟输出文件中读取加密后的签名的移动支付数据（步骤 S209）；对加密后的签名的移动支付数据进行解密处理（步骤 S210）；将解密后的签名的移动支付数据经无线通信网络发送给银行服务器（步骤 S2110）。

[0040] 如图 7 所示，本实施例的移动支付数据安全加密手机包括：手机本体和移动支付安全数码 SD 卡；移动支付 SD 卡通过 SD 卡接口与手机本体相连接；移动支付 SD 卡包括：移动支付数据下载单元 207，用于通过无线通信网络从银行服务器接收需要签名的移动支付数据；证书密码输入单元 208，用于通过用户界面接收用户输入的证书密码数据；第一加密单元 209，用于对移动支付数据和证书密码数据进行加密处理；签名数据写入单元 201，用于通过安全数码 SD 卡接口将已加密的移动支付数据和证书密码数据写入虚拟输入文件；第二解密单元 202，用于从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理；签名处理单元 203，用于对解密后的证书密码数据进行认证通过后对解密后的移动支付数据进行签名处理；第二加密单元 204，用于对签名的移动支付数据进行加密处理；签名数据存储单元 205，用于将加密后的签名的移动支付数据存储到虚拟输出文件；签名数据读出单元 206，用于经 SD 卡接口从虚拟输出文件中读取加密后的签名的移动支付数据；第一解密单元 210，用于对加密后的签名的移动支付数据进行解密处理；签名数据发送单元 211，用于将解密后的签名的移动支付数据经无线通信网络发送给银行服务器。

[0041] 如图 8 所示，本移动支付 SD 卡 100 在外观上与一个普通的 mincro SD 卡没有区别。该本移动支付 SD 卡除了提供数字签名功能外，还提供了存储功能和浏览器模块，客户完全可以将本本移动支付 SD 卡当成一块普通的 SD 卡使用，不改变客户的使用习惯。该移动支付 SD 卡可以直接插入到手机的 SD 卡接口中，携带方便。

[0042] 如图 9 所示，本实施例手机 200 的移动支付 SD 卡 100，采用手机支持的 SD 卡接口与手机进行通讯，所有与手机间的数据传输过程都模拟成文件读写操作，通过在手机中运行的 java 浏览器程序读取 SD 卡中的虚拟文件实现数据签名操作。由于现有手机中绝大多数都具有 SD 卡接口且支持 JAVA，所以本 SD 卡非常容易推广。

[0043] 1) 本实施例手机的移动支付 SD 卡硬件电路说明

[0044] 本移动支付 SD 卡硬件包括一个 SD 卡接口，一个单片机，一个存储芯片及其它外围元件。将所有元件集成在一块 mincro SD 卡大小的外壳内，制成本装置。单片机可以使用 89C51 系列单片机，SD 卡接口直接与单片机 P1 口相联，用于支持单片机与 SD 卡通讯。其中 SD 卡的 CLK 端口与单片机的 INT0 端口相联。如图 10 所示，通过从手机中接入的时钟信号，调用单片机中断，由中断程序控制 P1 口电位来达到接收或发送数据至手机的功能。单片机

的 P0 口联接存储芯片的 IO 接口，P2 口联接 FLASH 芯片的其它端口。当单片机需要读写存储在存储芯片中的数据时，通过 P2 接口向存储芯片传送读写命令，通过 P0 读写存储芯片中的数据。单片机的 X1、X2 联接晶振电路，单片机 RESET 接复位电路。

[0045] 2) 移动支付 SD 卡内各模块说明

[0046] 本移动支付 SD 卡内部通过单片机内部微码实现主控模块、SD 卡接口模块、装置个性化接口模块（加解密模块）、存储模块、签名模块等功能模块。

[0047] 主控模块功能：循环读取 SD 卡接口模块中的"读缓冲区"，根据"读缓存区"中的手机命令调度各模块。具体功能如下：

[0048] 当从 SD 卡接口模块收到的手机传来的命令为读一般 SD 卡文件时，调度存储模块将数据存储芯片中的数据读出，然后送到 SD 接口模块中；

[0049] 当从 SD 卡接口模块收到写一般 SD 卡文件时，判断该文件是否为只读文件，如果为只读文件，则返回写保护错，如果为正常文件，则调度存储模块将数据写入到存储芯片中，然后通知 SD 接口模块操作成功。

[0050] 当从 SD 卡接口模块收到的手机传来的命令为写虚拟文件命令时，调用装置个性化接口模块对收到的数据进行解密处理，解密成功后，送签名模块对数据中的证书密码进行认证，认证通过后对数据中待签名数据进行签名，签名成功的数据经装置个性化接口模块加密后保存在已签名数据缓冲区，解密失败后，将签名的标记写入到已签名数据缓冲区，供手机读取。

[0051] 当从 SD 卡接口模块收到的手机传来的命令为读虚拟文件命令时，至已签名数据缓冲区中取回已签名数据，返回给 SD 卡接口模块。

[0052] SD 卡接口模块功能：当手机需要读写 SD 卡时，将会向 SD 卡的 CLK 端口发送时钟信号，每发送一个时钟信号时由 CMD 端口向 SD 卡写入数据或由 DATA 端口从 SD 卡中读取数据。本 SD 卡在设计时，将 CLK 端口接入到单片机的中断接口 INT0，每当手机向 SD 卡发送一个时钟信号时，单片机中断会自动调本 SD 卡接口模块。根据手机发送的命令，将手机的发送来的数据保存该模块读缓存中或将写缓存中的数据发送至手机。

