(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114422261 B
(45)授权公告日 2024.06.07

(21)申请号 202210138256.3

(22)申请日 2022.02.15

(65)同一申请的已公布的文献号
申请公布号 CN 114422261 A

(43)申请公布日 2022.04.29

(73)专利权人 北京无字天书科技有限公司
地址 100089 北京市海淀区西三环北路89号4层A-01-54号

(72)发明人 封维端 郑志梅 袁峰 张立圆 葯乐 李中声

(74)专利代理机构 北京知汉亭知识产权代理事务所(普通合伙) 16011
专利代理师 刘金龙

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 101872399 A,2010.10.27
CN 109067766 A,2018.12.21
CN 109728909 A,2019.05.07
WO 2007121641 A1,2007.11.01

审查员 许婵

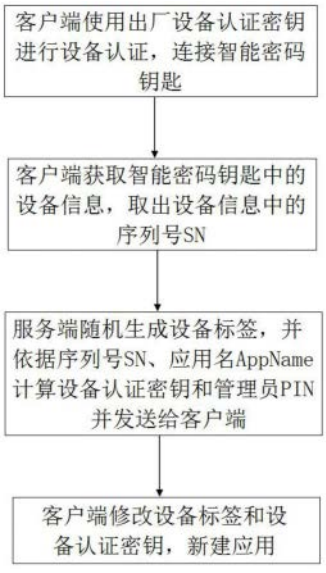
权利要求书4页 说明书12页 附图3页

(54)发明名称

管理方法、管理系统、计算机设备和计算机可读存储介质

(57)摘要

本发明提供一种用于管理智能密码钥匙的设备认证密钥和管理员PIN的管理方法、管理系统、计算机设备和计算机可读存储介质,所述管理方法包括下列方法中的一种或几种:方法A、对智能密码钥匙进行初始化的方法,包括设置设备认证密钥和设置管理员个人身份识别码;方法B、所述设备认证密钥和管理员个人身份识别码的使用方法;方法C、所述设备认证密钥和管理员个人身份识别码的修改方法。本发明的管理方法中,设备认证密钥和管理员PIN由服务端生成,且可以更改,有效的避免了设备认证密钥和管理员PIN不安全、易泄露等问题,使得智能密码钥匙的使用安全性大大增加。



CN 114422261 B

1.管理方法,其特征在于,包括下列方法中的一种或几种:

方法A、对智能密码钥匙进行初始化的方法,包括设置设备认证密钥和设置管理员个人身份识别码;

方法B、所述设备认证密钥和管理员个人身份识别码的使用方法;

方法C、所述设备认证密钥和管理员个人身份识别码的修改方法,

其中,

所述方法A包括步骤:

AB、客户端获取所述智能密码钥匙中的设备信息,取出所述设备信息中的序列号SN;

AC、服务端随机生成设备标签,并依据所述序列号SN、应用名AppName计算所述设备认证密钥和管理员个人身份识别码,然后发送给所述客户端;

AD、所述客户端修改所述智能密码钥匙中的设备标签和设备认证密钥,建立新的应用,

所述方法B包括步骤:

BB、所述客户端获取所述智能密码钥匙中的设备信息中的序列号SN和设备标签,将所述序列号SN、设备标签和应用名AppName发送给所述服务端;

BC、所述服务端计算所述设备认证密钥和管理员个人身份识别码并发送给所述客户端,

所述方法C包括步骤:

CB、所述客户端获取到当前的设备认证密钥和管理员个人身份识别码;

CC、所述客户端向服务端申请计算得到新的设备标签NewLabel、新的设备认证密钥NewDevAuthKey和新的管理员个人身份识别码NewAdminPIN;

CD、所述客户端更新所述设备标签、设备认证密钥和管理员个人身份识别码;

所述步骤AC中,若所述客户端和服务端之间的连接为可信信道,则执行下列步骤:

所述客户端将所述序列号SN、应用名AppName发送给所述服务端;

所述服务端生成32字节随机数作为第一设备标签Label1,再将所述第一设备标签Label1和序列号SN进行字节拼接,得到第一数据data1:data1=Label1||SN,其中,||表示字节的拼接;

所述服务端调用服务器密码机,使用所述服务器密码机内的密钥索引为index的SM2密钥,并通过使用导入会话密钥并用内部椭圆曲线加密算法私钥解密接口导入会话密钥,并得到会话密钥句柄;

所述服务端调用所述服务器密码机,使用所述会话密钥句柄,并通过使用SM4加密算法加密所述第一数据data1,得到第一密文C1;

所述服务端计算C1||ID的第一SM3杂凑值S01=SM3(C1||ID),得到32字节SM3杂凑值S01,其中,ID为信息系统的固定标识字符串或空,所述服务端为所述信息系统的服务器;

所述服务端取所述SM3杂凑值S01的前16字节为第一设备认证密钥DevAuthKey1:DevAuthKey1=S01[0:16],设构成字符串D的各字节均具有下标(为整数),且以各字节的下标由小至大依次标识对应的各字节在字符串D中由前至后的顺序,D[m:n]表示对字符串D取从下标m(初始下标)至下标n-1的字节,m和n均为整数,且m<n,S01中初始下标m为0;

所述服务端计算S1=SM3(S01||AppName),以及S2=Base64(S1),得到44字节可打印字符串S2,Base64(E)表示把二进制数据E使用Base64编码转为44个可打印字符;

所述服务端取所述可打印字符串S2的前16字节为第一管理员个人身份识别码AdminPIN1:AdminPIN1＝S2[0:16];

所述服务端将所述第一设备标签Label1、第一设备认证密钥DevAuthKey1、第一管理员个人身份识别码AdminPIN1发送给所述客户端;

所述客户端修改第一设备标签Label1和第一设备认证密钥DevAuthKey1,并使用第一管理员PIN AdminPIN1和用户输入的用户个人身份识别码建立新的应用;

所述步骤AC中,若所述客户端和服务端的连接为非可信信道,则执行下列步骤:

所述客户端建立一个新的临时应用,所述临时应用的临时用户个人身份识别码和临时管理员个人身份识别码由所述客户端随机生成;

所述客户端使用所述临时应用建立临时容器;

所述客户端在所述临时容器内生成椭圆曲线加密算法签名密钥对,并输出椭圆曲线加密算法签名密钥对中的临时签名公钥TempSignPubKey;

所述客户端将所述序列号SN、应用名AppName、临时签名公钥TempSignPubKey发送给所述服务端;

所述服务端生成32字节随机数作为第二设备标签Label2,将所述第二设备标签Label2和序列号SN进行字节拼接,得到第二数据data2:data2＝Label2||SN;

所述服务端调用服务器密码机,使用所述服务器密码机内的密钥索引为index的SM2密钥,并通过使用导入会话密钥并用内部椭圆曲线加密算法私钥解密接口导入会话密钥,并得到会话密钥句柄;

所述服务端调用所述服务器密码机,使用所述会话密钥句柄,并通过使用SM4加密算法加密所述第二数据data2,得到第二密文C2;

所述服务端计算C2||ID的第二SM3杂凑值S02＝SM3(C2||ID),得到32字节的所述第二SM3杂凑值S02,其中,ID为信息系统的固定标识字符串或空;

