(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113014393 B
(45)授权公告日 2023.04.28

(21)申请号 202110193077.5

(22)申请日 2021.02.20

(65)同一申请的已公布的文献号
申请公布号 CN 113014393 A

(43)申请公布日 2021.06.22

(73)专利权人 中易通科技股份有限公司
地址 518000 广东省深圳市南山区西丽街道松坪山社区乌石头路8号天明科技大厦11楼

(72)发明人 刘俊 刘睿 荆鸿远

(74)专利代理机构 深圳市中兴达专利代理有限公司 44637
专利代理师 林丽明

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 9/06(2006.01)
H04L 9/40(2022.01)

(56)对比文件
CN 107769913 A,2018.03.06

审查员 李文聪

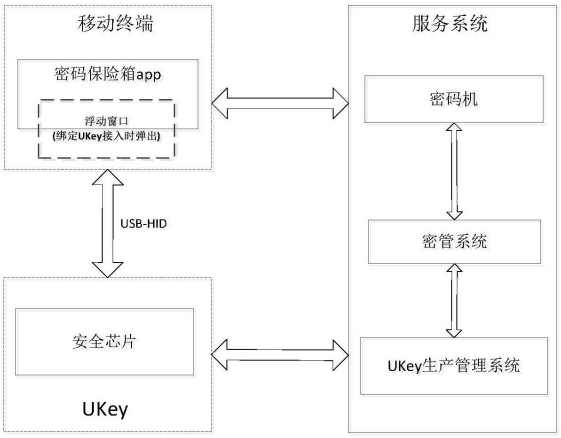
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种基于硬件加密的密码保险箱系统及应用方法

(57)摘要

本发明提供一种基于硬件加密的密码保险箱系统及应用方法,所述系统包括移动终端、安全芯片和服务系统,其中:所述移动终端包括安装在移动终端的程序端;UKey装置,与移动终端通过USB-HID连接;所述服务系统,包括密码机、密钥管理系统和UKey生产管理系统,其中,UKey生产管理系统用于对UKey生产及日常管理的支持后端系统;密钥管理系统,部署在服务器后端,需要密码机支撑,向UKey生产管理系统提供服务。本发明的有益效果是:用户密码的加密传输、保存至安全芯片再提取及自动输入到目标密码框,并且能做到保护密钥无法获取或泄露。



CN 113014393 B

1.一种基于硬件加密的密码保险箱系统,其特征在于,包括移动终端、安全芯片和服务系统,其中:

所述移动终端,包括安装在移动终端的程序端,所述程序端用于初始化及管理用户的安全密码及UKey装置的功能,同时绑定了移动终端对UKey的插入时服务监听处理及浮动窗口;

UKey装置,用于安装安全芯片,与移动终端通过USB-HID连接;

所述服务系统,包括密码机、密钥管理系统和UKey生产管理系统,其中,UKey生产管理系统用于对UKey生产及日常管理的支持后端系统;

密钥管理系统,部署在服务器后端,需要密码机支撑,向UKey生产管理系统提供服务;

所述UKey装置所生产的密钥包括工作密钥及管理密钥,所述工作密钥是UKey装置用于传输用户所设置的密码及内部加密保存密码的工作密钥,工作密钥由安全芯片内部所产生,且不能导出,管理密钥是用于对UKey装置的合法性鉴别及UKey装置的维护、安全密码维护;所述工作密钥包括用于密码传输的非对称密钥、用于密码保护的对称密钥以及UKey公钥列表,其中:非对称密钥是用于传输用户所设置密码,非对称密钥的私钥由安全芯片内部撑控,其公钥部分可导出,非对称密钥所生产的是一次性的临时公私钥对,当UKey装置掉电或重置即丢失;对称密钥为密码内部保存的密钥,由非对称密钥的私钥解密后转为该对称密钥加密再冷保存,对称密钥是在初始化时产生的,且永久保存到安全芯片内部直至UKey装置销毁。

2.根据权利要求1所述的密码保险箱系统,其特征在于,所述管理密钥包括:身份认证非对称公私钥、UKey装置维护对称密钥及安全密码维护对称密钥,其中:

身份认证非对称公私钥是在生产时,由UKey装置内部产生,登记入生产管理系统并建立对应关系供后续合法性鉴别使用;

UKey装置维护对称密钥是根据UKey装置序列号派生再写入UKey装置,用于更新或写入时保护安全密码维护对称密钥;

安全密码维护对称密钥是在用户更新安全密码或设置安全密码时,加密保护密码的密钥,由密钥管理系统根据UKey装置序列号派生再写入UKey装置。

3.根据权利要求1所述的密码保险箱系统,其特征在于,所述UKey公钥列表,是对已发布UKey登记入库的公钥和序列号的对应关系表。

4.一种密码保险箱的应用方法,其特征在于,所述应用方法作用于如权利要求1～3任意一项所述的密码保险箱系统,所述应用方法包括设置密码的方法,包括以下步骤:

步骤1、安全芯片与移动终端连接后,程序端提示:输入密码;

步骤2、安全芯片验证身份,通过则进入步骤3,不通过则结束流程;

步骤3、验证通过后,安全芯片随机产生“临时非对称公私钥”,响应公钥数据;

步骤4、程序端提示:输入“密码标识”、“密码描述信息”及“密码”,使用由安全芯片响应的公钥对以上信息进行加密并发送至安全芯片;

步骤5、安全芯片内部使用临时非对称公私钥对加密的信息解密,并检查数据格式有效性,通过则进入步骤6,不通过则结束流程;

步骤6、通过后,安全芯片提取加密的信息,由“密码保护对称密钥”加密后冷存储;

