

# 用动态口令保护网络证券交易

网上证券作为证券行业的一个重要组成部分，由于其具有维护管理成本低廉、使用方便、经济效益好的特点，所以受到券商和广大用户的喜爱，因此取得了快速的发展。

证券服务形式是指券商向其用户提供的服务形式，主要包括四种方式：柜台递单委托、电脑自动委托、电话自动委托和远程终端委托。不同的证券交易方式存在不同的安全问题，主要的安全问题是帐号和密码泄露，下面对几种交易方式面临的主要安全问题分别说明：

序号	交易方式	潜在安全问题
1	柜台递单委托	输入帐号和密码时被人偷看到
2	电脑自动委托	输入帐号和密码被人偷看到
3	电话自动委托	输入帐号和密码被人偷看到 帐号和密码通过电话重拨偷看到 帐号和密码在电话线上被人窃取
4	远程终端委托	输入帐号和密码被人偷看到 帐号和密码被木马程序窃取 帐号和密码在网络传输时被窃取

针对不同的使用环境，其主要的安全风险不同，下面就其中可能性最大的几种作一简单介绍：

- 窥视泄密，当用户输入帐号和密码的时候，可能被周围的人有意或无意看到，这种情况容易发生在公共场所，比如在证券公司营业部。

- 盗号木马（比如证券大盗木马），木马程序记录用户在特定窗口的特定区域（比如帐号和密码输入框）输入的信息并将这些信息保存下来，在适当的时候发送给木马作者。

- 数据窃听，通过窃听用户计算机向外发送的信息，经过分析处理从而得出用户的帐号和密码。

- 重放攻击，将用户向券商服务器发送的信息完全记



录下来，再次发送同样的信息，从而通过服务器的验证。

- 密码猜测，猜测用户密码，这种情况在用户安全意识薄弱，设置密码安全性不高时，容易被猜测。

- 穷举攻击，尝试所有可能的密码组合。

- 记录泄密，用户可能为了安全而设置复杂的密码，同时又为了避免自己忘记帐号和密码，所以就将其写在自己的笔记本上，遗憾的是，没能很好地保证笔记本的安全，被别人看到了自己记录的帐号和密码。

- 共享泄密，有的用户为了方便，将自己的多个应用（比如银行卡密码、各种邮箱密码、计算机登录密码、网络登录密码等）密码设置为一个，当一个密码泄露时，全部都没有安全保障了。

ePass OTP是北京飞天诚信科技有限公司推出的动态口令身份认证产品，系统对各种应用环境具有广泛的灵活性和适应性，能够适应多种使用环境，包括柜台递单委托、电脑自动委托、电话自动委托和远程终端委托。

ePass OTP身份认证解决方案采用基于模块化的分层体系结构、成熟的技术和开放接口设计，系统具有高可靠性、可用性和可维护性，同时向证券服务提供商和证券用户提供良好的灵活性和易用性。ePass OTP认证服务器和

备份服务器完全独立于证券服务器系统，只需要在原有认证服务器系统中安装认证代理模块即可，不用更改原有网络结构设计。

### 1. 认证服务器

认证服务器是系统的核心部分，安装在证券服务提供商的内部网络，与证券服务器通过局域网连接，向证券服务器提供身份认证的功能。当证券服务器接收到证券用户发送的登录信息时，由证券服务器传递登录信息给认证服务器，认证服务器根据其存储的信息验证证券用户的登录信息是否正确，如果正确，认证服务器返回认证成功，证券用户成功登录证券服务器并可以进行后续操作，否则，认证服务器返回认证失败，证券用户登录证券服务器失败。

### 2. 认证备份服务器

后备认证服务器是对认证服务器的完全备份，它能够在认证服务器发生故障或检修时，及时接管认证服务器的认证工作。

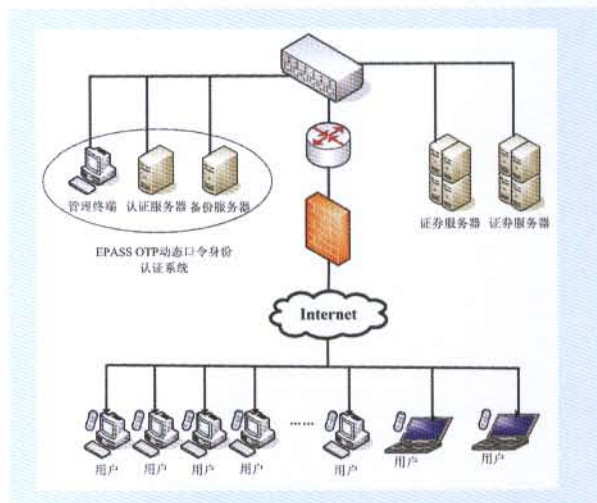
### 3. 管理工作站

管理工作站提供动态身份认证系统的管理界面，它在网络管理员与认证服务器之间提供一个友好的操作界面，便于网络管理员对系统维护和用户管理。通过管理工作站，网络管理员可以进行网络配置、动态口令令牌管理（比如添加、删除、和用户绑定、锁定、解锁等）、用户管理（比如添加、删除、分配令牌等）以及认证日志管理等操作。

