

## 网上银行动态口令多系统集成解决方案

网上银行（以下简称“网银”）作为近年来推出的一种全新的银行业务，由于给用户带来极大的方便性和成本效益，受到广大用户的欢迎，越来越多的用户开始使用网银服务。银行作为网银服务的提供者，也从网银业务得到两个方面的好处，以低廉的成本提供了高效的服务，从而实现了良好的经济效益。

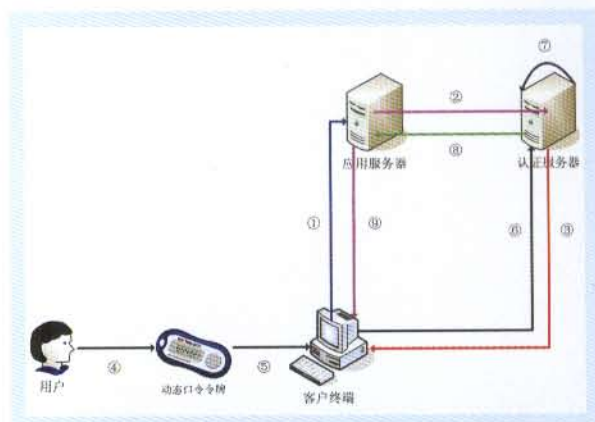
网银的快速发展主要得益于两个方面的原因，一方面，计算机技术、网络技术以及相关安全技术的发展和成熟，为网银的发展奠定了基础；另一方面，人们在越来越频繁的经济活动中希望能够安全、方便、高效地使用银行服务。

由于网银建立在普通计算机和公共网络平台上，其安全性相当程度上依赖于计算机和网络的安全。近年来，受到利益的驱动，利用计算机和网络的安全漏洞进行犯罪活动的事件频繁发生。网银在提供方便性的同时，其安全性也引起了银行和广大网银用户的极大关注。为此，银行方面积极采取有效措施，提供高安全性的解决方案，并积极引导网银用户使用新的安全技术来保障其网银的安全。各种安全技术纷纷推出，其中之一就是动态口令技术，该技术结合网银原有静态口令认证技术，提供双因素强身份认证，为网银的安全提供了保障。

动态口令身份认证技术的出现，弥补了静态口令身份认证技术的不足，再加上其本身具有使用方便、操作简单的特点，所以得到广泛的应用。

动态口令也称一次性口令，动态口令是变动的口令，其变动来源于产生口令的运算因子是变化的。动态口令的产生因子一般都采用双运算因子：其一，为用户的私有密钥，它是代表用户身份的识别码，是固定不变的。其二，为变动因子，正是变动因子的不断变化，才产生了不断变动的动态口令。采用不同的变动因子，形成了不同的动态口令认证技术：基于时间同步认证技术、基于事件同步认证技术和挑战/应答方式的非同步认证技术。

下面以基于事件同步认证技术的动态口令身份认证系统来说明其身份认证过程：

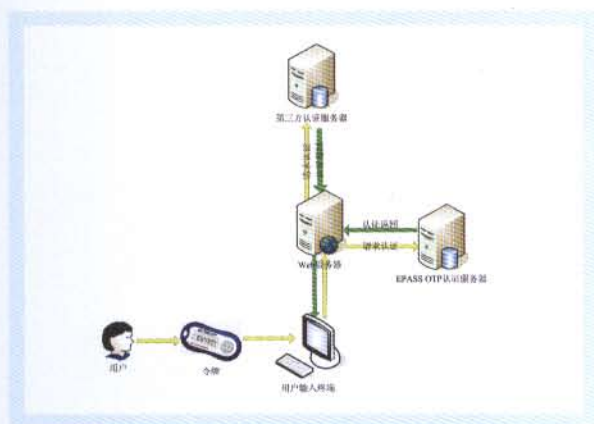


(图一) 动态口令身份认证系统工作过程

- ①客户请求接入应用服务器；
- ②应用服务器请求认证服务器对客户的身体的合法性和真实性进行认证；
- ③客户终端弹出身份认证对话框；
- ④客户激活动态口令令牌，生产动态口令；
- ⑤客户将帐号和动态口令键入终端的身份认证对话框；
- ⑥客户终端将帐号和动态口令通过网络传输给认证服务器；
- ⑦认证服务器调用客户信息，产生与客户信息和变动因子相关的随机序列，并与客户输入的口令进行比对，判别客户身份的合法性和真实性；
- ⑧认证服务器将认证结果报告给应用服务器；
- ⑨应用服务器根据客户身份的合法性和真实性反馈给客户终端，并决定提供服务或拒绝服务。

