(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 1 月 30 日 (30.01.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/015827 A1

(51) 国际专利分类号:
G07F 19/00 (2006.01)

(21) 国际申请号: PCT/CN2013/080167

(22) 国际申请日: 2013 年 7 月 26 日 (26.07.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210262725.9 2012 年 7 月 27 日 (27.07.2012) CN

(71) 申请人: **中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.)** [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: **钟国业 (ZHONG, Guoye)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **吴金坛 (WU, Jintan)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **万高峰 (WAN, Gaofeng)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: **中国专利代理（香港）有限公司 (CHINA PATENT AGENT (HK)LTD.)**; 中国香港特别行政区香港湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (CN)。

(81) **指定国** (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国** (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,

[见续页]

WO 2014/015827 A1

(54) **Title**: METHOD FOR AUTHENTICATION OF IC CARD AND SECURITY INFORMATION INTERACTIVE TERMINAL, IC CARD, AND SECURITY INFORMATION INTERACTIVE TERMINAL

(54) **发明名称**: 用于 IC 卡和安全性信息交互终端的认证方法以及 IC 卡和安全性信息交互终端

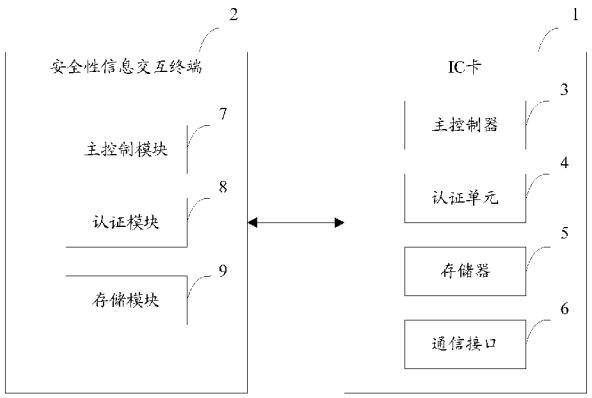


图 1/ FIG. 1

1 IC card
2 Security information interactive terminal
3 Master controller
4 Authentication unit
5 Storage
6 Communication interface
7 Master control module
8 Authentication module
9 Storage module

(57) **Abstract**: The present invention provides a method for offline authentication of an IC card and a security information interactive terminal, and an IC card and a security information interactive terminal that are capable of using the method. The method comprises: after a data communication link is established between an IC card and a security information interactive terminal, the security information interactive terminal sending an authentication instruction to the IC card, so as to perform an authentication process on the security information interactive terminal, the authentication process being performed in an offline state. The disclosed method for offline authentication of an IC card and a security information interactive terminal, and the disclosed IC card and security information interactive terminal that are capable of using the method achieve enhanced security.

(57) **摘要**: 摘要本发明提出了用于 IC 卡和安全性信息交互终端的脱机认证的方法以及能够使用该方法的 IC 卡和安全性信息交互终端。其中，所述方法包括：在 IC 卡与安全性信息交互终端之间已建立了数据通信链路后，所述安全性信息交互终端向所述 IC 卡发送认证指令以执行对所述安全性信息交互终端的认证过程，其中，在脱机情况下执行所述认证过程。本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法以及能够使用该方法的 IC 卡和安全性信息交互终端具有增强的安全性。

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

用于 IC 卡和安全性信息交互终端的认证方法以及 IC 卡和安全性信息交互终端

技术领域

本发明涉及认证方法以及 IC 卡和信息交互终端，更具体地，涉及用于 IC 卡和安全性信息交互终端的脱机认证方法以及 IC 卡和安全性信息交互终端。

背景技术

目前，随着 IC 卡应用的日益广泛以及不同领域的业务种类的日益丰富，通过 IC 卡（例如交通卡）和安全性信息交互终端（例如 POS 机）之间的安全性信息（即对安全性要求较高的信息，例如密码）交互（尤其是脱机情况下的安全性信息交互）而实现不同的应用（例如交通卡充值）变得越来越普遍。

然而，在现有的安全性信息交互系统中，IC 卡和安全性信息交互终端之间在进行相关的脱机情况下的安全性信息交互（例如交通卡的脱机充值操作）之前不进行合法性检查或者以对称认证的方式执行合法性检查（示例性地，在现在的技术方案中，当执行脱机操作（如充值）时，需要在终端上放置一个用于存放对称密钥的 PSAM 卡（终端安全存取模块），然而。该 PSAM 卡暴露在终端上，极易受到攻击，同时密钥管理（如传输、分散、更新、回收等）复杂，从而限制了卡片的跨地区使用），从而导致如下潜在的安全隐患：伪造的未授权的终端（例如 POS 机）可以与 IC 卡（例如交通卡）进行脱机情况下的安全性信息交互（例如执行交通卡的脱机充值操作）。

因此，存在如下需求：提供用于 IC 卡和安全性信息交互终端的脱机认证的方法以及能够使用该方法的 IC 卡和安全性信息交互终端。

发明内容

为了解决上述现有技术方案所存在的问题，本发明提出了用于 IC 卡和安全性信息交互终端的脱机认证的方法以及能够使用该方法的 IC 卡和安全性信息交互终端。

本发明的目的是通过以下技术方案实现的：

一种 IC 卡，所述 IC 卡包括:

通信接口，所述通信接口用于建立所述 IC 卡与安全性信息交互终端之间的数据通信链路;

