(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 102752265 B
(45)授权公告日 2017.04.19

(21)申请号 201110098478.9

(22)申请日 2011.04.19

(65)同一申请的已公布的文献号
申请公布号 CN 102752265 A

(43)申请公布日 2012.10.24

(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 海涛 刘风军 徐晋耀 李春欢 马天舒

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 臧霁晨 高为

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 102694781 A,2012.09.26,

审查员 牛爽

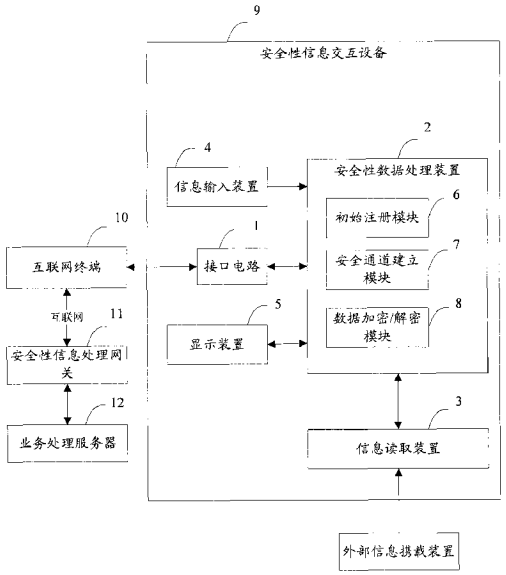
权利要求书3页 说明书8页 附图2页

(54)发明名称

基于互联网的安全性信息交互系统及方法

(57)摘要

本发明提出了一种安全性信息交互系统及方法。其中，所述安全性信息交互系统包括安全性信息交互设备，所述安全性信息交互设备用于获取用户输入的安全性信息以及从外部信息携载装置读取的信息数据，并通过互联网终端建立与安全性信息处理网关的安全通道，从而完成业务功能。其中，所述安全性信息处理网关执行所有业务逻辑的处理。本发明所公开的安全性信息交互系统及方法提高了信息处理系统的灵活性和效率以及降低了安全性信息交互设备的运算负载，并提高了信息处理系统的安全性。



CN 102752265 B

1.一种安全性信息交互系统，所述安全性信息交互系统包括：

安全性信息交互设备，所述安全性信息交互设备用于获取用户输入的安全性信息以及从外部信息携载装置读取的信息数据，并通过互联网终端建立与安全性信息处理网关的安全通道，从而完成业务功能；

互联网终端，所述互联网终端用于建立所述安全性信息交互设备和所述安全性信息处理网关之间的互联网上的连接；

安全性信息处理网关，所述安全性信息处理网关用于根据预定的业务逻辑处理所述安全性信息交互设备传送来的与业务相关的请求和数据，并向业务处理服务器发送相应的业务处理请求；

业务处理服务器，所述业务处理服务器根据接收到的所述业务处理请求完成相应的业务功能；

其中，所述安全性信息处理网关执行所有业务逻辑的处理；

其中，当使用所述安全性信息交互设备时，用户需要输入设备密码，并且所述安全性信息交互设备在初始使用时执行注册过程，所述注册过程包括将所述安全性信息交互设备与用户的特定外部信息携载装置相关联；

其中，所述安全性信息交互设备进一步包括安全加密/解密装置，所述安全加密/解密装置用于存储和处理所述安全性信息，并且所述安全加密/解密装置进一步包括安全通道建立模块，所述安全通道建立模块用于基于握手协议在所述安全性信息交互设备和所述安全性信息处理网关之间建立互联网上的安全通道。

2.根据权利要求1所述的安全性信息交互系统，其特征在于，所述安全性信息交互设备进一步包括：

接口电路，所述接口电路用于将所述安全性信息交互设备连接到互联网终端；

信息输入装置，所述信息输入装置用于用户输入安全性信息；

安全加密/解密装置，所述安全加密/解密装置用于存储和处理所述安全性信息；

信息读取装置，所述信息读取装置用于从外部信息携载装置读取信息数据；

其中，所述安全加密/解密装置结合所述信息数据处理所述安全性信息，并通过与所述安全性信息处理网关的交互而在安全通道上完成业务功能。

3.根据权利要求2所述的安全性信息交互系统，其特征在于，所述安全加密/解密装置进一步包括：

初始注册模块，所述初始注册模块用于在所述安全性信息交互设备首次使用时结合用户的外部信息携载装置完成初始注册；

安全通道建立模块，所述安全通道建立模块用于基于握手协议在所述安全性信息交互设备和所述安全性信息处理网关之间建立互联网上的安全通道；

数据加密/解密模块，所述数据加密/解密模块用于基于记录层协议完成应用数据的加密/解密传输。

4.根据权利要求3所述的安全性信息交互系统，其特征在于，所述安全性信息交互设备进一步包括显示装置，所述显示装置用于向所述安全性信息交互设备的用户显示信息。

5.根据权利要求4所述的安全性信息交互系统，其特征在于，所述信息读取装置是IC卡阅读装置，所述IC卡阅读装置用于阅读IC卡中的信息数据。

6.根据权利要求5所述的安全性信息交互系统，其特征在于，所述安全加密/解密装置采用硬件加密方式。

7.根据权利要求1所述的安全性信息交互系统，其特征在于，所述外部信息携载装置是IC卡。

8.根据权利要求7所述的安全性信息交互系统，其特征在于，所述安全性信息交互系统采用的证书系统包括：根证书、终端根CA、设备证书注册系统、设备证书、安全性信息处理网关证书、服务提供商证书以及设备制造商证书。