动态口令身份认证技术之所以能够提高系统的安全性并得到广泛的应用，主要是其具有以下特点：

- 动态性：动态口令令牌产生的动态口令每次变化，每次使用不同口令登录，每个口令只能使用一次。
- 随机性：动态口令每次都是随机产生的，不可预测。



(图二) ePass OTP 前置模式结构图

■ 一次性：每个动态口令使用过一次后，不能再连续重复使用。

■ 抗偷看窃听性：由于动态性和一次性的特点，即使某一个动态口令被人偷看或窃听了，也无法使用。

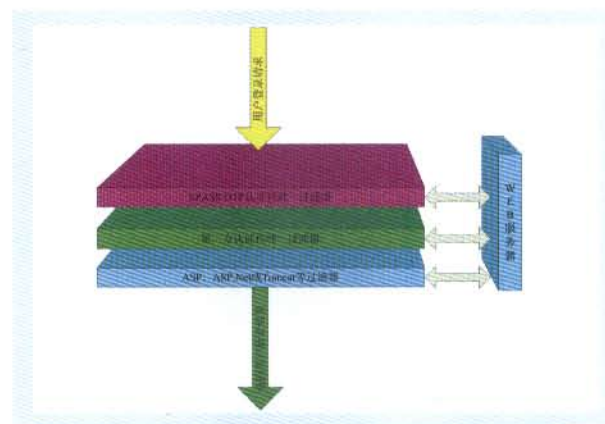
■ 不可复制性：动态口令与口令令牌是紧密相关的，不同的口令令牌产生不同的动态口令。而且口令令牌是密封的，令牌内密钥数据一旦断电就会丢失。因此也就保证只有拥有口令令牌的用户才能使用动态口令，其他用户无法获得，也无法共享。

■ 方便性：口令令牌随身携带，动态口令显示在令牌上，无需再为记忆复杂的、定期更改的密码而烦恼。

■ 危险及时发现：口令令牌随身携带，一旦遗失或失窃，就会及时发现、及时挂失，把损失降到最小。

多系统集成方案是指将多家供应商提供的动态口令身份认证解决方案集成为一个完整的解决方案，各个系统互相协作完成整个身份认证功能。可能的集成包括相同技术方案集成（比如时间同步认证技术方案和时间同步认证技术方案）和不同技术方案集成（比如事件同步认证技术方案和挑战应答非同步认证技术方案）。

下面以北京飞天诚信科技有限公司推出的事件同步身份认证技术方案 ePass OTP 为例，说明其与其它供应商提供的动态口令身份认证方案进行集成的思路和方法。



(图三) ePass OTP 前置模式认证代理位置图

ePass OTP 身份认证系统在多系统集成方案中提供四种架构供选择，具体选择哪一种需要根据具体环境以及具体需求来进行选择。这四种方式分别是 ePass OTP 混用模式、ePass OTP 前置模式、ePass OTP 后置模式以及 ePass OTP 并行模式。

下面以 ePass OTP 前置模式为例说明 ePass OTP 在多系统集成方案中的基本要求、模式特点、具体方案实施过程以及认证流程进行。配置结构如图二所示。ePass OTP 动态口令身份认证系统的认证代理安装位置如图三所示。

### 1. 基本要求：

要求设置两个内容完全相同但名称不同的用户身份认证目录，其中一个由 ePass OTP 保护，另一个由第三方动态口令系统保护，并且 ePass OTP 保护的目录总是首先获得用户的认证请求。

