(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
2017 年 7 月 13 日 (13.07.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/118315 A1

(51) 国际专利分类号:
G06F 21/34 (2013.01)

(21) 国际申请号: PCT/CN2016/112265

(22) 国际申请日: 2016 年 12 月 27 日 (27.12.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610006062.2 2016 年 1 月 5 日 (05.01.2016) CN

(71) 申请人: **阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED)** [—/CN]; 开曼群岛英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: **修超 (XIU, Chao)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **王磊 (WANG, Lei)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **施晨杰 (SHI, Chenjie)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: **北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.)**; 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: SECURITY VERIFICATION METHOD AND DEVICE FOR SMART CARD APPLICATION

(54) **发明名称**: 一种智能卡应用安全验证方法及装置

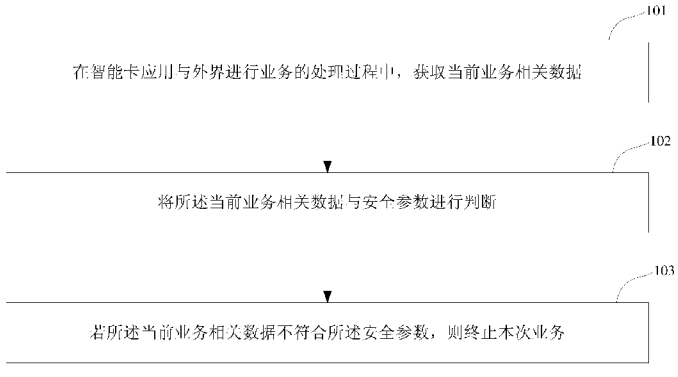

图 1

101 IN A PROCESS IN WHICH A SMART CARD APPLICATION CARRIES OUT A SERVICE WITH THE OUTSIDE, OBTAINING DATA RELATED TO THE CURRENT SERVICE
102 DETERMINING DATA AND SECURITY PARAMETERS RELATED TO THE CURRENT SERVICE
103 IF THE DATA RELATED TO THE CURRENT SERVICE DOES NOT SATISFY THE SECURITY PARAMETERS, TERMINATING THIS SERVICE

(57) **Abstract**: A security verification method and device for a smart card application. The method comprises: in a process in which a smart card application carries out a service with the outside, obtaining data related to the current service (101); determining data and security parameters related to the current service (102); and if the data related to the current service does not satisfy the security parameters, terminating this service (103). The device corresponding to the method can be built in a virtual smart card application or a smart card application independent from an eSE chip so as to implement the method; by means of the method and the device, judgments related to geographical position, time and transaction information and other content can be carried out on a service, and accordingly, the security when the service is carried out by using the smart card application can be further ensured.

(57) **摘要**: 一种智能卡应用安全验证方法及装置，其中该方法包括在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据（101）；将所述当前业务相关数据与安全参数进行判断（102）；若所述当前业务相关数据不符合所述安全参数，则终止本次业务（103）。方法相应的装置可以内置于虚拟智能卡应用中或者独立于 eSE 芯片中的智能卡应用以执行上述方法，通过该方法和装置对业务进行时地理位置、时间、交易信息等内容的判断，可以进一步的确保使用智能卡应用进行业务时的安全性。

WO 2017/118315 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种智能卡应用安全验证方法及装置

本申请要求2016年01月05日递交的申请号为201610006062.2、发明名称为“一种智能卡应用安全验证方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及信息安全技术领域，特别涉及一种智能卡应用安全验证方法及装置。

背景技术

随着移动互联网的发展，越来越多的业务可以通过智能终端的智能卡应用来实现，例如通过在智能终端实现移动支付、实现乘坐公共交通工具、实现进入自己的工作区域等，均可以通过给智能终端增加近场通信芯片来实现上述智能卡应用。但是，智能终端的通途越来越广，在用户生活中所扮演的角色也越来越重要，如果智能终端丢失后被恶意盗用可能会给用户甚至公司、社会造成严重后果。现在亟需一种增强智能终端智能卡应用安全性的技术方案。

发明内容

为了解决现有技术中智能终端被盗用后无法保证智能卡应用安全性的问题，提出了一种智能卡应用安全验证方法及装置，用于根据用户的设定或者用户的使用习惯限制智能卡应用的使用，从而保证了智能卡应用的安全性。

本申请实施例具体提供了一种智能卡应用安全验证方法，包括，

在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据；

将所述当前业务相关数据与安全参数进行判断；

若所述当前业务相关数据不符合所述安全参数，则终止本次业务。

本申请实施例还提供了一种智能卡应用安全验证装置，包括，

获取单元，用于在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据；

判断单元，用于将所述当前业务相关数据与安全参数进行判断；

处理单元，用于若所述当前业务相关数据不符合所述安全参数，则终止本次业务。

由以上本申请实施例提供的技术方案可见，对业务进行时地理位置、时间、交易信

息等内容的判断，可以进一步的确保使用智能卡应用进行业务时的安全性；并且在根据了智能卡应用的不同种类（eSE 芯片或者 HCE 等），设计了适用于不同种类智能卡应用的安全验证方法，例如获取 eSE 芯片内的智能卡应用与通信模块之间的业务过程，从而进行验证，或者通过内置于 HCE 智能卡应用中的安全验证方法来对业务进行安全验证。

当然实施本申请的任一产品或者方法必不一定需要同时达到以上所述的所有优点。

附图说明

为了更清楚地说明本申请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申请中记载的一些实施例，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。