### 4. 动态口令令牌

动态口令令牌是一个单独的硬件设备，使用时无需连接任何外部设备，所以具有很大的灵活性，登录证券服务器时，只需要激活动态口令令牌，将生成的动态口令输入登录窗口中的对应位置即可。

前面提到证券交易方式主要包括四种，它们分别是柜台递单委托、电脑自动委托、电话自动委托和远程终端委



(图五) ePass OTP 认证解决方案系统组成图

托。ePass OTP 在这些交易方式下都可以发挥其功能，保护证券帐户的安全。

■ 柜台递单委托，该交易方式的主要安全威胁是在帐号和密码可能在输入的时候被周围的人有意或无意看到，从而导致帐号和密码泄露的风险。此时如果用户使用动态口令可以有效解决这样的问题，即使别人看到了输入的帐号和动态口令，使用过以后就不能再继续使用了。

■ 电脑自动委托，该交易方式通过证券营业部的电脑进行操作，由于是公共场所，人员活动也比较频繁，可能存在周围的人有意或无意直接看到自己的帐号和密码，还可能通过摄像设备（比如有摄像功能的手机）对整个操作过程进行记录。使用动态口令可以有效避免自己的帐号被盗用，因为动态口令只能使用一次，即使有人看到或者得到你输入的帐号和动态口令，当别人试图通过这些信息进行登录时，系统会提示帐号或动态口令无效，从而有效防止帐号和动态口令泄露导致的安全威胁。

■ 电话自动委托，该交易方式通过电话输入用户帐号和密码，根据使用电话的环境不同，如果使用传统的密码方

式,可能存在三种安全风险,即输入时被看到、通过电话重拨键查看到或者通过电话窃取到,具有相当的危险性。使用动态口令以后,因为动态口令不能重复使用,所以即使别人窃取到帐号和动态口令,别人通过其窃取到的帐号和动态口令进行登录的时候,还是不能成功,这样就有效保护了用户的帐户安全。

■ 远程终端委托,该方式主要是通过计算机或者智能终端连接证券服务商的服务器来完成,同样可能存在帐号和密码泄露的可能性。当使用动态口令时,即使用户的帐号和动态口令在使用过程中被人窃取,得到帐号和动态口令的人还是无法登录用户的帐户进行非法操作,因为动态口令只能使用一次,下次登录必须使用不同的动态口令才能成功,而新的动态口令只有用户手里的专用设备才能生成。

采用ePass OTP身份认证解决方案提高证券帐号安全性具有很大的灵活性和性价比。

○对券商而言:

■ 向证券用户提供帐号保护功能,满足证券用户对帐号安全性的需求。

■ 安装配置灵活方便,不用更改原有网络结构。

■ 完善和提供证券帐号安全服务,提高证券用户的信心。

■ 减少因帐号被盗引起的投诉,从而减少相关管理费用。

■ 减少因帐号被盗引起的证券用户不满意,从而减少证券用户转移到其它证券公司的可能性。

■ 减少因证券帐号被盗引起的名誉损失,有利于建立良好的公众形象。

■ 提供更好的证券帐号安全服务,吸引更多证券用户。



○证券用户而言:

■ 防止帐号和密码泄露时可能造成的各种损失,提高证券用户帐号的安全性。

■ 方便密码管理,通过动态口令令牌产生口令,避免密码遗忘或记错。

■ 使用方便,无需安装任何软件,也无需连接计算机。

■ 具有广泛的适应性和灵活性,对使用环境没有限制,可以在四种交易方式的任何一种中使用。

■ 无需改变用户的操作习惯,无需用户付出时间和精力来学习如何使用,完全实现即看即会。

ePass OTP身份认证解决方案在防止证券用户因帐号和密码泄露时造成各种损失方面有其独特优势。但同时还应认识到,安全问题错综复杂,要全面保护证券用户的各种交易安全,需要证券服务商、证券用户以及相关安全厂商的共同努力和全力配合,唯有如此,才能构筑真正安全的证券交易平台,才能充分地享受到现代科技带来的好处,共创美好的明天。