所述服务端取所述第二SM3杂凑值S02的前16字节为第二设备认证密钥DevAuthKey2:DevAuthKey2＝S02[0:16];

所述服务端计算S11＝SM3(S02||AppName),以及S21＝Base64(S11),得到44字节可打印字符串S21;

所述服务端取所述可打印字符串S21的前16字节为第二管理员个人身份识别码:AdminPIN2＝S21[0:16];

所述服务端生成临时会话密钥TempSessionKey,并使用所述临时会话密钥TempSessionKey和SM4算法加密组合数据Label2||DevAuthKey2||AdminPIN2得到加密数据EncryptedData:

EncryptedData＝SM4(TempSessionKey,

Label2||DevAuthKey2||AdminPIN2),其中,SM4(K,D1)表示使用密钥K,对数据D1使用SM4加密算法加密得到的密文;

所述服务端生成SM2加密密钥对(TempEncPrivateKey,TempEncPubKey),使用其中的加密密钥TempEncPubKey加密所述临时会话密钥TempSessionKey得到数字信封EnvelopedSessionKey:

EnvelopedSessionKey＝SM2(TempEncPubKey,

TempSessionKey),其中,SM2(PubKey,D2)表示使用SM2公钥PubKey,对数据D2使用SM2加密算法加密得到的密文;

所述服务端使用所述客户端的临时签名公钥TempSignPubKey对所述加密密钥TempEncPrivateKey加密并组成椭圆曲线加密密钥对保护结构EnvelopedKeyBlob;

所述服务端将所述椭圆曲线加密密钥对保护结构EnvelopedKeyBlob、数字信封EnvelopedSessionKey、加密数据EncryptedData发送给所述客户端;

所述客户端使用导入椭圆曲线加密密钥对接口将所述椭圆曲线加密密钥对保护结构EnvelopedKeyBlob导入所述临时容器中;

所述客户端使用导入会话密钥接口将所述数字信封EnvelopedSessionKey导入到所述临时容器中,并得到会话密钥句柄;

所述客户端使用所述会话密钥句柄和单组数据解密接口解密所述加密数据EncryptedData得到组合数据Label2||DevAuthKey2||AdminPIN2,并根据数据长度分别截取得到所述第二设备标签Label2、第二设备认证密钥DevAuthKey2和第二管理员个人身份识别码AdminPIN2;

所述步骤BC包括:

所述服务端调用服务器密码机,使用密钥索引为index的SM2密钥,导入会话密钥,并用内部椭圆曲线加密私钥解密接口导入所述会话密钥中的SM2加密密文KeyCipher并得到会话密钥句柄;

所述服务端调用所述服务器密码机,使用所述会话密钥句柄和SM4加密算法,加密Label||SN,得到密文C;

所述服务端计算C||ID的第三SM3杂凑值S03=SM3(C||ID),得到32字节第三SM3杂凑值S03;

所述服务端取所述第三SM3杂凑值S03的前16字节为第三设备认证密钥DevAuthKey3:DevAuthKey3=S03[0:16];

所述服务端计算SS1=SM3(S03||AppName),以及SS2=Base64(SS1),得到44字节可打印字符串SS2;

所述服务端取所述可打印字符串SS2的前16字节为第三管理员个人身份识别码AdminPIN3:AdminPIN3=SS2[0:16];

所述服务端将第三设备认证密钥DevAuthKey3和第三管理员个人身份识别码AdminPIN3发送给客户端;

所述步骤CB同所述步骤BB至步骤BC,所述客户端获取到当前的设备认证密钥:第四设备认证密钥DevAuthKey4和当前的第四管理员个人身份识别码:第四管理员PIN AdminPIN4;

所述步骤CC同所述步骤AC,由所述客户端向服务端申请计算得到新的设备标签NewLabel、新的设备认证密钥NewDevAuthKey和新的管理员个人身份识别码NewAdminPIN;

所述步骤CD包括:

所述客户端使用所述第四设备认证密钥DevAuthKey4进行设备认证,认证成功后,客户端使用修改设备认证密钥接口将所述第四设备认证密钥DevAuthKey4修改为所述新的设备认证密钥NewDevAuthKey;

所述客户端使用修改个人身份识别码接口将所述第四管理员个人身份识别码AdminPIN4修改为新的管理员个人身份识别码NewAdminPIN;

所述客户端使用设置设备标签接口将所述新的设备标签NewLabel写入所述智能密钥钥匙的设备标签字符串中。

2.根据权利要求1所述的管理方法,其特征在于,

在所述步骤AB之前,执行如下步骤:

所述客户端使用出厂设备认证密钥进行设备认证,连接所述智能密钥钥匙。

3.根据权利要求2所述的管理方法,其特征在于,

所述步骤AB包括:

所述客户端调用获取设备信息接口获取所述智能密钥钥匙的设备信息,取出所述设备信息中的序列号SN。

4.根据权利要求1所述的管理方法,其特征在于,

所述步骤AD包括:

所述客户端得到所述第一设备标签Label1、第一设备认证密钥DevAuthKey1、第一管理员个人身份识别码AdminPIN1或所述第二设备标签Label2、第二设备认证密钥DevAuthKey2、第二管理员个人身份识别码AdminPIN2后,修改所述设备标签和设备认证密钥,建立新的应用,包括如下步骤:

将所述第一设备标签Label1或第二设备标签Label2写入所述智能密钥钥匙的设备标签的字符串中;

使用修改设备认证密钥接口修改所述设备认证密钥为所述第一设备认证密钥DevAuthKey1或第二设备认证密钥DevAuthKey2;

建立新的应用,并设置所述管理员个人身份识别码为第一管理员个人身份识别码AdminPIN1或第二管理员个人身份识别码AdminPIN2,用户个人身份识别码由用户输入;

建立所述新的应用后,删除所述临时应用。

5.根据权利要求4所述的管理方法,其特征在于,

所述步骤BB包括:

所述客户端调用获取设备信息接口来获取所述智能密钥钥匙的设备信息,取出所述设备信息中的序列号SN和设备标签Label;

所述客户端将所述序列号SN、设备标签Label和应用名AppName发送给所述服务端。

6.管理系统,用于实现权利要求1-5任一项所述的管理方法,其特征在于,包括客户端、智能密码钥匙和服务端。

7.计算机设备,包括存储器、第一处理器及储存在所述存储器上并可在所述第一处理器上运行的第一计算机程序,其特征在于,所述第一计算机程序被第一处理器执行时实现如权利要求1-5任一项所述的管理方法的步骤。

8.计算机可读存储介质,其特征在于,储存有第二计算机程序,所述第二计算机程序可被至少一个第二处理器所执行,以使所述至少一个第二处理器执行如权利要求1-5任一项所述的管理方法的步骤。

管理方法、管理系统、计算机设备和计算机可读存储介质

技术领域

[0001] 本发明属于信息安全技术领域,特别涉及一种管理方法、管理系统、计算机设备和计算机可读存储介质。

背景技术

[0002] 智能密码钥匙(USB KEY,也称为智能秘钥钥匙)是一种公钥基础设施(Public Key Infrastructure,PKI)体系下的终端设备,为使用者提供身份认证、数字证书、数据保护等服务,广泛应用于网上银行、电子签章等领域。智能密码钥匙接口规范遵循GB/T 35291《信息安全技术智能密码钥匙应用接口规范》。

