

交易授权技术创新 阻断网银大盗黑手

既然用户计算机的安全环境是无法控制的，银行发行的 USB Key 就成为客户端唯一安全可信的信息载体。为了保证交易数据不被篡改，就必须在 USB Key 上提供无法通过计算机控制的交易授权手段。

● 网上银行的安全软肋

随着互联网和电子商务的发展，越来越多的人开始接受网上银行这种方便快捷的金融服务方式。然而，随着网上银行用户数量和交易金额的迅速增长，涉及网上银行资金安全的案件也层出不穷，不法分子针对网上银行的攻击手段也越来越变化多端。“安全已经成为阻碍网上银行健康发展的最大障碍。”（CFCA 曹小青）

银行作为专业金融服务机构，具备比较完善的安全管理技术和体系，而作为非专业使用者的网上银行用户，往往没有足够的意识和技术能力来保护自身客户端的安全，同时，互联网上各种木马和黑客软件的泛滥，也在严重威胁着客户端的安全环境。因此，客户端的安全已经成为网上银行安全的软肋。

● 目前交易授权技术的不足

为了保证用户的资金安全，各商业银行都采取了多种措施，来提高用户身份认证的安全性。目前网上银行使用最普遍的也是安全强度最高的是基于智能卡的 USB Key 安全数字证书。

USB Key 结合了智能卡技术与 PKI 技术，使用内置操作系统的智能卡芯片来保护用户的私钥，可以实现可靠的数字身份认证和交易数字签名。

目前常用的普通 USB Key，所有操作都是通过计算机向 USB Key 发送指令来进行的。用户进行资金交易时需要输入的交易指令，包括对方帐号、转账金额等关键数据，以及交易授权时需要输入的 USB Key 密码，都是通过计算机键盘输入，并在计算机的显示器上显示的。由于客户端计算机环境的不安全，理论上说只要在计算机内存中出现的数据，都有可能被黑客截取。因此用户输入的 PIN 码有可能被黑客木马截取，交易数据也有可能被黑客木马篡改。因此使用目前的普通 USB Key，无法保证用户计算机发送给网银服务器的交易指令以及发送给

USB Key 的待签名数据与用户发起交易真实意图完全一致。而黑客木马完全有可能在用户实施交易时通过篡改收款帐号和付款金额来盗取用户资金。

● 结合用户复核和交互机制保障用户真实交易意图

既然用户计算机的安全环境是无法控制的，银行发行的 USB Key 就成为客户端唯一安全可信的信息载体。为了保证交易数据不被篡改，就必须在 USB Key 上提供无法通过计算机控制的交易授权手段。

为了解决这个问题，飞天诚信专门针对网上银行的需求，推出 InterPass 系列可复核交易信息的用户交互型 USB Key。InterPass 内置液晶显示屏或语音芯片，可以将 USB Key 接收到的关键交易信息，包括对方帐号和转账金额，通过液晶显示或语音读取提示给用户，用户可以复核交易信息无误后，按下 USB Key 上的交易授权按键，USB Key 才会执行交易签名。如果用户交易信息被篡改，用户在复核时就能够发觉，并且取消交易。即使黑客盗取了用户 PIN 码，如果没有用户按动 USB Key 上的按钮，也不可能骗取交易签名。因此，USB Key 扩展了用户复核功能和物理互动操作，就可以杜绝黑客远程劫持客户端计算机而导致的非法交易。

● 通过完善的流程设计确保交易授权的万无一失

InterPass 提供了用户复核确认交易信息的功能，但是要保证用户资金的安全，还需要与网银服务端交易验证流程相配合才能确保交易授权真正万无一失。

在大部分网上银行应用中，除了资金划转交易以外，用户私钥还可能会用于非交易类操作的签名或加密，如登陆 SSL 网站、账户查询等操作。因此需要 USB Key 签名的数据，可能有交易签名和非交易签名两种，而非交易签名没有对方帐号和金额等关键信息可供用户复核确认的。如果使用不同的签名流程来操作交易签名和非交易签名，就有可能存在黑客使用将交易签名数据通过不需要复核确认的非交易签名指令操作来骗取交易签名值的可能性。反之，如果对所有签名操作均需要用户手工确认，对用户的正常使用也会带来很大困扰

为了解决这一矛盾，InterPass 设计了一套完整的交易签名授权和验证流程。该流程中，仅使用一条签名指令，但是对于是否需要用户复核确认，由 USB Key 根据待签名数据的格式来判断，而不是对所有数据的签名都需要用户确认。

在通常的应用中，所谓数字签名通常需要将待签名数据都进行 Hash 后才能

进行签名。但是签名数据如果经过 Hash 后再传入 USB Key 内，COS 就解析不到待签名数据中的关键交易信息。因此，InterPass3000 要求将待签名的数据明文传入 Key 内，通过 USB Key 硬件进行 Hash 运算。在执行 Hash 操作之前，COS 会对传入的待签名数据进行格式检查，数据中不符合交易签名格式，则按照非交易签名流程进行正常 Hash 操作；如果待签名数据符合交易签名格式，则 COS 就将该 Hash 结果设置为交易签名数据，并从中提取关键的帐号和金额，用于在执行签名时显示或者发音提示给用户。

InterPass3000 在执行签名时，先检查 Key 内部的交易签名标志，如果待签名的 Hash 值是交易签名状态，COS 就会中断签名操作，显示或者语音提示交易帐号和金额，并等待用户按键确认；如果是非交易签名状态，COS 就会按照普通的签名流程处理，不需要用户干预。对于交易签名所使用的 Hash 算法，签名指令不支持对 Key 外部传入 Hash 值进行签名，只能对通过 COS 的 Hash 指令进行 Key 内 Hash 的 Hash 值进行签名。这样处理，既可以确保用户资金交易的万无一失，又提供了非交易签名的“绿色通道”，在执行用户登录等非交易操作时，不需要用户不断的按按键。

对不同银行的网上银行系统，其登录和交易时使用的签名数据格式和 Hash 算法可能是各不相同的，由于 InterPass 是通过交易数据格式和交易签名使用的 Hash 算法对交易签名进行识别和判断的，为了保证整个交易流程的安全性，就需要网银服务器也必须在交易授权时对交易数据格式和签名使用的 Hash 算法进行强制性验证。同时 InterPass 在实施时也要与不同网银的交易系统进行配合定制。

网银安全是一个系统工程，单一解决服务器端或者客户端的问题，是无法保证整个系统的安全性的。只有从整个交易流程出发，针对可能发生的攻击，同时对服务器端和客户端的交易授权手段进行创新和改进，才能够真正阻断网银大盗的黑手。