图 1 所示为本申请实施例一种智能卡应用安全验证方法的流程图；

图 2 所示为本申请实施例一种智能卡应用安全验证装置的结构示意图；

图 3 所示为本申请实施例一种智能卡应用安全验证方法的具体流程图；

图 4 所示为本申请实施例安装智能卡应用到 eSE 芯片中的系统结构图；

图 5 所示为本申请实施例另一种智能卡应用安全验证方法的具体流程图；

图 6 所示为本申请实施例安装智能卡应用到智能手机中的系统结构图。

具体实施方式

本申请实施例提供一种智能卡应用安全验证方法及装置。

为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

在本申请中的智能卡应用包括了例如门禁、交通卡、银行卡等应用，在智能终端中设置 eSE 芯片（嵌入式安全元件），在该 eSE 芯片中置入所述智能卡应用，或者通过 HCE（卡模拟）的技术来实现智能卡应用，以上两种方式均为现有技术，在本申请中不再赘述。

如图 1 所示为本申请实施例一种智能卡应用安全验证方法的流程图，在本实施例中，

智能终端与交易终端进行业务处理的过程中，在智能终端根据判断规则判断当前业务是否安全，如果不安全则中断该业务，否则允许业务继续进行，其中的判断规则可以为根据位置信息、时间信息、业务内容等诸多信息的判断，可以由用户自行设定，或者有系统端统计分析后给所述智能终端，通过上述方式可以对智能卡应用进行安全控制，防止智能终端丢失后的危害。

该图具体包括步骤 101，在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据。

步骤 102，将所述当前业务相关数据与安全参数进行判断。

步骤 103，若所述当前业务相关数据不符合所述安全参数，则终止本次业务。

根据本申请的一个实施例，还包括若所述当前业务相关数据符合所述安全参数，则允许继续进行本次业务。通过对当前业务相关数据的判断，可以中断或者授权本次业务，从而可以进一步保证智能卡应用所进行的本次业务的安全性。

根据本申请的一个实施例，所述当前业务相关数据至少包括当前位置信息、当前时间信息、交易信息中的一个或者多个的组合。其中，通过当前位置信息可以与安全参数中设定的位置信息进行判断，如果超出所述安全参数中设定的位置范围，则不应当允许业务的继续进行，例如，当智能卡应用正在进行业务的当前位置为天津，而用户设定的安全参数中的位置范围为北京，则认为智能卡应用所进行的本次业务是不安全的；或者，当智能卡应用正在进行业务的交易为付款 1000 元，而用户设定的安全参数的交易信息中为 800 元，则认为智能卡应用所进行的本次业务是不安全的。

所述当前业务相关数据可以通过智能终端的 GPS 模块或者基站的定位方式获得当前位置信息，通过系统时钟或者网络时钟获得当前时间信息，通过交易订单获得交易信息。其中定位的具体方法可以参考现有技术中的定位技术，获取当前时间信息也可以参考现有技术中的具体方案，在此不再赘述。

根据本申请的一个实施例，在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据之中还包括，在内置于 eSE 芯片（嵌入式安全元件）的智能卡应用与 NFC（近场通信单元）控制器的通信过程中，监测双方的通信过程，并获取当前业务相关数据。

在本步骤的实施例中，本申请实施例中的方法可以以软件方式或者以硬件模块的方式实施，该获取当前业务相关数据以及后面的判断分析等处理过程构成的方法是以监测 eSE 芯片中智能卡应用与 NFC 控制器（或者类似其它智能卡应用所使用的通信模块）之

间的通信过程而激活的，或者还可以由 NFC 控制器在进行某个业务过程中通知本申请的安全验证应用，也就是说本申请实施例的安全验证方法监测 eSE 芯片中智能卡应用与 NFC 控制器之间是否正在进行业务处理，如果出现业务处理，则启动安全验证。

本实施例还可以在智能卡应用与 NFC 控制器通信的任意过程中获取当前业务相关数据以及后继步骤，例如在 NFC 控制器向智能卡应用转发业务指令之前进行安全验证。

根据本申请的一个实施例，在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据之中还包括，在虚拟智能卡的应用（HCE）与 NFC 控制器的通信过程中，在虚拟智能卡的应用中监测双方的通信过程，并获取当前业务相关数据。

在本步骤中的实施例中，当智能卡应用是通过模拟智能卡的应用（HCE）来实现的，那么可以在该应用中加入本申请的安全验证方法，可以在该模拟智能卡的应用进行业务过程中的任意步骤之前或者之后进行本申请实施例的安全验证方法，当通过安全验证，则可以继续业务过程，否则将中断业务过程。

根据本申请的一个实施例，在将所述当前业务相关数据与安全参数进行判断之前还包括，接收并保存用户输入的安全参数；

或者，接收并保存服务器根据用户的相关数据分析得到的安全参数。

在本步骤的实施例中，安全参数可以由用户自行设定，也可以通过服务器基于用户历史行为的分析确定，例如通过统计分析该用户从而出现在 A 区域，而本次业务的位置信息为 A 区域，则认为该业务可能存在安全风险，可以拒绝用户的本次业务，再进一步的实施例中，例如当业务为门禁认证时，该用户从来未要求进入过 A 区，本次要求进入 A 区，可能是由于具有门禁智能卡应用的手机丢失，被人捡到后的行为。

通过本申请实施例的方法，对业务进行时地理位置、时间、交易信息等内容的判断，可以进一步的确保使用智能卡应用进行业务时的安全性；并且在根据了智能卡应用的不同种类（eSE 芯片或者 HCE 等），设计了适用于不同种类智能卡应用的安全验证方法，例如获取 eSE 芯片内的智能卡应用与通信模块之间的业务过程，从而进行验证，或者通过内置于 HCE 智能卡应用中的安全验证方法来对业务进行安全验证。