9.根据权利要求8所述的安全性信息交互系统，其特征在于，所述安全性信息交互系统采用非对称密钥体系。

10.根据权利要求9所述的安全性信息交互系统，其特征在于，所述安全性信息交互设备能够通过所述安全性信息处理网关执行不同归属方的自有资源的转移。

11.根据权利要求10所述的安全性信息交互系统，其特征在于，所述信息输入装置是键盘。

12.一种安全性信息交互方法，所述安全性信息交互方法包括：

(A1)当需要进行与业务相关的安全性信息交互时，建立安全性信息交互设备和安全性信息处理网关之间的互联网上的安全通道；

(A2)所述安全性信息交互设备的信息读取装置从外部信息携载装置读取信息数据；

(A3)所述安全性信息交互设备中的安全加密/解密装置基于用户通过所述安全性信息交互设备的信息输入装置输入的安全性信息并结合所述信息数据处理所述安全性信息，并通过加密传输的方式基于所述安全通道完成与联机业务相关的业务功能；

其中，所述安全性信息处理网关执行所有业务逻辑的处理；

其中，当使用所述安全性信息交互设备时，用户需要输入设备密码，并且所述安全性信息交互方法还包括将所述安全性信息交互设备与至少一个外部信息携载装置相关联的初始注册步骤；

其中，所述安全加密/解密装置进一步包括安全通道建立模块，所述安全通道建立模块用于基于握手协议在所述安全性信息交互设备和所述安全性信息处理网关之间建立互联网上的安全通道。

13.根据权利要求12所述的安全性信息交互方法，其特征在于，所述初始注册步骤包括：

(B1)将所述安全性信息交互设备连接到互联网终端，并将外部信息携载装置与所述信息读取装置相连接；

(B2)使用终端设备证书登录指定的注册服务器；

(B3)验证所述终端设备证书的有效性，并且如果验证成功，则进入步骤(B4)，如果验证失败，则注册失败；

(B4)所述注册服务器获取安全性信息交互设备信息，并验证安全性信息交互设备是否已被绑定，如果验证成功，则注册完成，如果验证失败，则进入步骤(B5)；

(B5)用户填写注册信息并提交；

(B6)所述注册服务器通过所述安全性信息交互设备提取所述外部信息携载装置的信息；

(B7)所述注册服务器对所述外部信息携载装置进行合法性验证，并且如果验证成功，则进入步骤(B8)，如果验证失败，则注册失败；

(B8)所述注册服务器对用户的注册信息进行实名验证，如果验证成功，则进入步骤(B9)，如果验证失败，则注册失败；

(B9)所述注册服务器将用户信息与所述安全性信息交互设备相关联，注册完成。

14.根据权利要求13所述的安全性信息交互方法，其特征在于，所述安全性信息交互方法采用硬件加密方式处理所述安全性信息。

15.根据权利要求14所述的安全性信息交互方法，其特征在于，所述步骤(A1)进一步包括：所述安全性信息交互设备中的安全通道建立模块基于握手协议在所述安全性信息交互设备和安全性信息处理网关之间建立互联网上的安全通道。

16.根据权利要求15所述的安全性信息交互方法，其特征在于，所述步骤(A3)进一步包括：所述安全性信息交互设备中的数据加密/解密模块基于记录层协议完成应用数据的加密/解密传输。

17.根据权利要求16所述的安全性信息交互方法，其特征在于，所述信息读取装置是卡阅读装置，并且所述IC卡阅读装置用于阅读IC卡中的信息数据。

18.根据权利要求17所述的安全性信息交互方法，其特征在于，所述步骤(A3)进一步包括：将与所述业务功能相关的结果信息显示在所述安全性信息交互设备的显示装置上。

19.根据权利要求18所述的安全性信息交互方法，其特征在于，所述安全性信息交互方法采用的证书系统包括：根证书、终端根CA、设备证书注册系统、设备证书、安全性信息处理网关证书、服务提供商证书以及设备制造商证书。

