

基于 USB Key 的网上银行应用

一 网上银行的现状

1.1 何为网上银行

网上银行的定义

网上银行又称网络银行、在线银行，是指银行利用 Internet 技术，通过 Internet 向客户提供开户、销户、查询、对帐、行内转帐、跨行转帐、信贷、网上证券、投资理财等传统服务项目，使客户可以足不出户就能够安全便捷地管理活期和定期存款、支票、信用卡及个人投资等。可以说，网上银行是在 Internet 上的虚拟银行柜台。

网上银行的一般步骤，以网上储蓄为例。进入银行网站，点击“网上理财”，再点击“个人理财计算器”，输入你的存款金额及存款期限，然后点击确认。网络就会为你算出准确的存款利息、缴纳利息税额和实得本息。如果你想办理住房贷款，点击此网页的“个人住房贷款计算器”同样会为你计算出每月利息、月还款额及累计利息和还款总额。进入“提前支取与存单质押贷款比较”，输入现有定期存款本金、存款期限、存入日期以及计划提前取款的日期等内容，单击确认，就可以立即得出存款提前支取和办理质押贷款那个更合算的结果。

1.2 网上银行提供的服务和优势

“网上银行”究竟能给银行和用户以及商户带来什么好处呢？

首先，网上银行可以减少固定网点数量、降低经营成本，而用户却可以不受空间、时间的限制，只要一台 PC、一根电话线，无论在家里，还是在旅

途中都可以与银行相连，享受每周 7 天、每天 24 小时的不间断服务。

其次，网上银行的客户端由标准 PC、浏览器组成，便于维护。网上 E-mail 通信方式也非常灵活方便，便于用户与银行之间，以及银行内部之间的沟通。

总的说来网上银行给我们带来的好处有以下几点：

- 1、坐在家中即能点阅账户结余、转帐、交易纪录，省了去银行或柜员机的时间与费用。
- 2、直接下载交易数据到您最喜欢的理财软件；
- 3、轻松转帐到各个户头
- 4、电子账单付款
- 5、网上直接申请信用卡
- 6、网上即可申请贷款
- 7、安全可靠的电子邮件让您向银行直接提出问题或要求服务

与传统银行业务相比，网上银行的优势效应正日益显现：

一是低成本和价格优势。这是因为：

- 1、组建成本低。一般而言，网络银行的创建费用只相当于传统银行开办一个小分支机构的费用。
- 2、业务成本低。就银行一笔业务的成本来看，手工交易约为 1 美元，ATM 和电话交易约为 25 美分，而互联网交易仅需 1 美分，只有手工交易单位成本的 1%。

3、价格优势。由于网上银行运营成本比较低，可将节省的成本与客户共享，通过提供较传统银行高的存款利率、低收费、部分服务免费等方法争夺客户和业务市场。不仅如此，通过网络电子确认系统，还可避免诈骗和损失。如在美国，目前支票占

支付市场的60%，传统纸制支票诈骗曾使零售商每年损失120亿美元，而电子支票不仅消除了支票诈骗的可能性，而且节省了处理大量纸制支票的费用和时间。

二是互动性与持续性服务。网上银行系统与客户之间，可以通过电子邮件、账户查询、贷款申请或档案的更新等途径，实现网络在线实时沟通，客户可以在任何时间、任何地方通过因特网就能得到银行的金融服务。银行业务不受时空限制，每天可向客户提供24小时不间断服务。

三是私密性与标准化服务。网上银行通过私码与公码两套加密系统对客户进行隐私保护。网上银行提供的服务比营业网点更标准、更规范，避免了因工作人员的业务素质高低及情绪好坏所带来的服务满意度的差异。

四是业务全球化。网上银行是一个开放的体系，是全球化的银行。网上银行利用因特网能够提供全球化的金融服务，可以快捷地进行不同语言文字之间的转换，为银行开拓国际市场创造了条件。传统银行是通过设立分支机构开拓国际市场的，而网上银行只需借助因特网，便可以将其金融业务和市场延伸到全球的每个角落，把世界上每个公民都当做自己的潜在客户去争取。网上银行无疑是金融运营方式的革命，它使得银行竞争突破国界变为全球性竞争。

随着互联网络的发展，拥有良好网络技术和营销经验的国外大银行或其他金融机构，完全可以不在国内设立分支机构而利用网上银行争揽金融业务，抢占金融市场。网上银行业务的竞争将是无形的、无国界的竞争。因此，网上银行将是未来中外银行竞争的主要领

