**权利要求书**

1.一种移动支付安全保护的实现方法，其特征在于，包括：

根据所接收的工作密码和私钥，计算第一加密私钥；

接收并发送用户输入的待验证工作密码至服务器中进行验证；接收服务器的验证结果；

如待验证工作密码通过验证，则利用密钥导出函数和所述待验证工作密码，计算第一中间密码，通过所述第一中间密码解密所述第一加密私钥，得到私钥；进行含有所述私钥的移动支付。

2.按照权利要求1所述的方法，其特征在于，还包括初始化操作：

根据所接收的工作密码和私钥，生成备用密码和随机数；

根据所述备用密码和所述私钥，计算第二加密私钥；

根据所述随机数，计算初始校验密码；

将所述第一加密私钥和所述第二加密私钥存储到客户端中；将所述备用密码、所述随机数和所述初始校验密码存储到服务器中。

3.按照权利要求1所述的方法，其特征在于，所述计算第一加密私钥，具体包括：

利用密钥导出函数和所述工作密码，计算第一中间密码；利用对称加密函数、所述第一中间密码和所述私钥，计算第一加密私钥。

4.按照权利要求2所述的方法，其特征在于，

；

所述计算初始校验密码，具体包括：

利用哈希消息认证码函数、所述随机数和所述第一中间密码，计算初始校验密码。

5. 按照权利要求2所述的方法，其特征在于，所述服务器进行验证的过程为：

利用哈希消息认证码函数、所述随机数和所述待验证工作密码，计算校验密码；比较所述校验密码和所述初始校验密码，如果相等，则验证通过；如果不同，则验证不通过。

6. 按照权利要求2所述的方法，其特征在于，还包括：

核实用户身份后，从服务器中调取所述备用密码至客户端中；

根据所述备用密码和密钥导出函数，计算第二中间密码；

通过所述第二中间密码解密第二加密私钥，得到私钥；

根据所述私钥和新的工作密码，重新进行初始化操作，生成新的第一加密私钥，新的第二加密私钥、新的备用密码、新的随机数和新的初始校验密码；并将所述新的第一加密私钥和新的第二加密私钥存储到客户端；将所述新的备用密码、新的随机数和新的初始校验密码存储到服务器中。

7.一种移动支付安全保护的实现系统，其特征在于，

暂时省略！

**说明书**

**一种移动支付安全保护的实现方法及其系统**

**技术领域**

本发明涉及移动支付的安全加密技术领域，具体来说，涉及一种移动支付安全保护的实现方法及其系统，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。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，所谓近场支付是指用手机刷卡的方式坐车、买东西等，十分便利。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。例如，支付宝、易付宝、微信支付等都属于远程支付。

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。

当前移动终端远程支付的私钥存储，第一种方法是其依赖于本地用户口令存储在移动终端。第一种方法需要单独设置一条口令来保护私钥，用户体验很差。第二种方法是将用户的私钥一部分存储在移动终端，另一部分存储在服务端。第二种方法在理论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。第三种方法是将用户私钥存储在服务端。第三种方法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。同时，签名私钥独立存储在服务端，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。

**发明内容**

针对目前对移动支付便捷性和安全性的要求，本发明实施例提出一种移动支付安全保护的实现方法及其系统，以提高移动支付的安全性能和用户体验。

为解决上述技术问题，本发明实施例采用以下技术方案：

暂时省略！

本发明实施例的移动支付安全保护的实现方法及其系统，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”加密和备用密码，满足移动支付的安全需求。本发明实施例的实现方法，根据所接收的工作密码和私钥，进行初始化操作，生成第一加密私钥、第二加密私钥、备用密码、随机数和初始校验密码；验证所接收的待验证工作密码；如待验证工作密码通过验证，则利用密钥导出函数和所述待验证工作密码，计算第一中间密码；通过所述第一中间密码解密第一加密私钥，得到私钥；进行含有所述私钥的移动支付。