20.根据权利要求19所述的安全性信息交互方法，其特征在于，所述安全性信息交互方法采用非对称密钥体系。

21.根据权利要求20所述的安全性信息交互方法，其特征在于，所述信息输入装置是键盘。

22.根据权利要求21所述的安全性信息交互方法，其特征在于，所述安全性信息交互方法能够通过所述安全性信息处理网关执行不同归属方的自有资源的转移。

基于互联网的安全性信息交互系统及方法

技术领域

[0001] 本发明涉及信息交互系统及方法，更具体地，涉及基于互联网的安全性信息交互系统及方法。

背景技术

[0002] 目前，随着电子计算机应用及网络通信应用的日益广泛以及不同领域的业务种类的日益丰富，基于互联网的安全性信息交互系统及方法变的越来越重要。在现有的基于互联网的安全性信息交互系统(例如基于USB key的系统)中，对于不同的业务，使用不同的信息处理设备进行信息交互。因此，当同一用户需要完成多种业务时，需要分别借助不同的信息交互设备完成，从而信息处理的复杂性显著增加并缺乏通用性和便捷性。此外，在现有的基于互联网的安全性信息交互系统中，安全性信息交互设备通常通过互联网终端(例如PC、便携式电脑等)接收用户输入的安全性信息(例如设备开机PIN、交易密码等)，因而存在测录风险，故系统安全性较低。另外，在在现有的基于互联网的安全性信息交互系统中，数据的加密和解密通常在互联网终端完成，易于被攻击和监控，故存在较大的安全性隐患。另外，在现有的基于互联网的安全性信息交互系统中，安全性信息处理服务器(或网关)(例如第三方支付平台)通常不具有业务处理功能，即其仅提供安全性信息交互设备(例如POS机)和业务处理服务器之间的透明通道服务，而特定的业务处理功能(例如PBOC业务逻辑)全部由所述安全性信息交互设备完成，因而随着业务种类的日益增多，该安全性信息交互设备的运算压力和复杂度将会显著地增长。

[0003] 因此，为了适应不断增长和变化的应用类型，存在如下需求：提供一种可以处理多种业务类型的安全性信息并具有高的安全性以及可降低安全性信息交互终端的运算负载的安全性信息交互系统及方法。

发明内容

[0004] 为了解决上述现有技术方案所存在的缺陷，本发明提出了一种基于互联网的安全性信息交互系统及方法。

[0005] 本发明的目的是通过以下技术方案实现的：

[0006] 一种安全性信息交互系统，所述安全性信息交互系统包括：

[0007] 安全性信息交互设备，所述安全性信息交互设备用于获取用户输入的安全性信息以及从外部信息携载装置读取的信息数据，并通过互联网终端建立与安全性信息处理网关的安全通道，从而完成业务功能；

[0008] 互联网终端，所述互联网终端用于建立所述安全性信息交互设备和所述安全性信息处理网关之间的互联网上的连接；

[0009] 安全性信息处理网关，所述安全性信息处理网关用于根据预定的业务逻辑处理所述安全性信息交互设备传送来的与业务相关的请求和数据，并向业务处理服务器发送相应的业务处理请求；

[0010] 业务处理服务器，所述业务处理服务器根据接收到的所述业务处理请求完成相应的业务功能；

[0011] 其中，所述安全性信息处理网关执行所有业务逻辑的处理。

[0012] 在上面所公开的方案中，优选地，所述安全性信息交互设备进一步包括：

[0013] 接口电路，所述接口电路用于将所述安全性信息交互设备连接到互联网终端；

[0014] 信息输入装置，所述信息输入装置用于用户输入安全性信息；

[0015] 安全加密/解密装置，所述安全加密/解密装置用于存储和处理所述安全性信息；

[0016] 信息读取装置，所述信息读取装置用于从外部信息携载装置读取信息数据；

[0017] 其中，所述安全加密/解密装置结合所述信息数据处理所述安全性信息，并通过与所述安全性信息处理网关的交互而在安全通道上完成业务功能。

[0018] 在上面所公开的方案中，优选地，所述安全加密/解密装置进一步包括：

[0019] 初始注册模块，所述初始注册模块用于在所述安全性信息交互设备首次使用时结合用户的外部信息携载装置完成初始注册；

[0020] 安全通道建立模块，所述安全通道建立模块用于基于握手协议在所述安全性信息交互设备和所述安全性信息处理网关之间建立互联网上的安全通道；

[0021] 数据加密/解密模块，所述数据加密/解密模块用于基于记录层协议完成应用数据的加密/解密传输。

[0022] 在上面所公开的方案中，优选地，所述安全性信息交互设备进一步包括显示装置，所述显示装置用于向所述安全性信息交互设备的用户显示信息。

[0023] 在上面所公开的方案中，优选地，所述信息读取装置是IC卡阅读装置，所述IC卡阅读装置用于阅读IC卡中的信息数据。

[0024] 在上面所公开的方案中，优选地，所述安全加密/解密装置采用硬件加密方式。

[0025] 在上面所公开的方案中，优选地，当使用所述安全性信息交互设备时，用户需要输入设备密码。

[0026] 在上面所公开的方案中，优选地，所述安全性信息交互设备在初始使用时执行注册过程，所述注册过程包括将所述安全性信息交互设备与用户的特定外部信息携载装置相关联。

[0027] 在上面所公开的方案中，优选地，所述外部信息携载装置是IC卡。

[0028] 在上面所公开的方案中，优选地，所述安全性信息交互系统采用的证书系统包括：根证书、终端根CA、设备证书注册系统、设备证书、安全性信息处理网关证书、服务提供商证书以及设备制造商证书。

[0029] 在上面所公开的方案中，优选地，所述安全性信息交互系统采用非对称密钥体系。

[0030] 在上面所公开的方案中，优选地，所述安全性信息交互设备能够通过所述安全性信息处理网关执行不同归属方的自有资源的转移。

[0031] 在上面所公开的方案中，优选地，所述信息输入装置是键盘。

[0032] 本发明的目的还通过以下技术方案实现：

[0033] 一种安全性信息交互方法，所述安全性信息交互方法包括：

[0034] (A1)当需要进行与业务相关的安全性信息交互时，建立安全性信息交互设备和安全性信息处理网关之间的互联网上的安全通道；

[0035] (A2)所述安全性信息交互设备的信息读取装置从外部信息携载装置读取信息数据；

[0036] (A3)所述安全性信息交互设备中的安全加密/解密装置基于用户通过所述安全性信息交互设备的信息输入装置输入的安全性信息并结合所述信息数据处理所述安全性信息，并通过加密传输的方式基于所述安全通道完成与联机业务相关的业务功能；

