**一种新型移动支付安全保护系统及其实现方法**

**技术领域**

本发明涉及移动支付的安全流程设计和安全加密技术领域，具体涉及一种基于移动端的安全保护系统和方法，尤其是对客户支付过程中签名私钥的保护。

**背景技术**

随着智能手机和移动互联网技术的飞速发展，人们越来越多地使用各种移动终端从事电子商务活动，而作为移动电子商务主要支付手段的移动支付，也得到了迅猛发展。移动支付也称为手机支付，就是允许用户使用其移动终端对所消费的商品或服务进行账务支付的一种服务方式。移动支付主要分为近场支付和远程支付两种，所谓近场支付，就是用手机刷卡的方式坐车、买东西等，很便利。远程支付是指：通过发送支付指令进行的支付方式，待验证用户身份后对用户的银行账户扣款以完成支付。如支付宝、易付宝、微信支付等都是属于远程支付。

尽管移动支付方式给我们的日常消费带来了极大的便利，但同时也存在着安全隐患。一旦设备丢失，不法分子可以通过反编译等先进的破解技术窃取用户的密码信息，尤其是没有较好防护措施的支付签名私钥，这将可能给用户带来大量且广泛的财产损失。

当前移动端远程支付的私钥存储通常的方案是其依赖于本地用户口令存储在移动端，但这样需要单独设置一条口令来保护私钥，用户体验很差；另外一类方案是将用户的私钥一部分存储在本地，另一部分存储在服务端，这种方式在理论是上增加了秘钥的安全性，但在支付环节涉及到本地和服务端两个解密验证操作，不仅增加了移动端的资源消耗，而且需要联网才能支付；还有一类解决方案是将用户私钥存储在服务端，这种方式是依赖于服务端的安全，虽然避免了本地存储的不安全性，但同样造成了用户支付必须联网，无法进行离线支付的弊端，且签名私钥独立放在服务端，用户一旦有支付误操作或者口令被不法分子冒用，造成服务端有不法的嫌疑，背离采用私钥的初衷。本发明试图充分利用常规支付系统的支付用户已有密码，在保护好用户本地私钥，同时支持支付用户已有密码变更时仍旧能良好运行。

**发明内容**

**1、解决的技术问题**

针对目前对移动便捷性和安全性的新要求，本发明提出一种新型的移动端支付安全加密流程和私钥存储的安全方法。通过设计一个毋须存储在系统上的工作密码来保护签名用的私钥，当工作密码变化时又能通过备用密码找回私钥进行重新初始化，从而一举解决工作密码变更的问题和杜绝服务端存储用户私钥的争议。

**2、本发明的完整的技术方案**

本发明的技术方案如下：

将用户工作密码和备用密码首先通过密码导出函数得到两个加密密钥，同时用一个随机密码对工作密码进行散列等变化，得到工作密码的校验码，再将两个加密密钥对待保护的私钥分别进行加密，并把两个加密后的私钥存储在用户本地，把备用密码，随机密码和校验码存储在服务系统上完成初始化工作。正常情况下，用户的可以直接通过工作密码解密出私钥，并进行私钥的签名等相关操作，当用户变更过工作密码时，则可以通过生成校验码和服务端存储的初始校验码比较判定，并通过例如SMS等其他方式取回用户的备用密码，通过备用密码和用户变更过的工作密码再次完成初始，从而进行新的正常情况的工作。

整个过程分三个部分

1 初始化过程，输入工作密码P1，私钥pvk

对输入的工作密码和待保护的私钥进行加密处理，并生成备用密码，校验随机数，工作密码的验证码。加密后的私钥存储在客户本地，备用密码，校验随机数，工作密码的验证码存储在服务器上。