[0003] 智能密码钥匙通过使用设备认证密钥(DevAuthKey)(参见GB/T 35291,设备认证密钥是用于设备认证的密钥)对调用智能密码钥匙的应用程序进行认证。设备认证密钥一般为16字节的SM4密钥。应用程序通过设备认证密钥完成设备认证后,可以对智能密码钥匙中的应用进行新建、删除等管理。

[0004] 智能密码钥匙中可以存在多个应用[参见GB/T 35291,一个设备中存在设备认证密钥和多个应用,应用之间相互独立,应用由管理员(Admin)个人身份识别码(Personal Identification Number,PIN)、用户PIN、文件和容器组成]。其中,容器(参见GB/T 35291,容器是密码设备中用于保存密钥所划分的唯一性存储空间)用于存放密钥数据和数字证书。用户PIN用于验证使用者身份以打开容器,调用相关接口使用容器内密钥进行密码运算。在实际的应用中,如果用户PIN和管理员PIN多次重复输入错误会锁死,虽然用户PIN锁死后可以使用管理员PIN进行解锁并设置新的用户PIN,但若管理员PIN被锁死,则该应用就无法再使用。据此,考虑到管理员PIN的重要性,需要严格对其进行保护和管理。

[0005] 在现有信息系统中,设备认证密钥一般由智能密码钥匙的厂商设置为固定值,用户PIN理应由使用者进行管理,对于管理员PIN,现有的信息系统一般同时也交由使用者管理,或有的信息系统将其统一设置为固定值,然后由信息系统的系统管理员管理。

[0006] 以上对设备认证密钥和管理员PIN的管理方式的不足之处在于:1、设备认证密钥为固定值会导致智能密码钥匙内的应用可被恶意删除。2、管理管理员PIN不常使用,若交由使用者管理会容易被遗忘,造成智能密码钥匙一旦被锁死后不再可用;3、若管理管理员PIN使用固定值,则不易定期更换,并且一旦泄露会造成所有智能密码钥匙的管理员PIN泄露。因此,如何提供一个高效安全的机制来管理所述设备认证密钥和管理员PIN,是一个亟待解决的问题。

发明内容

[0007] 针对上述问题,本发明提供一种用于管理设备认证密钥和管理员PIN的管理方法。

[0008] 本发明提供的管理方法,包括下列方法中的一种或几种:

[0009] 方法A、对智能密码钥匙进行初始化的方法,包括设置设备认证密钥和设置管理员个人身份识别码;

[0010] 方法B、所述设备认证密钥和管理员个人身份识别码的使用方法；

[0011] 方法C、所述设备认证密钥和管理员个人身份识别码的修改方法，

[0012] 其中，

[0013] 所述方法A包括步骤：

[0014] AB、客户端获取所述智能密码钥匙中的设备信息，取出所述设备信息中的序列号SN；

[0015] AC、服务端随机生成设备标签，并依据所述序列号SN、应用名AppName计算所述设备认证密钥和管理员个人身份识别码，然后发送给所述客户端；

[0016] AD、所述客户端修改所述智能密码钥匙中的设备标签和设备认证密钥，建立新的应用，

[0017] 所述方法B包括步骤：

[0018] BB、所述客户端获取所述智能密码钥匙中的设备信息中的序列号SN和设备标签，将所述序列号SN、设备标签和应用名AppName发送给所述服务端；

[0019] BC、所述服务端计算所述设备认证密钥和管理员个人身份识别码并发送给所述客户端，

[0020] 所述方法C包括步骤：

[0021] CB、所述客户端获取到当前的设备认证密钥和管理员个人身份识别码；

[0022] CC、所述客户端向服务端申请计算得到新的设备标签NewLabel、新的设备认证密钥NewDevAuthKey和新的管理员个人身份识别码NewAdminPIN；

[0023] CD、所述客户端更新所述设备标签、设备认证密钥和管理员个人身份识别码。

[0024] 进一步，

[0025] 在所述步骤AB之前，执行如下步骤：

[0026] 所述客户端使用出厂设备认证密钥进行设备认证，连接所述智能密钥钥匙。

[0027] 进一步，

[0028] 所述步骤AB包括：

[0029] 所述客户端调用获取设备信息接口获取所述智能密钥钥匙的设备信息，取出所述设备信息中的序列号SN。

[0030] 进一步，

[0031] 所述步骤AC中，若所述客户端和服务端之间的连接为可信信道，则执行下列步骤：

[0032] 所述客户端将所述序列号SN、应用名AppName发送给所述服务端；

[0033] 所述服务端生成32字节随机数作为第一设备标签Label1，再将所述第一设备标签Label1和序列号SN进行字节拼接，得到第一数据data1：data1＝Label1||SN，其中，||表示字节的拼接；

[0034] 所述服务端调用服务器密码机，使用所述服务器密码机内的密钥索引为index的SM2密钥，并通过使用导入会话密钥并用内部椭圆曲线加密算法私钥解密接口导入会话密钥，并得到会话密钥句柄；

[0035] 所述服务端调用所述服务器密码机，使用所述会话密钥句柄，并通过使用SM4加密算法加密所述第一数据data1，得到第一密文C1；

[0036] 所述服务端计算C1||ID的第一SM3杂凑值SO1＝SM3(C1||ID)，得到32字节SM3杂凑

值S01,其中,ID为信息系统的固定标识字符串或空,所述服务端为所述信息系统的服务器;

[0037] 所述服务端取所述SM3杂凑值S01的前16字节为第一设备认证密钥DevAuthKey1:DevAuthKey1＝S01[0:16],设构成字符串D的各字节均具有下标(为整数),且以各字节的下标由小至大依次标识对应的各字节在字符串D中由前至后的顺序,D[m:n]表示对字符串D取从下标m(初始下标)至下标n-1的字节,m和n均为整数,且m<n,S01中初始下标m为0;

[0038] 所述服务端计算S1＝SM3(S01||AppName),以及S2＝Base64(S1),得到44字节可打印字符串S2,Base64(E)表示把二进制数据E使用Base64编码转为44个可打印字符;

[0039] 所述服务端取所述可打印字符串S2的前16字节为第一管理员个人身份识别码AdminPIN1:AdminPIN1＝S2[0:16];

[0040] 所述服务端将所述第一设备标签Label1、第一设备认证密钥DevAuthKey1、第一管理员个人身份识别码AdminPIN1发送给所述客户端;

[0041] 所述客户端修改第一设备标签Label1和第一设备认证密钥DevAuthKey1,并使用第一管理员PIN AdminPIN1和用户输入的用户个人身份识别码建立新的应用。

[0042] 进一步,

[0043] 所述步骤AC中,若所述客户端和服务端的连接为非可信信道,则执行下列步骤:

[0044] 所述客户端建立一个新的临时应用,所述临时应用的临时用户个人身份识别码和临时管理员个人身份识别码由所述客户端随机生成;