[0037] 其中，所述安全性信息处理网关执行所有业务逻辑的处理。

[0038] 在上面所公开的方案中，优选地，所述安全性信息交互方法还包括将所述安全性信息交互设备与至少一个外部信息携载装置相关联的初始注册步骤，

[0039] 在上面所公开的方案中，优选地，所述初始注册步骤包括：

[0040] (B1)将所述安全性信息交互设备连接到互联网终端，并将外部信息携载装置与所述信息读取装置相连接；

[0041] (B2)使用终端设备证书登录指定的注册服务器；

[0042] (B3)验证所述终端设备证书的有效性，并且如果验证成功，则进入步骤(B4)，如果验证失败，则注册失败；

[0043] (B4)所述注册服务器获取安全性信息交互设备信息，并验证安全性信息交互设备是否已被绑定，如果验证成功，则注册完成，如果验证失败，则进入步骤(B5)；

[0044] (B5)用户填写注册信息并提交；

[0045] (B6)所述注册服务器通过所述安全性信息交互设备提取所述外部信息携载装置的信息；

[0046] (B7)所述注册服务器对所述外部信息携载装置进行合法性验证，并且如果验证成功，则进入步骤(B8)，如果验证失败，则注册失败；

[0047] (B8)所述注册服务器对用户的注册信息进行实名验证，如果验证成功，则进入步骤(B9)，如果验证失败，则注册失败；

[0048] (B9)所述注册服务器将用户信息与所述安全性信息交互设备相关联，注册完成。

[0049] 在上面所公开的方案中，优选地，所述安全性信息交互方法采用硬件加密方式处理所述安全性信息。

[0050] 在上面所公开的方案中，优选地，所述步骤(A1)进一步包括：所述安全性信息交互设备中的安全通道建立模块基于握手协议在所述安全性信息交互设备和安全性信息处理网关之间建立互联网上的安全通道。

[0051] 在上面所公开的方案中，优选地，所述步骤(A3)进一步包括：所述安全性信息交互设备中的数据加密/解密模块基于记录层协议完成应用数据的加密/解密传输。

[0052] 在上面所公开的方案中，优选地，当使用所述安全性信息交互设备时，用户需要输入设备密码。

[0053] 在上面所公开的方案中，优选地，所述信息读取装置是卡阅读装置，并且所述IC卡阅读装置用于阅读IC卡中的信息数据。

[0054] 在上面所公开的方案中，优选地，所述步骤(A3)进一步包括：将与所述业务功能相关的结果信息显示在所述安全性信息交互设备的显示装置上。

[0055] 在上面所公开的方案中，优选地，所述安全性信息交互方法采用的证书系统包括：根证书、终端根CA、设备证书注册系统、设备证书、安全性信息处理网关证书、服务提供商证

书以及设备制造商证书。

[0056] 在上面所公开的方案中，优选地，所述安全性信息交互方法采用非对称密钥体系。

[0057] 在上面所公开的方案中，优选地，所述信息输入装置是键盘。

[0058] 在上面所公开的方案中，优选地，所述安全性信息交互方法能够通过所述安全性信息处理网关执行不同归属方的自有资源的转移。

[0059] 本发明所公开的安全性信息交互系统及方法具有如下优点：由于互联网终端可以选择各种硬件形式(例如电脑，手机等)，故可以随时随地进行业务交互，从而扩展了安全性信息交互的灵活性；同时，可以提高信息交互的安全性和保密性；此外，信息处理的复杂性显著降低并提高了通用性和便捷性以及降低了安全性信息交互终端的运算负载。

附图说明

[0060] 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：

[0061] 图1为根据本发明的实施例的安全性信息交互系统的结构图；

[0062] 图2为根据本发明的实施例的安全性信息交互方法的流程图；

具体实施方式

[0063] 图1为根据本发明的实施例的安全性信息交互系统的结构图。如图1所示，本发明所公开的安全性信息交互系统包括安全性信息交互设备9、互联网终端10、安全性信息处理网关11(例如银行或第三方交易平台)和业务处理服务器12。其中，所述安全性信息交互设备9用于获取用户输入的安全性信息以及从外部信息携载装置读取的信息数据，并通过所述互联网终端10建立与所述安全性信息处理网关12的安全通道，从而完成业务功能。所述互联网终端10用于建立所述安全性信息交互设备9和所述安全性信息处理网关11之间的互联网上的连接。所述安全性信息处理网关11用于根据预定的业务逻辑处理所述安全性信息交互设备9传送来的与业务相关的请求和数据，并向所述业务处理服务器12发送相应的业务处理请求。所述业务处理服务器12根据接收到的所述业务处理请求完成相应的业务功能。其中，所述安全性信息处理网关11执行所有业务逻辑的处理。

