(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 104282096 B
(45)授权公告日 2016.09.28

(21)申请号 201310283736.X

(22)申请日 2013.07.08

(65)同一申请的已公布的文献号
申请公布号 CN 104282096 A

(43)申请公布日 2015.01.14

(73)专利权人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路36号银联大厦

(72)发明人 周钰 严翔翔

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 俞华梁 朱海煜

(51)Int.Cl.
G07G 1/14(2006.01)
G06Q 20/40(2012.01)

审查员 黄丹

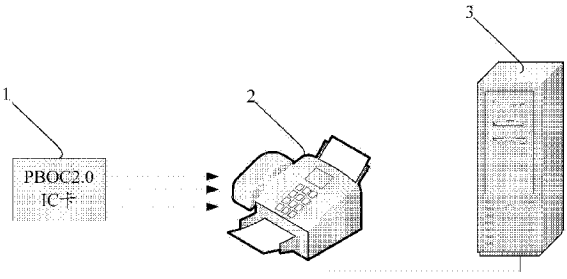
权利要求书1页 说明书5页 附图2页

(54)发明名称

实现数字签名的方法以及用于实现数字签名的POS终端

(57)摘要

本发明公开了一种在POS终端内实现“所见即所签”数字签名的方法，包括：(a) 从主机接收交易信息，其中，所述交易信息包括收款人名称、收款人账号和交易金额；(b) 将所述交易信息在显示屏上显示，供用户确认；(c) 在用户已经对交易确认后，将所述交易信息中的收款人名称设置到金融IC卡的动态数据认证数据对象列表DDOL中的“终端商户名称”域，将所述交易信息中的收款人账号设置到所述DDOL中的“应用主账号”域并且将所述交易信息中的交易金额设置到所述DDOL中的“授权金额”域；以及(d) 向所述金融IC卡发送动态数据认证命令以将来自所述金融IC卡的动态交易数据以及由所述动态数据认证数据对象列表DDOL所标识的终端数据生成一个数字签名。本发明还公开了一种用于实现上述数字签名方法的POS终端。



CN 104282096 B

1.一种在POS终端内实现“所见即所签”数字签名的方法,包括:

(a)从主机接收交易信息,其中,所述交易信息包括收款人名称、收款人账号和交易金额;

(b)将所述交易信息在显示屏上显示,供用户确认;

(c)在用户已经对交易确认后,将所述交易信息中的收款人名称设置到金融IC卡的动态数据认证数据对象列表DDOL中的“终端商户名称”域,将所述交易信息中的收款人账号设置到所述DDOL中的“应用主账号”域并且将所述交易信息中的交易金额设置到所述DDOL中的“授权金额”域;以及

(d)向所述金融IC卡发送动态数据认证命令以将来自所述金融IC卡的动态交易数据以及由所述动态数据认证数据对象列表DDOL所标识的终端数据生成一个数字签名;

(e)获取所述金融IC卡内部的应用交易序列号ATC;以及

(f)将所述ATC连同所述金融IC内的静态认证数据一起返回给服务器,以便于所述服务器验证所述数字签名以及所述金融IC卡的合法性。

2.如权利要求1所述的方法,其中,所述金融IC卡设置成支持静态数据认证SDA和动态数据认证DDA。

3.如权利要求1所述的方法,其中,所述动态数据认证数据对象列表DDOL配置成包括终端商户名称、应用主账号、授权金额以及不可预知数的域。

4.如权利要求1所述的方法,还包括在步骤(c)和(d)之间执行的如下步骤:

执行取交易选项GPO命令从而改变所述金融IC卡内部参与签名的动态数据。

5.如权利要求1所述的方法,还包括:

从所述服务器接收交易认证结果。

6.一种用于实现“所见即所签”数字签名的POS终端,包括:

接收单元,用于从主机接收交易信息,其中,所述交易信息包括收款人名称、收款人账号和交易金额;

显示单元,用于将所述交易信息在显示屏上显示,供用户确认;