2当工作密码发生变化的校验过程

传递工作密码到服务器端，在服务上通过备用密码，校验随机数，初始工作密码的验证码验证传递过来的工作密码是否变化。

3 正常工作过程

根据用户输入的工作密码，结合用户本地保存的加密私钥，解密出私钥，然后利用私钥进行签名等等其他工作。

4 处理工作密码的更新的过程

用户请求服务器，核实用户身份，取出备用密码，通过安全信道发送给用户，用户在本地通过备用密码解密出私钥。然后重新进行初始化。

**3、本发明的创新点、核心**

本发明方法的创新点为：

1.服务端不存储用户的私钥，从而保证了用户拥有私钥的独立性。

服务端不触碰用户的签名私钥，确保采用公钥体制的“非否认性”和“抗抵赖性”，确保用户利用私钥签名的法律和合规范效力。

2. 客户端可以用工作密码对私钥进行加密存储，保证私钥的安全。

此工作密码可以是支付系统的支付密码，客户端不会把工作密码存在本地系统上，拿不到工作密码也就解密不了私钥,即不能进行正常签名。。

3. 通过服务器上其他认证和安全信道获取备用密码完成工作密钥更新。

4. 工作密码毋须存储在系统上，只是由用户记忆在大脑中，从而可以直接采用支付密码来代替。

**4、采用本发明技术方案带来的技术效果**

本发明方法可以在保证支付便捷性的基础上（包括离线支付），采用本地私钥“加盐”加密和备用支付口令服务端存储，满足移动支付的安全需求，同时还可以提供SMS模式进行私钥安全找回。

**附图说明**

附图1为本发明流程处理框图。

初始化

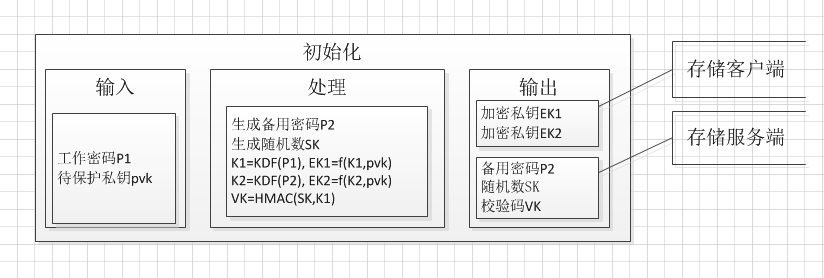


图1 初始化流程

工作密码校验

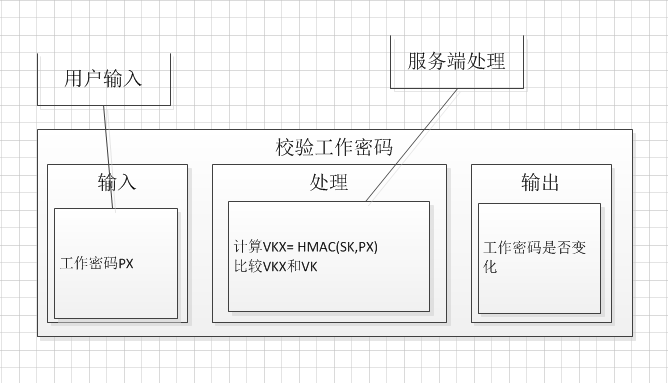


图2工作密码校验流程

正常工作

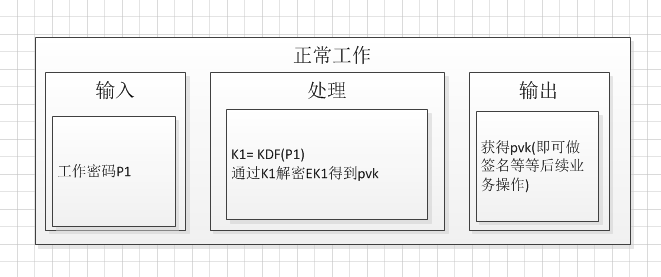


图2正常工作流程

工作密码更新

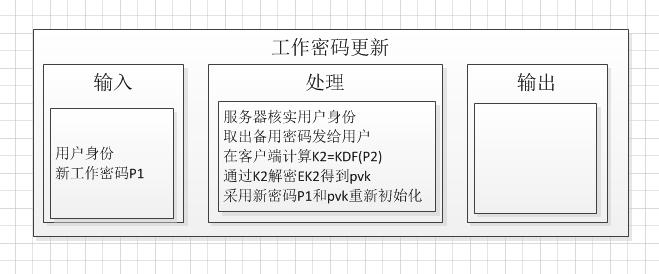


图4工作密码更新流程

说明：KDF为密钥导出函数；f为一分组对称加密函数；HMAC哈希消息认证码函数。

**具体实施方式**

下面结合附图，对本发明的具体实施方式做进一步详细的说明。

1 初始化：

1.1 向客户端输入工作密码P1和私钥pvk，利用啥方法？生成备用密码P2和随机数SK；答：输入工作密码正常工作流程得到私钥pvk，如步骤3{签名私钥采用RSA或ECC等非对称密码算法生产}