[0064] 如图1所示，优选地，在本发明所公开的安全性信息交互系统中，所述安全性信息交互设备9进一步包括接口电路1、安全加密/解密装置2、信息读取装置3和信息输入装置4。其中，所述接口电路1用于将所述安全性信息交互设备9连接到互联网终端。所述安全加密/解密装置2用于存储和处理所述安全性信息。所述信息读取装置3用于从外部信息携载装置(例如IC卡)读取信息数据(例如IC卡ID号)，以便所述安全加密/解密装置2结合所述信息数据处理所述安全性信息以完成业务功能。所述信息输入装置4用于用户输入安全性信息(例如密码)。

[0065] 如图1所示，所述接口电路1可以是USB接口、串行接口、并行接口、I2C接口、IO接口等任何标准有线接口或者蓝牙、WIFI等任何标准的无线接口、也可以是任何自定义的其他接口。此外，所述互联网终端10中运行有与所述安全性信息交互设备9相对应的驱动程序和应用程序。例如，但不限于，所述互联网终端10是电脑，或手机，或PDA，或上网本等。

[0066] 如图1所示，所述安全加密/解密装置2是存储和处理所述安全性信息的安全载体，其采用硬件加密，即将所述安全性信息保存在加密芯片中，只有与业务功能相关的特定的

系统能够将所述被加密的安全性信息解密。

[0067] 如图1所示，所述安全加密/解密装置2进一步包括初始注册模块6、安全通道建立模块7、数据加密/解密模块8。其中，所述初始注册模块6用于在所述安全性信息交互设备9首次使用时结合用户的外部信息携载装置(例如IC卡)完成初始注册。所述安全通道建立模块7用于基于握手协议在所述安全性信息交互设备9和安全性信息处理网关之间建立互联网上的安全通道。所述数据加密/解密模块8用于基于记录层协议完成应用数据的加密传输。

[0068] 如图1所示，本发明所公开的安全性信息交互系统具有双重安全性信息(例如密码)保护功能，即当使用该安全性信息交互设备9时，用户需要输入设备密码，随后，在进行业务交互时，用户需要输入所述外部信息携载装置的认证密码。因此，本发明所公开的安全性信息交互系统提高了信息交互的安全性和保密性。

[0069] 如图1所示，所述信息读取装置3是IC卡阅读装置。所述IC卡阅读装置用于阅读IC卡中的信息数据。

[0070] 可选地，所述安全性信息交互设备9进一步包括显示装置5。所述显示装置5用于向所述安全性信息交互设备9的用户显示信息。

[0071] 如图1所示，在本发明所公开的安全性信息交互系统中，所述安全性信息交互设备9首次使用时需要进行初始注册，基本过程如下：用户将所述安全性信息交互设备9连接到互联网终端10，并将外部信息携载装置与所述信息读取装置3相连接(例如将IC卡插入)；使用终端设备证书登录指定的注册服务器；验证所述终端设备证书的有效性，并且如果验证成功，则进入下一步，如果验证失败，则注册失败；所述注册服务器获取安全性信息交互设备信息，并验证安全性信息交互设备是否已被绑定(即该安全性信息交互设备与特定的外部信息携载装置(例如IC卡)相关联)，如果验证成功，则注册完成，如果验证失败，则进入下一步；用户填写注册信息并提交；所述注册服务器通过所述安全性信息交互设备提取所述外部信息携载装置的信息；所述注册服务器对所述外部信息携载装置进行合法性验证，并且如果验证成功，则进入下一步，如果验证失败，则注册失败；所述注册服务器对用户的注册信息进行实名验证，如果验证成功，则进入下一步，如果验证失败，则注册失败；所述注册服务器将用户信息与所述安全性信息交互设备相关联(即绑定)，注册完成。

[0072] 在本发明所公开的安全性信息交互系统中，采用如下证书系统：根证书，其是所有安全性信息交互设备CA系统签发证书的签名证书，其私钥保存在根CA中心的加密机中；终端根CA，用于签发安全性信息处理网关证书(也被称作渠道证书)、服务提供商证书(也被称作商户证书)、设备制造商证书(也被称作终端厂商证书)；设备证书注册系统(也被称为终端证书注册系统)，其被置于安全性信息交互设备的制造商处，用于所述制造商向根CA中心申请所需的设备证书(也称为终端证书)；设备证书，其是标识安全性信息交互设备身份的数字证书，每个安全性信息交互设备在预个人化时均会产生唯一的设备证书，此证书的公、私钥由安全性信息交互设备本身产生，并且私钥存储在安全性信息交互设备的敏感区内，不可导出；安全性信息处理网关证书，其是标识安全性信息处理网关(例如网银系统)的身份数字证书，每个安全性信息处理网关对应唯一的安全性信息处理网关证书，用于验证所述安全性信息处理网关的真伪，并在与安全性信息交互设备进行通信时证明服务器的身份；服务提供商证书，用于服务提供商与安全性信息交互设备建立安全数据传输通道；设备

制造商证书，用于验证设备制造商的合法身份和申请数据签名的真伪性。

[0073] 如图1所示，在本发明所公开的安全性信息交互系统中，使用硬件加密保证安全性信息（例如个人标识代码PIN、卡号、有效期等）的安全输入和加密处理，对与外部进行交互的数据进行加密和解密运算以及合法性、完整性验证。并且，所述安全性信息交互设备9能够安全地存储密钥，禁止对密钥的直接访问和输出，从而通过有效的安全机制防止密钥被非法注入、替换和使用。