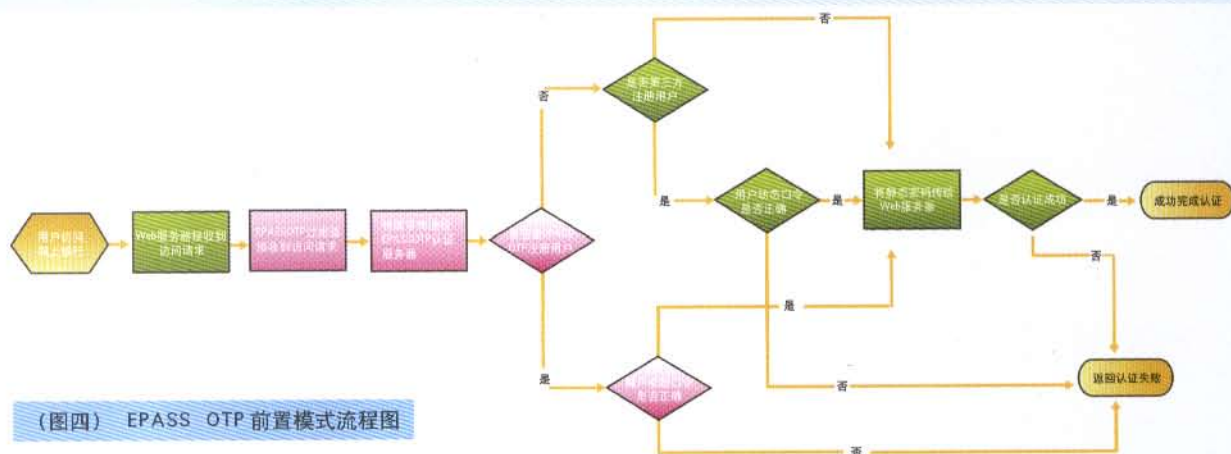
### 2. 模式特点：

该模式适用于第三方动态口令身份认证系统不支持未知用户继续传递认证请求的情况。

该模式在配置方面比另外模式稍微复杂一些。同时多系统认证代理的安装位置不可互换。

根据第三方系统的特点，需要做一定的定制开发，以支持两个系统的集成。

### 3. 方案实施：



该模式下的方案实施主要包括四个方面的内容：  
 (1) 在Web服务器上设置两个内容完全相同而名称不同的认证目录  
 (2) 安装并配置第三方动态口令身份认证系统  
 (3) 根据第三方提供的系统定制修改ePass OTP动态口令身份认证系统  
 (4) 安装并配置ePass OTP动态口令身份认证系统。

#### 4. 认证流程

该模式下认证过程是首先将认证请求传递给ePass OTP，如果ePass OTP确认该用户是其注册用户，则按照正常处理流程进行处理，如果不是其注册用户，则ePass OTP将认证请求传递到由第三方动态口令身份认证系统保护的认证目录（传递的过程对用户来说是透明的，并不需要用户进行任何操作），此时由第三方动态口令身份认证系统按照常规处理流程处理认证请求。

具体的流程如图四所示。

多系统集成方案的主要受益对象是银行和网银用户，下面对其进行简单的分析和整理。

##### ○ 对银行的好处

- 避免因为某个供应商不能及时提供服务（比如动态口令令牌供货不足）而导致整个系统受到影响。
- 长期的合作过程中，完成对供应商的考察，选择性性价比最高的供应商，有利于降低成本。

- 促使供应商提供高性价比的产品和服务。
- 促使供应商不断升级其系统，并使用新技术、推出新产品以应对新的安全风险。
- 促使供应商不断改进其系统的易用性，帮助银行工作人员提高工作效率、降低管理维护成本以及降低出错的机会。

- 向用户提供多样化的选择，树立良好的公众形象。

##### ○ 对网银用户的好处

- 可以根据自己的需要选择合适价格的动态口令令牌。
- 可以根据自己的爱好选择喜欢的款式。
- 促使安全方案提供商在必要的时候提供良好的服务，比如令牌损坏等。

网银的安全有赖于银行、安全服务提供商和网银用户的共同努力，这其中任何一个环节的疏忽都可能带来网银的安全风险。另外，随着技术的发展，新的安全威胁还会继续出现，所以除了有效利用当前的安全措施来解决当前的安全问题以外，还应持续保持对网银新的安全威胁以及新的安全技术的关注，以便能够及时采取有效措施防范网银可能出现的安全威胁。