如图 2 所示为本申请实施例一种智能卡应用安全验证装置的结构示意图，在本实施例中的装置可以内置并运行于智能终端上，其中智能终端例如包括智能手机、平板电脑等设备，所述智能卡应用验证装置可以由可编程逻辑器件（FPGA）等专用芯片实现，或者在模拟智能卡应用（HCE）中通过软件实现。

该图具体包括获取单元 201，用于在智能卡应用与外界进行业务的处理过程中，获

取当前业务相关数据。

判断单元 202，用于将所述当前业务相关数据与安全参数进行判断。

处理单元 203，用于若所述当前业务相关数据不符合所述安全参数，则终止本次业务。

根据本申请的一个实施例，所述处理单元还用于若所述当前业务相关数据符合所述安全参数，则允许继续进行本次业务。

根据本申请的一个实施例，所述当前业务相关数据至少包括当前位置信息、当前时间信息、交易信息中的一个或者多个的组合。

其中，所述当前位置信息可以通过智能终端内部的 GPS 模块获得，所述当前时间信息可以通过网络通信模块获得，或者通过智能终端内部的时钟晶振获得，所述交易信息可以通过智能终端的交易订单获得。

根据本申请的一个实施例，所述获取单元监测内置于 eSE 芯片（嵌入式安全元件）的智能卡应用与 NFC（近场通信单元）控制器的通信过程，并获取当前业务相关数据。

根据本申请的一个实施例，所述获取单元内置于虚拟智能卡的应用中，获取虚拟智能卡的应用（HCE）与 NFC 控制器的通信过程中的当前业务相关数据。

根据本申请的一个实施例，还包括安全参数接收单元 204，用于接收并保存用户输入的安全参数；

或者，接收并保存服务器根据用户的相关数据分析得到的安全参数。

通过本申请实施例的装置，对业务进行时地理位置、时间、交易信息等内容的判断，可以进一步的确保使用智能卡应用进行业务时的安全性；并且在根据了智能卡应用的不同种类（eSE 芯片或者 HCE 等），设计了适用于不同种类智能卡应用的安全验证方法，例如获取 eSE 芯片内的智能卡应用与通信模块之间的业务过程，从而进行验证，或者通过内置于 HCE 智能卡应用中的安全验证方法来对业务进行安全验证。

如图 3 所示为本申请实施例一种智能卡应用安全验证方法的具体流程图，在该图中的智能卡应用内置于 eSE 安全芯片之中，本实施例中的智能终端可以为智能手机，读卡器可以为 POS 机上安装的 NFC 读卡器，NFC 控制器为智能手机上的硬件，用于与 POS 机上的 NFC 读卡器通信以完成支付业务。在智能手机中内置本申请实施例中的装置或者用软件方式运行的方法，监测智能卡应用与 NFC 控制器之间的支付业务处理过程，从而实现对支付业务进行安全验证的目的。

具体包括步骤 301，内置于 eSE 芯片中的支付应用在 NFC 控制器上注册，在 NFC

控制器中记录有支付应用 ID。

在本实施例中智能卡应用可以通过智能卡应用管理终端安装到 eSE 芯片中，或者通过空中发卡单元（可以内置于智能手机的 eSE 芯片内部）通过网络安装到 eSE 芯片中，具体系统结构图可以如图 4 所示，其中，POS 机上的 NFC 读卡器通过近场通信的方式与智能手机的 NFC 控制器进行通信，智能卡应用管理终端也是通过该近场通信方式将智能卡应用安装于智能手机的 eSE 芯片中，或者还可以通过空中发卡单元从远端获取智能卡应用安装于 eSE 芯片中，本申请中的安全验证应用也内置于智能手机中，监测 eSE 芯片和 NFC 控制器之间的通信，该安全验证应用也可以通过 NFC 控制器中的通信接口监测 eSE 芯片和 NFC 控制器之间的通信。

在本步骤中或者在本步骤之前，用户可以通过智能手机的输入设备，例如触摸屏幕、按键等方式，在内置于智能手机的本申请的安全验证应用中输入安全参数，其中安全参数在智能卡的支付应用中可以例如为限定位置地点或者范围、交易金额门限值等，或者可以根据实际的需要增加或者减少安全参数的设定，在本实施例中限定位置例如为 A 地区、B 地区、C 地区以及贯穿这三个地区的沿途都是允许使用智能卡的支付应用，在其它地区禁止使用该支付应用，交易金额门限值例如可以为 1000 块，即无论在什么地区，均不允许消费超过 1000 元，当然本领域技术人员通过上述本申请的公开可以联想到其它组合的安全参数，例如交易金额与限定位置组合，即，在限定位置区域内交易金额可以不受限制，在限定位置以外的区域交易金额只能为 100，如果安全参数中考虑到时间参数，则可以出现更多种组合可能的安全参数，在本申请实施例中不能穷尽各种可能的组合，因此不再赘述。

步骤 302，POS 机的 NFC 读卡器与智能手机的 NFC 控制器近距离通信进行支付业务。

在本步骤中，NFC 读卡器与 NFC 控制器之间的支付业务处理过程可以参考现有技术中的方案，例如，NFC 读卡器选择 NFC 控制器中注册的支付应用 ID，然后执行相应的智能卡支付业务流程。