[0045] 所述客户端使用所述临时应用建立临时容器;

[0046] 所述客户端在所述临时容器内生成椭圆曲线加密算法签名密钥对,并输出椭圆曲线加密算法签名密钥对中的临时签名公钥TempSignPubKey;

[0047] 所述客户端将所述序列号SN、应用名AppName、临时签名公钥TempSignPubKey发送给所述服务端;

[0048] 所述服务端生成32字节随机数作为第二设备标签Label2,将所述第二设备标签Label2和序列号SN进行字节拼接,得到第二数据data2:data2＝Label2||SN;

[0049] 所述服务端调用服务器密码机,使用所述服务器密码机内的密钥索引为index的SM2密钥,并通过使用导入会话密钥并用内部椭圆曲线加密算法私钥解密接口导入会话密钥,并得到会话密钥句柄;

[0050] 所述服务端调用所述服务器密码机,使用所述会话密钥句柄,并通过使用SM4加密算法加密所述第二数据data2,得到第二密文C2;

[0051] 所述服务端计算C2||ID的第二SM3杂凑值S02＝SM3(C2||ID),得到32字节的所述第二SM3杂凑值S02,其中,ID为信息系统的固定标识字符串或空;

[0052] 所述服务端取所述第二SM3杂凑值S02的前16字节为第二设备认证密钥DevAuthKey2:DevAuthKey2＝S02[0:16];

[0053] 所述服务端计算S11＝SM3(S02||AppName),以及S21＝Base64(S11),得到44字节可打印字符串S21;

[0054] 所述服务端取所述可打印字符串S21的前16字节为第二管理员个人身份识别码:AdminPIN2＝S21[0:16];

[0055] 所述服务端生成临时会话密钥TempSessionKey,并使用所述临时会话密钥TempSessionKey和SM4算法加密组合数据

[0056] Label2||DevAuthKey2||AdminPIN2得到加密数据EncryptedData:

[0057] EncryptedData＝SM4(TempSessionKey,Label2||DevAuthKey2||AdminPIN2),其中,SM4(K,D1)表示使用密钥K,对数据D1使用SM4加密算法加密得到的密文;

[0058] 所述服务端生成SM2加密密钥对(TempEncPrivateKey,TempEncPubKey),使用其中的加密密钥TempEncPubKey加密所述临时会话密钥TempSessionKey得到数字信封EnvelopedSessionKey:

[0059] EnvelopedSessionKey＝SM2(TempEncPubKey,TempSessionKey),其中,SM2(PubKey,D2)表示使用SM2公钥PubKey,对数据D2使用SM2加密算法加密得到的密文;

[0060] 所述服务端使用所述客户端的临时签名公钥TempSignPubKey对所述加密密钥TempEncPrivateKey加密并组成椭圆曲线加密密钥对保护结构EnvelopedKeyBlob;

[0061] 所述服务端将所述椭圆曲线加密密钥对保护结构EnvelopedKeyBlob、数字信封EnvelopedSessionKey、加密数据EncryptedData发送给所述客户端;

[0062] 所述客户端使用导入椭圆曲线加密密钥对接口将所述椭圆曲线加密密钥对保护结构EnvelopedKeyBlob导入所述临时容器中;

[0063] 所述客户端使用导入会话密钥接口将所述数字信封EnvelopedSessionKey导入到所述临时容器中,并得到会话密钥句柄;

[0064] 所述客户端使用所述会话密钥句柄和单组数据解密接口解密所述加密数据EncryptedData得到组合数据Label2||DevAuthKey2||AdminPIN2,并根据数据长度分别截取得到所述第二设备标签Label2、第二设备认证密钥DevAuthKey2和第二管理员个人身份识别码AdminPIN2。

[0065] 进一步,

[0066] 所述步骤AD包括:

[0067] 所述客户端得到所述第一设备标签Label1、第一设备认证密钥DevAuthKey1、第一管理员个人身份识别码AdminPIN1或所述第二设备标签Label2、第二设备认证密钥DevAuthKey2、第二管理员个人身份识别码AdminPIN2后,修改所述设备标签和设备认证密钥,建立新的应用,包括如下步骤:

[0068] 将所述第一设备标签Label1或第二设备标签Label2写入所述智能密钥钥匙的设备标签的字符串中;

[0069] 使用修改设备认证密钥接口修改所述设备认证密钥为所述第一设备认证密钥DevAuthKey1或第二设备认证密钥DevAuthKey2;

[0070] 建立新的应用,并设置所述管理员个人身份识别码为第一管理员个人身份识别码AdminPIN1或第二管理员个人身份识别码AdminPIN2,用户个人身份识别码由用户输入;

[0071] 建立所述新的应用后,删除所述临时应用。

[0072] 进一步,

[0073] 所述步骤BB包括:

[0074] 所述客户端调用获取设备信息接口来获取所述智能密钥钥匙的设备信息,取出所述设备信息中的序列号SN和设备标签Label;

[0075] 所述客户端将所述序列号SN、设备标签Label和应用名AppName发送给所述服务端。

[0076] 进一步,

[0077] 所述步骤BC包括:

[0078] 所述服务端调用服务器密码机,使用密钥索引为index的SM2密钥,导入会话密钥,并用内部椭圆曲线加密私钥解密接口导入所述会话密钥中的SM2加密密文KeyCipher并得到会话密钥句柄;

[0079] 所述服务端调用所述服务器密码机,使用所述会话密钥句柄和SM4加密算法,加密Label||SN,得到密文C;

[0080] 所述服务端计算C||ID的第三SM3杂凑值S03=SM3(C||ID),得到32字节第三SM3杂凑值S03;

[0081] 所述服务端取所述第三SM3杂凑值S03的前16字节为第三设备认证密钥DevAuthKey3:DevAuthKey3=S03[0:16];

[0082] 所述服务端计算SS1=SM3(S03||AppName),以及SS2=Base64(SS1),得到44字节可打印字符串SS2;

[0083] 所述服务端取所述可打印字符串SS2的前16字节为第三管理员个人身份识别码AdminPIN3:AdminPIN3=SS2[0:16];

[0084] 所述服务端将第三设备认证密钥DevAuthKey3和第三管理员个人身份识别码AdminPIN3发送给客户端。

[0085] 进一步,

[0086] 所述步骤CB同所述步骤BB至步骤BC,所述客户端获取到当前的设备认证密钥:第四设备认证密钥DevAuthKey4和当前的第四管理员个人身份识别码:第四管理员PIN AdminPIN4。

[0087] 进一步,

[0088] 所述步骤CC同所述步骤AC,由所述客户端向服务端申请计算得到新的设备标签NewLabel、新的设备认证密钥NewDevAuthKey和新的管理员个人身份识别码NewAdminPIN。

[0089] 进一步,

[0090] 所述步骤CD包括:

[0091] 所述客户端使用所述第四设备认证密钥DevAuthKey4进行设备认证,认证成功后,客户端使用修改设备认证密钥接口将所述第四设备认证密钥DevAuthKey4修改为所述新的设备认证密钥NewDevAuthKey;

[0092] 所述客户端使用修改个人身份识别码接口将所述第四管理员个人身份识别码AdminPIN4修改为新的管理员个人身份识别码NewAdminPIN;