步骤7、安全芯片用“密码”产生哈希sha1数据,与“密码标识”一并响应;

步骤8、程序端收到响应后，检查哈希sha1数据与“密码标识”根据结果提示用户并结束流程。

5.一种密码保险箱的应用方法，其特征在于，所述应用方法作用于如权利要求1～3任意一项所述的密码保险箱系统，包括提取“密码”用于目标应用的密码输入的方法，包括以下步骤：

步骤1、移动终端接入安全芯片时，程序端发出绑定的浮动窗口，浮动窗口提示输入“安全密码”或“指纹密码”；

步骤2、安全芯片验证通过则开启身份验证通过的权限标识；

步骤3、浮动窗口显示读取安全芯片内部“密码标识”列表并显示；

步骤4、由浮动窗口根据用户选择，组织提取该“密码标识”的密码数据；

步骤5、安全芯片检查权限通过后，内部解密对应“密码”数据；

步骤6、安全芯片开启USB-HID输入数据模式，移动终端接收密码输入，完成目标应用的密码输入及确认验证，结束本流程。

一种基于硬件加密的密码保险箱系统及应用方法

技术领域

[0001] 本发明涉及信息、数据安全技术领域，具体地，涉及一种基于硬件加密的密码保险箱系统及应用方法。

背景技术

[0002] 在互联网及移动互联网的快速发展下，超来超多的移动应用软件的出现，而几乎每款应用软件都是需要用户的密码作为保护，这也给用户带来记住多个密码的烦恼。密码是用户重要且极为敏感隐私信息，所以用户需要记住更多个密码的助手软件

[0003] 市场现有的类似密码助手软件存在一些明显的安全隐患及不足，其主要的表现在于：

[0004] 软件本身只依靠软加密方式采用固定密钥直接对用户输入的密码明文进行简单的加密存储，且加解密的密钥本身是固定在软件本身或者存在于系统存储设备中，这非常容易受到劫持软件或者本马的截获以及通过软件本身的反编译处理，提取解密密钥，对密码密文进行外部解密，造成密码泄露。

发明内容

[0005] 针对现有技术的缺陷，本发明的目的是通过集成在UKey上的安全芯片结合软件APP进行安全通讯，利用国密算法通过硬件加密构建一个基于硬件加密的密码传输、存储、HID键盘输入，并且密码的对称保护密钥及传输公私钥是在初始化及设置时随机产生的，生产管理系统只对UKey本身的管理密钥进行管理。最终能达到对用户密码的加密传输、保存至UKey的安全芯片再安全提取及安全自动输入到目标密码框，并且能做到保护密钥是该软件开发人员无法获取或泄露。是通过如下技术方案实现的。

[0006] 本发明提供了一种基于硬件加密保护的移动智能密码保险箱系统，系统包括了集成安全芯片的UKey和密码保险箱APP、密钥管理系统、硬件密码机、UKey生产管理系统组成。密钥管理系统需要硬件密码机作为UKey及系统的管理密钥的存储计算，通过UKey生产管理系统与密管系统的交互初始化UKey的唯一的管理密钥，包括对称及非对称密钥，对UKey安全芯片进行初始化生产。UKey有支持手机类型的USB接口可接入手机端，用户通过密码保险箱APP对UKey进行设置安全密码或指纹等用户身份确认方式后设置用户需要保护的密码，并通过UKey安全芯片内部随机的非对称公钥方式保护传输至UKey装置的安全芯片内部转为对称密钥加密处理后存储。用户在需要提取指定密码时，需要确认用户身份正确后，才可由安全芯片内部解密后，通过HID键盘输入方式输入目标框完成密码提取。

[0007] 一种基于硬件加密的密码保险箱系统，包括移动终端、安全芯片和服务系统，其中：

[0008] 所述移动终端，包括安装在移动终端的程序端，所述程序端用于初始化及管理用户的安全密码及UKey装置的功能，同时绑定了移动终端对UKey的插入时服务监听处理及浮动窗口；

[0009] UKey装置,用于安装安全芯片,与移动终端通过USB-HID连接;

[0010] 所述服务系统,包括密码机、密钥管理系统和UKey生产管理系统,其中,UKey生产管理系统用于对UKey生产及日常管理的支持后端系统;

[0011] 密钥管理系统,部署在服务器后端,需要密码机支撑,向UKey生产管理系统提供服务。

[0012] 优选方案是,所述UKey装置所生产的密钥包括工作密钥及管理密钥,所述工作密钥是UKey装置用于传输用户所设置的密码及内部加密保存密码的工作密钥,工作密钥的由安全芯片内部所产生,且不能导出,管理密钥是用于对UKey装置的合法性鉴别及UKey装置的维护、安全密码维护。

[0013] 优选方案是,所述工作密钥包括用于密码传输的非对称密钥、用于密码保护的对称密钥以及UKey公钥列表,其中:

[0014] 非对称密钥是用于传输用户所设置密码,非对称密钥的私钥由安全芯片内部撑控,其公钥部分可导出,非对称密钥所生产的是一次性的临时公私钥对,当UKey装置掉电或重置即丢失;

[0015] 对称密钥的密码内部的保存的密钥,由非对称密钥的私钥解密后转为该对称密钥加密再冷保存,对称密钥是在初始化时产生的,且永久保存到安全芯片内部直至UKey装置销毁。

[0016] 优选方案是,所述管理密钥包括:身份认证非对称公私钥、UKey装置维护对称密钥及安全密码维护对称密钥,其中:

[0017] 身份认证非对称公私钥是在生产时,由UKey装置内部产生,登记入生产管理系统并建立对应关系供后续合法性鉴别使用;

[0018] UKey装置维护对称密钥是根据UKey装置序列号派生再写入UKey装置,用于更新或写入时保护安全密码维护对称密钥;

[0019] 安全密码维护对称密钥是在用户更新安全密码或设置安全密码时,加密保护密码的密钥,由密钥管理系统根据UKey装置序列号派生再写入UKey装置。

[0020] 优选方案是,所述UKey公钥列表,是对已发布UKey登记入库的公钥和序列号的对应关系表。

[0021] 一种密码保险箱系统的应用方法,所述应用方法包括设置密码的方法,包括以下步骤:

[0022] 步骤1、安全芯片与移动终端连接后,程序端提示:输入密码;

[0023] 步骤2、安全芯片验证身份,通过则进入步骤3,不通过则结束流程;

[0024] 步骤3、验证通过后,安全芯片随机产生“临时非对称公私钥”,响应公钥数据;

[0025] 步骤4、程序端提示:输入“密码标识”、“密码描述信息”及“密码”,使用由安全芯片响应的公钥对以上信息进行加密并发送至安全芯片;

[0026] 步骤5、安全芯片内部使用临时非对称公私钥对加密的信息解密,并检查数据格式有效性,通过则进入步骤6,不通过则结束流程;

[0027] 步骤6、通过后,安全芯片提取加密的信息,由“密码保护对称密钥”加密后冷存储;

[0028] 步骤7、安全芯片用“密码”产生哈希sha1数据,与“密码标识”一并响应;

[0029] 步骤8、程序端收到相应后,检查哈希sha1数据与“密码标识”根据结果提示用户并

结束流程。

[0030] 优选方案是，上述应用方法还包括提取“密码”用于目标应用的密码输入的方法，包括以下步骤：

[0031] 步骤1、移动终端接入安全芯片时，程序段出发绑定的浮动窗口，浮动窗口提示输入“安全密码”或“指纹密码”；

[0032] 步骤2、安全芯片验证通过则开启身份验证通的权限标识；

[0033] 步骤3、浮动窗口显示读取安全芯片内部“密码标识”列表并显示；

[0034] 步骤4、由浮动窗口根据用户选择，组织提取该“密码标识”的密码数据；

[0035] 步骤5、安全芯片检查权限通过后，内部解密对应“密码”数据；

[0036] 步骤6、安全芯片开启USB-HID输入数据模式，移动终端接收密码输入，完成目标应用的密码输入及确认验证，结束本流程。

[0037] 本发明的有益效果是：利用安全芯片、密码机等硬件密码设备，通过国密对称和非对称算法结合，用于内部存储加解密用户“密码”的对称密钥是随机生成，用于设定时的传输是采用非对称公钥加密，公私钥是临时一次性的，故并不会被软件开发人员预先所知。数据通信过程采用非对称算法加密，可防止中间人攻击和重放攻击，保证通信的机密性、完整性和抗抵赖性，解决密码的安全传输。在用户提取“密码”时，用户只需插入UKey，浮动窗口自动弹出，验用用户身份后使用USB-HID输入密码，不需要用户手动输入。

附图说明

[0038] 图1是本发明实施例的保险箱系统结构框图。

[0039] 图2是本发明实施例的保险箱所需密钥及关系结构图。

[0040] 图3是本发明实施例的UKey装置的安全芯片在UKey生产系统的生产过程功能图。

[0041] 图4是本发明实施例的程序端对UKey设备基本管理功能图。

[0042] 图5是本发明实施例的程序端对UKey装置初始化流程图。

[0043] 图6是本发明实施例的程序端与UKey装置设置需要保护的密码流程图。

[0044] 图7是是本发明实施例用户提取UKey装置密码的应用方法流程图。

具体实施方式

[0045] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0046] 本发明实施例中：

[0047] UKey装置：承载安全芯片的硬件，有手机的USB接口。

[0048] HID：完整简称为USB-UID，Universal Serial Bus-Human Interface Device的缩写，是直接与人交互的设备，例如键盘、鼠标与游戏杆等。

[0049] 程序端：泛指手机上的APP应用软件，在本发明实施例中指密码保险箱应用APP。

[0050] 图1所示为基于硬件加密保护的移动智能密码保险箱系统的总体结构框图。

[0051] 整体的移动密码箱系统主要组成分为四大部分组成，分别是移动终端(即手机)；

程序端,即安装在移动终端的“密码保险箱APP”、UKey装置(内含安全加密芯片)、UKey生产管理系统及密钥管理系统。

[0052] 程序端,即密码保险箱APP:用于初始化及管理用户的安全密码及UKey装置的功能,同时绑定了手机对特定型号的UKey装置的插入时服务监听处理及浮动窗口。初始化时用户需要初始化“安全密码”或“指纹密码”,此处的安全密码是对用户的身份确认的一种方式,也可以使用指纹密码替代(根据UKey装置硬件条件决定)。用户在完成身份确认后,可通过该程序端向UKey装置的安全芯片设置用户的“密码”及增删查改等功能。当特定型号的UKey装置接入时,通过服务监听开启程序端的浮动窗口,该浮动窗口是置顶层于其它应用之上,用于提示用户输入密码或触碰指纹及后续显示密码标识列表供用户选择等交互性功能。

[0053] UKey装置:是安全芯片的承载体,有适配于手机的USB接口,能根据场景需要模拟USB-HID功能服务。根据实际型号集成了指纹传感器及触控开关等其它验证功能模块,拥有独立处理的内部操作系统能力。通过USB接口接收来自移动终端上的程序端(密码保险箱APP)的指令做对应处理及响应结果。