步骤 303，NFC 控制器向安全验证应用发送支付业务的提示，以启动安全验证应用。

步骤 304，内置于智能手机中的安全验证应用获取支付业务相关数据。

在本步骤中安全验证应用可以通过 NFC 控制器的接口获得支付业务相关数据，此时支付应用不会获得该支付业务相关数据。

所述支付业务相关数据包括当前的位置信息和当前交易金额。其中，安全验证应用

通过智能手机中的GPS模块获取当前的位置信息，或者可以通过基站定位的方式或者网络定位的方式获得当前位置信息，通过截获的业务处理结果可以获得本次交易金额。

步骤305，根据安全参数验证当前位置信息和当前交易金额。

在本实施例中，截获的位置信息为D区域，交易金额为2000元，将支付业务相关数据与安全参数中的限定位置和交易金额门限值进行比较，判断结果为不符合安全参数。

步骤306，安全验证应用终止本次支付业务，并将本次支付业务失败的执行结果发送给NFC控制器。

在本步骤中，还可以将安全验证的结果通过智能手机的屏幕向用户进行提示。

若上述步骤305中的判断结果为符合安全参数，则允许本次支付业务继续进行（即不作为），不干扰NFC控制器和eSE芯片中智能卡应用进行的支付业务过程，在图中以虚线的方式显示允许支付业务继续进行时支付应用进行业务处理的过程，NFC控制器将支付业务指令转发给内置于eSE芯片中的支付应用，支付应用进行业务处理，并通过NFC控制器向NFC读卡器返回业务处理结果，支付应用可能与NFC读卡器之间还具有多次的通信，以使得支付业务流程顺利进行，但是这部分内容作为现有技术中不在本实施例中赘述。

步骤307，NFC控制器将本次支付业务失败的执行结果发送给POS机NFC读卡器，本次支付失败。

通过上述实施例，本申请的技术方案可以根据用户设定的安全参数控制进行智能卡应用，当进行未授权（即安全参数以外）的业务时，将会及时终止不安全的智能卡应用的业务处理，保证了用户财产、信息的安全，避免由于智能终端丢失后被他人恶意使用而造成的损失。

如图5所示为本申请实施例另一种智能卡应用安全验证方法的具体流程图，在该实施例中以虚拟智能卡应用为例介绍本申请的技术方案，虚拟智能卡主要是针对一些没有内置eSE芯片的智能终端，使这种智能终端可以支持智能卡应用，本申请的安全验证方法或者装置可以内置于虚拟智能卡应用中，从而可以实现对该虚拟智能卡应用进行安全验证的目的。在本实施例中还是以支付业务作为说明，智能终端为智能手机，POS机读卡器还是NFC读卡器，智能手机通过NFC控制器与NFC读卡器进行通信，当然，在其它实施例中，还可以采用其它模式的近场通信技术进行通信，在此不做限定。

具体包括步骤501，虚拟智能卡应用在NFC控制器中注册支付应用ID。

在本实施例中虚拟智能卡应用可以通过智能卡应用管理终端安装到智能手机的存储

器中，具体系统结构图可以如图 6 所示，其中，POS 机上的 NFC 读卡器通过近场通信的方式与智能手机的 NFC 控制器进行通信，智能卡应用管理终端也是通过该近场通信方式将虚拟智能卡应用安装于智能手机的存储器中，或者还可以通过智能手机的联网功能从远端获取虚拟智能卡应用安装于智能手机中，本申请的安全验证应用可以内置于所述虚拟智能卡应用中。

步骤 502，POS 机的 NFC 读卡器与 NFC 控制器通信，选择虚拟智能卡应用 ID 进行支付业务。

步骤 503，NFC 控制器将进行支付业务的指令发送给虚拟智能卡应用。

步骤 504，虚拟智能卡应用中的安全验证应用可以获取当前位置信息、当前时间信息。

其中，获取当前位置信息可以通过智能手机中的 GPS 模块获取当前的位置信息，或者可以通过基站定位的方式或者网络定位的方式获得当前位置信息；当前时间信息可以通过智能手机的系统时间中获得，或者也可以通过智能手机的联网功能从互联网中获取。

步骤 505，通过智能手机的通信模块从远端服务器中获取该用户的安全参数。

在本步骤中的安全参数是通过互联网，从远端服务器中获得，所述远端服务器通过对用户的历史数据进行分析，或者通过对该用户相关的大数据分析得到相应安全参数，例如通过该用户日常的支付交易习惯、金额、地点、时间、商品类别等数据中分析得到该用户安全参数，根据用户的数据判断本次交易的安全风险在电子交易领域中有很多实现方法，本申请中所涉及的具体安全参数计算方法可以参考现有技术中的内容，此处只是利用到该部分的现有技术。

本实施例中获取安全参数的方法和图 3 所示实施例中由用户设定安全参数的方法可以互换。

步骤 506，根据安全参数验证本次支付业务的当前位置信息和当前时间信息。

若安全参数中的位置信息与当前位置信息不同，并且安全参数中的时间信息与当前时间信息不同，即说明该用户通常不会在当前时间、当前位置进行支付业务，该支付业务可能不是用户本人实施，可能存在风险。

步骤 507，终止本次支付业务，产生相应业务处理结果，并传送给 NFC 控制器。

若上述步骤 506 的判断结果为安全支付业务，则继续执行虚拟智能卡应用的支付业务流程，期间可能通过 NFC 控制器与 POS 级的 NFC 读卡器进行一次或者数次通信，已完成支付业务流程。