[0093] 所述客户端使用设置设备标签接口将所述新的设备标签NewLabel写入所述智能密钥钥匙的设备标签字符串中。

[0094] 本发明还提供一种管理系统,所述管理系统用于实现上述的管理方法,所述管理系统包括客户端、智能密码钥匙和服务端。

[0095] 本发明还提供一种计算机设备,所述计算机设备包括存储器、第一处理器及储存在所述存储器上并可在所述第一处理器上运行的第一计算机程序,所述第一计算机程序被第一处理器执行时实现上述的管理方法的步骤。

[0096] 本发明还提供一种计算机可读存储介质,所述计算机可读存储介质储存有第二计

算机程序,所述第二计算机程序可被至少一个第二处理器所执行,以使所述至少一个第二处理器执行上述的管理方法的步骤。

[0097] 本发明的管理方法中,设备认证密钥和管理员PIN由服务端生成,且可以更改,有效的避免了设备认证密钥和管理员PIN不安全、易泄露等问题,使得智能密码钥匙的使用安全性大大增加。设备认证密钥和管理员PIN的生成要素由客户端、智能密码钥匙和服务端等多方面组成,更进一步提高了安全性。使用设备认证密钥和管理员PIN时,需要在信息系统上进行身份认证后,由信息系统的客户端进行操作,使得本发明能有效安全的对信息系统中所使用的智能密码钥匙的设备认证密钥和管理员PIN进行集中的管控。

[0098] 本发明的其它特征和优点将在随后的说明书中阐述,并且,部分地从说明书中变得显而易见,或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所指出的结构来实现和获得。

附图说明

[0099] 为了更清楚地说明本发明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,下面描述中的附图是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0100] 图1示出了根据本发明实施例的对智能密码钥匙进行初始化的方法流程图;

[0101] 图2示出了根据本发明实施例的设备认证密钥和管理员PIN的使用方法流程图;

[0102] 图3示出了根据本发明实施例的设备认证密钥和管理员PIN的修改方法流程图。

具体实施方式

[0103] 为使本发明实施例的目的、技术方案和优点更加清楚,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、完整地说明,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,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。

[0104] 除非另有定义,本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同;本文中在申请的说明书中所使用的术语只是为了描述具体的实施例的目的,不是旨在于限制本申请;本申请的说明书和权利要求书及上述附图说明中的术语“包括”和“具有”以及它们的任何变形,意图在于覆盖不排他的包含。本申请的说明书和权利要求书或上述附图中的术语“第一”、“第二”、“第三”等是用于区别不同对象,而不是用于描述特定顺序或主次关系。本申请中出现的“多个”指的是两个以上(包括两个)。

[0105] 在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0106] 采用智能密钥钥匙的信息系统包括客户端和服务端。客户端可以为可执行程序,浏览器插件等,使用GB/T 35291-2017《信息安全技术智能密码钥匙应用接口规范》中的接口调用智能密钥钥匙。服务端为信息系统服务器,并通过调用服务器密码机执行加解密等

密码服务,调用服务器密码机遵循GB/T 36322-2018《信息安全技术密码设备应用接口规范》。

[0107] 服务端在信息系统运行前,在服务器密码机上为信息系统分配密钥索引为index的SM2密钥,再调用生成会话密钥并用内部椭圆曲线加密算法(ECC)公钥加密输出接口(SDF_GenerateKeyWithIPK_ECC接口),生成会话密钥并输出会话密钥的SM2加密密文KeyCipher(KeyCipher是通过使用SM2公钥加密会话密钥所得到的SM2加密密文),将SM2加密密文KeyCipher保存至数据库或磁盘,即会话密钥在使用SM2公钥进行加密后以密文形式导出存储于数据库或磁盘,在需要使用会话密钥的时候,将会话密钥的SM2加密密文KeyCipher导入密码机解密后再使用。其中,会话密钥用于数据加解密和消息认证码(Message Authentication Codes,MAC)运算,会话密钥一般是16字节的对称密钥,比如SM4密钥。

[0108] 智能密钥钥匙中可以存在多个应用,但一般在实际使用中,一个智能密码钥匙只建立一个应用,因此本发明针对一个智能密码钥匙只建立一个应用的情况。

[0109] 本发明实施例提供一种用于管理智能密码钥匙设备认证密钥和管理员PIN的管理方法。所述管理方法包括:

[0110] 方法A、对智能密码钥匙进行初始化的方法,包括设置设备认证密钥和建立应用设置管理员PIN;

[0111] 方法B、设备认证密钥和管理员PIN的使用方法;

[0112] 方法C、设备认证密钥和管理员PIN的修改方法。

[0113] 下面将结合附图,对本发明的实施例进行详细说明。

[0114] 信息系统的用户使用出厂设置的智能密码钥匙在客户端进行智能密钥钥匙的初始化操作,该操作为智能密码钥匙设置设备认证密钥,建立应用名为AppName的应用并设置该应用的管理员PIN和用户PIN。其中,设备认证密钥和管理员PIN由信息系统生成,用户PIN由用户输入。

[0115] 图1示出了本发明的对智能密码钥匙进行初始化的方法流程图。参见图1,所述方法A涉及智能密钥钥匙的设备信息中的序列号(SerialNumber,SN)、设备标签(Label)以及服务器密码机的密钥,具体而言,对智能密码钥匙进行初始化的方法包括:

[0116] AA、客户端使用出厂设备认证密钥进行设备认证(即智能密码钥匙对应用程序的认证),连接智能密钥钥匙;

[0117] AB、客户端获取所述智能密码钥匙中的设备信息,取出所述设备信息中的序列号SN,包括:

[0118] 客户端调用获取设备信息接口(SKF_GetDevInfo接口)获取智能密钥钥匙的设备信息,取出设备信息中的序列号SN,该序列号由厂商写入,一般各智能密码钥匙的序列号均不相同,其中,设备信息包括版本号、设备厂商信息、设备发行信息、设备标签、序列号等;

[0119] AC、服务端随机生成设备标签,调用服务器密码机并依据序列号SN、应用名AppName为客户端计算设备认证密钥和管理员PIN,然后发送给客户端,包括:

[0120] ACa、若客户端和服务端之间的连接为可信信道,则执行下列步骤:

[0121] ACa1、客户端将序列号SN、应用名AppName发送给服务端;

[0122] ACa2、服务端生成32字节随机数作为第一设备标签Label1,再将第一设备标签

Label1和序列号SN进行字节拼接,得到第一数据data1:

[0123] data1=Label1||SN,

[0124] 其中,||表示字节的拼接,本发明中,服务端生成的32字节随机数是由服务端调用服务器密码机生成,并保存在智能密钥钥匙的设备信息的Label字段中,服务端不保存该随机数;