[0074] 在本发明所公开的安全性信息交互系统的第一示例性工作过程如下：将所述用户安全性信息交互设备9与互联网终端10通过接口电路1相连接；所述安全通道建立模块7基于握手协议在安全性信息交互设备9和安全性信息处理网关之间建立互联网上的安全通道，即完成双向身份认证和会话密钥的交换；用户根据提示使至少一个外部信息携载装置与所述信息读取装置3相互通信（例如插入IC卡）；用户根据提示输入设备的开机PIN；所述安全性信息交互设备9根据所述安全性信息处理网关的指令提示用户输入外部信息携载装置的认证密码；基于所述安全通道，完成认证过程以及特定的业务功能（例如消费交易），其中，所述数据加密/解密模块8基于记录层协议完成应用数据的加密和解密。

[0075] 本发明所公开的安全性信息交互系统的第二示例性工作过程如下：将所述用户安全性信息交互设备9与互联网终端10通过接口电路1相连接；所述安全通道建立模块7基于握手协议在安全性信息交互设备和安全性信息处理网关11之间建立互联网上的安全通道，即完成双向身份认证和会话密钥的交换；用户根据提示使至少一个外部信息携载装置与所述信息读取装置3相互通信（例如插入IC卡）；用户根据提示输入设备的开机PIN；所述安全性信息交互设备根据所述安全性信息处理网关11的指令提示用户输入外部信息携载装置的认证密码；基于所述安全通道，完成认证过程以及特定数据的查询功能（例如查询余额），其中，所述数据加密/解密模块8基于记录层协议完成应用数据的加密和解密；所述安全性信息交互设备9将查询结果显示在所述显示装置5上，或者所述查询结果显示在所述互联网终端10的显示器上。

[0076] 本发明所公开的安全性信息交互系统的第三示例性工作过程如下：将所述用户安全性信息交互设备9与互联网终端10通过接口电路1相连接；所述安全通道建立模块7基于握手协议在安全性信息交互设备和安全性信息处理网关之间建立互联网上的安全通道，即完成双向身份认证和会话密钥的交换；用户根据提示使至少一个外部信息携载装置与所述信息读取装置3相互通信（例如插入IC卡）；用户根据提示输入设备的开机PIN；所述安全性信息交互设备9根据所述安全性信息处理网关的指令提示用户输入外部信息携载装置的认证密码，以及输入转出方外部信息携载装置的信息数据（例如IC卡ID号）以及认证密码并输入需要转移到选定的外部信息携载装置的自有资源（该自有资源在转移前归属于所述转出方外部信息携载装置，所述自有资源例如包括数据、信息以及资金等）的信息数据；基于所述安全通道，完成认证过程以及完成自有资源从转出方外部信息携载装置的转出，其中，所述数据加密/解密模块8基于记录层协议完成应用数据的加密和解密。

[0077] 优选地，本发明所公开的安全性信息交互系统采用非对称密钥体系。

[0078] 优选地，在本发明所公开的安全性信息交互系统中，所述信息输入装置4是键盘。

[0079] 图2为根据本发明的实施例的安全性信息交互方法的流程图。如图2所示，本发明所公开的安全性信息交互方法包括如下步骤：(A1) 当需要进行与业务相关的安全性信息交

互时，建立安全性信息交互设备和安全性信息处理网关之间的互联网上的安全通道；(A2)所述安全性信息交互设备的信息读取装置从外部信息携载装置(例如IC卡)读取信息数据；(A3)所述安全性信息交互设备中的安全加密/解密装置基于用户通过所述安全性信息交互设备的信息输入装置输入的安全性信息并结合所述信息数据处理所述安全性信息，并通过加密传输的方式基于所述安全通道完成相关的业务功能(例如消费交易)。其中，所述安全性信息处理网关执行所有业务逻辑的处理。

[0080] 如图2所示，所述安全性信息交互方法还包括将所述安全性信息交互设备与至少一个外部信息携载装置(例如IC卡)相关联(即绑定)的初始注册步骤，包括：(B1)用户将所述安全性信息交互设备连接到互联网终端，并将外部信息携载装置与所述信息读取装置3相连接(例如将IC卡插入)；(B2)使用终端设备证书登录指定的注册服务器；(B3)验证所述终端设备证书的有效性，并且如果验证成功，则进入下一步，如果验证失败，则注册失败；(B4)所述注册服务器获取安全性信息交互设备信息，并验证安全性信息交互设备是否已被绑定(即该安全性信息交互设备与特定的外部信息携载装置(例如IC卡)相关联)，如果验证成功，则注册完成，如果验证失败，则进入下一步；(B5)用户填写注册信息并提交；(B6)所述注册服务器通过所述安全性信息交互设备提取所述外部信息携载装置的信息；(B7)所述注册服务器对所述外部信息携载装置进行合法性验证，并且如果验证成功，则进入下一步，如果验证失败，则注册失败；(B8)所述注册服务器对用户的注册信息进行实名验证，如果验证成功，则进入下一步，如果验证失败，则注册失败；(B9)所述注册服务器将用户信息与所述安全性信息交互设备相关联(即绑定)，注册完成