[0054] UKey生产管理系统:对UKey生产及日常管理的支持后端系统,提供对UKey装置的安全芯片的安全维护密钥初始化、序列号登记、状态管理、等功能。

[0055] 密钥管理系统:安全布署在服务器后端,需要硬件密码机支撑。不直接对外部开放服务,只对内部系统,即向UKey生产管理系统提供密钥的初始化、更新、销毁、计算等服务。

[0056] 如图2所示,是基于硬件加密保护的移动智能密码保险箱系统所需密钥及关系结构图,在图2中:

[0057] UKey装置的安全芯片密钥结构:分为“工作密钥”及“管理密钥”两部分,“工作密钥”是UKey装置用于传输用户所设置的密码及内部加密保存密码的工作密钥。“工作密钥”是极为敏感及重要的密钥,故本发明将“工作密钥”的产生全放在安全芯片内部,并且没有任何的接口或方式能导出。“管理密钥”是用于对UKey装置的合法性鉴别及UKey装置的维护、安全密码维护。

[0058] 密码传输非对称密钥:本发明定义传输用户所设置密码的方式为非对称公钥,私钥由内部撑控,只导出可公开的公钥,并且是一次性的临时公私钥对,当UKey装置掉电或重置即丢失。

[0059] 密码保护对称密钥:本发明定义密码内部的保存密钥为对称密钥,由传输的私钥解密后转为该对称密钥加密再冷保存,该密钥是在初始化时产生的,并且永久保存至安全芯片内部直至UKey装置销毁。

[0060] 身份认证非对称公私钥:合法性鉴别使用“身份认证非对称公私钥”,是在生产时,由UKey装置内部产生,只导出公钥,登记入生产管理系统并建立对应关系供后续合法性鉴别使用。

[0061] UKey维护密钥对称密钥:是在生产时由“密钥管理系统”根据UKey装置序列号派生再写入UKey装置,用于更新或写入时保护“安全密码维护对称密钥”。

[0062] 安全密码维护对称密钥:是用于用户更新安全密码或设置安全密码时,加密保护密码的密钥,由“密钥管理系统”根据UKey装置序列号派生再写入UKey装置。

[0063] 密钥管理系统密钥结构:本部分均由硬件密码机内部产生,并且不允许外部导出。

[0064] UKey维护对称密钥主密钥:用于派生UKey装置序列号对应功能的子密钥;

[0065] 安全密码维护对称密钥:用于派生UKey装置序列号对应功能的子密钥;

[0066] UKey公钥列表:是对已发布UKey登记入库的公钥及序列号的关系表,公钥属可公开数据,故本发明采用存储于普通关系型数据库。

[0067] 注):再次强调,本发明将“工作密钥”在安全芯片内部产生,保证“安全性”,“管理密钥”由系统有规则产生再写入安全芯片,保证“可控性”。

[0068] 图3所示为UKey的安全芯片在UKey生产系统的生产过程功能,UKey的生产是在用户持有之前完成的,用户不需要参与其中。

[0069] ①:UKey装置在生产时,内部随机产生“身份认证非对称公私钥对”保存安全芯片内部,只导出公钥,将公钥及序列号上报UKey生产管理系统;

[0070] ②:UKey生产管理系统将上报的UKey装置序列号及公钥数据入库建立对应关系表;

[0071] ③:UKey生产管理系统用UKey装置序列号派生对应的“UKey维护密钥子密钥”并使用UKey装置默认的维护密钥加密保护后下发;

[0072] ④:将“UKey维护密钥子密钥”替换UKey装置默认的维护密钥。

[0073] ⑤:UKey生产管理系统用UKey装置序列号派生对应的“安全密码维护密钥子密钥”并使用上一步派生的“UKey维护密钥子密钥”加密保护后下发;

[0074] ⑥:将“安全密码维护密钥子密钥”替换UKey装置默认的安全密码维护密钥。

[0075] 如图4所示,程序端(密码保险箱APP)对UKey装置基本管理功能包括:

[0076] 程序端(密码保险箱APP)对UKey装置的基本功能是对UKey装置本身及密码的日常管理,需要完成生产阶段后才可使用。

[0077] 用户验证:本发明对用户验证的方式保留多种方式,可以是预设的“安全密码”或“指纹密码”及“触控开关”等方式。

[0078] 修改“安全密码”或指纹密码:对已经设置的“安全密码”或“指纺密码”进行修改,该功能需要用户完成验证才可使用。

[0079] 修改“设定密码”:对已经设定的用户“密码”进行修改,本功能需要用户完成验证才可显示即有的“密码标识”列表,用户选择需要修改的“密码标识”进行修改。

[0080] 查看“设定密码”:对已经设定的用户“密码”进行查看,本功能需要用户完成验证才可显示即有的“密码标识”列表,选定标识显示设定日期、时间、用途等信息。

[0081] 删除“设定密码”:对已经设定的用户“密码”进行删除,本功能需要用户完成验证才可显示即有的“密码标识”列表,选定标识进行删除。

[0082] 完全销毁:对UKey的设定密码进行完全销毁,不影响“密理密钥”及“工作密钥”等数据。

[0083] 如图5所示,是密码保险箱APP对UKey初始化流程,UKey的初始化是用户初次持有使用时,对UKey的基本信息进行配置,并登记的处理过程。

[0084] 步骤①:UKey装置初次接入手机后,程序端读取UKey装置序列号,并获取由UKey装置安全芯片内部的“身份认证非对称公私钥”签名的数据及用户设定“安全密码”上送UKey生产管理系统;