设置单元,用于在用户已经对交易确认后,将所述交易信息中的收款人名称设置到金融IC卡的动态数据认证数据对象列表DDOL中的“终端商户名称”域,将所述交易信息中的收款人账号设置到所述DDOL中的“应用主账号”域并且将所述交易信息中的交易金额设置到所述DDOL中的“授权金额”域;以及

发送单元,用于向所述金融IC卡发送动态数据认证命令以将来自所述金融IC卡的动态交易数据以及由所述动态数据认证数据对象列表DDOL所标识的终端数据生成一个数字签名;获取单元,用于获取所述金融IC卡内部的应用交易序列号ATC;以及

返回单元,用于将所述ATC连同所述金融IC内的静态认证数据一起返回给服务器,以便于所述服务器验证所述数字签名以及所述金融IC卡的合法性。

7.如权利要求6所述的POS终端,还包括:

执行单元,用于执行取交易选项GPO命令从而改变所述金融IC卡内部参与签名的动态数据。

8.如权利要求6所述的POS终端,还包括:

接收单元,用于从所述服务器接收交易认证结果。

实现数字签名的方法以及用于实现数字签名的POS终端

技术领域

[0001] 本发明涉及金融数据处理领域，尤其涉及在POS终端内实现“所见即所签”的数字签名的技术。

背景技术

[0002] 截至2009年初，据官方统计，中国网民数已达到2亿多人，随着网络的普及，网络炒股、炒金、投资理财等多种理财方式已逐渐被老百姓接受。很多老百姓为方便快捷，选择了网络电子自助服务，比如手机银行、电话银行、网上银行等。

[0003] 为了保证网上银行的安全性，多家银行推出了网上银行高级安全工具——U盾。随着互联网身份识别技术和智能芯片制造技术的发展进步，目前U盾已经提升至第二代。二代U盾的安全防护建立在“双因子，双渠道”认证基础上，与一代相比，二代U盾在原1024位硬件数据加密的基础上，增加了液晶显示屏和物理按钮，可视屏幕可将客户的签名信息显示在屏幕上供客户确认，做到“所见即所签”。

[0004] 但是，为了在网银中实现数字签名，用户还得另外掏钱购买该U盾产品，这导致了很大程度上的资源浪费。现有的PBOC2.0 借贷记卡片虽然有非对称算法的能力，但是其却不具备类似于第二代U盾所拥有的用户参与数字签名的功能。

发明内容

[0005] 为了解决上述问题，本发明的发明人提出对PBOC2.0 借贷记IC卡进行功能扩充，与POS终端相结合实现“所见即所签”的数字签名的功能。

[0006] 根据本发明的一个方面，提供了一种在POS终端内实现“所见即所签”数字签名的方法，包括：(a) 从主机接收交易信息，其中，所述交易信息包括收款人名称、收款人账号和交易金额；(b) 将所述交易信息在显示屏上显示，供用户确认；(c) 在用户已经对交易确认后，将所述交易信息中的收款人名称设置到金融IC卡的动态数据认证数据对象列表DDOL中的“终端商户名称”域，将所述交易信息中的收款人账号设置到所述DDOL中的“应用主账号”域并且将所述交易信息中的交易金额设置到所述DDOL中的“授权金额”域；以及(d) 向所述金融IC卡发送动态数据认证命令以将来自所述金融IC卡的动态交易数据以及由所述动态数据认证数据对象列表DDOL所标识的终端数据生成一个数字签名。

[0007] 上述方法还可包括：(e) 获取所述金融IC卡内部的应用交易序列号ATC；以及(f) 将所述ATC连同所述金融IC内的静态认证数据一起返回给服务器，以便于所述服务器验证所述数字签名以及所述金融IC卡的合法性。