[0125] ACa3、服务端调用服务器密码机,使用服务器密码机内的密钥索引为index的SM2密钥,并通过使用导入会话密钥并用内部ECC私钥解密接口(SDF_ImportKeyWithISK_ECC接口)导入会话密钥,并得到会话密钥句柄,具体过程为:在SDF_ImportKeyWithISK_ECC接口输入index和SM2加密密文keyCipher后,服务器密码机先用密码机index索引位的SM2私钥解密SM2加密密文keyCipher得到会话密钥,把会话密钥存放在服务器密码机内,并生成一个会话密钥句柄返回给调用者。调用者不会直接得到会话密钥,要加密的时候,调用者把加密数据和会话密钥句柄发送至服务器密码机,服务器密码机对加密数据加密后得到密文,再把密文发回调用者;

[0126] ACa4、服务端调用服务器密码机,使用会话密钥句柄,并通过使用SM4加密算法加密第一数据data1,得到第一密文C1;

[0127] ACa5、服务端计算C1||ID的第一SM3杂凑值S01=SM3(C1||ID),得到32字节SM3杂凑值S01,其中ID为信息系统的固定标识字符串,也可以为空,杂凑值的计算参照GB/T 35291-2017的7.6.40-7.6.43;

[0128] ACa6、服务端取SM3杂凑值S01的前16字节为第一设备认证密钥DevAuthKey1:DevAuthKey1=S01[0:16],设构成字符串D的各字节均具有下标(为整数),且以各字节的下标由小至大依次标识对应的各字节在字符串D中由前至后的顺序,D[m:n]表示对字符串D取从下标m(初始下标)至下标n-1的字节,m和n均为整数,且m<n,S01中初始下标m为0;

[0129] 例如,若32字节的SM3杂凑值S01为{0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x0e,0x0f,0x10,0x11,0x12,0x13,0x14,0x15,0x16,0x17,0x18,0x19,0x1a,0x1b,0x1c,0x1d,0x1e,0x1f},则DevAuthKey1={0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x0e,0x0f}。

[0130] ACa7、服务端计算S1=SM3(S01||AppName),以及S2=Base64(S1),得到44字节可打印字符串S2,Base64(E)表示把二进制数据E使用Base64编码转为可打印字符即字节。

[0131] 例如若S1为{0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x0e,0x0f,0x10,0x11,0x12,0x13,0x14,0x15,0x16,0x17,0x18,0x19,0x1a,0x1b,0x1c,0x1d,0x1e,0x1f},则

[0132] S2=AAECAwQFBgcICQoLDA0ODxAREhMUFRYXGBkaGxwdHh8=;

[0133] ACa8、服务端取S2的前16字节为第一管理员PIN AdminPIN1:AdminPIN1=S2[0:16];

[0134] ACa9、服务端将第一设备标签Label1、第一设备认证密钥DevAuthKey1、第一管理员PIN AdminPIN1发送给客户端;

[0135] ACa10、客户端修改第一设备标签Label1和第一设备认证密钥DevAuthKey1,并使用第一管理员PIN AdminPIN1和用户输入的用户PIN建立新的应用,所述修改的目的在于把智能密码钥匙中原来的设备标签改为第一设备标签Label1,及把智能密码钥匙中原来的设

备认证密钥改为第一设备认证密钥DevAuthKey1。本发明思想在于,第一设备认证密钥DevAuthKey1和第一管理员PIN AdminPIN1是通过第一设备标签Label1,序列号SN和会话密钥计算得到的。其中,第一设备标签Label1,序列号SN放ukey上保存,会话密钥放服务端(加密)保存。因而在要使用到第一设备认证密钥DevAuthKey1和第一管理员PIN AdminPIN1的时候必须由客户端通过服务端将二者临时计算出来。

[0136] 需注意,若客户端和服务端之间为可信信道,所述服务器密码机的SM4密钥,是由服务端调用密码机生成会话密钥后,利用内部ECC公钥加密输出接口(SDF_GenerateKeyWithIPK_ECC接口)输出的会话密钥的SM2加密密文。SM4密钥,即会话密钥的SM2加密密文保存于数据库或磁盘中,需要使用时,将SM4密钥的SM2加密密文导入到密码机中使用,即由服务器密码机导入会话密钥,并用内部ECC私钥解密接口(SDF_ImportKeyWithISK_ECC接口),导入会话密钥的SM2加密密文并得到会话密钥句柄,SM4加解密通过会话密钥句柄进行调用。

[0137] ACb、若客户端和服务端的连接为非可信信道,则执行下列步骤:

[0138] ACb1、客户端建立一个新的临时应用,该临时应用的临时用户PIN和临时管理员PIN为客户端随机生成;

[0139] ACb2、客户端使用临时应用建立临时容器;

[0140] ACb3、客户端在临时容器内生成ECC签名密钥对,并输出ECC签名密钥对中的临时签名公钥TempSignPubKey;

[0141] ACb4、客户端将序列号SN、应用名AppName、临时签名公钥TempSignPubKey发送给服务端;

[0142] ACb5、服务端生成32字节随机数作为第二设备标签Label2。将Label2和序列号SN进行字节拼接,得到第二数据data2:data2=Label2||SN;

[0143] ACb6、同上述步骤ACa3,即服务端调用服务器密码机,使用服务器密码机内的密钥索引为index的SM2密钥,并通过使用导入会话密钥并用内部ECC私钥解密接口(SDF_ImportKeyWithISK_ECC接口)导入会话密钥,并得到会话密钥句柄;

[0144] ACb7、服务端调用服务器密码机,使用会话密钥句柄,并通过使用SM4加密算法加密第二数据data2,得到第二密文C2;

[0145] ACb8、服务端计算C2||ID的第二SM3杂凑值S02=SM3(C2||ID),得到32字节的第二SM3杂凑值S02,其中ID为信息系统的固定标识字符串,也可以为空;

[0146] ACb9、服务端取第二SM3杂凑值S02的前16字节为第二设备认证密钥DevAuthKey2:DevAuthKey2=S02[0:16];

[0147] A3b10、服务端计算S11=SM3(S02||AppName),以及S21=Base64(S11),得到44字节可打印字符串S21;

[0148] ACb11、服务端取S21的前16字节为第二管理员PIN:AdminPIN2=S21[0:16];

[0149] ACb12、服务端生成临时会话密钥TempSessionKey,并使用临时会话密钥TempSessionKey和SM4算法加密组合数据

[0150] Label2||DevAuthKey2||AdminPIN2得到加密数据EncryptedData:

[0151] EncryptedData=SM4(TempSessionKey,Label2||DevAuthKey2||AdminPIN2);

[0152] 其中,SM4(K,D1)表示使用密钥K,对数据D1使用SM4加密算法加密得到的密文,SM4

算法参见GB/T 32907-2016《信息安全技术SM4分组密码算法》。密文EncryptedData为二进制的字符串。

[0153] ACb13、服务端生成SM2加密密钥对(TempEncPrivateKey,TempEncPubKey),使用其中的加密密钥TempEncPubKey加密临时会话密钥TempSessionKey得到数字信封EnvelopedSessionKey:

[0154] EnvelopedSessionKey＝SM2(TempEncPubKey,TempSessionKey);

[0155] 其中,SM2(PubKey,D2)表示使用SM2公钥PubKey,对数据D2使用SM2加密算法加密得到的密文,SM2加密算法参见GB/T 32918.4-2016《信息安全技术SM2椭圆曲线公钥密码算法第4部分:公钥加密算法》。密文EnvelopedSessionKey为二进制的字符串。