1.3 网上银行的安全隐患

●到2005年，中国的网上银行用户数将由目前的250万飙升到1.4亿

●“密码泄漏”和“冒充站点”都是网上银行的安全隐患

●网上银行的安全隐患进一步证明，比尔·盖茨关于“传统商业银行要在21世纪灭绝”的预言过于乐观

在中国，网上银行成为传统银行业务的延伸已经吸引了250万的用户，但是也有相当一部分人群因为安全隐患的存在而对网上银行“望而却步”。

比尔·盖茨曾经预言：“传统商业银行是要在21世纪灭绝的一群恐龙。”他甚至说，银行业是必需的，银行是不必要的。传统商业银行的网上金融变革将改变比尔·盖茨的预言。

而网上银行的安全隐患进一步证明，比尔·盖茨的预言未免过于乐观。

用户的担心并不是没有道理。

在日本，“1600万日元突然从自己的账户中不翼而飞”的网络银行案件再次给网络银行的使用者提了醒——网络银行的安全问题并不如想象中那样简单和容易解决。

据了解，此次事件中用于非法窃取ID和密码的软件是“KeyLogger”。其实这种特殊软件并没有多高明，它的功能非常单一，通过常驻系统来监视键盘输入，并将所输入的文字全部作为日志保存在文本文件中。

由于部分用户网络银行的安全意识淡薄，随意在公用电脑，诸如网吧输入账号和密码，导致案犯有机可乘。

业内人士认为，作为银行来说，银行的ID和密码也非常脆弱。如果有随机数表，就可以防备此类事件。随机数表是指为每个客户指定各不相同的数字列表，申请时将该随机数表分配给客户。

除了用软件窃取密码这样的事件以外，“冒充站点”也是网上银行使用中一个非常重要的安全隐患。

比如，可以首先向客户发送一个“本行网站正

在进行促销活动！”等内容的虚假邮件，然后诱骗客户访问虚假站点。客户在不了解情况时就会向虚假站点发送ID和密码。客户发送完毕后，如果显示出一个“服务马上就要停止”的画面，或者把客户访问重新引导到正规站点上，客户当时是很难察觉的。这样一来，就存在有人进行非法资金转移的可能性。

虽然迄今国内还没有某家银行网站被黑客入侵的案例，但多数客户仍心存顾虑，不敢在网上发送自己的信用卡账号等关键信息就是基于支付信息安全的原因，这就严重制约了网上银行的业务发展。

多家银行业已经开通了安全认证服务，通过向电子商务参与方发放数字证书来确认各方的身份，保证网上支付的安全性，对防范支付风险将起到积极的作用。

二 USBKEY如何增强网上银行安全性

2.1 网上银行技术风险的来源

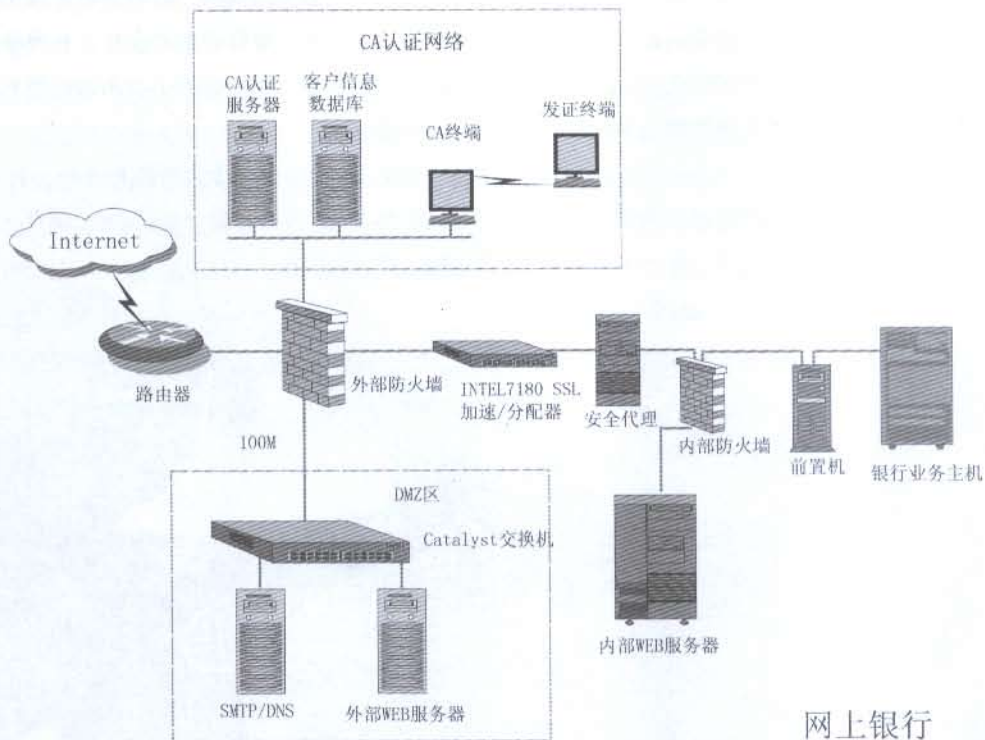
网上银行业务技术风险一般来源于三个渠道：首先是数据传输，一旦数据传输系统被攻破，就有可能造成用户的银行资料泄密，并由此威胁到用户的资金安全；其次是网上银行应用系统的设计，一旦其在安全设计上存在缺陷并被黑客利用，将直接危害到系统的安全性，造成严重损失；第三是来自计算机病毒的攻击，即由于网络防范不严，导致计算机病毒通过网上银行入侵到银行主机系统，从而造成数据丢失等严重后果。