步骤 508，NFC 控制器将支付业务处理结果发送给 POS 机的 NFC 读卡器。

通过上述本申请实施例中的方法及装置，对业务进行时地理位置、时间、交易信息等内容的判断，可以进一步的确保使用智能卡应用进行业务时的安全性；并且在根据了智能卡应用的不同种类（eSE 芯片或者 HCE 等），设计了适用于不同种类智能卡应用的安全验证方法，例如获取 eSE 芯片内的智能卡应用与通信模块之间的业务过程，从而进行验证，或者通过内置于 HCE 智能卡应用中的安全验证方法来对业务进行安全验证。

对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片 2。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用 “逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language ） 与 Verilog2。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，

存储器控制器还可以被实现为存储器的控制逻辑的一部分。

本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。

为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例或者实施例的某些部分所述的方法。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本申请可用于众多通用或专用的计算机系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的消费电子设备、网络 PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

虽然通过实施例描绘了本申请，本领域普通技术人员知道，本申请有许多变形和变化而不脱离本申请的精神，希望所附的权利要求包括这些变形和变化而不脱离本申请的精神。

权 利 要 求 书

1、一种智能卡应用安全验证方法，其特征在于包括，

在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据；

将所述当前业务相关数据与安全参数进行判断；

若所述当前业务相关数据不符合所述安全参数，则终止本次业务。

2、根据权利要求 1 所述的方法，其特征在于，还包括若所述当前业务相关数据符合所述安全参数，则允许继续进行本次业务。

3、根据权利要求 1 所述的方法，其特征在于，所述当前业务相关数据至少包括当前位置信息、当前时间信息、交易信息中的一个或者多个的组合。

4、根据权利要求 1 所述的方法，其特征在于，在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据之中还包括，在内置于嵌入式安全芯片的智能卡应用与 NFC 控制器的通信过程中，监测双方的通信过程，并获取当前业务相关数据。

5、根据权利要求 1 所述的方法，其特征在于，在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据之中还包括，在虚拟智能卡的应用与 NFC 控制器的通信过程中，在虚拟智能卡的应用中监测双方的通信过程，并获取当前业务相关数据。

6、根据权利要求 1 所述的方法，其特征在于，在将所述当前业务相关数据与安全参数进行判断之前还包括，接收并保存用户输入的安全参数；

或者，接收并保存服务器根据用户的相关数据分析得到的安全参数。

7、一种智能卡应用安全验证装置，其特征在于包括，

获取单元，用于在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据；

判断单元，用于将所述当前业务相关数据与安全参数进行判断；

处理单元，用于若所述当前业务相关数据不符合所述安全参数，则终止本次业务。

8、根据权利要求 7 所述的装置，其特征在于，所述处理单元还用于若所述当前业务相关数据符合所述安全参数，则允许继续进行本次业务。

9、根据权利要求 7 所述的装置，其特征在于，所述当前业务相关数据至少包括当前位置信息、当前时间信息、交易信息中的一个或者多个的组合。

10、根据权利要求 7 所述的装置，其特征在于，所述获取单元监测内置于嵌入式安全芯片的智能卡应用与 NFC 控制器的通信过程，并获取当前业务相关数据。

11、根据权利要求 7 所述的装置，其特征在于，所述获取单元内置于虚拟智能卡的

应用中，获取虚拟智能卡的应用与 NFC 控制器的通信过程中的当前业务相关数据。

12、根据权利要求 7 所述的装置，其特征在于，还包括安全参数接收单元，用于接收并保存用户输入的安全参数；

或者，接收并保存服务器根据用户的相关数据分析得到的安全参数。

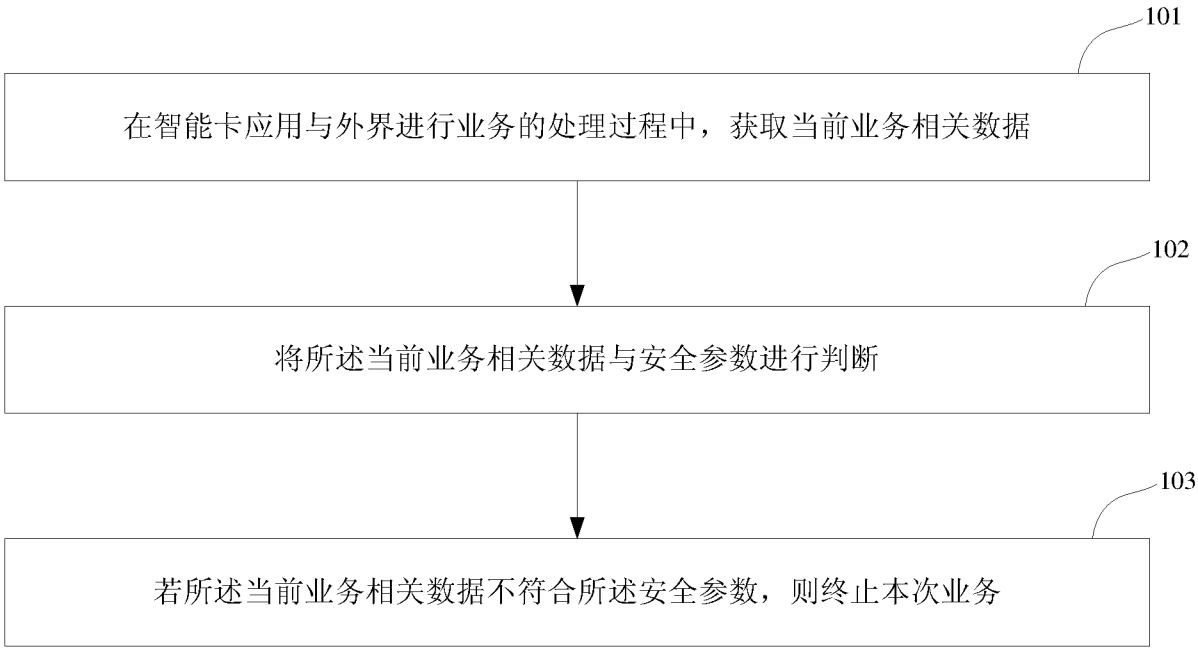
101
在智能卡应用与外界进行业务的处理过程中，获取当前业务相关数据
102
将所述当前业务相关数据与安全参数进行判断
103
若所述当前业务相关数据不符合所述安全参数，则终止本次业务