[0053] 存储模块功能：接收主控模块传来的读写指令及要写入的数据，根据指令读出或写入数据至存储模块。存储芯片分成三部分，分别为：读写区、只读区、内部区。其中读写区为客户存放文件的区域，该区域中的数据客户可以通过手机自由读写。只写区域为银行专用区，该区域中的数据只能由银行在生产该 SD 卡时写入，客户无法自行修改，该区域一般用来存放客户专用浏览器程序，客户可以通过手机查看或运行该区域内的程序，但如果客户要修改或删除该区域内的内容时，将会报写保护错误。内部区为本 SD 卡自己保留使用的区域，客户无法通过手机访问到该区域，该区域可以用于保存已签名数据及客户证书等数据。

[0054] SD 卡个性化接口模块（加解密模块）功能：接收主控模块传来的签名命令及数据。将数据采用该模块内部的个性解密程序进行解密，并将解密成功后的数据通过主控模块传送给签名模块进行签名操作。个性化解密程序由已知的多个加密算法的源代码（如 DES、3DES、RC2、RC4，IDEA、DSA、AES、BLOWFISH、ElGamal、Diffie-Hellman、TEA、RAS）中的一部分，经随机排列组合，生成的复合加密算法，并为每种算法随机生成唯一密钥。该算法排列组合方式为本装置生产过程中随机生成，并自动编译，该算法及密钥与存放在存储芯

片中只读区的浏览器程序中的浏览器个性化接口模块相同。实现不同的装置的算法不同、密钥不同，保证了客户必须使用本装置上的浏览器才能访问本 SD 卡的签名模块。

[0055] 签名模块功能：与现银行使用的 USB-KEY 的签名模块功能相同。当签名模块接收到主控模块传来的待签名数据后，使用 RAS 算法，根据客户私钥对数据进行签名，签名完成后，将生成的数据返传给主控模块。

[0056] 3) 可实现的功能

[0057] 本 SD 卡不仅具有原 SD 卡功能，还提供一种不可被修改的专用浏览器和签名功能。

[0058] SD 卡功能：当客户使用手机访问 SD 卡时，由本 SD 卡模拟一块 SD 卡为客户服务，客户感觉不到本装置和 SD 卡的区别。不影响客户正常使用扩展存储空间的需要，客户数据保存在存储芯片中读写区域。

[0059] 专用浏览器：是为实现安全访问网银，并在交易过程中使用本 SD 卡签名而专门设计的一款可在手机上运行的 java 软件。该软件存储在存储芯片中只读区域，该区域中的数据不可更改，确保了客户端程序安全。签名时，客户输入的证书密码及客户通过该软件写入 SD 卡中的签名数据都需要通过本软件中内置的浏览器个性化接口模块加密；从 SD 卡中读取的数据都需要通过本软件中内置的浏览器个性化接口模块（加解密模块）解密，该个性化接口模块的加解密算法及密钥和个性化接口模块（加解密模块）相同且该算法及密钥都是在本装置生产过程中随机生成的，完全对外保密，可保证非法客户端无法与本 SD 卡中签名模块通讯（见图 11）。

[0060] 签名功能：在 SD 卡内虚拟出 input 及 output 两个文件，分别作为手机与本装置通讯的写和读接口，当手机中浏览器向 input 文件中写入数据时，将数据送给 SD 卡个性化签名模块解密后进行签名处理，然后保存，当客户从 output 文件中读取数据时，从个性化签名模块中取出数据送给手机。

[0061] 4) 使用方法

[0062] 当客户办理手机银行开户业务时，可以从柜面领取一块本 SD 卡。客户可直接将本 SD 卡安装到手机上的 SD 卡插槽中。这时，可以在客户手机中 SD 卡目录中看到本装置内置的专用浏览器相关文件，及由本 SD 卡虚拟的 input、及 output 两个文件。

[0063] 如图 11 所示，当客户需要通过手机银行办理业务时，需要通过运行 SD 卡上专用浏览器程序，该程序能够自动登陆银行服务器，并展示相关页面，当办理需要签名业务时，手机浏览器将会从银行服务器下载需要签名的数据，然后提示客户输入证书密码，再调用浏览器个性化接口模块对该数据及客户输入的密码进行加密，加密后的数据写到 SD 卡上文件名为 input 的文件中；本 SD 卡读取该数据后，经 SD 卡个性化接口模块解密后，送签名模块对证书密码进行认证，认证成功后进行签名处理，签名后的数据经过 SD 卡个性化接口加密后放到存储区域的内部区中。浏览器通过从 output 文件中读取刚刚保存到存储区域的内部区中的文件，并经浏览器个性化接口（浏览器加 / 解密模块）解密，得到签名后的数据，然后将签名后的数据经网络传送至银行服务器，完成一次签名操作。根据具体的签名算法，一般一笔业务可以通过一次性与本装置通讯模式实现，也可以通过多次与本装置通讯模式实现。

[0064] 5) 使用步骤

[0065] 本装置的使用方法分成如下步骤：

[0066] 步骤 1 :到银行柜面申领本 SD 卡。

[0067] 步骤 2 :将本 SD 卡放到手机 SD 卡插槽中。

[0068] 步骤 3 :运行本 SD 卡中的专用浏览器程序。

[0069] 步骤 4 :办理支付交易,如转账业务,输入对方账号、金额等数据。

[0070] 步骤 5 :浏览器提示客户输入证书密码。

[0071] 步骤 6 :浏览器自动与本 SD 卡通讯,完成数据签名操作。

[0072] 通过使用本发明实施例的方法、装置及手机,在客户的移动设备中存放用户的硬件数字证书,采用接口与移动设备进行通讯,所有与移动设备间的数据传输过程都模拟成文件读写操作,通过在移动设备中运行的浏览器程序读取虚拟文件的方式实现数据签名操作,从而实现了对移动支付的硬件签名,提高了移动支付签名的安全性。