总结如下：一般来说，人们担心的网上银行安全问题主要是：

1. 银行交易系统被非法入侵。
2. 信息通过网络传输时被窃取或篡改。
3. 交易双方的身份识别；账户被他人盗用。

2.2 USBKEY保证网上银行安全

网上交易不是面对面的，客户可以在任何时间、任何地点发出请求，传统的身份识别方法通常



网上银行

是靠用户名和登录密码对用户的身份进行认证。但是,用户的密码在登录时以明文的方式在网络上传输,很容易被攻击者截获,进而可以假冒用户的身份,身份认证机制就会被攻破。

在网上银行系统中,用户的身份认证依靠基于“RSA 公钥密码体制”的加密机制、数字签名机制和用户登录密码的多重保证。银行对用户的数字签名和登录密码进行检验,全部通过后才能确认该用户的身份。用户的惟一身份标识就是银行签发的“数字证书”。用户的登录密码以密文的方式进行传输,确保了身份认证的安全可靠性。数字证书的引入,同时实现了用户对银行交易网站的身份认证,以保证访问的是真实的银行网站,另外还确保了客户提交的交易指令的不可否认性。

由于数字证书的惟一性和重要性,各家银行为开展网上业务都成立了CA 认证机构,专门负责签发和管理数字证书,并进行网上身份审核。2000年6月,由中国人民银行牵头,12家商业银行联合共建的中国金融认证中心(CFCA)正式挂牌运营。这标志着中国电子商务进入了银行安全支付的新阶段。中国金融认证中心作为一个权威的、可信赖的、公正的第三方信任机构,为今后实现跨行交易提供了身份认证基础。

现在存储数字证书和用户密钥也有两种方式,一种是直接存储在网银用户的硬盘中,另一种是存储在USB Key中,如飞天诚信公司的ePass系列身份认

证锁。无疑,将数字证书存储在计算机硬盘上存在一定的风险性,当网银用户遭受病毒或被黑客种植了木马程序,数字证书很可能就此无法使用或被他人盗用。而把数字证书存储在USB Key中,它的安全性就有保障得多。

USB Key采用双钥(公钥)加密的认证模式,USB Key是一种USB接口的硬件设备,外形如下图所示。它内置单片机或智能卡芯片,有一定的存储空间,可以存储用户的私钥以及数字证书,利用USB Key内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中,理论上使用任何方式都无法读取,因此保证了用户认证的安全性。

USB Key的硬件和PIN码构成了可以使用证书的两个必要因素。如果用户PIN码被泄漏,只要USB Key本身不被盗用即安全。同样的,如果USB KEY遗失了,可是拾到的人不知道密码,此人的账户也是安全的。USB Key的使用方法是,当登录网银系统的时候,在电脑上插入USB Key,然后输入PIN码,如果验证通过,则可以进行相关交易。这种加密方式使用了双钥加密,私钥安全地保存在Key中,在网络应用的环境下,可以更安全,弥补了动态密码锁单钥加密的一些缺陷。

综上所述,基于网上银行特有特点,将PKI体系,与USBKEY安全存储介质相结合,将更有效的保证网上银行的安全。