认证单元，所述认证单元用于在所述 IC 卡与安全性信息交互终端之间已建立了数据通信链路后接收并处理来自所述安全性信息交互终端的认证指令而执行对所述安全性信息交互终端的认证过程，并将认证结果传送回所述安全性信息交互终端;

主控制器，所述主控制器用于在认证通过所述安全性信息交互终端后接收来自所述安全性信息交互终端的安全性信息交互请求并加载相应的应用以执行后续的安全性信息交互过程;

存储器，所述存储器用于存储至少一个应用以及与所述认证相关联的参数;

其中，在脱机情况下执行对所述安全性信息交互终端的所述认证过程。

在上面所公开的方案中，优选地，所述认证指令包括终端记录读取命令、卡随机数获取命令和内部认证命令。

在上面所公开的方案中，优选地，所述与所述认证相关联的参数包括认证中心公钥以及卡片认证支持能力标志，所述卡片认证支持能力标志的值指示所述 IC 卡对脱机认证支持的能力。

在上面所公开的方案中，优选地，当接收到来自所述安全性信息交互终端的终端记录读取命令后，所述认证单元从所述终端记录读取命令中解析出认证中心公钥索引、通用服务提供方公钥证书和终端公钥证书，并通过所述认证中心公钥索引获取存储在所述存储器中的认证中心公钥，所述认证单元进一步基于所述认证中心公钥和所述通用服务提供方公钥证书而恢复得到通用服务提供方公钥，并且基于所述通用服务提供方公钥验证所述终端公钥证书以恢复得到所述终端公钥证书中的终端公钥，所述认证单元随后将终端记录读取响应发送回所述安全性信息交互终端。

在上面所公开的方案中，优选地，如果所述卡片认证支持能力标志指示所述 IC 卡不支持脱机认证，则所述 IC 卡不执行所述脱机认证过程。

在上面所公开的方案中，优选地，所述主控制器进一步用于如果未认证通

过所述安全性信息交互终端，则终止与所述安全性信息交互终端的安全性信息交互过程。

在上面所公开的方案中，优选地，当接收到来自所述安全性信息交互终端的卡随机数获取命令后，所述认证单元生成卡片随机数，并将卡随机数获取响应传送回所述安全性信息交互终端，其中，所述卡随机数获取响应包括所述卡片随机数和 ATC（即应用交易计数器）。

在上面所公开的方案中，优选地，当接收到来自所述安全性信息交互终端的内部认证命令后，所述认证单元从所述内部认证命令中解析出动态签名数据，并使用所述终端公钥验证所述动态签名数据，以及如果验证通过，则向所述安全性信息交互终端发送指示“认证成功”的内部认证响应，并且如果验证未通过，则向所述安全性信息交互终端发送指示“认证失败”的内部认证响应，并终止与所述安全性信息交互终端的安全性信息交互过程。

在上面所公开的方案中，优选地，使用非对称密钥算法执行所述认证过程。

本发明的目的也可以通过以下技术方案实现：

一种安全性信息交互终端，所述安全性信息交互终端包括：

认证模块，所述认证模块用于在所述安全性信息交互终端与IC卡之间已建立了数据通信链路后向所述IC卡发送认证指令以执行对所述安全性信息交互终端的认证过程；

主控制模块，所述主控制模块用于在所述认证通过后向所述IC卡发送安全性信息交互请求，以完成后续的安全性信息交互过程；

存储模块，所述存储模块用于存储与所述认证相关联的参数；

其中，在脱机情况下执行所述认证过程。

在上面所公开的方案中，优选地，所述认证指令包括终端记录读取命令、卡随机数获取命令和内部认证命令。

在上面所公开的方案中，优选地，所述与所述认证相关联的参数包括通用服务提供方公钥证书、终端公钥证书、终端私钥、认证中心公钥索引、终端认证支持能力标志、认证执行标志和认证未执行标志，所述终端认证支持能力标志的值指示所述安全性信息交互终端对脱机认证支持的能力，所述认证执行标志的值指示对所述安全性信息交互终端的脱机认证已经被执行并通过，所述认

证未执行标志的值指示所述安全性信息交互终端的动态签名未验证通过。

在上面所公开的方案中，优选地，在所述 IC 卡与所述安全性信息交互终端之间已建立了数据通信链路后，所述认证模块向所述 IC 卡发送终端记录读取命令，其中，所述终端记录读取命令包括认证中心公钥索引、通用服务提供方公钥证书和终端公钥证书。

在上面所公开的方案中，优选地，在接收到来自所述 IC 卡的终端记录读取响应后，所述认证模块向所述 IC 卡发送卡随机数获取命令。

在上面所公开的方案中，优选地，在接收到来自所述 IC 卡的卡随机数获取响应后，所述认证模块基于解析出的卡片随机数和 ATC（即应用交易计数器）以及终端数据生成动态签名数据，并向所述 IC 卡发送内部认证命令，其中，所述内部认证命令包括所述动态签名数据。

在上面所公开的方案中，优选地，在接收到来自所述 IC 卡的内部认证响应后，如果所述内部认证响应指示“认证成功”，则所述认证模块将所述认证执行标志的值设置为“认证已执行通过”，并且如果所述内部认证响应指示“认证失败”，则所述认证模块将所述认证未执行标志的值设置为“认证未执行通过”。