[0073] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想 ;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

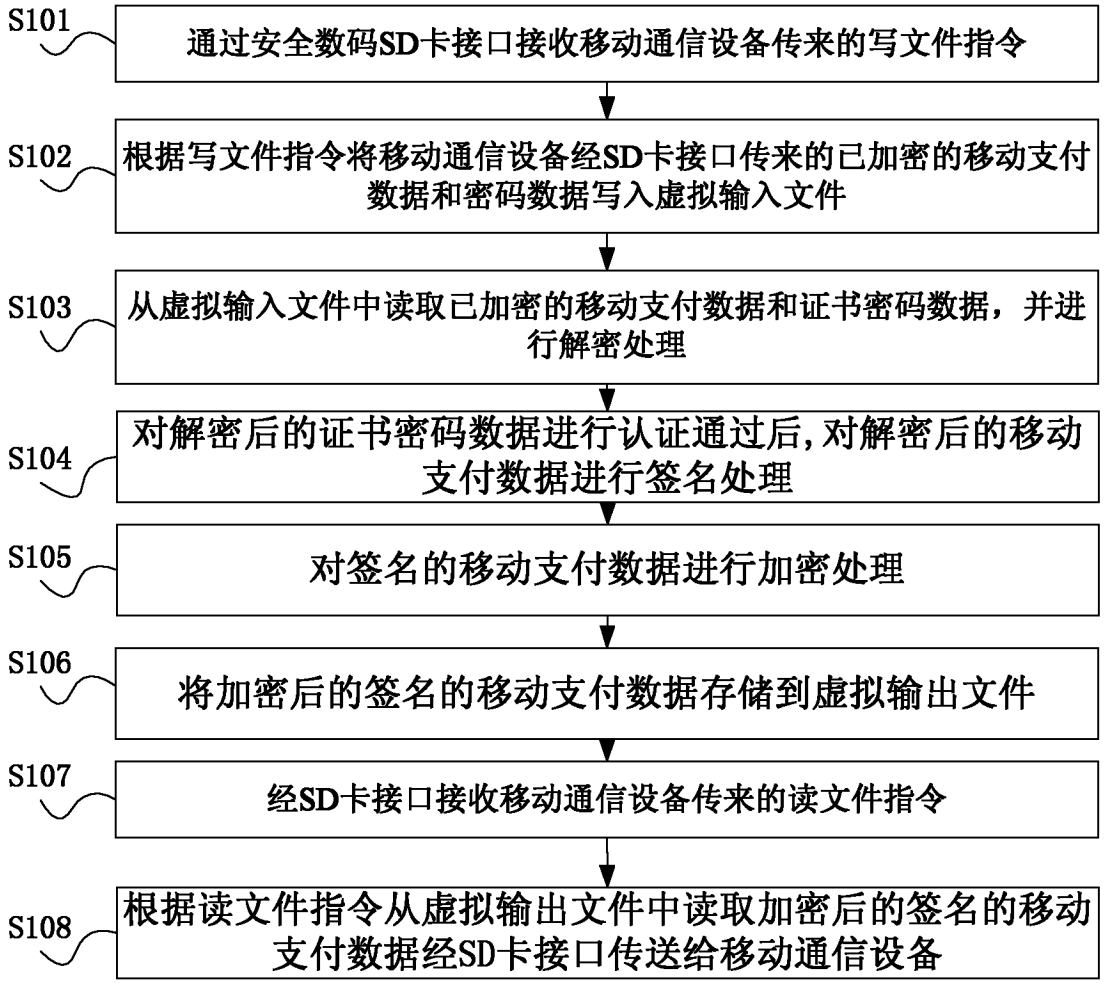

S101
通过安全数码SD卡接口接收移动通信设备传来的写文件指令
S102
根据写文件指令将移动通信设备经SD卡接口传来的已加密的移动支付数据和密码数据写入虚拟输入文件
S103
从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理
S104
对解密后的证书密码数据进行认证通过后，对解密后的移动支付数据进行签名处理
S105
对签名的移动支付数据进行加密处理
S106
将加密后的签名的移动支付数据存储到虚拟输出文件
S107
经SD卡接口接收移动通信设备传来的读文件指令
S108
根据读文件指令从虚拟输出文件中读取加密后的签名的移动支付数据经SD卡接口传送给移动通信设备