图 1

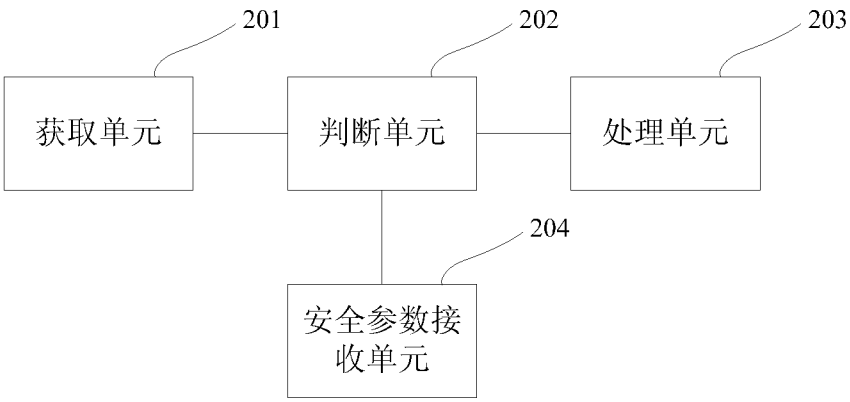
201
202
203
获取单元
判断单元
处理单元
204
安全参数接收单元

图 2

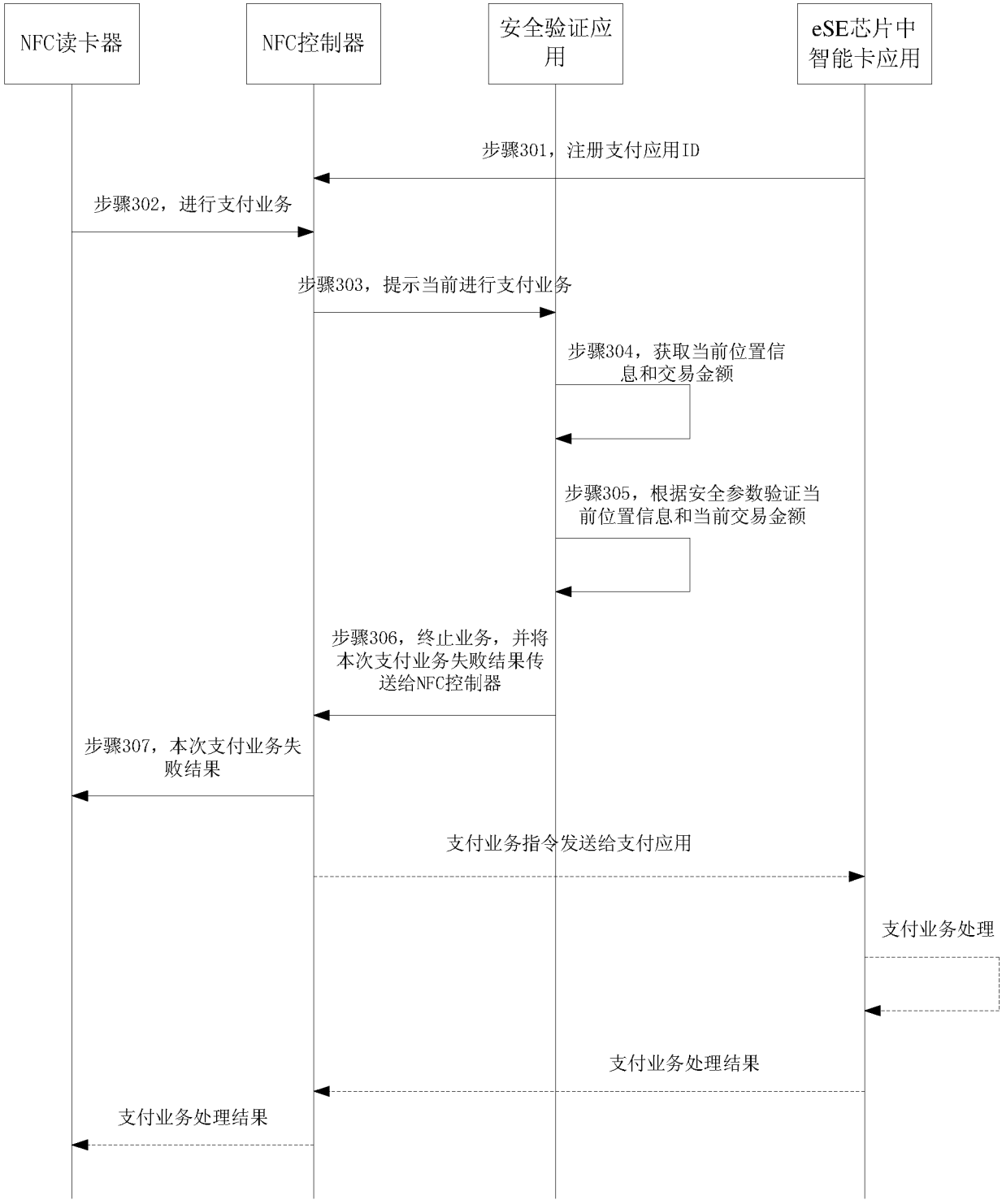
NFC读卡器
NFC控制器
安全验证应用
eSE芯片中智能卡应用
步骤301，注册支付应用ID
步骤302，进行支付业务
步骤303，提示当前进行支付业务
步骤304，获取当前位置信息和交易金额
步骤305，根据安全参数验证当前位置信息和当前交易金额
步骤306，终止业务，并将本次支付业务失败结果传送给NFC控制器
步骤307，本次支付业务失败结果
支付业务指令发送给支付应用
支付业务处理
支付业务处理结果
支付业务处理结果

