(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 102867255 A
(43)申请公布日 2013.01.09

(21)申请号 201210263217.2

(22)申请日 2012.07.27

(71)申请人 郑州信大捷安信息技术股份有限公司

地址 450046 河南省郑州市郑东新区东四环西、商都路北郑州国家干线公路物流港综合服务楼A塔楼14层

(72)发明人 何骏 刘熙胖 梁松涛 董建强 赵国磊 张鲁国 苏庆会

(74)专利代理机构 北京鑫浩联德专利代理事务所(普通合伙) 11380

代理人 李荷香

(51)Int.Cl.

G06Q 20/38(2012.01)

G06Q 20/42(2012.01)

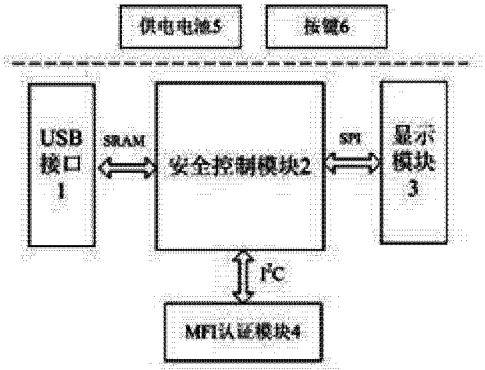
权利要求书 2 页 说明书 4 页 附图 3 页

(54)发明名称

多操作系统平台和移动支付设备的网银U盾及其工作方法

(57)摘要

本发明涉及一种作为网银二代有源U盾使用的多操作系统平台和移动支付设备的网银U盾及其工作方法，该U盾包括miniUSB3.0接口、安全控制模块、显示模块、MFI认证模块、5V锂电池和按键部分，miniUSB接口和相应的数据连接线配套使用，实现与各类移动设备以及PC机的物理连接；安全控制模块为上层网银应用提供密码服务；MFI认证模块完成iOS系列设备对U盾的设备认证；有源U盾自带电池、支持主设备工作模式，能够适应安全移动支付领域下移动设备多样性和操作系统平台多样性，全面解决了iOS系统、Android系统等移动设备无法基于U盾保护网银应用安全的问题，为移动支付提供统一、有效、可靠的安全服务。



CN 102867255 A

1. 一种多操作系统平台和移动支付设备的网银 U 盾，其特征在于，包括：

USB 接口，用于实现与各类移动设备以及 PC 机的物理连接；

安全控制模块，用于接收来自 USB 接口的交易数据，提取用户网银交易数字证书并对交易数据进行数字签名；

显示模块，用于与安全控制模块通讯，获取用户交易信息，并采用 LCD 液晶显示屏显示；

电源，用于 U 盾的自主供电，支持 U 盾在主设备模式下的工作方式。

2. 如权利要求 1 所述的 U 盾，其特征在于，还包括：

按键部分，包括四个按键，确认键、取消键、上翻键和下翻键，实现确认、返回和查询菜单功能。

3. 如权利要求 1 所述的 U 盾，其特征在于：

所述 USB 接口由接口 1 和接口 2 两部分组成，接口 1 采用 USB2.0 接口，用于连接 iOS 系列和 Android 系列移动设备；接口 2 采用 USB3.0 接口，用于连接 PC 机。

4. 如权利要求 1 所述的 U 盾，其特征在于：

所述安全控制模块为上层网银应用提供密码服务，所述安全控制模块除包含标准的 RSA 算法、DES 算法外，还包含国家商用密码标准算法，包括 SM1 对称算法、SM2 椭圆曲线算法、SM3 杂凑算法和随机数发生器。

