一种新型的网上银行应用安全解决方案

1.背景

随着电子银行业务的快速发展，网上银行已成为银行业务拓展、客户服务和品牌宣传的最重要渠道之一。但在实际应用中，网上银行的安全问题也日益凸显，如密码窃取、钓鱼欺诈、木马病毒等。对此，虽然各家银行普遍采用了传统智能密码钥匙（以下简称USBKey）或动态令牌（以下简称Token）等认证手段，但仍不足以应对全部安全威胁，资金失窃事件时有发生。本文主要讨论采用可实现客户端与服务器双向认证、关键信息显示及敏感输入保护的一种新型智能密码钥匙，建立网上银行服务器到客户新型智能密码钥匙之间端到端的安全，更好地解决网上银行安全问题。

2.应用安全需求

网上银行是一种电子交易系统，交易的本质是非等价物的交换，其安全的基础是确保交换过程中认证的安全和授权的安全。认证的安全要求可信双向认证且不泄露机密信息，授权的安全要求信息完整且不可抵赖。因此，网上银行安全的基本需求包括：

(1) 双向认证：用户终端需鉴别来自服务器的交易指令，服务器也需鉴别用户的交易授权和签名；

(2) 信息机密：机密信息需在用户终端上安全输入或存储并保护，然后通过安全通道传输，最后在银行服务器安全计算和存储，整个环节都需保障信息的机密性；

(3) 信息完整：用户终端需校验来自服务器的交易指令，任何篡改和伪冒都将被发现，同时用户对交易的授权和签名需包含交易金额、交易对象、交易时间、流水号等关键信息，可防止重放、篡改和伪冒；

(4) 不可抵赖：服务器的交易指令及用户对交易指令的授权签名都需采用数字签名机制，保证交易的不可抵赖性；

(5) 安全审计：各种交易、操作都有完整的记录，保留备查并可用于争议处理和责任认定。

采用 USBKey 和 Token 的网上银行系统安全现状比较

认证介质 / 安全要求	采用 USBKey 身份认证	采用 Token 身份认证
身份认证	单向认证，服务器可认证 USBKey，但 USBKey 无法鉴别合法程序及非法程序，交易易被篡改和伪冒。	单向认证，服务端可认证 Token，但需人工判断 PC 环境安全及访问网站的合法性，易被钓鱼攻击。
信息机密	USBKey 密码、网银密码及银行卡密码等在 PC 上输入，易被窃取。	网银密码、银行卡密码及动态口令在 PC 上输入，易被窃取。
信息完整	交易信息在 PC 到 USBKey 传递时易被篡改和伪冒。	动态口令与交易信息无关联，盗取动态口令后可随心所欲转账。
不可抵赖	可防抵赖，但由于交易被篡改和伪冒的风险，易有争议存在。	不符合电子签名法要求，无法防止抵赖。
安全审计	与认证手段关联较小。	与认证手段关联较小。

3.应用安全设计

网上银行和网上支付的特点是交易网络的开放性和交易终端的非专用性。由于互联网总是开放的，个人电脑也不可能成为专用交易设备，必须通过建立一套简单有效的客户端与服务器双向认证安全方案，以切实保障网络交易的安全。其主要的应用安全设计包括：