图 3

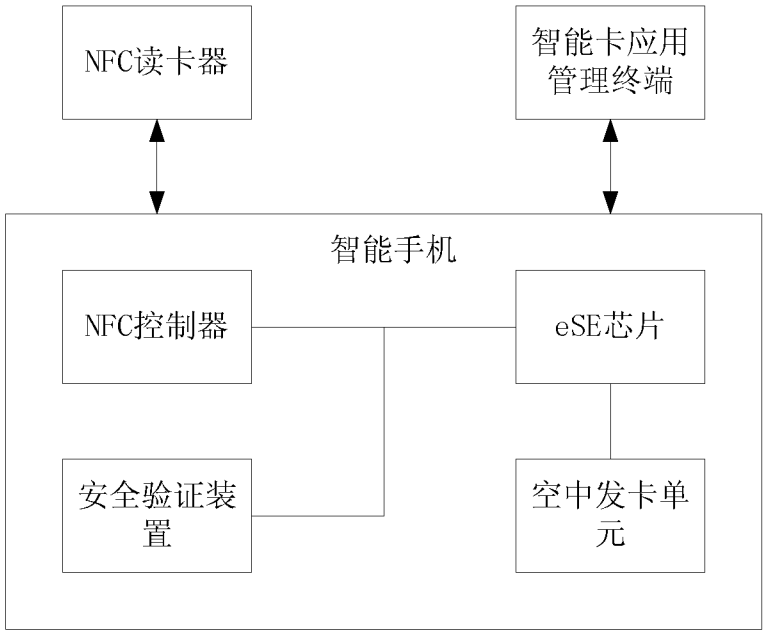

图 4

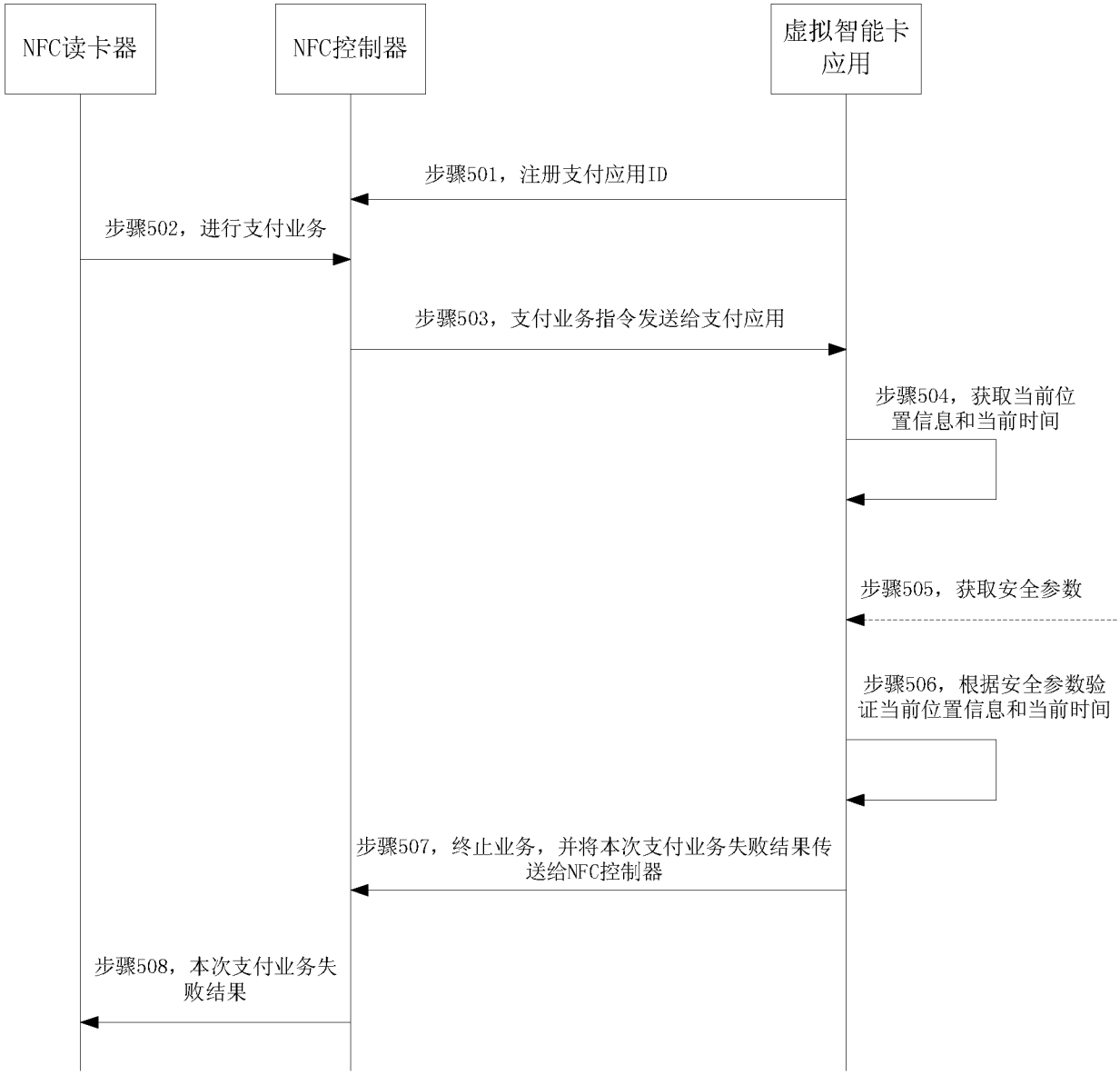
NFC读卡器
NFC控制器
虚拟智能卡应用
步骤501，注册支付应用ID
步骤502，进行支付业务
步骤503，支付业务指令发送给支付应用
步骤504，获取当前位置信息和当前时间
步骤505，获取安全参数
步骤506，根据安全参数验证当前位置信息和当前时间
步骤507，终止业务，并将本次支付业务失败结果传送给NFC控制器
步骤508，本次支付业务失败结果

