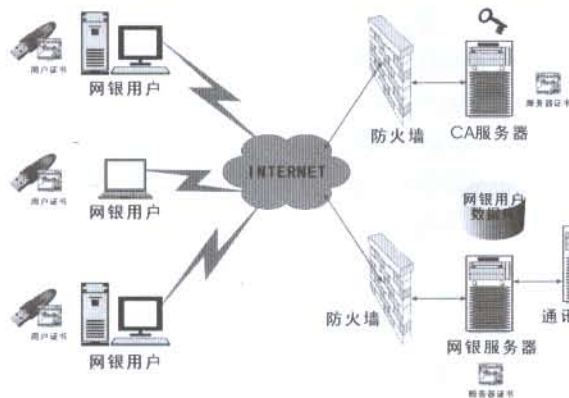


飞天 ePass 系列 USB Key 网上银行身份安全解决方案

网上银行已经成为影响未来银行业竞争一块新高地。国内外各银行都越来越注重网上银行的建设与发展。然而，正是由于网上银行的实时性和虚拟性，其安全性成了决定网上银行成败的关键。

飞天 ePass 系列 USB Key，是国内推出最早、技术最成熟、产品线最完善的 USB Key 系列产品，由于结合了智能卡和现代密码学技术，可以在 ePass 内部生成 RSA 密钥对，所有涉及用户私钥的运算都在 ePass 内部进行，有效保障了网银用户身份和交易数据的安全，经广泛应用于国内外各大商业银行的网银系统，成为保障网银用户身份安全的最佳解决方案。

在飞天 ePass USB Key 网银身份安全解决方案中，使用存储在 ePass 中的数字证书对用户和服务器双方进行身份验证，通过数字证书认证、完整性签名和数据加密来建立安全套接层（SSL）连接，提供安全可靠的通信信道，保障了数据的机密性、完整性以及交易信息的不可抵赖性。其中用户私钥是惟一存储在 USB Key 中，并且不可导出和复制的，凡经



过用户私钥签名的指令即可以认为是用户实际交易要求，用户无法抵赖。

其网络结构如下图所示：

以飞天诚信于 2004 年推出的全球首款 32 位智能卡型 USB Key——ePass3000 为例，简要介绍 ePass 系列 USB Key 在网上银行中的应用流程：

1、 用户到银行柜台开户并领取存有该用户证书的 ePass3000。

2、 用户在使用网上银行时，插入 ePass3000，通过浏览器或网银客户端程序与网银服务器建立 SSL 连接。

3、 用户输入 ePass3000 的正确 PIN 码，验证用户证书后显示用户帐户页面，所有的用户帐户信息都经过用户公钥的加密和服务器证书的签名，保证了用户数据的机密性和完整性。

4、 用户进行的所有操作，都经过 ePass3000 中的用户私钥签名，并使用服务器证书加密后传送到网银服务器，保证了交易信息的安全性和不可否认性。

5、 用户可以在任何联网的计算机上使用 ePass3000 登录网上银行，一旦拔出 ePass3000，不会在计算机上留下用户的任何信息。没有合法的 ePass3000 和正确的 PIN 码，任何人也无法伪造用户身份使用网银帐户。

从以上步骤可以看出，在整个网上银行交易过程中，所有服务器和用户端的数据传输都经过了数字证书的加密，而所有涉及用户私钥的计算都在 USB Key 中进行，用户私钥只存在于 USB Key 中，永远不能被导出或出现在计算机内存中。没有保存用户证书

的 USB Key 或者不知道该 USB Key 的 PIN 码，任何人也无法伪造用户身份使用网上银行系统，有效保障了网上银行的安全性。

使用 USB Key 作为网上银行的 用户身份认证手段，是目前最为成熟且安全的网上银行身份安全解决方案，已经得到国内外众多商业银行和用户的认可。可以预见在不久的将来，绝大多数开展网上银行业务的商业银行都将采用 USB Key 来保障其网上银行系统的安全。