(1) 可信通讯：新型智能密码钥匙和交易服务器之间使用公钥密码体制，在开放的网络上建立一条类似于专线的安全通道，保障信息的传输安全；

(2) 可信输出：新型智能密码钥匙使用数字签名机制鉴别来自服务器的交易指令的真伪，将指令真实、准确、完整的传达给用户，并将用户对

该交易的授权和签名结果真实、准确、完整的回传给服务器；

(3) 可信输入：用户账号、密码等敏感信息在新型智能密码钥匙上输入并使用银行密钥进行保护，输入内容完整、准确、不被篡改和截获；

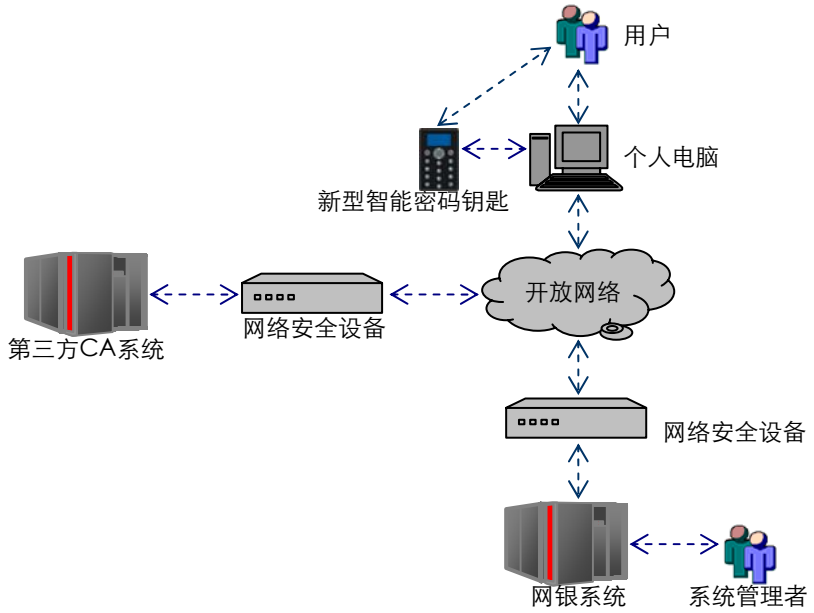
(4) 可信存储：用户存储在新型智能密码钥匙及银行服务器上的私钥、密码等关键信息完整、准确、有效、不被篡改和非法获取；

(5) 可信运算：运算指令完全符合使用者意图，不被欺骗、攻击和篡改，运算过程安全可靠，不泄露信息。

采用新型智能密码钥匙的网上银行安全分析

双向认证	服务端可以鉴别新型智能密码钥匙，新型智能密码钥匙也可以鉴别服务端的交易指令，发现篡改和伪冒后可拒绝交易；合法服务端的交易指令可在新型智能密码钥匙上显示，并由用户确认。
信息机密	密码钥匙保护密码、网上银行密码和银行卡密码等敏感信息可在新型智能密码钥匙上直接输入；网上银行密码和银行卡密码在提交到服务端之前，由新型智能密码钥匙进行加密保护。
信息完整	新型智能密码钥匙可发现对服务端交易指令的篡改和伪冒；新型智能密码钥匙提交的交易请求中包含卡号、金额、密码、时间等关键信息的签名，对其篡改和伪冒也将被服务端发现。
不可抵赖	采用数字签名机制，可防止抵赖。
安全审计	与认证手段关联较小。

4.应用实例



如上图所示，按照《电子签名法》，通过国家认可的第三方电子认证服务机构，为网上银行参与主体——个人用户和网银系统，提供具有法律效力的数字证书，个人用户数字证书使用新型智能密码钥匙作为载体，网上银行交易流程如下：

(1) 用户使用个人电脑通过互联网等开放网络登录网银系统，连接在电脑上的新型智能密码钥匙对服务器进行认证并鉴别服务器的登录指令；

(2) 用户根据新型智能密码钥匙的提示进行确认或取消。如确认，则生成登录签名，并通过个人电脑和开放网络发送到网银系统，由网银系统对用户进行身份认证；

(3) 用户选择网上银行交易——如转账，网银系统通过网络和个人电脑发送交易指令到新型智能密码钥匙，新型智能密码钥匙自动校验交易指令，如失败则拒绝；否则，用户在新型智能密码钥匙上核对交易信息并输入转入账户及密码等敏感信息，新型智能密码钥匙对上述信息加密并签名后，通过网络和个人电脑提交到网银系统；

(4) 网银系统解密并验证用户签名，如合法，则进行交易授权、返回交易

结果并保存完整交易信息，供可能的争议处理和审计使用；否则，拒绝交易。

5.商用密码产品清单

该应用系统构建主要涉及以下密码产品：

(1) 第三方电子认证服务系统

(2) 新型智能密码钥匙

(3) 交易认证和安全服务系统

(4) 电子签章系统

(5) 密码服务中间件

(6) 银行密钥管理系统

（神州融安科技（北京）有限公司供稿）