图 5

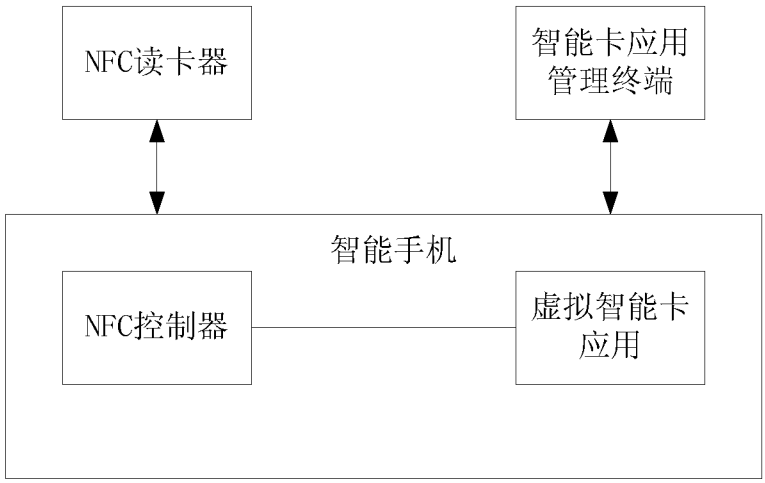

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/112265

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/34 (2013.01) 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)

G06F

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)

CNPAT, WPI, EPODOC, CNKI, IEEE: security chip, virtual smart card, terminate, mobile, pay, security, safe, location, operation, transaction, smart, card, terminal, eSE, HCE, limit, quota, virtual

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104751329 A (SHENZHEN ZTE MOBILE TECHNOLOGY CO., LTD.) 01 July 2015 (01.07.2015) description, paragraphs [0078]-[0114]	1-12
X	CN 103065240 A (ZTE CORPORATION) 24 April 2013 (24.04.2013) description, paragraphs [0005] and [0041]-[0073]	1-12
A	CN 104504568 A (WANGYIBAO CO., LTD.) 08 April 2015 (08.04.2015) the whole document	1-12
A	CN 102855560 A (NATIONZ TECHNOLOGIES INC.) 02 January 2013 (02.01.2013) the whole document	1-12
A	US 2010145819 A1 (PANTECH CO., LTD.) 10 June 2010 (10.06.2010) the whole document	1-12

☐ 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
09 March 2017	31 March 2017
Name and mailing address of the ISA 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 LIU, Changyong Telephone No. (86-10) 53318983

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/112265

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104751329 A	01 July 2015	None	
CN 103065240 A	24 April 2013	None	
CN 104504568 A	08 April 2015	None	
CN 102855560 A	02 January 2013	WO 2013000351 A1	03 January 2013
US 2010145819 A1	10 June 2010	KR 20060041346 A	11 May 2006
		US 2006100966 A1	11 May 2006

国际检索报告

国际申请号
PCT/CN2016/112265

A. 主题的分类

G06F 21/34(2013.01)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)

G06F

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））

CNPAT,WPI,EPODOC,CNKI,IEEE:移动，支付，安全，额度，位置，业务，交易，安全芯片，虚拟智能卡，智能卡，终止，mobile，pay，security，safe，location，operation，transaction，smart，card，terminal，eSE，HCE，limit，quota，virtual

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	CN 104751329 A (深圳市中兴移动通信有限公司) 2015年 7月 1日 (2015-07-01) 说明书第[0078]-[0114]段	1-12
X	CN 103065240 A (中兴通讯股份有限公司) 2013年 4月 24日 (2013-04-24) 说明书第[0005]，[0041]-[0073]	1-12
A	CN 104504568 A (网易宝有限公司) 2015年 4月 8日 (2015-04-08) 全文	1-12
A	CN 102855560 A (国民技术股份有限公司) 2013年 1月 2日 (2013-01-02) 全文	1-12
A	US 2010145819 A1 (PANTECH CO., LTD.) 2010年 6月 10日 (2010-06-10) 全文	1-12

☐ 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
2017年 3月 9日	2017年 3月 31日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 刘长勇 电话号码 (86-10)010-53318983

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/112265

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104751329	A	2015年 7月 1日	无			
CN	103065240	A	2013年 4月 24日	无			
CN	104504568	A	2015年 4月 8日	无			
CN	102855560	A	2013年 1月 2日	WO	2013000351	A1	2013年 1月 3日
US	2010145819	A1	2010年 6月 10日	KR	20060041346	A	2006年 5月 11日
				US	2006100966	A1	2006年 5月 11日