5. 如权利要求 2 所述的 U 盾，其特征在于：

所述按键部分通过按键选择，实现对 U 盾在 USB 协议下的主设备（Host）模式和从设备（Slave）模式之间的切换。

6. 如权利要求 1 所述的 U 盾，其特征在于，还包括：

MFI 认证模块，包含对 iOS 设备的认证证书，由安全控制模块调用，完成 iOS 系列设备对 U 盾的设备认证。

7. 一种多操作系统平台和移动支付设备的网银 U 盾的工作方法，其特征在于：

当支付设备为 Android、Windows Mobile 系列设备时，设置 U 盾为主设备，U 盾按照主模式的工作方式与支付设备通信；

安全控制模块接收来自 USB 接口的交易数据，将交易信息送至显示模块；

用户通过按键对交易信息二次确认后，安全控制模块读取用户证书，对交易数据进行数字签名，将证书和数字签名交易信息通过 USB 接口返回至支付设备。

8. 如权利要求 7 所述的 U 盾的工作方法，其特征在于：

所述 USB 接口由接口 1 和接口 2 两部分组成，接口 1 采用 USB2.0 接口，用于连接 iOS 系列和 Android 系列移动设备；接口 2 采用 USB3.0 接口，用于连接 PC 机；当 U 盾通过 USB 接口与支付设备连接后，首先通过显示屏和按键进行工作方式选择。

9. 如权利要求 8 所述的 U 盾的工作方法，其特征在于：

当支付设备为 PC 机、iOS 系列的具有主控功能的设备时，设置 U 盾为从模式，按照从模式与 PC 机设备完成 USB 通信协议，如果主设备是 PC 机，则通过 USB 接口中的接口 2 完成通信；如果主设备是 iOS 系列手机移动终端，则通过 USB 接口中的接口 1 完成通信。

10. 如权利要求 8 所述的 U 盾的工作方法，其特征在于：

当支付设备为 Android、Windows Mobile 系列设备时，设置 U 盾为主模式，按照主模式

与支付设备之间完成 USB 通信协议，通过 USB 接口中的接口 1 完成通信。

11. 如权利要求 7 所述的 U 盾的工作方法，其特征在于：

如果移动支付设备为 iOS 系列设备，则安全控制模块在接收交易数据前，调用 MFI 认证模块，基于 MFI 认证协议完成与 iOS 系列设备的设备认证。

多操作系统平台和移动支付设备的网银U盾及其工作方法

技术领域

[0001] 本发明涉及一种网银二代U盾，具体涉及一种作为网银U盾使用的多操作系统平台和移动支付设备的网银U盾及其工作方法。

背景技术

[0002] 网银U盾是网上交易时用户个人身份确认的认证介质，具有数字签名和身份认证功能，是保护网上银行账户资金安全的重要工具。网银二代U盾在一代U盾的基础上，增加了可视化液晶显示屏和用户按键，能够回显交易金额、交易账号等关键交易信息，需用户按键二次确认后才完成操作，与一代U盾相比，能够更有效地防止各类木马病毒对用户提交的网银交易信息进行篡改，增强了网上交易的安全性。

[0003] 现有的网银二代U盾仅支持具有USB物理接口的Windows系列操作系统平台，只能以从设备工作模式(Slave模式)应用于个人或办公PC机，依靠PC机作为主设备(PC机为Master模式)为自身供电。然而随着移动支付的广泛应用，智能手机、平板电脑等移动支付设备具有操作系统多样性(iOS、Android、Windows Mobile等)和通讯接口多样的特点，并且这些移动支付设备多数以从设备(Slave)工作模式为主，现有的网银二代U盾受到物理接口、供电方式、工作模式、操作平台等各个方面条件限制，无法应用于各类移动支付设备，极大限制了安全移动支付的应用。

发明内容

[0004] 本发明的目的在于克服现有网银二代U盾的不足而提供一种基于多种操作系统平台自带电池、支持主设备工作模式的多操作系统平台和移动支付设备的网银U盾及其工作方法，能够适应安全移动支付领域下移动设备多样性和操作系统平台多样性。

[0005] 本发明采用以下技术方案：

一种多操作系统平台和移动支付设备的网银U盾，其特征在于，包括：

USB接口，用于实现与各类移动设备以及PC机的物理连接；

安全控制模块，用于接收来自USB接口的交易数据，提取用户网银交易数字证书并对交易数据进行数字签名；

显示模块，用于与安全控制模块通讯，获取用户交易信息，并采用LCD液晶显示屏显示；

电源，用于U盾的自主供电，支持U盾在主设备模式下的工作方式。

[0006] 还包括：按键部分，包括四个按键，确认键、取消键、上翻键和下翻键，实现确认、返回和查询等菜单功能。

[0007] 所述USB接口由接口1和接口2两部分组成，接口1采用USB2.0接口，用于连接iOS系列和Android系列等移动设备；接口2采用USB3.0接口，用于连接PC机。