在上面所公开的方案中，优选地，如果所述终端认证支持能力标志的值指示所述安全性信息交互终端不支持脱机认证，则所述安全性信息交互终端不执行所述脱机认证过程。

在上面所公开的方案中，优选地，所述主控制模块进一步用于如果所述脱机认证未通过，则终止与所述 IC 卡的安全性信息交互过程。

在上面所公开的方案中，优选地，使用非对称密钥算法执行所述认证过程。

本发明的目的也可以通过以下技术方案实现：

一种用于 IC 卡和安全性信息交互终端的脱机认证的方法，所述用于 IC 卡和安全性信息交互终端的脱机认证的方法包括下列步骤：

（A1）在 IC 卡与安全性信息交互终端之间已建立了数据通信链路后，所述安全性信息交互终端向所述 IC 卡发送认证指令以执行对所述安全性信息交互终端的认证过程，其中，在脱机情况下执行所述认证过程。

（A2）在所述认证通过后，所述安全性信息交互终端通过与所述 IC 卡的进

一步的数据通信而完成后续的安全性信息交互过程。

本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法以及能够使用该方法的 IC 卡和安全性信息交互终端具有如下优点：由于在进行相关的脱机情况下的安全性信息交互之前进行终端的合法性检查，故能够获得增强的安全性，从而避免了潜在的安全隐患（例如使用伪造的安全性信息交互终端完成安全性信息交互过程）。

附图说明

结合附图，本发明的技术特征以及优点将会被本领域技术人员更好地理解，其中：

图1是包含根据本发明的实施例的 IC 卡和安全性信息交互终端的安全性信息交互系统的示意性结构图；

图2是根据本发明的实施例的用于 IC 卡和安全性信息交互终端的脱机认证的方法的流程图。

具体实施方式

图1是包含根据本发明的实施例的 IC 卡和安全性信息交互终端的安全性信息交互系统的示意性结构图。如图1所示，本发明所公开的 IC 卡1包括主控制器3、认证单元4、存储器5和通信接口6。其中，所述通信接口6用于建立所述 IC 卡1与安全性信息交互终端2之间的数据通信链路（例如将 IC 卡靠近或接触安全性信息交互终端）。所述认证单元4用于在所述 IC 卡1与安全性信息交互终端2之间已建立了数据通信链路后接收并处理来自所述安全性信息交互终端2的认证指令而执行对所述安全性信息交互终端2的认证过程，并将认证结果传送回所述安全性信息交互终端2。所述主控制器3用于在认证通过所述安全性信息交互终端2后接收来自所述安全性信息交互终端2的安全性信息交互请求并加载相应的应用以执行后续的安全性信息交互过程（例如脱机充值操作）。所述存储器5用于存储至少一个应用以及与所述认证相关联的参数。其中，在脱机情况下执行对所述安全性信息交互终端2的所述认证过程。

优选地，在本发明所公开的 IC 卡1中，所述认证指令包括终端记录读取命

令、卡随机数获取命令和内部认证命令。

优选地，在本发明所公开的 IC 卡1中，所述与所述认证相关联的参数包括认证中心（即 CA，如本领域技术人员所知的，其为第三方认证服务提供机构）公钥以及卡片认证支持能力标志，所述卡片认证支持能力标志的值指示所述 IC 卡1对脱机认证支持的能力（即是否支持脱机认证）。

优选地，在本发明所公开的 IC 卡1中，当接收到来自所述安全性信息交互终端2的终端记录读取命令后，所述认证单元4从所述终端记录读取命令中解析出认证中心公钥索引（CPKI）、通用服务提供方（例如银联）公钥证书和终端公钥证书，并通过所述认证中心公钥索引（以及应用提供商标识 CRID）获取存储在所述存储器5中的认证中心公钥，所述认证单元4进一步基于所述认证中心公钥和所述通用服务提供方公钥证书而恢复得到通用服务提供方公钥（例如银联公钥），并且基于所述通用服务提供方公钥验证所述终端公钥证书以恢复得到所述终端公钥证书中的终端公钥，所述认证单元4随后将终端记录读取响应发送回所述安全性信息交互终端2。

示例性地，在本发明所公开的IC卡1中，所述恢复得到通用服务提供方公钥的步骤包括：a）检查通用服务提供方公钥证书与认证中心公钥的模长度是否相同；b）利用认证中心公钥对通用服务提供方公钥证书执行恢复操作，以得到通用服务提供方公钥；c）检查恢复数据中的下列各项是否正确：恢复的数据尾、恢复的数据头、证书格式、通用服务提供方标识、证书有效期和通用服务提供方算法标识；d）计算静态认证数据的哈希结果，并与从证书里恢复的哈希结果进行比较以判断是否一致；e）将恢复出的数据中的通用服务提供方公钥的模部分与余项部分（如果有的话）相组合以获得通用服务提供方公钥。

示例性地，在本发明所公开的 IC 卡1中，所述恢复得到所述终端公钥证书中的终端公钥的步骤包括：a）检查终端公钥证书与通用服务提供方公钥的模长度是否相同；b）利用通用服务提供方公钥对终端公钥证书进行恢复以获得终端公钥证书里的数据；c）检查恢复的数据中的下列各项是否正确：恢复的数据尾、恢复的数据头、证书格式、证书有效期、终端密钥算法标识；d）依次连接从终端公钥证书恢复出的数据、由 IC 卡1与终端共同指定的用于动态数据认证的记录数据，计算其哈希结果；e）将计算出的哈希结果与从终端公钥证书恢复出的