图 1

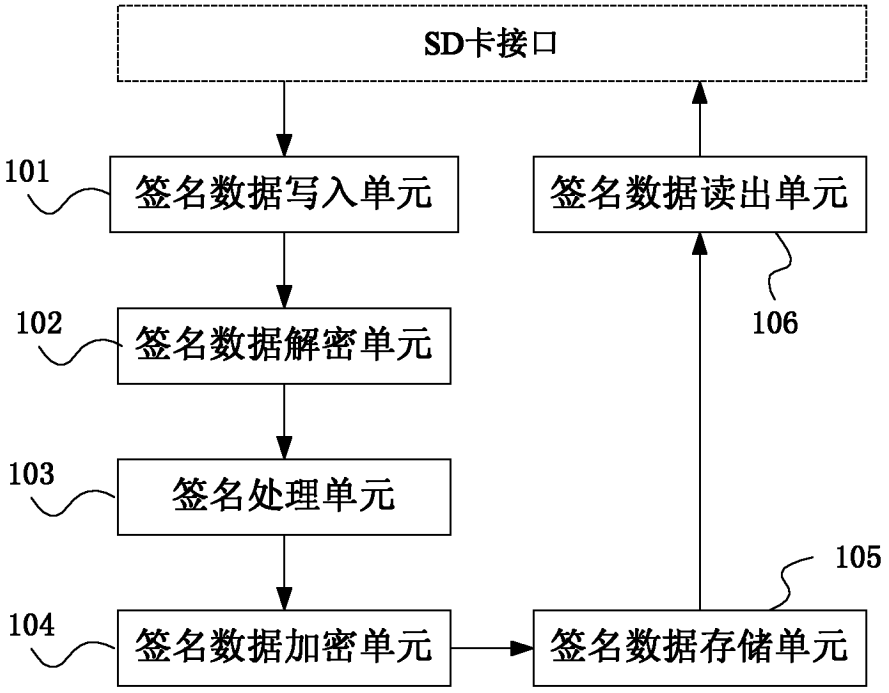

SD卡接口
101
签名数据写入单元
签名数据读出单元
106
102
签名数据解密单元
103
签名处理单元
105
104
签名数据加密单元
签名数据存储单元