[0008] 在上述方法中，所述金融IC卡设置成支持静态数据认证SDA和动态数据认证DDA。

[0009] 在上述方法中，所述动态数据认证数据对象列表DDOL配置成包括终端商户名称、应用主账号、授权金额以及不可预知数的域。

[0010] 上述方法还可包括在步骤(c)和(d)之间执行的如下步骤：执行取交易选项GPO命令从而改变所述金融IC卡内部参与签名的动态数据。

[0011] 上述方法还可包括:从所述服务器接收交易认证结果。

[0012] 根据本发明的另一个方面,提供了一种用于实现“所见即所签”数字签名的POS终端,包括:接收单元,用于从主机接收交易信息,其中,所述交易信息包括收款人名称、收款人账号和交易金额;显示单元,用于将所述交易信息在显示屏上显示,供用户确认;设置单元,用于在用户已经对交易确认后,将所述交易信息中的收款人名称设置到金融IC卡的动态数据认证数据对象列表DDOL中的“终端商户名称”域,将所述交易信息中的收款人账号设置到所述DDOL中的“应用主账号”域并且将所述交易信息中的交易金额设置到所述DDOL中的“授权金额”域;以及发送单元,用于向所述金融IC卡发送动态数据认证命令以将来自所述金融IC卡的动态交易数据以及由所述动态数据认证数据对象列表DDOL所标识的终端数据生成一个数字签名。

[0013] 上述POS终端还可包括:获取单元,用于获取所述金融IC卡内部的应用交易序列号ATC;以及返回单元,用于将所述ATC连同所述金融IC内的静态认证数据一起返回给服务器,以便于所述服务器验证所述数字签名以及所述金融IC卡的合法性。

[0014] 上述POS终端还可包括:执行单元,用于执行取交易选项GPO命令从而改变所述金融IC卡内部参与签名的动态数据。

[0015] 上述POS终端还可包括:接收单元,用于从所述服务器接收交易认证结果。

[0016] 本发明的技术方案在不改变PBOC金融应用原有应用处理逻辑的前提下,利用PBOC应用的动态数据认证功能,设计了一种新的方法使得金融IC卡能够对“收款人名称,收款人账号,交易金额”等信息认证签名。通过POS显示上述信息,并把动态数据认证后的信息发给收单后台,实现“所见即所签”效果。

附图说明

[0017] 在参照附图阅读了本发明的具体实施方式以后,本领域技术人员将会更清楚地了解本发明的各个方面。本领域技术人员应当理解的是:这些附图仅仅用于配合具体实施方式说明本发明的技术方案,而并非意在对本发明的保护范围构成限制。

[0018] 图1是根据本发明的一个实施例、由PBOC 2.0 IC卡、POS终端和服务器所组成的系统的结构示意图;

[0019] 图2是根据本发明的一个实施例、交易签名过程和交易验证过程的流程示意图。

具体实施方式

[0020] 下面介绍的是本发明的多个可能实施例中的一些,旨在提供对本发明的基本了解,并不旨在确认本发明的关键或决定性的要素或限定所要保护的范围。容易理解,根据本发明的技术方案,在不变更本发明的实质精神下,本领域的一般技术人员可以提出可相互替换的其它实现方式。因此,以下具体实施方式以及附图仅是对本发明的技术方案的示例性说明,而不应当视为本发明的全部或者视为对本发明技术方案的限定或限制。

[0021] 图1是根据本发明的一个实施例、由PBOC 2.0 IC卡1、POS终端2和服务器3所组成的系统的结构示意图。

[0022] 需要说明的是,PBOC是中国人民银行的英文名称的缩写,也就是我们平时所说的央行。PBOC2.0 IC卡是中国人民银行颁布的第二代金融IC卡规范的简称,利用该金融IC卡,

能够有效解决目前使用磁条卡时存在的假卡、脱机交易安全等问题。

[0023] 金融IC卡借记/贷记应用中的IC卡数据认证在IC卡支付过程中的作用是进行脱机IC数据认证，包括：静态数据认证(SDA)和动态数据认证(DDA)。动态数据认证又包括：标准动态数据认证和复合动态数据认证。

[0024] 静态数据认证

[0025] 静态数据认证由终端验证卡片中的静态数据的数字签名来完成。其目的是确认存放在银联标准IC卡中关键的静态数据的合法性，可以发现在卡片个人化以后对卡内的发卡机构数据未经授权的改动，能有效地检测银联标准IC卡内关键静态数据的真实性。