[0085] 步骤②:UKey生产管理系统根据UKey装置序列号获取对应公钥数据验证UKey合法

性；

[0086] 步骤③:UKey生产管理系统根据UKey装置序列号请求密钥管理系统派生“UKey安全密码维护密钥”的子密钥并加密“安全密码”响应；

[0087] 步骤④:程序端收到响应后,发起UKey内部解密“安全密码”数据,格式正确后设置“安全密码”或指纹密码；

[0088] 步骤⑤:UKey装置内部安全芯片随机产生“密码保护对称密钥”并保存至内部存储。

[0089] 图6所示为密码保险箱APP与UKey设置需要保护的密码流程图,在用户已经初始化好了UKey,并且已经设定好了“安全密码”或“指纹密码”后,设置用户的“密码”的详细过程。

[0090] S1:用户接入UKey装置至移动终端；

[0091] S2:程序端提示用户输入“安全密码”或“指纹密码”；

[0092] S3:UKey装置安全芯片内部验证用户身份,不通过时响应错误信息及代码进入S4结束流程,通过身份验证时进入S5流程；

[0093] S4:程序端提示用户身份验证未通过,不满足操作权限；

[0094] S5:UKey装置身份验证通过,随机产生“临时非对称公私钥”,响应公钥数据；

[0095] S6:程序端提示用户输入“密码标识”、“密码描述信息”及“密码”,使用由UKey装置响应的公钥对以上信息进行加密发送至UKeyy装置；

[0096] S7:UKey装置安全芯片内部使用S5随机产生的“临时非对称公私钥”私钥解密,检查数据格式有效性,不正确时响应错误信息及代码进入S8结束流程,通过时进入S9流程；

[0097] S8:程序端提示用户数据非法错误信息；

[0098] S9:数据格式正确,UKey装置内部提取用户在S6输入“密码标识”、“密码描述信息”及“密码”,由“密码保护对称密钥”加密后冷存储；

[0099] S10:UKey装置完成冷存储后,用“密码”产生哈希sha1数据,与“密码标识”一并响应；

[0100] S11:程序端收到响应后,检查哈希sha1数据与“密码标识”根据结果提示用户结束流程。

[0101] 如图7所示,用户提取UKey装置密码流程图,在用户已经对UKey装置设定了“密码”后,用户提取“密码”用于目标应用的密码输入详细过程。

[0102] S21:用户打开目标应用,将光标移至需要输入密码的地方；

[0103] S22:接入UKey装置；

[0104] S23:移动终端的系统触发绑定的浮动窗口,该浮动窗口是包含在程序端内部的；

[0105] S24:程序端的浮动窗口显示提示用户输入“安全密码”或“指纹密码”；

[0106] S25:UKey装置身份验证如果不通过,进入S26流程,如果通过进入S27流程；

[0107] S26:浮动窗口提示用户身份验证未通过,不满足操作权限,结束本流程；

[0108] S27:UKey装置身份验证通过,UKey装置开启身份验证通的权限标识；

[0109] S28:浮动窗口(由密码保险箱APP生成)读取UKey装置内部“密码标识”列表并显示；

[0110] S29:用户选择需要的“密码标识”,由浮动窗口(密码保险箱APP)组织提取该“密码标识”的密码数据；

[0111] S30:UKey装置检查权限通过后,内部解密对应“密码”数据;

[0112] S31:UKey装置开启USB-HID输入数据模式,完成输入后,尾补“回车”的确认键;

[0113] S32:移动终端由USB-HID服务接收密码输入,完成目标应用的密码输入及确认验证,结束本流程。

[0114] 尽管已经示出和描述了本发明的实施例,对于本领域的普通技术人员而言,可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型,本发明的范围由所附权利要求及其等同物限定。