图 2

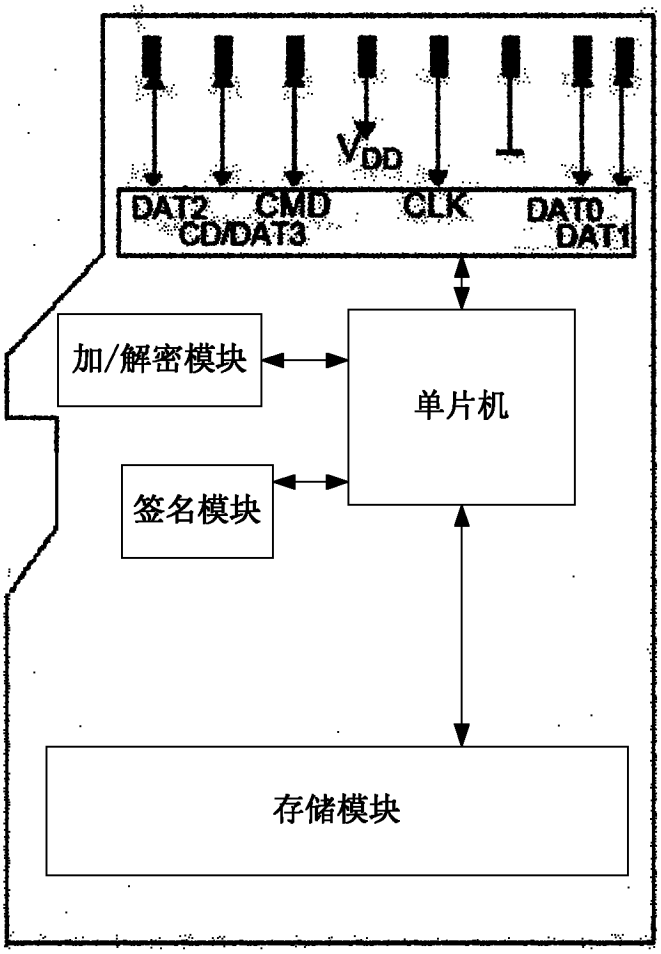


图 3

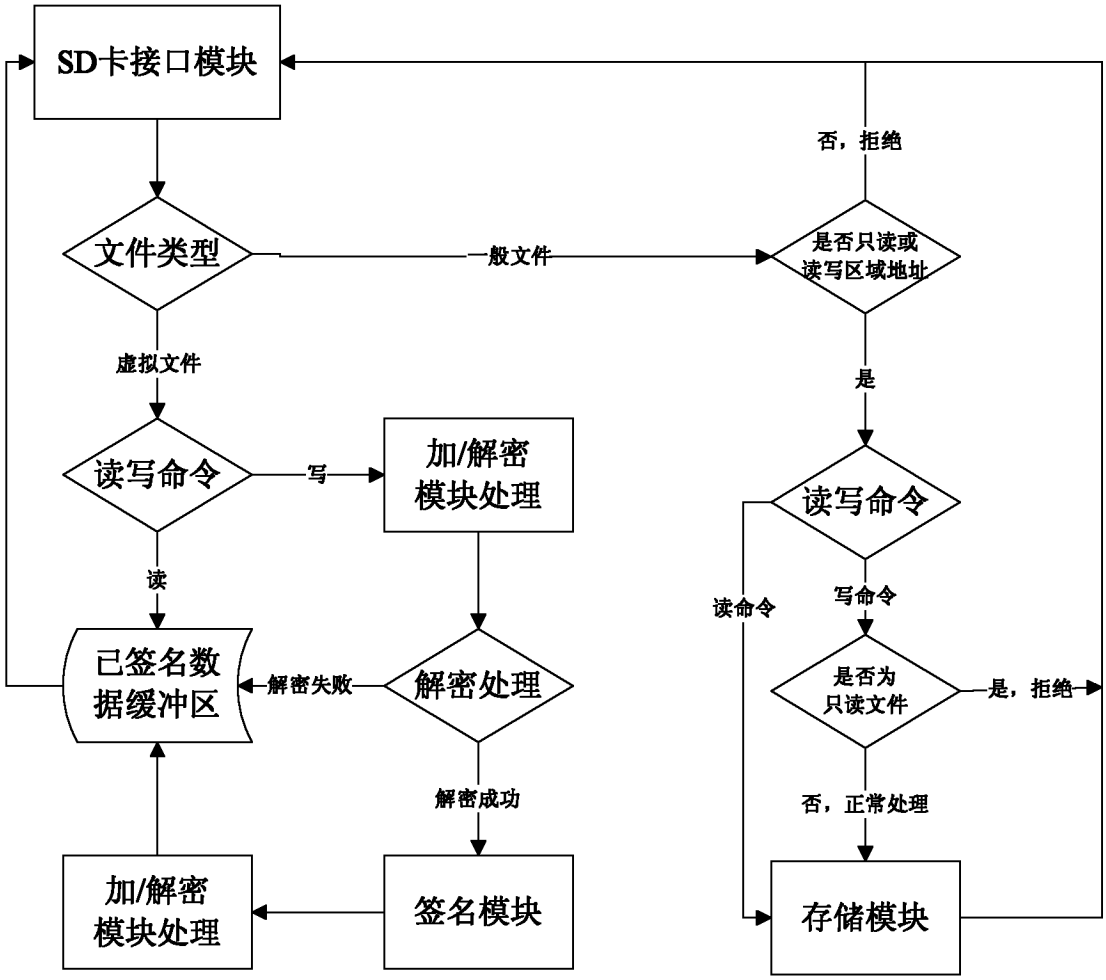

SD卡接口模块
文件类型
一般文件
否，拒绝
是否只读或
读写区域地址
虚拟文件
是
读写命令
写
加/解密
模块处理
读
读命令
写命令
已签名数
据缓冲区
解密失败
解密处理
是否为
只读文件
是，拒绝
解密成功
否，正常处理
加/解密
模块处理
签名模块
存储模块

图 4

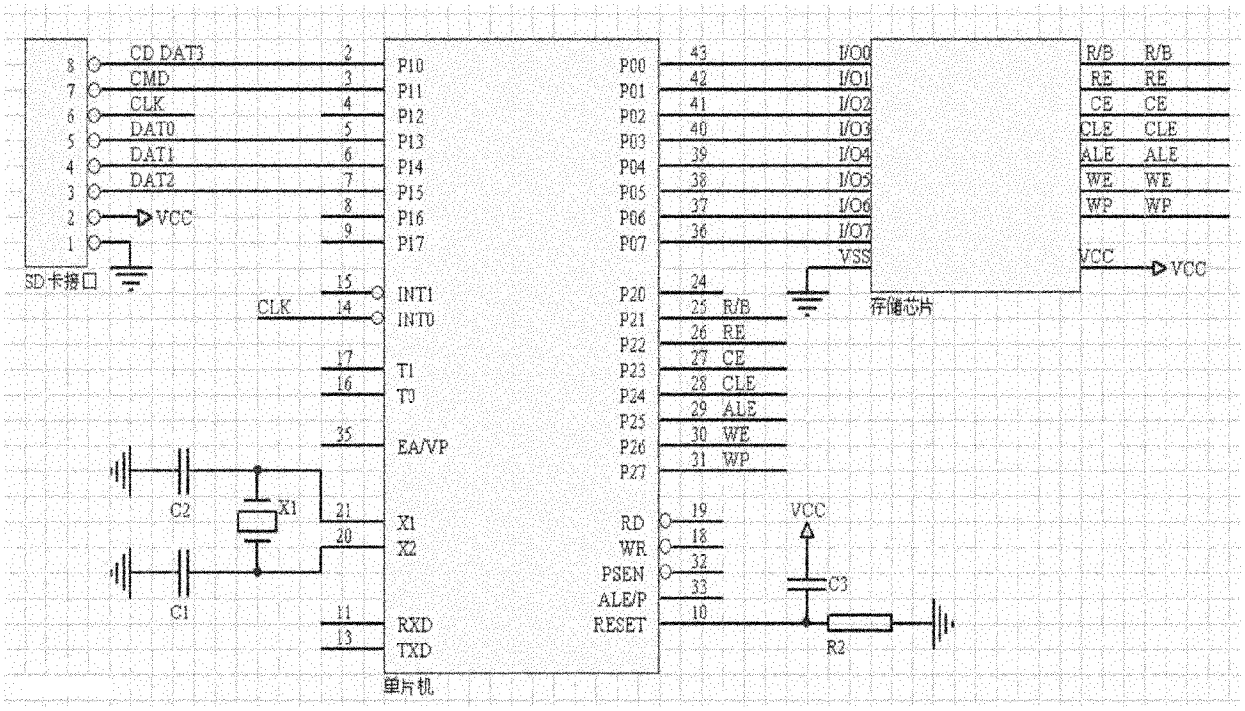

SD卡接口
CD DAT3
CMD
CLK
DAT0
DAT1
DAT2
VCC
单片机
P10
P11
P12
P13
P14
P15
P16
P17
INT1
INT0
T1
T0
EA/VP
X1
X2
RXD
TXD
P00
P01
P02
P03
P04
P05
P06
P07
P20
P21
P22
P23
P24
P25
P26
P27
RD
WR
PSEN
ALE/P
RESET
I/O0
I/O1
I/O2
I/O3
I/O4
I/O5
I/O6
I/O7
VSS
R/B
RE
CE
CLE
ALE
WE
WP
存储芯片
C1
C2
C3
R2