哈希结果相比较，如果不一致，则认证失败；f)将恢复出的数据中的终端公钥的模部分与余项部分（如果有的话）相组合以获得终端公钥。

优选地，在本发明所公开的 IC 卡1中，如果所述卡片认证支持能力标志指示所述 IC 卡1不支持脱机认证，则所述 IC 卡1不执行所述脱机认证过程。

优选地，在本发明所公开的 IC 卡1中，所述主控制器3进一步用于如果未认证通过所述安全性信息交互终端2，则终止与所述安全性信息交互终端2的安全性信息交互过程。

优选地，在本发明所公开的 IC 卡1中，当接收到来自所述安全性信息交互终端2的卡随机数获取命令后，所述认证单元4生成卡片随机数，并将卡随机数获取响应传送回所述安全性信息交互终端2，其中，所述卡随机数获取响应包括所述卡片随机数和 ATC（即应用交易计数器）。

优选地，在本发明所公开的 IC 卡1中，当接收到来自所述安全性信息交互终端2的内部认证命令后，所述认证单元4从所述内部认证命令中解析出动态签名数据，并使用所述终端公钥验证所述动态签名数据，以及如果验证通过，则向所述安全性信息交互终端2发送指示“认证成功”的内部认证响应，并且如果验证未通过，则向所述安全性信息交互终端2发送指示“认证失败”的内部认证响应，并终止与所述安全性信息交互终端2的安全性信息交互过程。

示例性地，在本发明所公开的IC卡1中，所述验证所述动态签名数据的步骤包括：a)检查所述动态签名数据中的动态应用数据与终端公钥的模的长度是否相同；b)利用终端公钥对所述动态签名数据中的动态应用数据进行恢复；c)检查恢复出的数据中的下列各项是否正确：恢复的数据尾，恢复的数据头，数据格式；d)依次连接从所述动态签名数据中恢复出的数据、所述卡片随机数和 ATC（应用交易计数器），并计算其哈希结果；e)将计算出的哈希结果与从所述动态签名数据中恢复出的哈希结果相比较，并且如果不一致，则验证未通过。

如上可见，优选地，在本发明所公开的IC卡1中，使用非对称密钥算法执行所述认证过程。

如图1所示，本发明所公开的安全性信息交互终端2包括主控制模块7、认证模块8和存储模块9。其中，所述认证模块8用于在所述安全性信息交互终端2与 IC 卡1之间已建立了数据通信链路后向所述 IC 卡1发送认证指令以执行对所

述安全性信息交互终端2的认证过程。所述主控制模块7用于在所述认证通过后向所述 IC 卡1发送安全性信息交互请求，以完成安全性信息交互过程。所述存储模块9用于存储与所述认证相关联的参数。其中，在脱机情况下执行所述认证过程。

优选地，在本发明所公开的安全性信息交互终端2中，所述认证指令包括终端记录读取命令、卡随机数获取命令和内部认证命令。

优选地，在本发明所公开的安全性信息交互终端2中，所述与所述认证相关联的参数包括通用服务提供方（例如银联）公钥证书、终端公钥证书、终端私钥、认证中心公钥索引（CPKI）、终端认证支持能力标志、认证执行标志和认证未执行标志，所述终端认证支持能力标志的值指示所述安全性信息交互终端2对脱机认证支持的能力（即是否支持脱机认证），所述认证执行标志的值指示对所述安全性信息交互终端2的脱机认证已经被执行并通过，所述认证未执行标志的值指示所述安全性信息交互终端2的动态签名未验证通过。

优选地，在本发明所公开的安全性信息交互终端2中，在所述 IC 卡1与所述安全性信息交互终端2之间已建立了数据通信链路后，所述认证模块8向所述 IC 卡1发送终端记录读取命令，其中，所述终端记录读取命令包括认证中心公钥索引（CPKI）、通用服务提供方（例如银联）公钥证书和终端公钥证书。

优选地，在本发明所公开的安全性信息交互终端2中，在接收到来自所述 IC 卡1的终端记录读取响应后，所述认证模块8向所述 IC 卡1发送卡随机数获取命令。

优选地，在本发明所公开的安全性信息交互终端2中，在接收到来自所述 IC 卡1的卡随机数获取响应后，所述认证模块8基于解析出的卡片随机数和 ATC（应用交易计数器）以及终端数据（示例性地，所述终端数据可以包括商户代码、终端代码、交易日期、交易时间、终端流水号、终端不可预知数等）生成动态签名数据，并向所述 IC 卡2发送内部认证命令，其中，所述内部认证命令包括所述动态签名数据。

示例性地，在本发明所公开的安全性信息交互终端2中，所述生成动态签名数据的步骤包括：a)连接卡片数据（即卡片随机数和ATC）和指定的终端数据以构成动态应用数据；b) 用上一步连接的数据执行哈希运算；c) 将哈希运

算结果包括在所述动态应用数据中；d）使用终端私钥给所述动态应用数据做签名以形成动态签名数据；e）在所述内部认证命令中携带所述动态签名数据。

优选地，在本发明所公开的安全性信息交互终端2中，在接收到来自所述IC 卡1的内部认证响应后，如果所述内部认证响应指示“认证成功”，则所述认证模块8将所述认证执行标志的值设置为“认证已执行通过”（例如将其值设置为“1”），并且如果所述内部认证响应指示“认证失败”，则所述认证模块8将所述认证未执行标志的值设置为“认证未执行通过”（例如将其值设置为“1”）。