**附图说明**

图1是本发明实施例方法的实现构架图；

图2是本发明实施例方法的流程框图；

图3是本发明实施例方法中工作密码没有通过验证时的信息流图；

图4是本发明实施例方法中进行初始化操作的流程框图；

图5是本发明实施例方法中进行初始化操作的信息流图；

图6是本发明实施例方法中正常进行业务操作时的信息流图；

图7是本发明实施例方法中工作密码通过验证时的信息流图；

图8是本发明实施例系统的结构框图。

**具体实施方式**

本发明实施例的方法可以在如图1所示的系统中实现。该系统包括客户端和服务器。客户端为手机等可移动的智能装置。用户向客户端输入工作密码和私钥。客户端根据接收的工作密码和私钥，进行初始化操作，生成第一加密私钥、第二加密私钥、备用密码、随机数和初始校验密码。第一加密私钥和第二加密私钥存储在客户端中。服务器用于存储备用密码、随机数和初始校验密码，以及用于对待验证工作密码进行验证。服务器可以为单台机器，也可以多台机器形成集群。

本发明实施例的一种移动支付安全保护的实现方法，如图2所示，包括：

S10根据所接收的工作密码和私钥，进行初始化操作，生成第一加密私钥、第二加密私钥、备用密码、随机数和初始校验密码；

S20验证所接收的待验证工作密码；如待验证工作密码通过验证，则利用密钥导出函数KDF和所述待验证工作密码，计算第一中间密码K1，K1=KDF(P1)，通过所述第一中间密码K1解密第一加密私钥EK1，得到私钥pvk；进行含有所述私钥pvk的移动支付。

上述步骤S10实现了加密的功能，步骤S20实现了解密功能。通过步骤S10和步骤S20，提高了移动支付的安全性。如图3所示，当待验证工作密码没有通过验证时，向客户端反馈错误信息。

作为优选例，如图4所示，步骤S10具体包括：

S101根据所接收的工作密码P1和私钥pvk，生成备用密码P2和随机数SK；

S102根据所述工作密码P1和所述私钥pvk，计算第一加密私钥EK1；根据所述备用密码P2和所述私钥pvk，计算第二加密私钥EK2；根据所述随机数SK，计算初始校验密码VK；

S30将所述第一加密私钥EK1和所述第二加密私钥EK2存储到客户端中；将所述备用密码P2、所述随机数SK和所述初始校验密码VK存储到服务器中。

上述方法中，如图5所示，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，同时用一个随机数对工作密码进行散列等变化，得到工作密码的初始校验码，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客户端，把备用密码、随机数和初始校验码存储在服务系统上，完成初始化工作。

上述实施例的方法中，在客户端中，可以用工作密码对私钥进行加密存储，保证私钥的安全。所述工作密码可以是支付系统的支付密码。工作密码既不存储在客户端中，也不存储在服务器中。工作密码由用户记忆。不知晓工作密码，就无法解密私钥,也就不能进行正常签名等业务操作。用工作密码和备用密码对私钥进行加密后，生成的第一加密私钥和第二加密私钥存储到客户端中，没有存储在服务端中，从而保证了用户拥有私钥的独立性。服务端中不存储用户的签名私钥，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。

作为优选例，所述步骤S102中，计算第一加密私钥，具体包括：

利用密钥导出函数KDF和所述工作密码P1，计算第一中间密码K1，K1=KDF(P1)；利用对称加密函数f、所述第一中间密码K1和所述私钥pvk，计算第一加密私钥EK1，EK1=f(K1,pvk)。

作为优选例，所述步骤S102中，所述计算第二加密私钥，具体包括：

利用密钥导出函数KDF和所述备用密码P2，计算第二中间密码K2，K2=KDF(P2)；利用对称加密函数f、所述第二中间密码K2和所述私钥pvk，计算第二加密私钥EK2，EK2=f(K2,pvk)。

作为优选例，所述步骤S102中，所述计算初始校验密码，具体包括：

利用哈希消息认证码函数HMAC、所述随机数SK和所述第一中间密码K1，计算初始校验密码VK，VK=HMAC(SK,K1)。

上述实施例的实现方法，通过步骤S102、S102和S103实现了加密。同时，将加密后的第一加密私钥和所述第二加密私钥存储到客户端中，而不是服务器中，增加了安全性能。