图 5

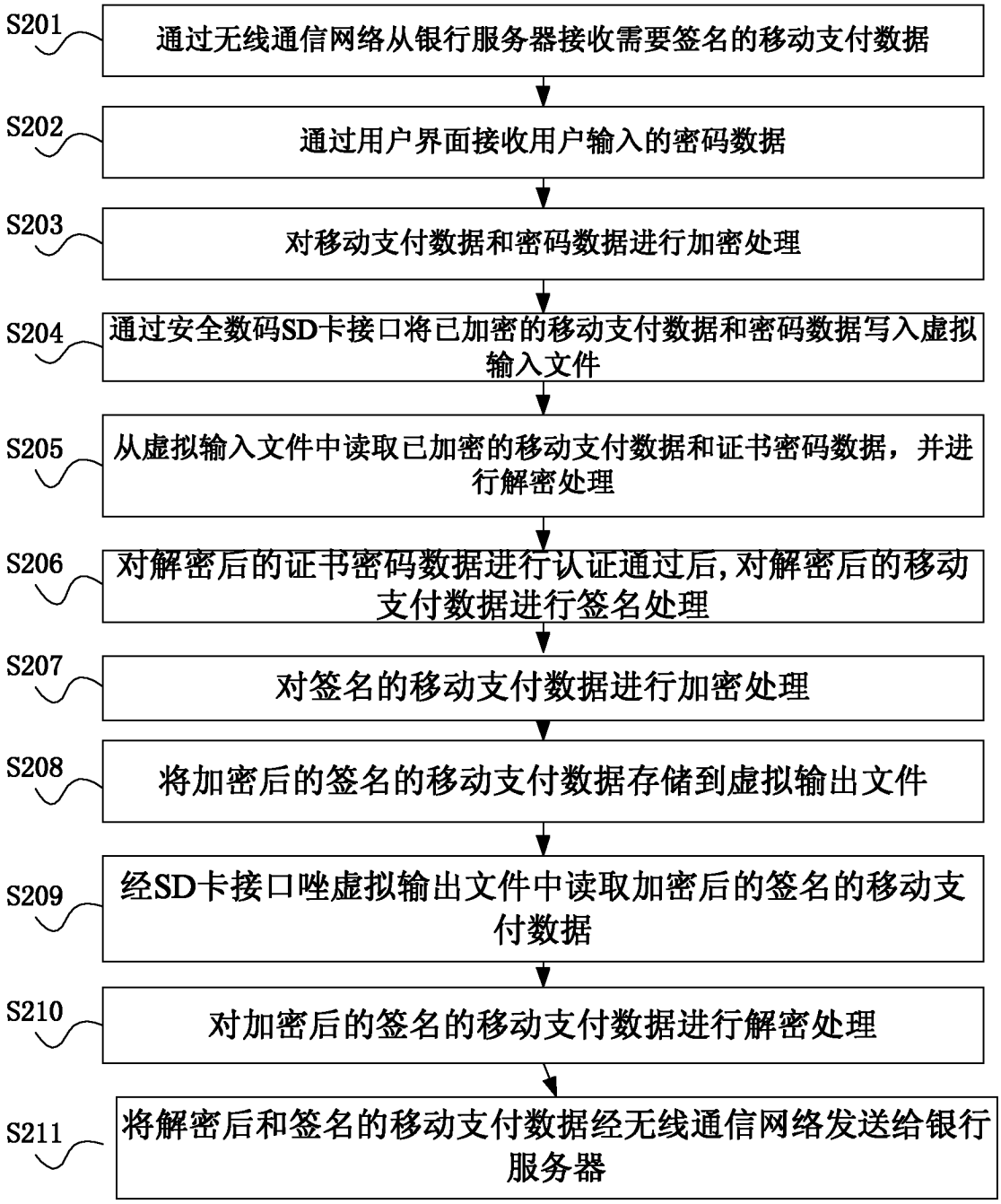

S201
通过无线通信网络从银行服务器接收需要签名的移动支付数据
S202
通过用户界面接收用户输入的密码数据
S203
对移动支付数据和密码数据进行加密处理
S204
通过安全数码SD卡接口将已加密的移动支付数据和密码数据写入虚拟输入文件
S205
从虚拟输入文件中读取已加密的移动支付数据和证书密码数据，并进行解密处理
S206
对解密后的证书密码数据进行认证通过后,对解密后的移动支付数据进行签名处理
S207
对签名的移动支付数据进行加密处理
S208
将加密后的签名的移动支付数据存储到虚拟输出文件
S209
经SD卡接口唑虚拟输出文件中读取加密后的签名的移动支付数据
S210
对加密后的签名的移动支付数据进行解密处理
S211
将解密后和签名的移动支付数据经无线通信网络发送给银行服务器