优选地，在本发明所公开的安全性信息交互终端2中，如果所述终端认证支持能力标志的值指示所述安全性信息交互终端2不支持脱机认证，则所述安全性信息交互终端2不执行所述脱机认证过程。

优选地，在本发明所公开的安全性信息交互终端2中，所述主控制模块7进一步用于如果所述脱机认证未通过，则终止与所述 IC 卡1的安全性信息交互过程。

如上可见，优选地，在本发明所公开的安全性信息交互终端2中，使用非对称密钥算法执行所述认证过程。

可选地，本发明所公开的安全性信息交互终端2可以使用动态数据对象列表的方式指定构造所述动态签名数据所需的卡片数据（示例性地，所述卡片数据包括卡片随机数和 ATC（应用交易计数器））。

图2是根据本发明的实施例的用于 IC 卡和安全性信息交互终端的脱机认证的方法的流程图。如图2所示，本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法包括下列步骤：（A1）在 IC 卡与安全性信息交互终端之间已建立了数据通信链路后，所述安全性信息交互终端向所述 IC 卡发送认证指令以执行对所述安全性信息交互终端的认证过程；（A2）在所述认证通过后，所述安全性信息交互终端通过与所述 IC 卡的进一步的数据通信而完成后续的安全性信息交互过程（例如脱机充值操作）。其中，在脱机情况下执行所述认证过程。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述认证指令包括终端记录读取命令、卡随机数获取命令和内部认

证命令。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，使用下列与所述认证相关联的参数：认证中心（即 CA，如本领域技术人员所知的，其为第三方认证服务提供机构）公钥、通用服务提供方（例如银联）公钥证书、终端公钥证书、终端私钥、认证中心公钥索引（CPKI）。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述步骤（A1）进一步包括：在所述 IC 卡与所述安全性信息交互终端之间已建立了数据通信链路后，所述安全性信息交互终端向所述 IC 卡发送终端记录读取命令，其中，所述终端记录读取命令包括认证中心公钥索引（CPKI）、通用服务提供方（例如银联）公钥证书和终端公钥证书。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述步骤（A1）进一步包括：当接收到来自所述安全性信息交互终端的终端记录读取命令后，所述 IC 卡从所述终端记录读取命令中解析出认证中心公钥索引（CPKI）、通用服务提供方（例如银联）公钥证书和终端公钥证书，并通过所述认证中心公钥索引（以及应用提供商标识 CRID）获取认证中心公钥，所述 IC 卡进一步基于所述认证中心公钥和所述通用服务提供方公钥证书而恢复得到通用服务提供方公钥（例如银联公钥），并且基于所述通用服务提供方公钥验证所述终端公钥证书以恢复得到所述终端公钥证书中的终端公钥，所述 IC 卡随后将终端记录读取响应发送回所述安全性信息交互终端。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述步骤（A1）进一步包括：在接收到来自所述 IC 卡的终端记录读取响应后，所述安全性信息交互终端向所述 IC 卡发送卡随机数获取命令。

示例性地，在本发明所公开的用于IC卡和安全性信息交互终端的脱机认证的方法中，所述恢复得到通用服务提供方公钥的步骤包括：a)检查通用服务提供方公钥证书与认证中心公钥的模长度是否相同；b)利用认证中心公钥对通用服务提供方公钥证书执行恢复操作，以得到通用服务提供方公钥；c)检查恢复数据中的下列各项是否正确：恢复的数据尾、恢复的数据头、证书格式、通用服务提供方标识、证书有效期和通用服务提供方算法标识；d)计算静态认证数据的哈希结果，并与从证书里恢复的哈希结果进行比较以判断是否一致；e)

将恢复出的数据中的通用服务提供方公钥的模部分与余项部分（如果有的话）相组合以获得通用服务提供方公钥。

示例性地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述恢复得到所述终端公钥证书中的终端公钥的步骤包括：a) 检查终端公钥证书与通用服务提供方公钥的模长度是否相同；b) 利用通用服务提供方公钥对终端公钥证书进行恢复以获得终端公钥证书里的数据；c) 检查恢复的数据中的下列各项是否正确：恢复的数据尾、恢复的数据头、证书格式、证书有效期、终端密钥算法标识；d) 依次连接从终端公钥证书恢复出的数据、由 IC 卡1与终端共同指定的用于动态数据认证的记录数据，计算其哈希结果；e) 将计算出的哈希结果与从终端公钥证书恢复出的哈希结果相比较，如果不一致，则认证失败；f) 将恢复出的数据中的终端公钥的模部分与余项部分（如果有的话）相组合以获得终端公钥。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述步骤（A1）进一步包括：当接收到来自所述安全性信息交互终端的卡随机数获取命令后，所述 IC 卡生成卡片随机数，并将卡随机数获取响应传送回所述安全性信息交互终端，其中，所述卡随机数获取响应包括所述卡片随机数和 ATC（应用交易计数器）。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述步骤（A1）进一步包括：在接收到来自所述 IC 卡的卡随机数获取响应后，所述安全性信息交互终端基于解析出的卡片随机数和 ATC（应用交易计数器）以及终端数据（示例性地，所述终端数据可以包括商户代码、终端代码、交易日期、交易时间、终端流水号、终端不可预知数等）生成动态签名数据，并向所述 IC 卡发送内部认证命令，其中，所述内部认证命令包括所述动态签名数据。