[0026] 整个银联标准IC卡静态数据认证的过程说明如下：

[0027] 1)发卡机构的密钥管理系统产生发卡机构公/私钥对P_i和S_i，并将公钥P_i传送至根CA；

[0028] 2)根CA用自己的私钥S_{CA}对发卡机构公钥P_i进行数字签名，产生发卡机构公钥证书，连同根CA公钥证书(包括RID及根CA公钥索引)返回给发卡机构密钥管理系统；

[0029] 3)发卡机构密钥管理系统用发卡机构私钥S_i对卡片静态数据进行数字签名，将签名结果、发卡机构公钥证书、RID及根CA公钥索引传送至发卡系统；

[0030] 4)发卡系统在个人化时将静态数字签名、发卡机构公钥证书、RID及根CA公钥索引写入每一张卡片中；

[0031] 5)根CA将其公钥P_{CA}、RID、根CA公钥索引及其它相关信息经收单机构传送至终端管理系统；

[0032] 6)收单机构终端管理系统把根CA公钥P_{CA}、RID、根CA公钥索引及其它相关信息下载至终端；

[0033] 7)银联标准IC卡进行交易时，脱机静态数据认证过程如下：

[0034] —终端从卡片中读取发卡机构公钥证书及签名数据，使用根CA公钥索引和RID找到根CA公钥Pα，由Pα恢复出发卡机构公钥P_i并验证其有效性；

[0035] —终端使用恢复的发卡机构公钥P_i验证卡片签名数据的有效性。

[0036] 动态数据认证

[0037] 在动态数据认证(DDA)过程中，终端验证卡片上的静态数据以及卡片产生的当前动态交易数据的签名。DDA能确认卡片上的发卡机构应用数据自卡片个人化后没有被非法篡改，更重要的是DDA还能确认卡片的真实性，防止卡片的非法复制和伪造。

[0038] 可以是标准动态数据认证或复合动态数据认证/应用密文生成(CDA)。在动态数据认证方式下，银联标准IC卡将来自卡片的动态交易数据以及由动态数据认证数据对象列表(DDOL)所标识的终端数据生成一个数字签名。

[0039] 银联标准IC卡标准动态数据认证整体过程说明如下：

[0040] 1)发卡机构的密钥管理系统产生发卡机构公/私钥对P_i和S_i，并将发卡机构公钥P_i传送至根CA；

[0041] 2)根CA用自己的私钥S_{CA}对发卡机构公钥P_i进行数字签名，产生发卡机构公钥证书，连同根CA公钥证书(包括RID及根CA公钥索引)返回给发卡机构密钥管理系统；

[0042] 3)发卡机构密钥管理系统为每一张银联标准IC卡产生一对公私钥对S_{ICC}和P_{ICC}，并用发卡机构私钥S_i对IC卡公钥P_{ICC}进行数字签名，产生IC卡公钥证书；

[0043] 4)发卡机构密钥管理系统将发卡机构公钥证书、IC卡公钥证书、IC卡私钥、RID及根CA公钥索引传送至发卡系统；

[0044] 5)发卡系统在个人化时将发卡机构公钥证书、IC卡公钥证书、IC卡私钥、RID及根CA公钥索引写入卡片中；

[0045] 6)根CA将其公钥P_{CA}、RID、根CA公钥索引及其它相关信息经收单机构传送至终端管理系统；

[0046] 7)收单机构终端管理系统把根CA公钥P_{CA}、RID、根CA公钥索引及其它相关信息下载至终端；

[0047] 8)银联标准IC卡进行交易时，脱机静态数据认证过程如下：

[0048] —终端从卡片中读取发卡机构公钥证书、IC卡公钥证书、RID及根CA公钥索引，利用RID和根CA公钥索引定位根CA公钥P_{CA}，使用根CA公钥P_{CA}恢复出发卡机构公钥P_i并验证其有效性，使用恢复的发卡机构公钥P_i恢复出IC卡公钥P_{ICC}并验证其有效性；

[0049] —终端向IC卡发送内部认证命令请求一个动态签名；卡片对内部认证命令中的终端数据和IC卡交易动态数据进行连接，由IC卡私钥S_{ICC}对该连接数据进行数字签名并返回给终端；