图 6

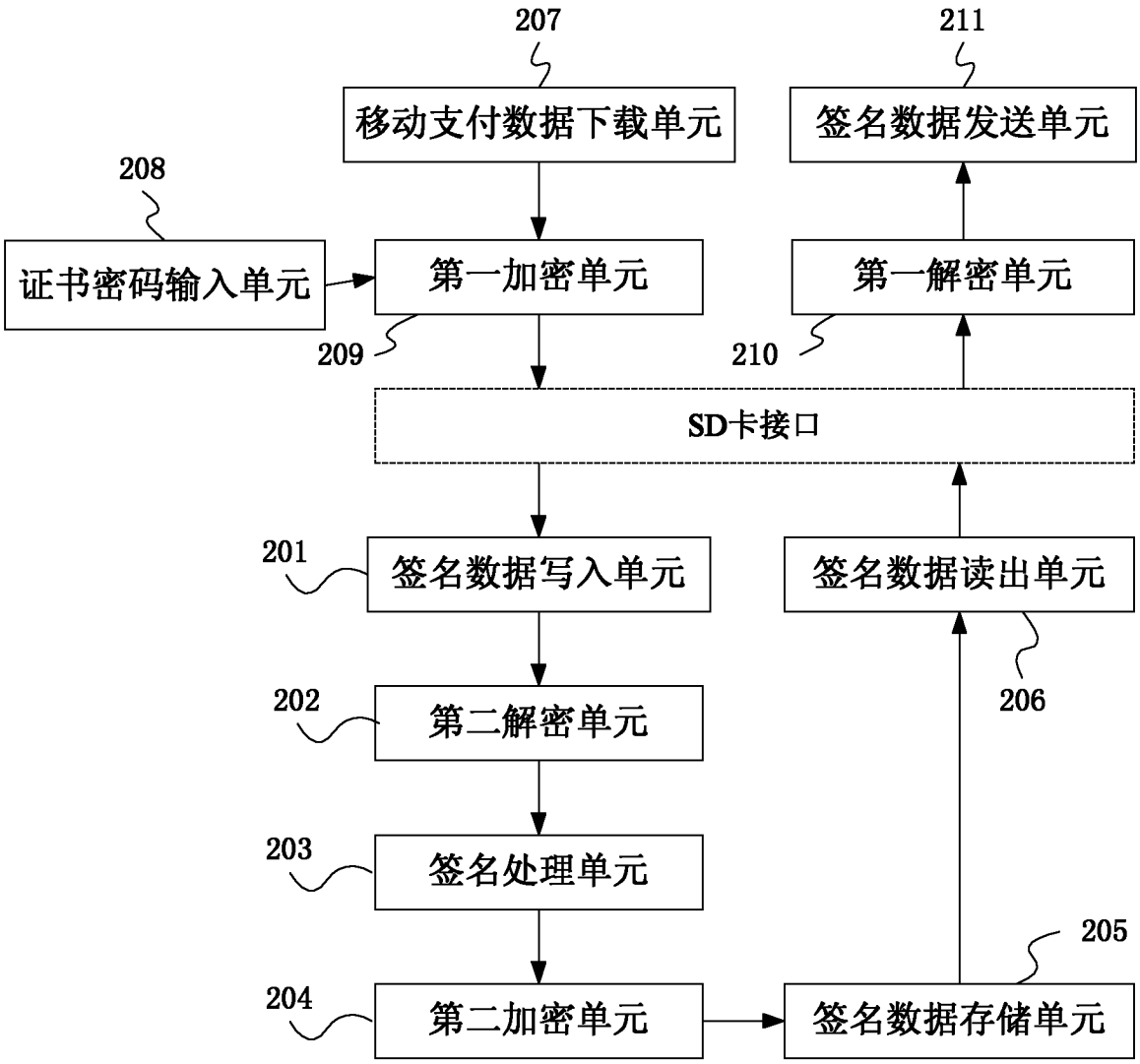

207
移动支付数据下载单元
211
签名数据发送单元
208
证书密码输入单元
第一加密单元
第一解密单元
209
210
SD卡接口
201
签名数据写入单元
签名数据读出单元
206
202
第二解密单元
203
签名处理单元
205
204
第二加密单元
签名数据存储单元