示例性地，在本发明所公开的用于IC卡和安全性信息交互终端的脱机认证的方法中，所述生成动态签名数据的步骤包括：a) 连接卡片数据（即卡片随机数和ATC）和指定的终端数据以构成动态应用数据；b) 用上一步连接的数据执行哈希运算；c) 将哈希运算结果包括在所述动态应用数据中；d) 使用终端私钥给所述动态应用数据做签名以形成动态签名数据；e) 在所述内部认证命令

中携带所述动态签名数据。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述步骤（A1）进一步包括：当接收到来自所述安全性信息交互终端的内部认证命令后，所述 IC 卡从所述内部认证命令中解析出动态签名数据，并使用所述终端公钥验证所述动态签名数据，以及如果验证通过，则向所述安全性信息交互终端发送指示“认证成功”的内部认证响应，并且如果验证未通过，则向所述安全性信息交互终端发送指示“认证失败”的内部认证响应，并终止与所述安全性信息交互终端的安全性信息交互过程。

示例性地，在本发明所公开的用于IC卡和安全性信息交互终端的脱机认证的方法中，所述验证所述动态签名数据的步骤包括：a)检查所述动态签名数据中的动态应用数据与终端公钥的模的长度是否相同；b)利用终端公钥对所述动态签名数据中的动态应用数据进行恢复；c)检查恢复出的数据中的下列各项是否正确：恢复的数据尾，恢复的数据头，数据格式；d)依次连接从所述动态签名数据中恢复出的数据、所述卡片随机数和ATC（应用交易计数器），并计算其哈希结果；e)将计算出的哈希结果与从所述动态签名数据中恢复出的哈希结果相比较，并且如果不一致，则验证未通过。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，所述步骤（A1）进一步包括：在接收到来自所述 IC 卡的内部认证响应后，如果所述内部认证响应指示“认证成功”，则所述安全性信息交互终端将所述安全性信息交互终端中的认证执行标志的值设置为“认证已执行通过”（例如将其值设置为“1”），并且如果所述内部认证响应指示“认证失败”，则所述安全性信息交互终端将所述安全性信息交互终端中的认证未执行标志的值设置为“认证未执行通过”（例如将其值设置为“1”）。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，如果所述安全性信息交互终端中的终端认证支持能力标志的值指示所述安全性信息交互终端不支持脱机认证，则所述安全性信息交互终端不执行所述脱机认证过程。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，如果所述 IC 卡中的卡片认证支持能力标志的值指示所述 IC 卡不支

持脱机认证，则所述 IC 卡1不执行所述脱机认证过程。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，如果未认证通过所述安全性信息交互终端，则所述 IC 卡终止与所述安全性信息交互终端的安全性信息交互过程。

优选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，如果所述脱机认证未通过，则所述安全性信息交互终端终止与所述 IC 卡的安全性信息交互过程。

如上可见，优选地，在本发明所公开的用于IC卡和安全性信息交互终端的脱机认证的方法中，使用非对称密钥算法执行所述认证过程。

可选地，在本发明所公开的用于 IC 卡和安全性信息交互终端的脱机认证的方法中，可以使用动态数据对象列表的方式指定构造所述动态签名数据所需的卡片数据（示例性地，所述卡片数据包括卡片随机数和 ATC（应用交易计数器））。

尽管本发明是通过上述的优选实施方式进行描述的，但是其实现形式并不局限于上述的实施方式。应该认识到：在不脱离本发明主旨和范围的情况下，本领域技术人员可以对本发明做出不同的变化和修改。

权利要求

1. 一种 IC 卡，所述 IC 卡包括:

通信接口，所述通信接口用于建立所述 IC 卡与安全性信息交互终端之间的数据通信链路;

认证单元，所述认证单元用于在所述 IC 卡与安全性信息交互终端之间已建立了数据通信链路后接收并处理来自所述安全性信息交互终端的认证指令而执行对所述安全性信息交互终端的认证过程，并将认证结果传送回所述安全性信息交互终端;

主控制器，所述主控制器用于在认证通过所述安全性信息交互终端后接收来自所述安全性信息交互终端的安全性信息交互请求并加载相应的应用以执行后续的安全性信息交互过程;

存储器，所述存储器用于存储至少一个应用以及与所述认证相关联的参数;

其中，在脱机情况下执行对所述安全性信息交互终端的所述认证过程。

2. 根据权利要求1所述的 IC 卡，其特征在于，所述认证指令包括终端记录读取命令、卡随机数获取命令和内部认证命令。

3. 根据权利要求2所述的 IC 卡，其特征在于，所述与所述认证相关联的参数包括认证中心公钥以及卡片认证支持能力标志，所述卡片认证支持能力标志的值指示所述 IC 卡1对脱机认证支持的能力。

4. 根据权利要求3所述的 IC 卡，其特征在于，当接收到来自所述安全性信息交互终端的终端记录读取命令后，所述认证单元从所述终端记录读取命令中解析出认证中心公钥索引、通用服务提供方公钥证书和终端公钥证书，并通过所述认证中心公钥索引获取存储在所述存储器中的认证中心公钥，所述认证单元进一步基于所述认证中心公钥和所述通用服务提供方公钥证书而恢复得到通用服务提供方公钥，并且基于所述通用服务提供方公钥验证所述终端公钥证书以恢复得到所述终端公钥证书中的终端公钥，所述认证单元随后将终端记录读取响应发送回所述安全性信息交互终端。