[0008] 所述安全控制模块为上层网银应用提供密码服务，所述安全控制模块除包含标准的RSA算法、DES算法外，还包含国家商用密码标准算法，包括SM1对称算法、SM2椭圆曲

线算法、SM3 杂凑算法和随机数发生器。

[0009] 所述按键部分通过按键选择，实现对 U 盾在 USB 协议下的主设备（Host）模式和从设备（Slave）模式之间的切换。

[0010] 还包括 :MFI 认证模块，包含对 iOS 设备的认证证书，由安全控制模块调用，完成 iOS 系列设备对 U 盾的设备认证。

[0011] 一种多操作系统平台和移动支付设备的网银 U 盾的工作方法，其特征在于 ：

当支付设备为 Android、Windows Mobile 等系列设备时，设置 U 盾为主设备，U 盾按照主模式的工作方式与支付设备通信 ；

安全控制模块接收来自 USB 接口的交易数据，将交易信息送至显示模块 ；

用户通过按键对交易信息二次确认后，安全控制模块读取用户证书，对交易数据进行数字签名，将证书和数字签名等交易信息通过 USB 接口返回至支付设备 ；

所述 USB 接口由接口 1 和接口 2 两部分组成，接口 1 采用 USB2.0 接口，用于连接 iOS 系列和 Android 系列等移动设备 ；接口 2 采用 USB3.0 接口，用于连接 PC 机。

[0012] 当 U 盾通过 USB 接口与支付设备连接后，首先通过显示屏和按键进行工作方式选择。

[0013] 当支付设备为 PC 机、iOS 系列等具有主控功能的设备时，设置 U 盾为从模式，按照从模式与 PC 机等设备完成 USB 通信协议，如果主设备是 PC 机，则通过 USB 接口中的接口 2 完成通信 ；如果主设备是 iOS 系列等手机移动终端，则通过 USB 接口中的接口 1 完成通信。

[0014] 当支付设备为 Android、Windows Mobile 等系列设备时，设置 U 盾为主模式，按照主模式与支付设备之间完成 USB 通信协议，通过 USB 接口中的接口 1 完成通信。

[0015] 如果移动支付设备为 iOS 等系列设备，则安全控制模块在接收交易数据前，调用 MFI 认证模块，基于 MFI 认证协议完成与 iOS 系列设备的设备认证。

[0016] 本发明的有益效果是 ：

支持多操作系统平台和移动支付设备的网银 U 盾是在普通二代 U 盾的基础上，除 PC 设备外，增加了对移动设备网上银行服务的支持，提供用户认证证书和数字签名服务，全面解决了 iOS 系统、Android 系统等移动设备无法基于 U 盾保护网银应用安全的问题，为移动支付提供统一、有效、可靠的安全服务。

附图说明

[0017] 图 1 为该网银 U 盾组成结构图。

[0018] 图 2 为该网银 U 盾与支付设备协商主从工作模式过程图。

[0019] 图 3 为该网银 U 盾处理交易信息过程图。

具体实施方式

[0020] 下面结合附图和实施例对本发明做进一步描述 ：

如图 1 所示，一种支持多操作系统平台和移动支付设备的网银 U 盾，包括 USB 接口 1、安全控制模块 2、显示模块 3、MFI 认证模块 4、供电电池 5 和按键部分 6 ；