图 7

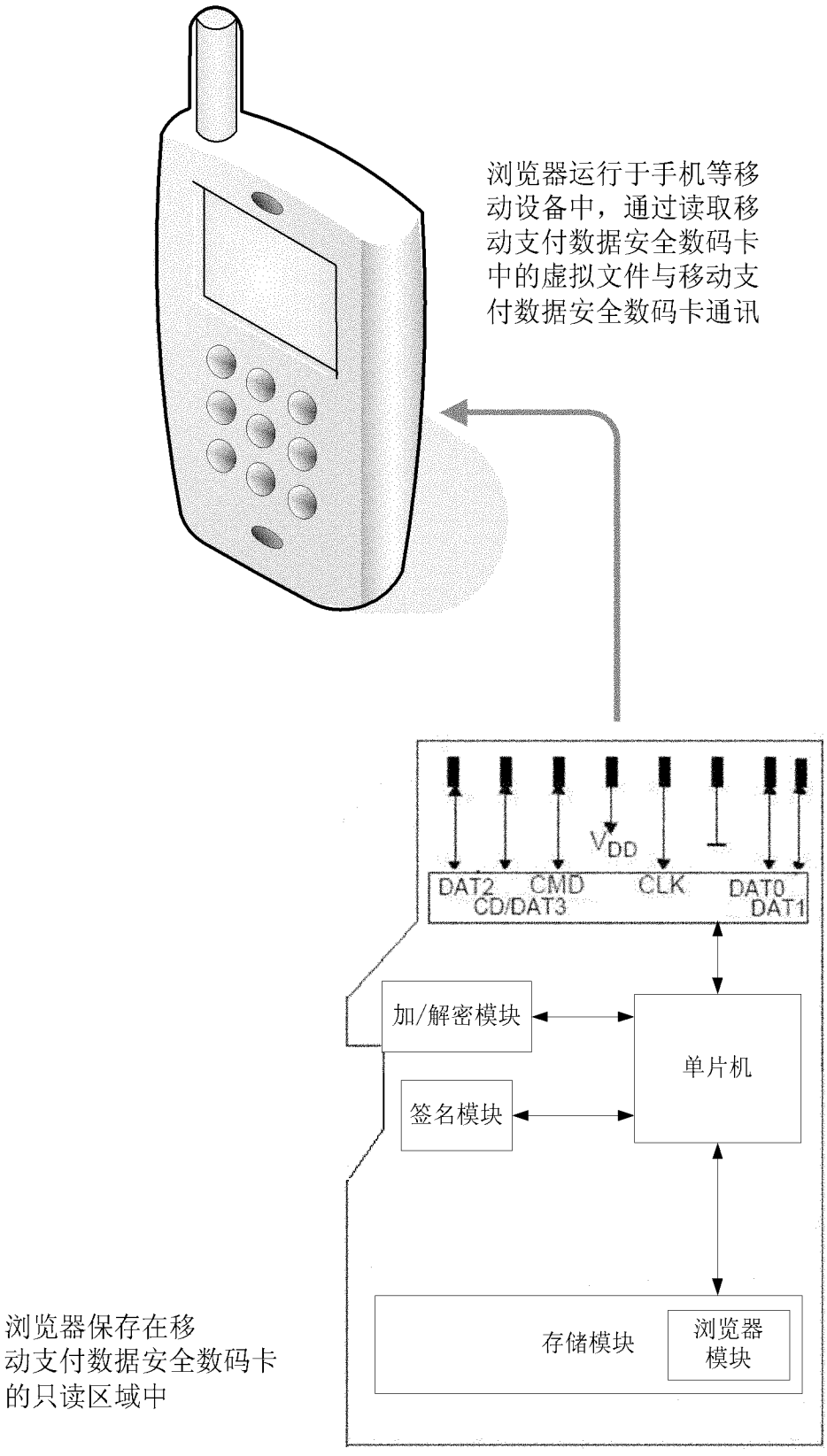

浏览器运行于手机等移动设备中，通过读取移动支付数据安全数码卡中的虚拟文件与移动支付数据安全数码卡通讯
VDD
DAT2
CMD
CLK
DAT0
CD/DAT3
DAT1
加/解密模块
单片机
签名模块
存储模块
浏览器模块
浏览器保存在移动支付数据安全数码卡的只读区域中

图 8

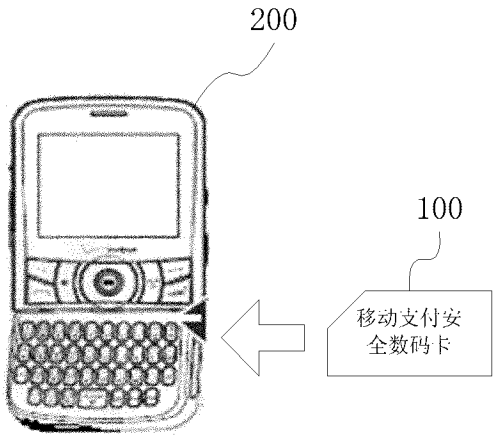

200
100
移动支付安全数码卡

图 9

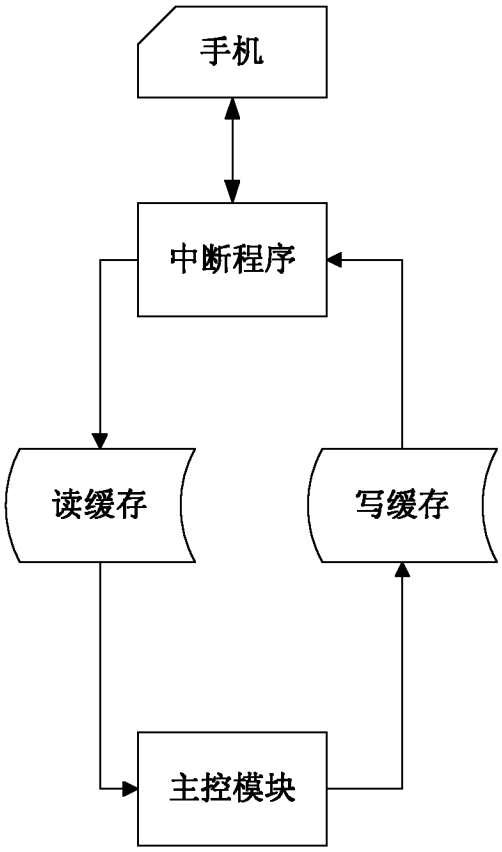

手机
中断程序
读缓存
写缓存
主控模块

图 10

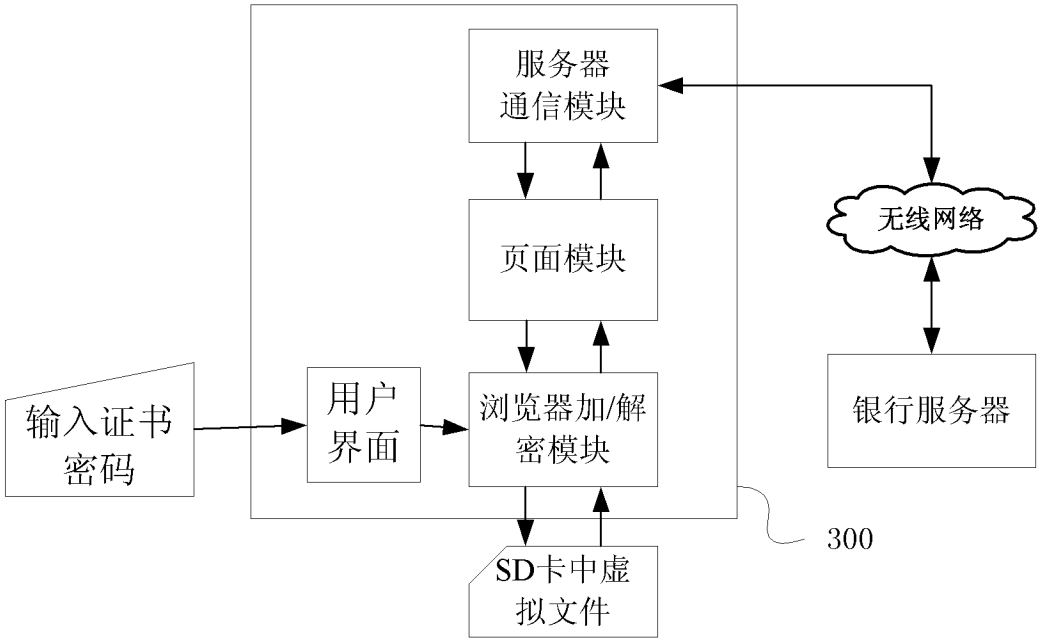

服务器通信模块
页面模块
浏览器加/解密模块
SD卡中虚拟文件
用户界面
输入证书密码
无线网络
银行服务器
300

图 11