互联网指纹认证推动网络银行用户“ 远行 ” PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/62/2021_2022__E4_BA_92_E8_81_94_E7_BD_91_E6_c40_62084.htm 【内容提要】数字证书（ID 密码）的键盘认证方式很难遏止“ 网银黑客 ”，采用指纹识别技术的网络认证，避开了键盘的认证方式，从而有效地解决网络银行安全威胁。 首先我带来几个问题：“ 凭什么说数字证书是可信的（数据传输）？数字证书是保护网络银行端还是用户端？ ”确切地说，数字证书是保证用户登陆（真）网络银行的安全受到保护，事实上，数字证书是128位加密的产品，它并不意味着网络银行的永久安全，只是目前黑客还不具备破解能力罢了，从这个意义上说，被破解只是时间问题。另外，即便它有效地确保了当前（真）网络银行的安全，（假）复制网络银行依然无法奏效。从运营上看，又一个问题是，工行是否应确保用户访问其他运营网站的安全责任呢？答案显然是否定的。那么无法帮助用户访问其他网站的安全，就无法使网络银行更安全。 长久以来，用户常用的传统认证“ ID 密码 ”这种安全保障系数较低的方式。由于传统密码本身并没有加密措施，使得网页病毒，木马甚至偷窥屡获成功的主要原因之一。此外由于用户的计算机安全管理意识淡薄也为病毒提供了有利的传播平台。因此，为了确保用户财产，个人信息及隐私获得有效保障，我们建议用户提高安全管理意识的同时，尽量选择那些具备无法复制，无需记忆，随身携带的互联网指纹认证产品。 目前，互联网指纹认证服务正悄然靠近用户视线，与传统认证相比，互联网指纹认证主要以ID 指纹的方式进行认证，第一，它完全避开

了键盘的认证方式，从而颠覆现有病毒的窃取方式。第二，指纹是无法复制的人体智能认证模式，因此，指纹本身就是一种加密形式。第三，由于指纹认证是图象对比模式，此对比是在指纹图象上，提取若干个特征点完成的，算法也是一种加密形式。第四，为了保证数据安全，在算法数据库与核心算法之间设置了对指纹数据的加密及解密程序（这种加密和解密完全在核心数据库内完成，没有对外工具或接口）第五，它也配置了用户通常接触的如数字证书，防火墙，网络管理器等等。