USB 接口 1，用于实现与各类移动设备以及 PC 机的物理连接 ；

安全控制模块 2，用于接收来自 USB 接口的交易数据，提取用户网银交易数字证书并对

交易数据进行数字签名；

显示模块 3，用于与安全控制模块通讯，获取用户交易信息，并采用 LCD 液晶显示屏显示；

电源（供电电池 5），用于 U 盾的自主供电，支持 U 盾在主设备模式下的工作方式。

[0021] 所述 USB 接口 1 采用标准 mini USB3.0 接口，该接口由接口 1 和接口 2 两部分组成。接口 1 采用 USB2.0 接口，用于连接 iOS、Android 等手机移动终端；接口 2 采用 USB3.0 接口，用于连接 PC 机。该接口实现与各类移动设备以及 PC 机的物理连接。

[0022] 所述安全控制模块 2 以 SRAM 方式接收来自 mini USB3.0 接口的数据，通过 SPI 接口将交易信息送至显示模块 3，对这些数据进行安全处理，为上层网银应用提供密码服务，提取用户网银交易数字证书并对交易数据进行数字签名。待用户通过按键对交易信息二次确认后，安全控制模块读取用户证书，对交易数据进行数字签名，将证书和数字签名等交易信息通过 USB 接口返回至支付设备。该安全控制模块除包含标准的 RSA 算法、DES 算法外，还包含国家商用密码标准算法，包括 SM1 对称算法、SM2 椭圆曲线算法、SM3 杂凑算法和随机数发生器。

[0023] 所述显示模块 3 通过标准 SPI 接口与安全控制模块通讯，获取用户交易信息，并采用 LCD 液晶显示屏显示，显示内容包括用户交易账户和交易金额等交易信息。

[0024] 所述 MFI 认证模块 4 包含对 iOS 设备的认证证书，由安全控制模块调用，通过 I^2C 总线与安全控制模块通信，完成 iOS 系列设备对 U 盾的设备认证。

[0025] 如果移动支付设备为 iOS 系列设备，则安全控制模块在接收交易数据前，调用 MFI 认证模块，基于 MFI 认证协议完成与 iOS 系列设备的设备认证。

[0026] 所述供电电池 5 为 5V 锂电池，用于 U 盾的自主供电，支持 U 盾在主设备模式下的工作方式。

[0027] 所述按键部分 6 包括四个按键，确认键、取消键、上翻键和下翻键，主要实现确认、返回、查询等菜单功能，为用户使用 U 盾提供信息交互。所述按键部分通过按键选择，实现对 U 盾在 USB 协议下的主设备（Host）模式和从设备（Slave）模式之间的切换。

[0028] 如图 2 所示，当网银 U 盾通过 mini USB3.0 接口与支付设备连接后，首先通过显示屏和按键进行工作方式选择，工作方式分为主模式和从模式两类。

[0029] 工作方式一：从（Slave）模式。当支付设备为 PC 机、iOS 系列等具有主控功能的设备时，设置 U 盾为从模式，按照从模式与 PC 机等设备完成 USB 通信协议，如果主设备是 PC 机，则通过 USB 接口中的接口 2 完成通信；如果主设备是 iOS 系列等智能移动终端，则通过 USB 接口中的接口 1 完成通信。

[0030] 工作方式二：主（Master）模式。当支付设备为 Android、Windows Mobile 等系列设备时，设置 U 盾为主模式，按照主模式与支付设备之间完成 USB 通信协议，通过 USB 接口中的接口 1 完成通信。

[0031] 如图 3 所示，当 U 盾设定工作模式并与支付设备之间建立通信通道之后，通过 U 盾进行网上银行交易，交易步骤如下：

步骤一：使用支付设备（PC 机、智能手机、平板电脑等）登录网银支付界面，输入 U 盾保护口令（PIN 码），如正确，用户进行支付操作，输入支付账户和支付金额；如口令错误，则交易过程中断；