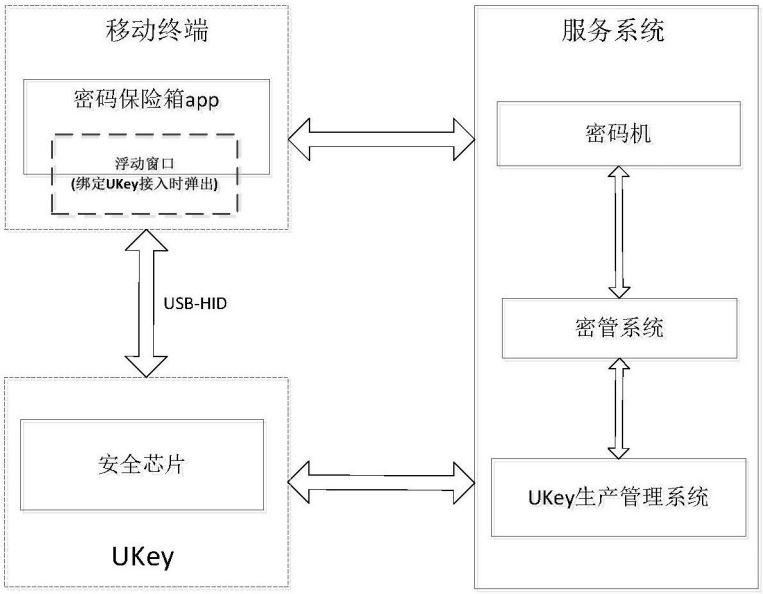

移动终端
密码保险箱app
浮动窗口
(绑定UKey接入时弹出)
USB-HID
安全芯片
UKey
服务系统
密码机
密管系统
UKey生产管理系统

图1

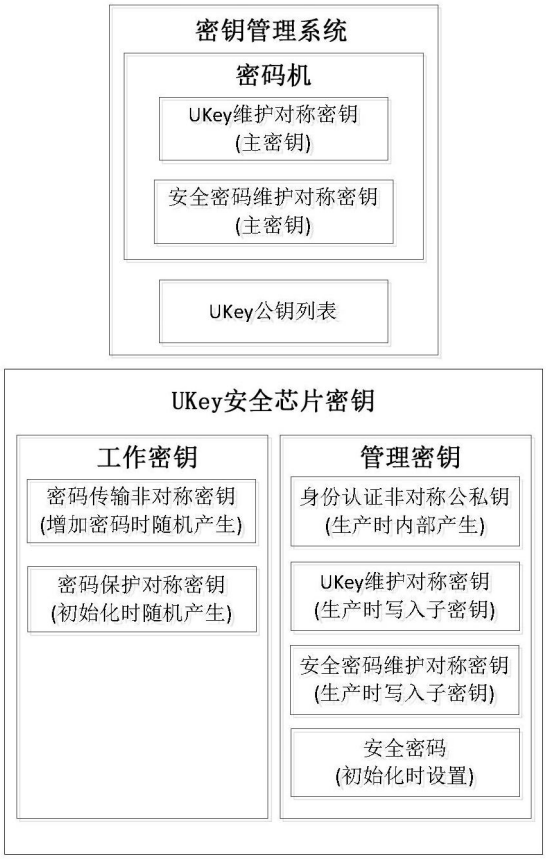

密钥管理系统
密码机
UKey维护对称密钥
(主密钥)
安全密码维护对称密钥
(主密钥)
UKey公钥列表
UKey安全芯片密钥
工作密钥
密码传输非对称密钥
(增加密码时随机产生)
密码保护对称密钥
(初始化时随机产生)
管理密钥
身份认证非对称公私钥
(生产时内部产生)
UKey维护对称密钥
(生产时写入子密钥)
安全密码维护对称密钥
(生产时写入子密钥)
安全密码
(初始化时设置)

图2

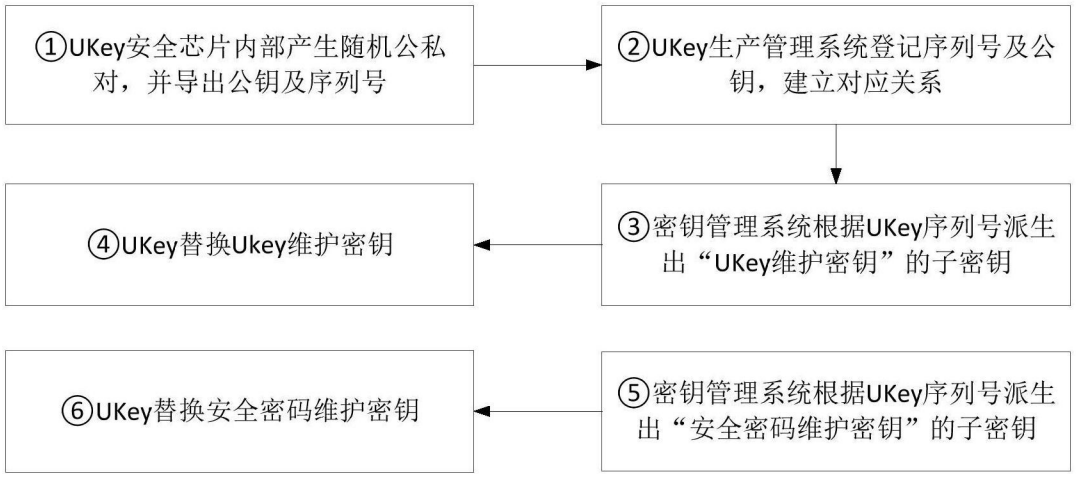

①UKey安全芯片内部产生随机公私对，并导出公钥及序列号
②UKey生产管理系统登记序列号及公钥，建立对应关系
③密钥管理系统根据UKey序列号派生出“UKey维护密钥”的子密钥
④UKey替换Ukey维护密钥
⑤密钥管理系统根据UKey序列号派生出“安全密码维护密钥”的子密钥
⑥UKey替换安全密码维护密钥