上述实施例中，步骤S20中所述验证所接收的待验证工作密码，如图6所示，具体包括：客户端将接收的待验证工作密码发送至服务器中；客户端接收服务器对待验证工作密码的验证结果。也就是说，验证工作是在服务器中进行的。服务器中存储有备用密码、随机数和初始校验密码。用户通过移动终端输入待验证工作密码后，移动终端将待验证工作密码发送到服务器中。更具体的来说，将接收的待验证工作密码PX发送至服务器中，利用哈希消息认证码函数HMAC、所述随机数SK和所述待验证工作密码PX，计算校验密码VKX，VKX=HMAC(SK,PX)；比较所述校验密码VKX和所述初始校验密码VK，如果相等，则验证通过；如果不同，则验证不通过。当验证不通过时，服务器向客户端反馈错误提示。

如果待验证工作密码通过验证，则在客户端进行支付行为。更具体的说，客户端利用密钥导出函数和所述待验证工作密码，计算第一中间密码；通过第一中间密码解密事先已存储在客户端的第一加密私钥，得到私钥；最后进行含有所述私钥的业务操作，例如支付等。

为提高安全性能，用户使用移动支付的过程中，常常需要更改工作密码。为此，本实施例的实现方法，如图7所示，还包括：

核实用户身份后，从服务器中调取所述备用密码P2至客户端中；

根据所述备用密码P2和密钥导出函数KDF，计算第二中间密码K2，K2=KDF(P2)；

通过所述第二中间密码K2解密第二加密私钥EK2，得到私钥pvk；

根据所述私钥pvk和新的工作密码，重新进行初始化，生成新的第一加密私钥、新的第二加密私钥、新的备用密码、新的随机数和新的初始校验密码；并将所述新的第一加密私钥和新的第二加密私钥存储到客户端；将所述新的备用密码、新的随机数和新的初始校验密码存储到服务器中。

当工作密码变更时，第一加密私钥、第二加密私钥、备用密码、随机数和初始校验密码都需要基于工作密码进行变更。在变更之前，首先需要核实用户身份。核实用户身份的方法可利用SMS短信验证用户身份，或者视频在线方式验证用户身份等。这属于现有技术。在核实无误后，从服务器中调取所述备用密码至客户端中。客户端根据备用密码和密钥导出函数，计算第二中间密码；通过第二中间密码解密已存储在客户端上的第二加密私钥，得到私钥。无论工作密码更改与否，私钥都是保持不变的。在客户端中，根据私钥和新的工作密码，重新进行初始化，也即重复步骤S10,生成新的第一加密私钥、新的第二加密私钥、新的备用密码、新的随机数和新的初始校验密码,并将新的第一加密私钥和新的第二加密私钥存储到客户端,将新的备用密码、新的随机数和新的初始校验密码存储到服务器中。

在正常情况下，用户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化操作，从而进行新的正常情况的工作。

上述实施例的方法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，同时支持用户已有密码变更时，仍能良好运行。

上述实施例的方法，KDF表示密钥导出函数，KDF(X)通常采用加盐的方式对X进行若干散列加密形成一个加密的密钥。F表示一分组对称加密函数，f(K,pvk)表示使用K来加密私钥pvk。HMAC表示哈希消息认证码函数，HMAC(SK,P)表示P的消息认证码，SK表示认证密钥。

如图8所示，本发明实施例还提供一种移动支付安全保护的实现系统，包括

暂时省略！

**说明书附图**

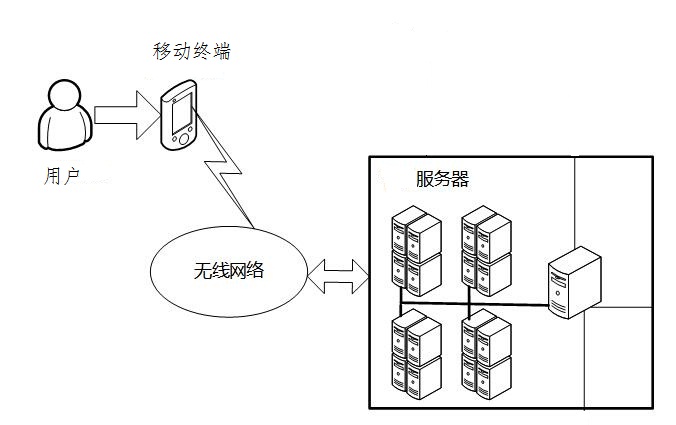
****

图1



图2



图3



图4



图5



图6



图7