[0050] —终端使用IC卡公钥P_{ICC}对上一步骤的数字签名进行验证。

[0051] 在复合动态数据认证/应用密文生成方式中，在第一个请求应用密文命令发出后执行。银联标准IC卡将来自卡片的数据包括应用密文以及来自终端的数据生成一个数据签名。

[0052] 银联标准IC卡复合动态数据认证/应用密文生成的整体过程如下：

[0053] 1)发卡机构的密钥管理系统产生发卡机构公/私钥对P_i和S_i，并将发卡机构公钥P_i传送至根CA；

[0054] 2)根CA用自己的私钥S_{CA}对发卡机构公钥P_i进行数字签名，产生发卡机构公钥证书，连同根CA公钥证书(包括RID及根CA公钥索引)返回给发卡机构密钥管理系统；

[0055] 3)发卡机构密钥管理系统为每一张银联标准IC卡产生一对公私钥对S_{ICC}和P_{ICC}，并用发卡机构私钥S_i对IC卡公钥P_{ICC}进行数字签名，产生IC卡公钥证书；

[0056] 4)发卡机构密钥管理系统将发卡机构公钥证书、IC卡公钥证书、IC卡私钥、RID及根CA公钥索引传送至发卡系统；

[0057] 5)发卡系统在个人化时将发卡机构公钥证书、IC卡公钥证书、IC卡私钥、RID及根CA公钥索引写入卡片中；

[0058] 6)根CA将其公钥P_{CA}、RID、根CA公钥索引及其它相关信息经收单机构传送至终端管理系统；

[0059] 7)收单机构终端管理系统把根CA公钥P_{CA}、RID、根CA公钥索引及其它相关信息下载至终端；

[0060] 8)银联标准IC卡进行交易时，脱机静态数据认证过程如下：

[0061] —终端从卡片中读取发卡机构公钥证书、IC卡公钥证书、RID及根CA公钥索引；

[0062] —终端使用RID和根CA公钥索引定位根CA公钥P_{CA}，使用根CA公钥P_{CA}验证发卡机构公钥证书的签名并恢复出发卡机构公钥P_i；

[0063] —终端使用发卡机构公钥P_i验证IC卡公钥证书的签名并恢复出IC卡公钥P_{ICC}；

[0064] —终端生成一不可预知数并与其它相关数据一并传给IC卡；

[0065] —IC卡使用其自身的私钥S_{ICC}对收到的终端数据(包括不可预知数、交易数据)和其它IC卡数据(包括TC/ARQC)做数字签名并发送给终端；

[0066] —终端使用IC卡公钥P_{ICC}验证IC卡传递的签名数据。

[0067] 根据本发明的一个实施例，实现“所见即所签”的数字签名的功能的系统处理流程如下：

[0068] 1)设置卡片支持静态数据认证(SDA)和动态数据(DDA)功能；

[0069] 2)发卡行将该应用下将动态数据认证数据对象列表(DDOL)设置为“终端商户名称、应用主账号(PAN)、授权金额”，或者设置为“终端商户名称、应用主账号(PAN)、授权金额、不可预知数(随机数)”以增强安全性；

[0070] 3)在网银交易时，由主机(可能为PC、手机、平板电脑等)传入“收款人名称、收款人账号、交易金额”等信息到POS中。POS将这些信息在显示屏上显示，供用户对交易进行确认；

[0071] 4)如果用户已经对交易进行确认，则POS内部将收款人名称设置到终端商户名称域，将收款人账号设置到应用主账号域，将交易金额设置到授权金额域以及可选存在的不可预知数(随机数)；

[0072] 5)POS可选择执行“取交易选项命令(GPO)”，来改变卡片内部参与签名的动态数据，以达到增加安全性的目的；

[0073] (步骤5为可选步骤)

[0074] 6)调用动态数据认证(DDA)命令；

[0075] 7)卡片内部执行动态数据认证过程，返回动态数据认证结果(即交易数据的签名结果)；

[0076] 8)POS获取卡片内部的应用交易序列号(ATC)，连同卡片内部的静态认证数据一起返回给服务器；

[0077] 9)服务器使用CA公钥从卡片内部的静态认证数据中恢复出卡片公钥；

[0078] 10)服务器验证卡片的合法性，并使用卡片公钥验证交易数据的签名结果。如果验证成功，则认为交易有效，否则无效。

[0079] 详细的交易签名过程和交易验证过程的流程示意图可参见图2。

[0080] 通过上面介绍的技术方案，用户使用现有的PBOC 2.0借贷记IC卡与本发明所述的POS终端结合，即可实现网银交易中“所见即所签”的数字签名功能，而无需购买额外的USB key产品。