图3

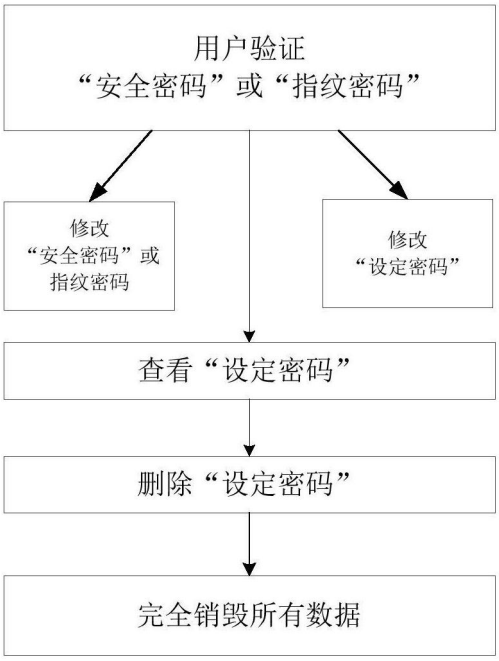

用户验证
“安全密码”或“指纹密码”
修改
“安全密码”或
指纹密码
修改
“设定密码”
查看“设定密码”
删除“设定密码”
完全销毁所有数据

图4

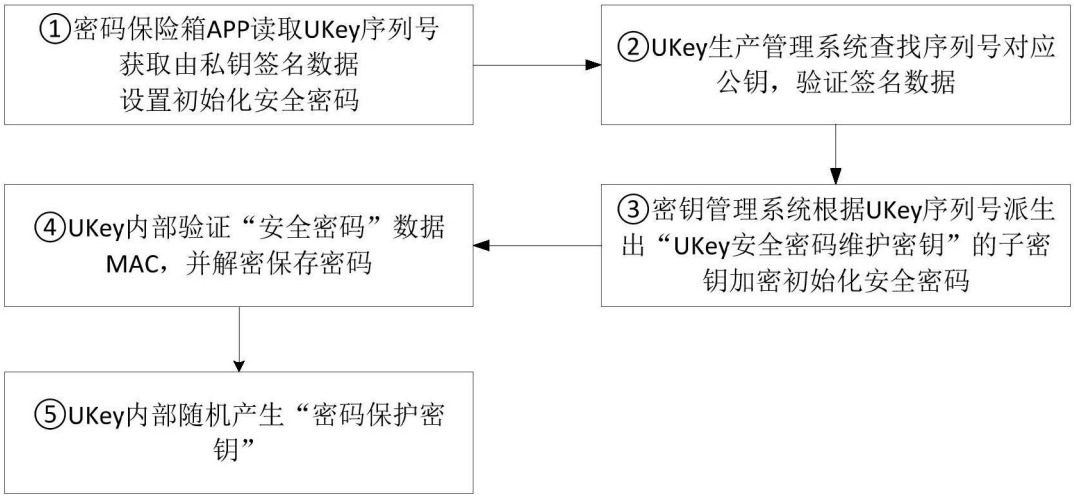

①密码保险箱APP读取UKey序列号
获取由私钥签名数据
设置初始化安全密码
②UKey生产管理系统查找序列号对应公钥，验证签名数据
③密钥管理系统根据UKey序列号派生出“UKey安全密码维护密钥”的子密钥加密初始化安全密码
④UKey内部验证“安全密码”数据MAC，并解密保存密码
⑤UKey内部随机产生“密码保护密钥”