[0156] ACb14、服务端使用客户端的临时签名公钥TempSignPubKey对加密密钥TempEncPrivateKey加密并组成ECC加密密钥(椭圆曲线加密密钥)对保护结构EnvelopedKeyBlob。

[0157] 其中,ECC加密密钥对保护结构及加密过程参见GB/T35291-2017《信息安全技术智能密码钥匙应用接口规范》的第6.4.10节。

[0158] ACb15、服务端将ECC加密密钥对保护结构

[0159] EnvelopedKeyBlob、数字信封EnvelopedSessionKey、加密数据EncryptedData发送给客户端;

[0160] ACb16、客户端使用导入ECC密钥对接口(SKF_ImportECCKeyPair接口)将ECC密钥对保护结构EnvelopedKeyBlob导入临时容器中;

[0161] ACb17、客户端使用导入会话密钥接口(SKF_ImportSessionKey接口)将数字信封EnvelopedSessionKey导入到临时容器中,并得到会话密钥句柄;

[0162] ACb18、客户端使用会话密钥句柄和单组数据解密接口解密加密数据EncryptedData得到组合数据Label2||DevAuthKey2||AdminPIN2,并根据数据长度分别截取得到Label2、DevAuthKey2和AdminPIN2。

[0163] 综上,若所述服务端和客户端之间为非安全信道,需客户端在智能密码钥匙中建立临时应用和临时容器,并生成SM2临时签名密钥,将SM2临时签名密钥和SN、AppName发送给服务端。服务端使用SM2临时签名密钥加密服务端生成的SM2临时加密密钥,使用SM2临时加密密钥加密临时会话密钥,使用临时会话密钥加密服务端生成的Label2、DevAuthKey2、AdminPIN2数据,从而可以防止信道上的窃听。

[0164] AD、客户端得到第一设备标签Label1、第一设备认证密钥DevAuthKey1、第一管理员PINAdminPIN1或第二设备标签Label2、第二设备认证密钥DevAuthKey2、第二管理员PIN AdminPIN2后,修改智能密钥钥匙中的设备标签和设备认证密钥,建立新的应用,包括如下步骤:

[0165] AD1、通过设置设备标签(SKF_SetLabel)将第一设备标签Label1或第二设备标签Label2写入智能密钥钥匙的设备标签的字符串中;

[0166] AD2、使用修改设备认证密钥接口(SKF_ChangeDevAuthKey接口)修改设备认证密钥为第一设备认证密钥DevAuthKey1或第二设备认证密钥DevAuthKey2;

[0167] AD3、建立新的应用,并设置管理员PIN为第一管理员PIN AdminPIN1或第二管理员PIN AdminPIN2,用户PIN由用户输入;

[0168] AD4、若客户端和服务端的连接为非可信信道,则删除临时应用。

[0169] AE、智能密钥钥匙的初始化设置完成。

[0170] 图2是本发明的设备认证密钥和管理员PIN的使用方法流程图。参见图2,所述方法B,即设备认证密钥和管理员PIN的使用方法包括如下步骤:

[0171] BA、使用者在客户端提交申请并经信息系统管理员审批;

[0172] BB、客户端获取设备信息中的序列号SN和设备标签Label,将序列号SN、设备标签Label和应用名AppName发送给服务端,包括:

[0173] BB1、客户端调用获取设备信息接口(SKF_GetDevInfo接口)来获取智能密钥钥匙的设备信息,取出设备信息中的序列号SN和设备标签Label;

[0174] BB2、客户端将序列号SN、设备标签Label和应用名AppName发送给服务端;

[0175] BC、服务端计算设备认证密钥和管理员个人身份识别码并发送给客户端,包括:

[0176] BC1、服务端调用服务器密码机,使用密钥索引为index的SM2密钥,导入会话密钥,并用内部ECC私钥解密接口(SDF_ImportKeyWithISK_ECC接口)导入会话密钥中的SM2加密密文KeyCipher并得到会话密钥句柄;

[0177] BC2、服务端调用服务器密码机,使用会话密钥句柄和SM4加密算法加密Label||SN,得到密文C;

[0178] BC3、服务端计算C||ID的第三SM3杂凑值S03=SM3(C||ID),得到32字节第三SM3杂凑值S03;

[0179] BC4、服务端取第三SM3杂凑值S03的前16字节为第三设备认证密钥DevAuthKey3:DevAuthKey3=S03[0:16]。

[0180] BC5、服务端计算SS1=SM3(S03||AppName),以及SS2=Base64(SS1),得到44字节可打印字符串SS2;

[0181] BC6、服务端取SS2的前16字节为第三管理员PIN AdminPIN3:AdminPIN3=SS2[0:16];

[0182] BC7、服务端将第三设备认证密钥DevAuthKey3和第三管理员PIN AdminPIN3发送给客户端。

[0183] 图3是本发明的设备认证密钥和管理员PIN的修改方法流程图。参见图3,所述方法C,即设备认证密钥和管理员PIN的修改方法包括如下步骤:

[0184] CA、使用者在客户端提交申请并经信息系统管理员审批;

[0185] CB、同上述步骤BB-BC,客户端获取到当前的DevAuthKey(称为第四设备认证密钥DevAuthKey4)和管理员PIN(称为第四管理员PIN AdminPIN4)。

[0186] CC、同上述步骤AC,客户端向服务端申请计算得到新的设备标签NewLabel、新的设备认证密钥NewDevAuthKey和新的管理员PIN NewAdminPIN;

[0187] CD、客户端更新设备标签、设备认证密钥和管理员个人身份识别码,包括:

[0188] CD1、客户端使用第四设备认证密钥DevAuthKey4进行设备认证,认证成功后,客户端使用修改设备认证密钥接口(SKF_ChangeDevAuthKey接口)将所述第四设备认证密钥DevAuthKey4修改为新的设备认证密钥NewDevAuthKey;

[0189] CD2、客户端使用修改PIN接口(SKF_ChangePIN接口)将智能密钥钥匙中的第四管理员PIN AdminPIN4修改为新的管理员PIN NewAdminPIN;

[0190] CD3、客户端使用设置设备标签接口(SKF_SetLabel接口)将新的设备标签NewLabel写入智能密钥钥匙的设备标签字符串中。

[0191] 本发明还提供一种用于管理智能密码钥匙设备认证密钥和管理员PIN的管理系统,所述管理系统用于实现上述管理方法,且包括客户端、智能密码钥匙和服务端。

[0192] 本发明还提供一种计算机设备,包括储存器、第一处理器及储存在所述存储器上并可在所述第一处理器上运行的第一计算机程序,第一计算机程序被第一处理器执行时实现上述管理方法。

[0193] 本发明还提供一种计算机可读存储介质,用于储存第二计算机程序,第二计算机程序可被至少一个第二处理器所执行,以使至少一个第二处理器执行上述管理方法。

[0194] 本发明的管理方法中,设备认证密钥和管理员PIN由服务端生成,且可以更改,有效的避免了设备认证密钥和管理员PIN不安全、易泄露等问题,使得智能密码钥匙的使用安全性大大增加。设备认证密钥和管理员PIN的生成要素由客户端、智能密码钥匙和服务端等多方面组成,更进一步提高了安全性。使用设备认证密钥和管理员PIN时,需要在信息系统上进行身份认证后,由信息系统的客户端进行操作,使得本发明能有效安全的对信息系统中所使用的智能密码钥匙的设备认证密钥和管理员PIN进行集中的管控。