[0081] 优选地，在本发明所公开的安全性信息交互方法中，所述安全性信息交互设备包括与互联网终端连接的接口电路1。所述接口电路1可以是USB接口、串行接口、并行接口、I2C接口、IO接口等任何标准有线接口或者蓝牙、WIFI等任何标准的无线接口、也可以是任何自定义的其他接口。此外，所述互联网终端中运行有与所述安全性信息交互设备相对应的驱动程序和应用程序。例如，但不限于，所述互联网终端是电脑，或手机，或PDA，或上网本等。

[0082] 优选地，在本发明所公开的安全性信息交互方法中，采用硬件加密方式，即将所述安全性信息保存在加密芯片中，只有与业务功能相关的特定的系统能够将所述被加密的安全性信息解密。

[0083] 优选地，在本发明所公开的安全性信息交互方法中，所述步骤(A1)进一步包括：所述安全性信息交互设备中的安全通道建立模块基于握手协议在所述安全性信息交互设备和安全性信息处理网关之间建立互联网上的安全通道。

[0084] 优选地，在本发明所公开的安全性信息交互方法中，所述步骤(A3)进一步包括：所述安全性信息交互设备中的数据加密/解密模块基于记录层协议完成应用数据的加密传输。

[0085] 有利地，本发明所公开的安全性信息交互方法采用双重安全性信息(例如密码)保护，即当使用该安全性信息交互设备时，用户需要输入设备密码，随后，在进行业务交互时，用户需要输入所述外部信息携载装置的认证密码。因此，本发明所公开的安全性信息交互方法提高了信息交互的安全性和保密性。

[0086] 优选地，所述信息读取装置是IC卡阅读装置。所述IC卡阅读装置用于阅读IC卡中

的信息数据。

[0087] 可选地，所述步骤(A3)进一步包括：将与所述业务功能相关的结果信息显示在所述安全性信息交互设备的显示装置上。

[0088] 优选地，在本发明所公开的安全性信息交互方法中，采用如下证书系统：根证书，其是所有安全性信息交互设备CA系统签发证书的签名证书，其私钥保存在根CA中心的加密机中；终端根CA，用于签发安全性信息处理网关证书(也被称作渠道证书)、服务提供商证书(也被称作商户证书)、设备制造商证书(也被称作终端厂商证书)；设备证书注册系统(也被称为终端证书注册系统)，其被置于安全性信息交互设备的制造商处，用于所述制造商向根CA中心申请所需的设备证书(也称为终端证书)；设备证书，其是标识安全性信息交互设备身份的数字证书，每个安全性信息交互设备在预个人化时均会产生唯一的设备证书，此证书的公、私钥由安全性信息交互设备本身产生，并且私钥存储在安全性信息交互设备的敏感区内，不可导出；安全性信息处理网关证书，其是标识安全性信息处理网关(例如网银系统)的身份数字证书，每个安全性信息处理网关对应唯一的安全性信息处理网关证书，用于验证所述安全性信息处理网关的真伪，并在与安全性信息交互设备进行通信时证明服务器的身份；服务提供商证书，用于服务提供商与安全性信息交互设备建立安全数据传输通道；设备制造商证书，用于验证设备制造商的合法身份和申请数据签名的真伪性。

[0089] 优选地，在本发明所公开的安全性信息交互方法中，使用硬件加密保证安全性信息(例如个人标识代码PIN、卡号、有效期等)的安全输入和加密处理，对与外部进行交互的数据进行加密和解密运算以及合法性、完整性验证。并且，所述安全性信息交互设备能够安全地存储密钥，禁止对密钥的直接访问和输出，从而通过有效的安全机制防止密钥被非法注入、替换和使用。

[0090] 优选地，本发明所公开的安全性信息交互方法采用非对称密钥体系。

[0091] 优选地，在本发明所公开的安全性信息交互方法中，所述信息输入装置是键盘。

[0092] 优选地，本发明所公开的安全性信息交互方法能够通过所述安全性信息处理网关执行不同归属方的自有资源(所述自有资源例如包括数据、信息以及资金等)的转移(例如圈存交易)。