图5

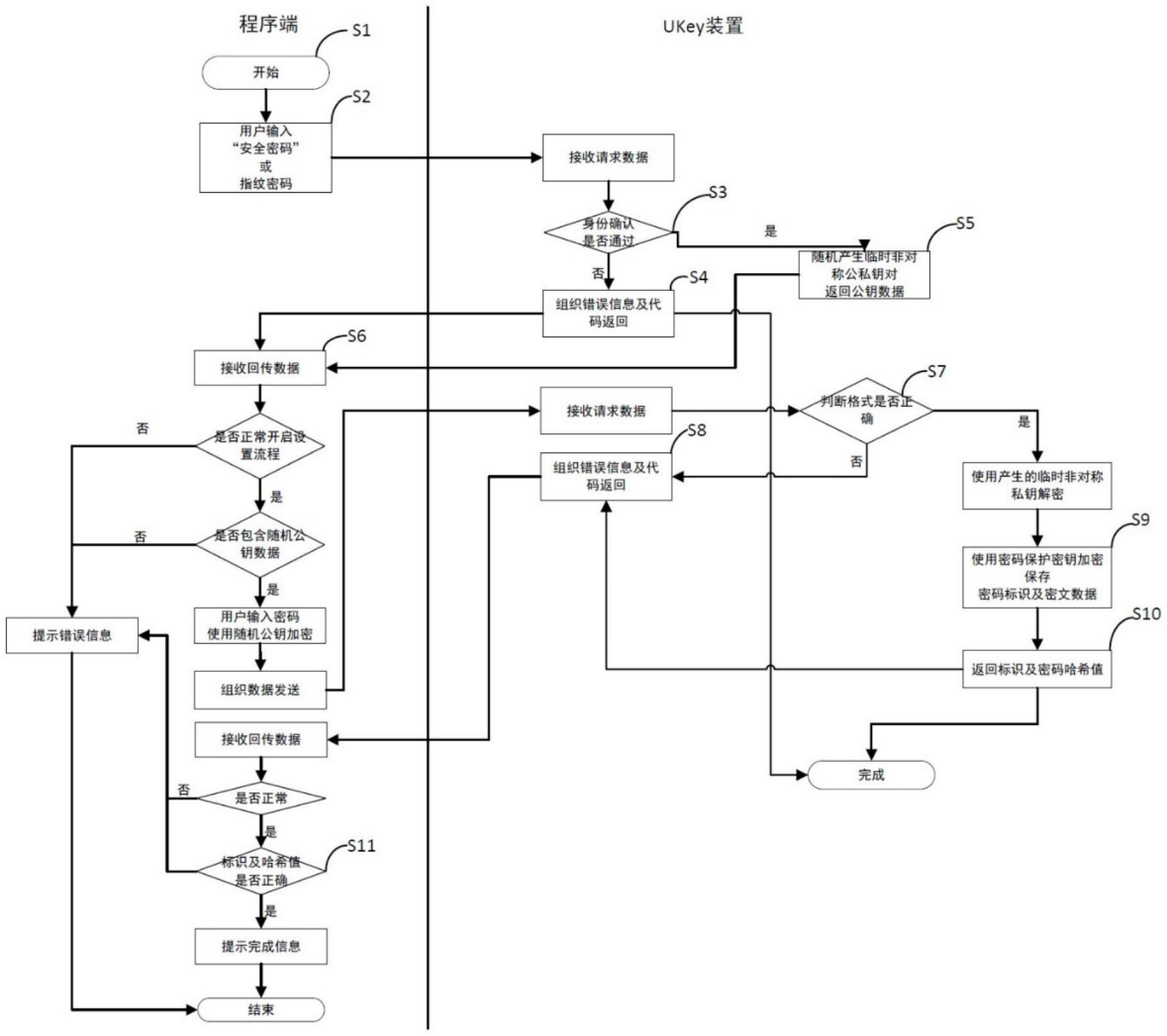

程序端
UKey装置
S1
开始
S2
用户输入
“安全密码”
或
指纹密码
接收请求数据
S3
身份确认
是否通过
是
否
S5
随机产生临时非对称公私钥对
返回公钥数据
S4
组织错误信息及代码返回
S6
接收回传数据
是否正常开启设置流程
否
是
是否包含随机公钥数据
否
是
用户输入密码
使用随机公钥加密
提示错误信息
组织数据发送
接收回传数据
否
是否正常
是
标识及哈希值是否正确
S11
是
提示完成信息
结束
接收请求数据
S7
判断格式是否正确
是
否
S8
组织错误信息及代码返回
使用产生的临时非对称私钥解密
S9
使用密码保护密钥加密保存
密码标识及密文数据
S10
返回标识及密码哈希值
完成

图6

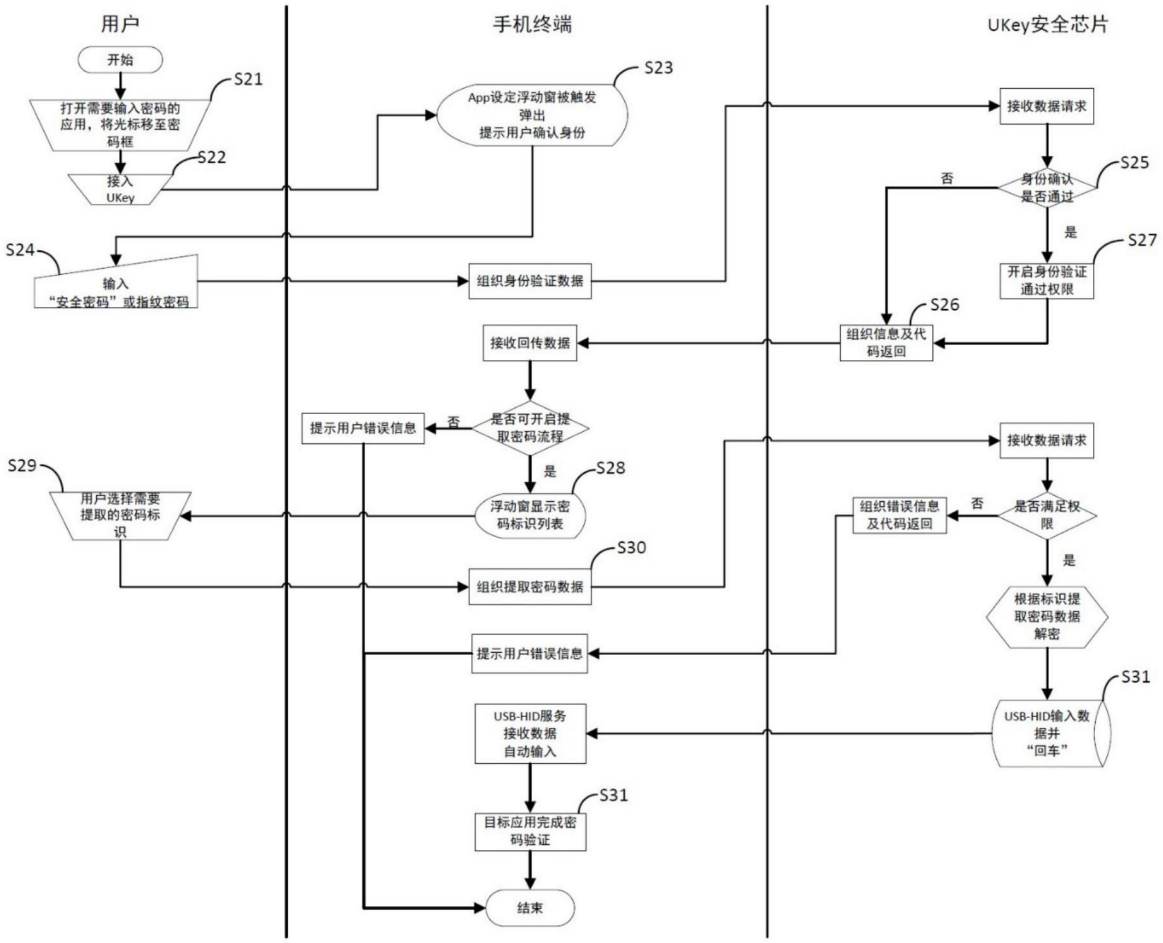

用户
手机终端
UKey安全芯片
开始
S21
打开需要输入密码的应用，将光标移至密码框
S22
接入UKey
S23
App设定浮动窗被触发弹出
提示用户确认身份
S24
输入“安全密码”或指纹密码
组织身份验证数据
接收数据请求
否
身份确认是否通过
S25
是
S27
开启身份验证通过权限
S26
组织信息及代码返回
接收回传数据
提示用户错误信息
否
是否可开启提取密码流程
是
S28
浮动窗显示密码标识列表
S29
用户选择需要提取的密码标识
组织提取密码数据
S30
接收数据请求
否
组织错误信息及代码返回
是否满足权限
是
根据标识提取密码数据解密
提示用户错误信息
USB-HID服务接收数据自动输入
S31
USB-HID输入数据并“回车”
目标应用完成密码验证
S31
结束

图7