[0195] 尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

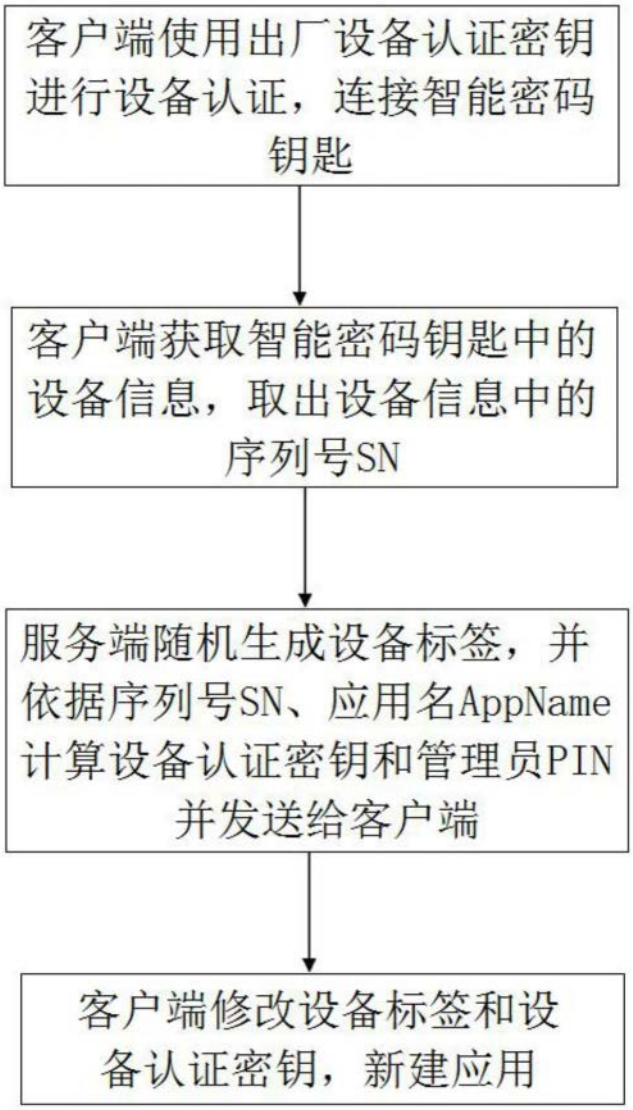

客户端使用出厂设备认证密钥进行设备认证，连接智能密码钥匙
客户端获取智能密码钥匙中的设备信息，取出设备信息中的序列号SN
服务端随机生成设备标签，并依据序列号SN、应用名AppName计算设备认证密钥和管理员PIN并发送给客户端
客户端修改设备标签和设备认证密钥，新建应用

图1

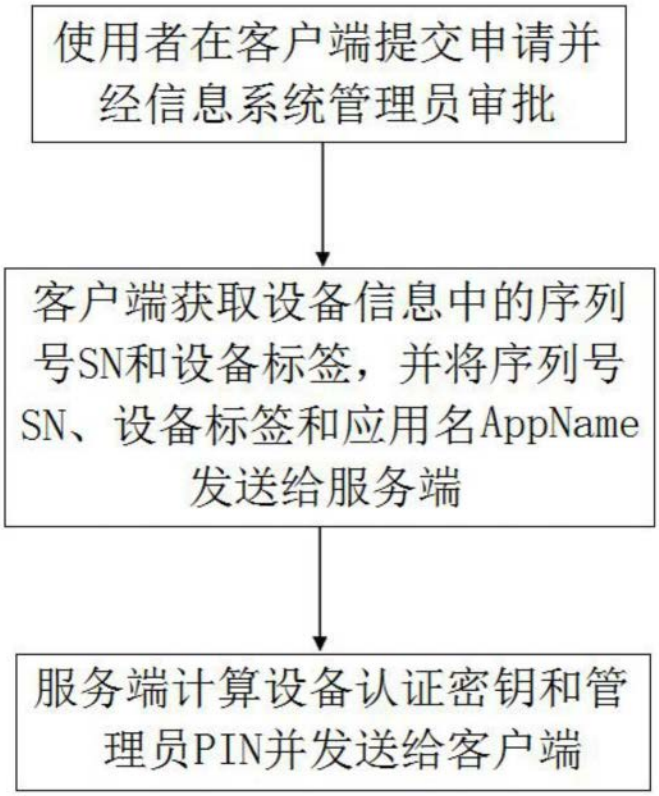

使用者在客户端提交申请并经信息系统管理员审批
客户端获取设备信息中的序列号SN和设备标签，并将序列号SN、设备标签和应用名AppName发送给服务端
服务端计算设备认证密钥和管理员PIN并发送给客户端

图2

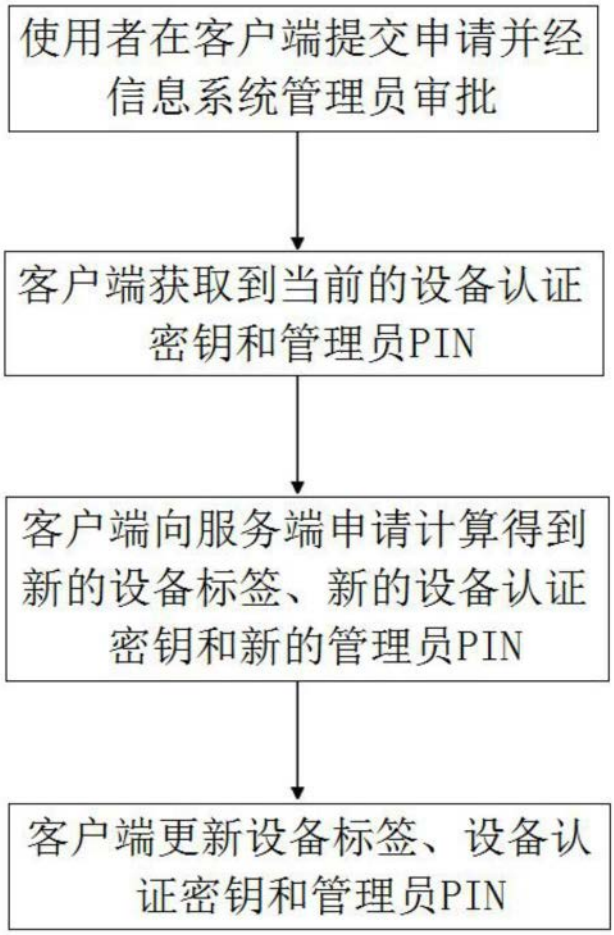

使用者在客户端提交申请并经信息系统管理员审批
客户端获取到当前的设备认证密钥和管理员PIN
客户端向服务端申请计算得到新的设备标签、新的设备认证密钥和新的管理员PIN
客户端更新设备标签、设备认证密钥和管理员PIN

图3