5. 根据权利要求4所述的 IC 卡，其特征在于，如果所述卡片认证支持能

力标志指示所述IC卡不支持脱机认证，则所述IC卡不执行所述脱机认证过程。

6. 根据权利要求5所述的 IC 卡，其特征在于，所述主控制器进一步用于如果未认证通过所述安全性信息交互终端，则终止与所述安全性信息交互终端的安全性信息交互过程。

7. 根据权利要求6所述的 IC 卡，其特征在于，当接收到来自所述安全性信息交互终端的卡随机数获取命令后，所述认证单元生成卡片随机数，并将卡随机数获取响应传送回所述安全性信息交互终端，其中，所述卡随机数获取响应包括所述卡片随机数和应用交易计数器（ATC）。

8. 根据权利要求7所述的 IC 卡，其特征在于，当接收到来自所述安全性信息交互终端的内部认证命令后，所述认证单元从所述内部认证命令中解析出动态签名数据，并使用所述终端公钥验证所述动态签名数据，以及如果验证通过，则向所述安全性信息交互终端发送指示“认证成功”的内部认证响应，并且如果验证未通过，则向所述安全性信息交互终端发送指示“认证失败”的内部认证响应，并终止与所述安全性信息交互终端的安全性信息交互过程。

9. 根据权利要求8所述的IC卡，其特征在于，使用非对称密钥算法执行所述认证过程。

10. 一种安全性信息交互终端，所述安全性信息交互终端包括:

认证模块，所述认证模块用于在所述安全性信息交互终端与IC卡之间已建立了数据通信链路后向所述IC卡发送认证指令以执行对所述安全性信息交互终端的认证过程;

主控制模块，所述主控制模块用于在所述认证通过后向所述IC卡发送安全性信息交互请求，以完成后续的安全性信息交互过程;

存储模块，所述存储模块用于存储与所述认证相关联的参数;

其中，在脱机情况下执行所述认证过程。

11. 根据权利要求10所述的安全性信息交互终端，其特征在于，所述认证指令包括终端记录读取命令、卡随机数获取命令和内部认证命令。

12. 根据权利要求11所述的安全性信息交互终端，其特征在于，所述与所述认证相关联的参数包括通用服务提供方公钥证书、终端公钥证书、终端私钥、认证中心公钥索引、终端认证支持能力标志、认证执行标志和认证未执行标志，

所述终端认证支持能力标志的值指示所述安全性信息交互终端对脱机认证支持的能力，所述认证执行标志的值指示对所述安全性信息交互终端的脱机认证已经被执行并通过，所述认证未执行标志的值指示所述安全性信息交互终端的动态签名未验证通过。

13. 根据权利要求12所述的安全性信息交互终端，其特征在于，在所述 IC 卡与所述安全性信息交互终端之间已建立了数据通信链路后，所述认证模块向所述 IC 卡发送终端记录读取命令，其中，所述终端记录读取命令包括认证中心公钥索引、通用服务提供方公钥证书和终端公钥证书。

14. 根据权利要求13所述的安全性信息交互终端，其特征在于，在接收到来自所述 IC 卡的终端记录读取响应后，所述认证模块向所述 IC 卡发送卡随机数获取命令。

15. 根据权利要求14所述的安全性信息交互终端，其特征在于，在接收到来自所述 IC 卡的卡随机数获取响应后，所述认证模块基于解析出的卡片随机数和应用交易计数器（ATC）以及终端数据生成动态签名数据，并向所述 IC 卡发送内部认证命令，其中，所述内部认证命令包括所述动态签名数据。

16. 根据权利要求15所述的安全性信息交互终端，其特征在于，在接收到来自所述 IC 卡的内部认证响应后，如果所述内部认证响应指示“认证成功”，则所述认证模块将所述认证执行标志的值设置为“认证已执行通过”，并且如果所述内部认证响应指示“认证失败”，则所述认证模块将所述认证未执行标志的值设置为“认证未执行通过”。

17. 根据权利要求16所述的安全性信息交互终端，其特征在于，如果所述终端认证支持能力标志的值指示所述安全性信息交互终端不支持脱机认证，则所述安全性信息交互终端不执行所述脱机认证过程。

18. 根据权利要求17所述的安全性信息交互终端，其特征在于，所述主控制模块进一步用于如果所述脱机认证未通过，则终止与所述 IC 卡的安全性信息交互过程。

19. 根据权利要求18所述的安全性信息交互终端，其特征在于，使用非对称密钥算法执行所述认证过程。

20. 一种用于 IC 卡和安全性信息交互终端的脱机认证的方法，所述用于

IC卡和安全性信息交互终端的脱机认证的方法包括下列步骤:

（A1）在IC卡与安全性信息交互终端之间已建立了数据通信链路后，所述安全性信息交互终端向所述IC卡发送认证指令以执行对所述安全性信息交互终端的认证过程，其中，在脱机情况下执行所述认证过程;