1.2 利用密钥导出函数KDF和所述的工作密码P1，计算中间密码K1，K1=KDF(P1)；利用对称加密函数f、中间密码K1和所述的私钥pvk，计算加密后的私钥EK1，EK1=f(K1,pvk)；

1.3 利用密钥导出函数KDF和所述的随机备用密码P2，计算中间密码K2，

K2=KDF(P2)；利用对称加密函数f、中间密码K2和所述的私钥pvk，计算加密后的私钥EK2，EK2=f(K2,pvk)；

1.4 利用哈希消息认证码函数HMAC、随机数SK和中间密码K1，计算初始校验密码VK，VK=HMAC(SK,K1)

1.5输出加密后的私钥 EK1，加密后的私钥EK2 存储到客户端；

1.6输出随机备用密码 P2，随机数SK，校验密码VK存储到服务器上。

以上1.1—1.6的过程是否都是在客户端完成？

答：是的

2 当工作密码发生变化的校验，输入PX

2.1服务端（确认？）计算VKX=HMAC(SK,PX)。

答：确认，是服务端。

具体过程为：向客户端输入工作密码PX，客户端将工作密码PX发送至服务端，服务端利用哈希消息认证码函数HMAC、随机数SK和工作密码PX，计算校验密码VKX，VKX=HMAC(SK,PX)。

2.2 比较校验密码VKX和初始校验密码VK，如果相等，则进入步骤3；如果不相等，则工作密码发生变化，进入步骤4还是仅仅向用户提示密码错误？；

答：是用户工作密码可能在其他终端渠道更改

第2步校验工作密码是在服务端完成的？

答：是的

3 正常工作的时候，输入工作密码P1，加密后的私钥EK1

3.1利用密钥导出函数KDF和所述的工作密码P1，计算中间密码K1，K1=KDF(P1)；

3.2 通过中间密码K1解密加密后的私钥EK1，得到私钥pvk；

3.3 进行含有私钥pvk的业务操作，例如签名等。

第3步是在客户端完成的吗？答：是的

第４步，是用户主动更新密码，还是因为用户记不得原先的工作密码，输入错误，才更新工作密码？

答：是用户主动更新密码。密码错误是在服务端最基础的验证，如果是错误直接提示。这里的密码变更是指原始密码变更之后客户端要完成一系列的安全加密的初始化工作。

4 处理工作密码的更新

4.1核实用户身份（具体举例），在服务器上取出备用密码P2。

答：利用SMS短信等方式验证用户身份{例如视频在线验证等}

4.2 把备用密码P2通过安全信道（例如SMS）发给用户

4.3 用户在本地计算中间密码K2，K2=KDF(P2)

4.4通过K2解密EK2得到pvk

4.5 采用新的工作密码进行（进行工作？）和pvk进行重新初始化。过程和第1步相同？pvk是始终不变的吧？

答：过程和第一步相同，变更密码完成客户端会进行重新初始化，私钥PVK在这个过程中不发生变更，除非相关系统更新数字证书经过步骤1再随之更新PVK｛｝

4.5是采用新的工作密码进行工作，然后工作结束后和ＰＶＫ重新初始化；还是新的工作密码和ＰＶＫ重新初始化，然后再解码，开始签名等工作？

答：新的工作密码和pvk

在步骤4.3中，用户是否需要输入啥数据？

答：不需要

步骤1是加密，步骤2、3是解密，步骤4是更改工作密码，重新加密，对吗？

答：对的

说明：KDF为密钥导出函数，KDF(X)通常情况采用加盐的方式对X进行若干散列加密形成一个加密的密钥；f为一分组对称加密函数，f(K,pvk)表示使用K来加密私钥pvk；HMAC哈希消息认证码函数，HMAC(SK,P)表示P的消息认证码，其中SK为认证密钥。这些函数都是已知的吧？答：对的，参考信息安全PKCS标准