[0093] 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。

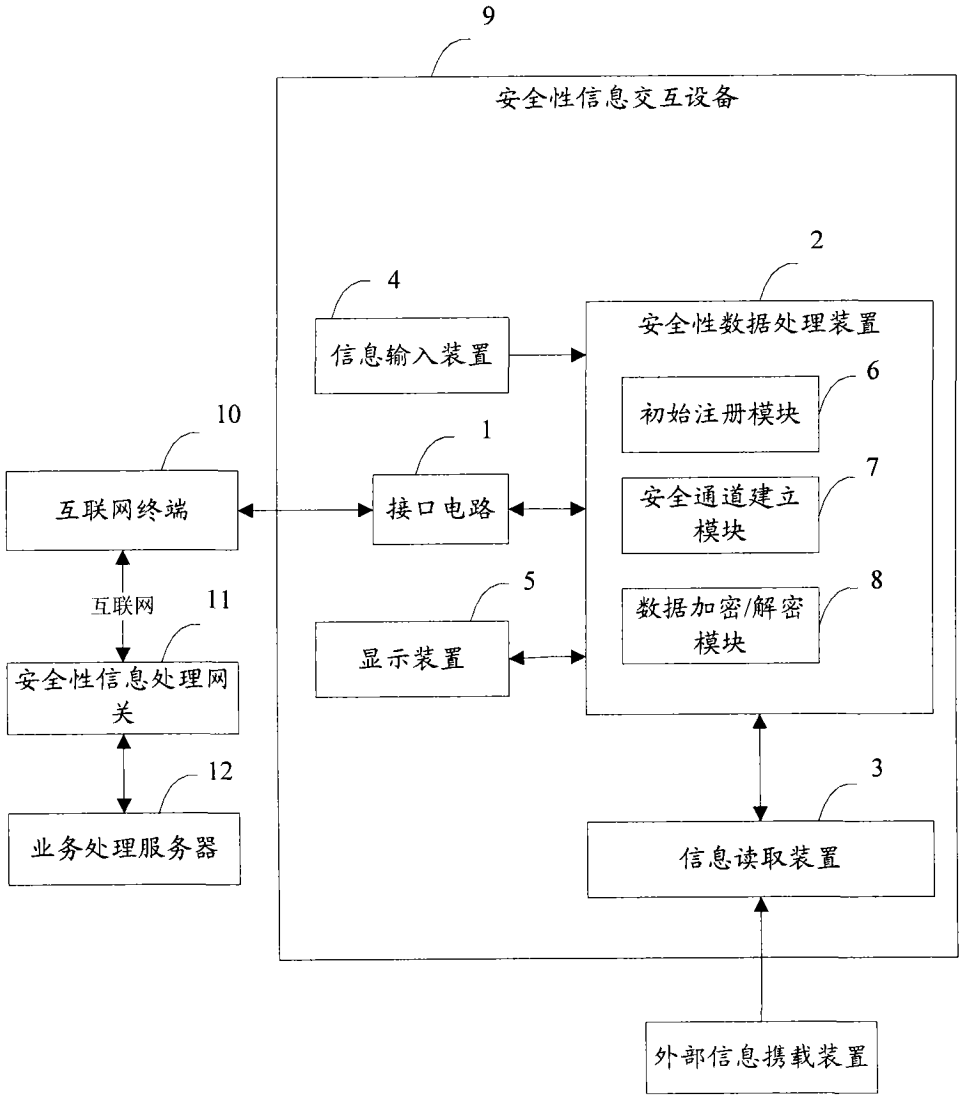

9
安全性信息交互设备
2
4
信息输入装置
安全性数据处理装置
6
初始注册模块
10
1
互联网终端
接口电路
7
安全通道建立模块
互联网
11
5
8
显示装置
数据加密/解密模块
安全性信息处理网关
12
3
业务处理服务器
信息读取装置
外部信息携载装置

图1

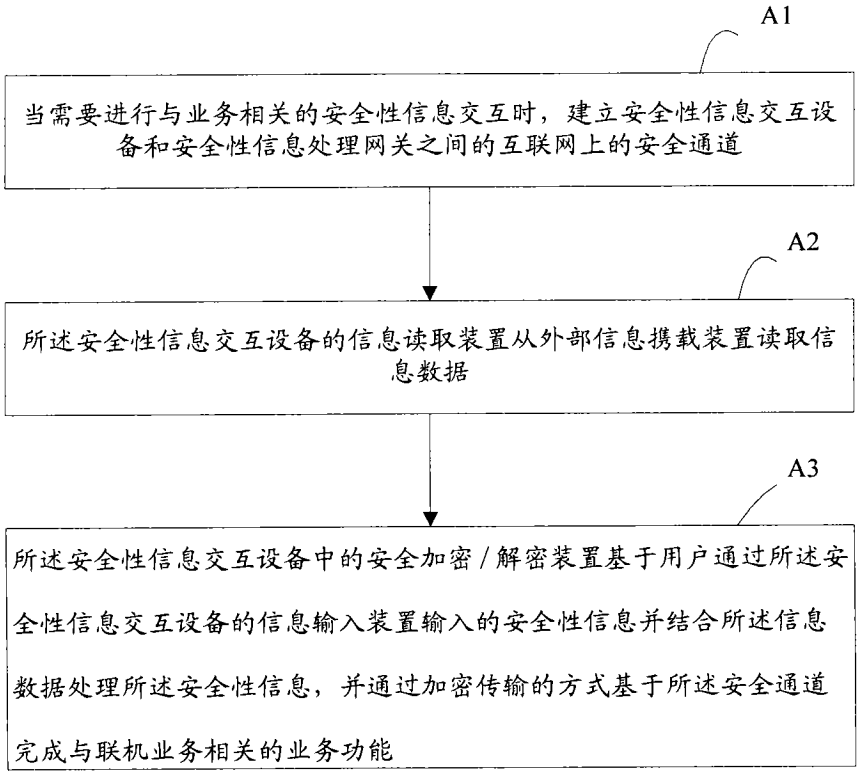

A1
当需要进行与业务相关的安全性信息交互时，建立安全性信息交互设备和安全性信息处理网关之间的互联网上的安全通道
A2
所述安全性信息交互设备的信息读取装置从外部信息携载装置读取信息数据
A3
所述安全性信息交互设备中的安全加密/解密装置基于用户通过所述安全性信息交互设备的信息输入装置输入的安全性信息并结合所述信息数据处理所述安全性信息，并通过加密传输的方式基于所述安全通道完成与联机业务相关的业务功能

图2