（A2）在所述认证通过后，所述安全性信息交互终端通过与所述IC卡的进一步的数据通信而完成后续的安全性信息交互过程。

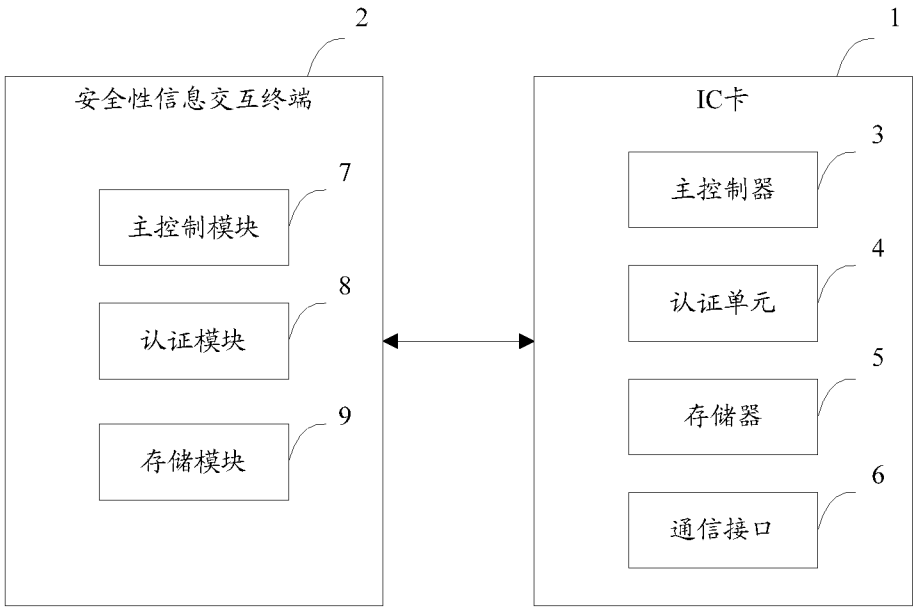


图 1

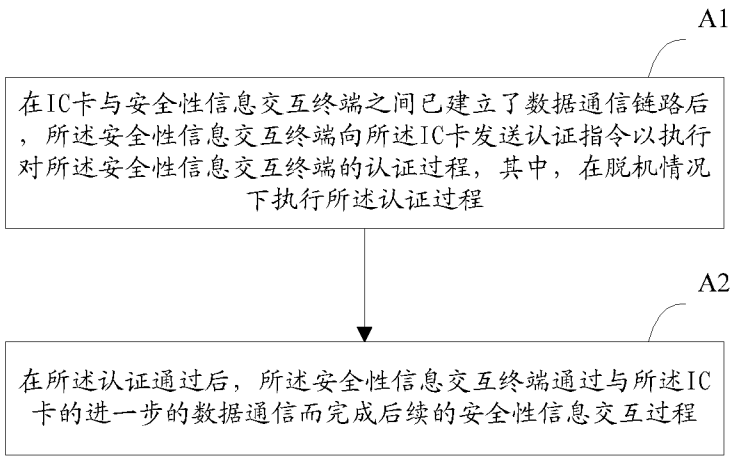

A1
在IC卡与安全性信息交互终端之间已建立了数据通信链路后，所述安全性信息交互终端向所述IC卡发送认证指令以执行对所述安全性信息交互终端的认证过程，其中，在脱机情况下执行所述认证过程
A2
在所述认证通过后，所述安全性信息交互终端通过与所述IC卡的进一步的数据通信而完成后续的安全性信息交互过程

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/080167

A. CLASSIFICATION OF SUBJECT MATTER

G07F 19/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F, H04L, G07F, G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPIEPOD, OC, CNKI, CNPAT: IEEE, IC, certificate authority, public key, terminal, offline, authenticate, ca, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102081821 A (CHINA UNIONPAY CO., LTD.), 01 June 2011 (01.06.2011), description, paragraphs [0068]-[0087], and figures 1-5	1-3, 10-11, 20
A	CN 101441722 A (CHINA UNIONPAY CO., LTD.), 27 May 2009 (27.05.2009), the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 October 2013 (12.10.2013)	**07 November 2013 (07.11.2013)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **JU, Bo** Telephone No.: (86-10) **62413661**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/080167

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102081821 A	01.06.2011	EP 2506226 A1	03.10.2012
		US 2013001304 A1	03.01.2013
		WO 2011063590 A1	03.06.2011
CN 101441722 A	27.05.2009	WO 2009065317 A1	28.05.2009

国际检索报告

国际申请号
PCT/CN2013/080167

A. 主题的分类

G07F 19/00 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:G06F,H04L,G07F,G06K

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI;EPODOC;CNKI;CNPAT;IEEE:IC,终端,脱机,认证,认证中心,公钥,terminal,offline,authenticate,ca,key

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN102081821A(中国银联股份有限公司)01.6 月 2011(01.06.2011) 说明书第[0068]-[0087]段、附图 1-5	1-3,10-11,20
A	CN101441722A(中国银联股份有限公司) 27.5 月 2009(27.05.2009)全文	1-20

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
12.10 月 2013(12.10.2013)	**07.11 月 2013 (07.11.2013)**

ISA/CN 的名称和邮寄地址：	受权官员
中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	鞠博 电话号码：(86-10) **62413661**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/080167

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN102081821A	01.06.2011	EP2506226A1	03.10.2012
		US2013001304A1	03.01.2013
		WO2011063590A1	03.06.2011
CN101441722A	27.05.2009	WO2009065317A1	28.05.2009