[0081] 上文中，参照附图描述了本发明的具体实施方式。但是，本领域中的普通技术人员能够理解，在不偏离本发明的精神和范围的情况下，还可以对本发明的具体实施方式作各种变更和替换。这些变更和替换都落在本发明权利要求书所限定的范围内。

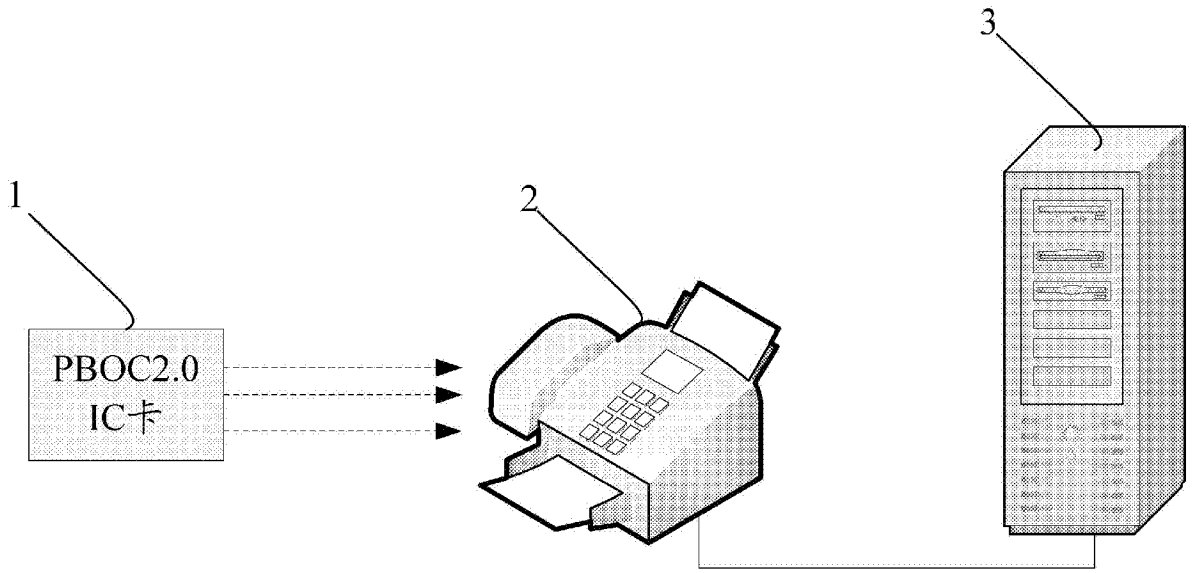


图 1

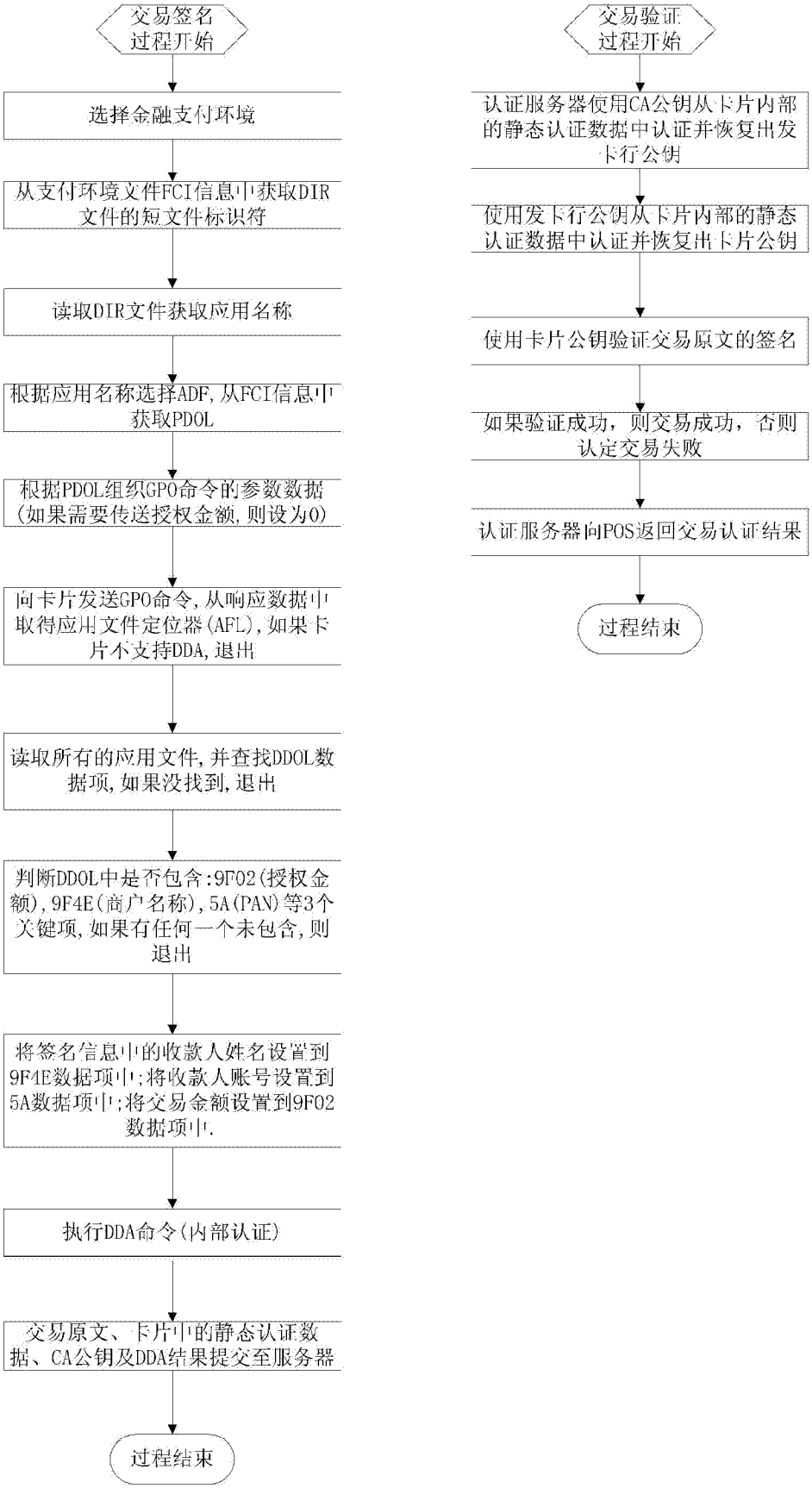

交易签名过程开始
选择金融支付环境
从支付环境文件FCI信息中获取DIR文件的短文件标识符
读取DIR文件获取应用名称
根据应用名称选择ADF,从FCI信息中获取PDOL
根据PDOL组织GPO命令的参数数据(如果需要传送授权金额,则设为0)
向卡片发送GPO命令,从响应数据中取得应用文件定位器(AFL),如果卡片不支持DDA,退出
读取所有的应用文件,并查找DDOL数据项,如果没找到,退出
判断DDOL中是否包含:9F02(授权金额),9F4E(商户名称),5A(PAN)等3个关键项,如果有任何一个未包含,则退出
将签名信息中的收款人姓名设置到9F4E数据项中;将收款人账号设置到5A数据项中;将交易金额设置到9F02数据项中.
执行DDA命令(内部认证)
交易原文、卡片中的静态认证数据、CA公钥及DDA结果提交至服务器
过程结束
交易验证过程开始
认证服务器使用CA公钥从卡片内部的静态认证数据中认证并恢复出发卡行公钥
使用发卡行公钥从卡片内部的静态认证数据中认证并恢复出卡片公钥
使用卡片公钥验证交易原文的签名
如果验证成功,则交易成功,否则认定交易失败
认证服务器向POS返回交易认证结果
过程结束

图 2