步骤二：用户交易过程中的数据信息通过USB接口传送至U盾，U盾则调用显示模块将交易数据显示在LCD液晶屏上；

步骤三：用户二次确认交易支付数据的正确性，如无误，按下确认键；如有错误，则按下返回键，取消该次交易；

步骤四：当用户按下确认键后，U盾调用安全控制模块提取用户证书并对交易数据进行数字签名，并将证书和签名数据通过USB接口返回至网银支付应用程序；

步骤五：网银支付应用程序向网银后台提交证书和经过签名的交易数据，本次网银交易完成。

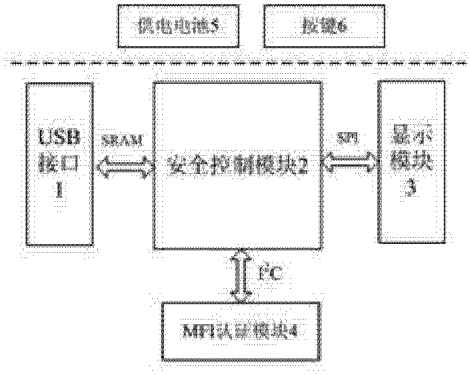


图 1

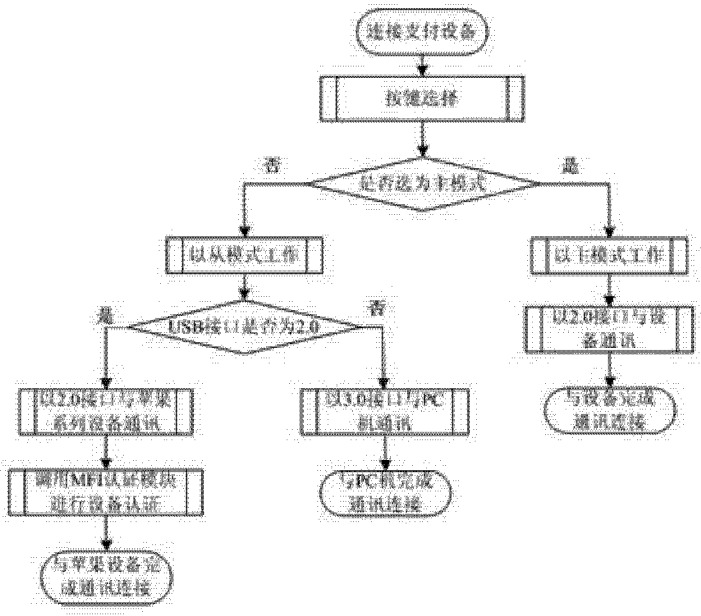

连接支付设备
按键选择
是否选为主模式
否
是
以从模式工作
以主模式工作
是
USB接口是否为2.0
否
以2.0接口与设备通讯
以2.0接口与苹果系列设备通讯
以3.0接口与PC机通讯
与设备完成通讯连接
调用MFI认证模块进行设备认证
与PC机完成通讯连接
与苹果设备完成通讯连接

图 2

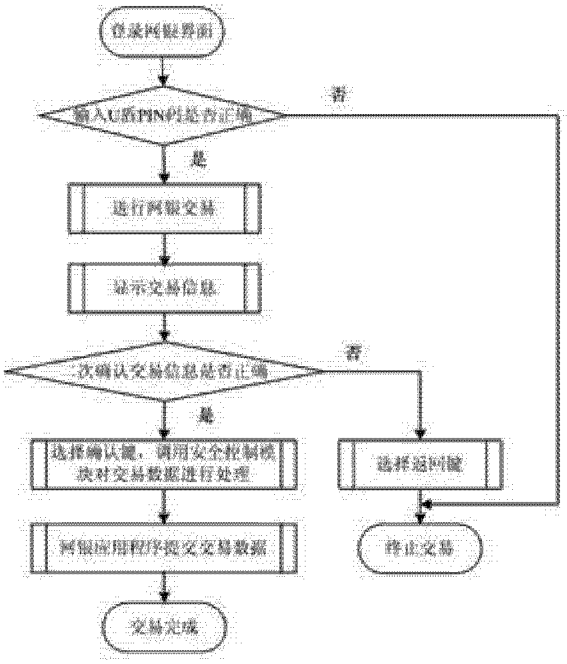

登录网银界面
输入U盾PIN码是否正确
否
是
进行网银交易
显示交易信息
二次确认交易信息是否正确
否
是
选择确认键，调用安全控制模块对交易数据进行处理
选择返回键
网银应用程序提交交易数据
终止交易
交易完成

图 3