OTP 与应用系统的集成方法

OTP 动态令牌是一种新型的强身份认证的信息安全产品，由于其具有使用简单，携带方便，安全性高，美观时尚等优点，已经广泛应用在网银系统，电子办公系统，网络游戏，网络支付等众多领域。

OTP 原理：

OTP 动态密码的产生主要是通过内置在硬件中不可导出的密钥与一个变化因子通过安全算法进行计算完成的。即：

算法{密钥（也称为种子），动态因子（时间，事件，冲击响应……）}＝OTP 口令

算法

可以看到算法有两个输入因子：密钥和动态因子。算法的好坏也决定了 OTP 的安全程序，一般算法应该考虑几点因素：

- 权威性：一个算法是需要经过长时间的研发积累，经过长期广泛的市场验证才能够走向成熟。真正成熟算法的研究需要几年，甚至十几年的时间。坚石诚信 ET 系列动态令牌采用 OTP 领域中公认的最具权威的 OATH 国际组织的安全算法。算法的安全性得到了有效保障。自定义算法未被广泛验证和认可，安全性是一个未知数。

- 安全性：OTP 的算法一般不采用对称加解密算法，如：3DES，AES 等。而采用单向散列算法。原因是这样的，拿时间型令牌说明，密钥＋时间（动态因子）＝OTP，时间是知道的，每分钟产生的动态口令能通过硬件知道，3DES 算法也是公开的，这样就有反推出密钥的可能性。而单向散列算法，即使知道通算法计算的结果 OTP，由于算法保证单向，那么从根本上就断绝了反推密钥的途径。

- 效率/耗电：OATH 算法是国际 OTP 领域中公认的安全算法。坚石诚信 ET 系列动态令牌的 OATH 算法单次运行时间<1ms，用时极短，耗电极少。保证电池能够正常使用 3 年以上。按键开关显示 OTP 设计，更能保证电池寿命可长达 5 年以上。

密钥

- 唯一性：每个动态令牌中的密钥都是唯一且不相同的，每个动态令牌与不同的用户绑定，那么该令牌中的密钥就代表这个用户的身份。坚石诚信 ET 系列 OTP 动态令牌产品的密钥符合 OATH 组织规定的 160 位（20 字节）长度。

- 不可复制：动态令牌硬件保证密钥不可导出，断电即毁。动态口令的计算在硬件内部完成。保证了密钥的安全。

- 产生/生产：两种模式保证了 OTP 密钥的唯一性：软实现（符合 FIPS140-2 标准），硬实现（使用国密办认证的硬件加密卡）。生产时密钥以密文的方式烧入到智能卡中（智能卡由专门的授权的人员负责，读卡器、通讯协议、COS 都是自主研发，不公开），使用工控机烧入动态令牌密钥时，智能卡的 COS 会将烧入成功的密钥删除，所有的密钥烧录成功完成后，智能卡中就没有密钥了。

动态因子

动态因子可以有多种选择，目前较多使用的有如下 3 种：

时间型：以时间为变化因子
事件型：以每次触发计算动态口令的计算事件行为为变化因子
冲击响应：以服务器产生的随机数为变化因子

目前国内以时间型最为流行。

- 精确性：动态令牌硬件中的时钟芯片的精确性保证 OTP 计算的准确性。当时钟芯片中的时间与计算机服务器的时间都符合标准时间，才能保证 OTP 认证系统的流畅运行。坚石诚信 ET 系列动态令牌对每只出厂的动态令牌中的时钟芯片及晶振都做了精确调整，保证每年内时间误差不超过 2 分钟。

- 认证窗口：认证窗口是用于调整硬件中时钟芯片的时间与计算机服务器时间偏差的一种手段。一般都是在计算机服务器中按照窗口范围计算多个动态口令，硬件产生的动态口令在这个范围内就视为认证通过。

OTP 动态令牌与应用系统集成：

提起动态令牌，大家都会想到认证服务器，而这个认证服务器又怎么应用到实际的应用系统中呢？在这里做一个分析和说明，帮助广大用户能够更好的使用 OTP 动态令牌这种身份认证产品。

从上述的 OTP 原理部分中可以看出，服务器端是在一个范围内计算出多个 OTP，然后检验客户端硬件产生的 OTP 口令是否在这个范围内。那么服务器端只要能够完成这样的验证就可以了。实际上所有厂家的 OTP 认证服务器都是建立在这个认证基础上的。即认证接口是服务器的本质和核心。

而 OTP 厂商提供的服务器软件无非就是在这个认证接口上增加其他的功能，如：数据库表定义、令牌管理工具、Radius 支持、各种认证代理插件等，但最终都会归到这个认证接

口完成最终的认证。另外，在某些情况下，OTP 厂商也会将认证服务器软件安装到硬件服务器上，将硬件设备一同销售给客户。

从上面的分析可以看出，可以有 3 种模式将 OTP 系统集成到应用系统中，即：核心接口开发模式、服务器接口开发模式和服务器代理模式。下面就来说明一下它们的特点。

核心接口开发模式

该模式是最为灵活，集成最为方便简单，与应用最为紧密结合的模式。由于与关联少，也是目前大型项目中常采用的模式（如：中国银行，同花顺证券系统，上海期货交易所等都是采用接口形式的开发）。该模式由OTP厂商提供认证和同步两个API接口供系统集成调用。接口不与数据库连接，应用系统使用系统中原有的数据库连接方式，将密钥与调整值从数据取出带入到接口中进行认证，认证成功后，将新的调整值写回到数据库中。数据库中用户存储令牌信息的数据表可以根据应用系统实际情况进行设计，方便灵活。
集成过程如下：

（1） 在数据库中增加一张用于存储 OTP 动态令牌信息的数据表。里面至少存储以下字段：“令牌号”（背面条形码）、“密钥”（authkey）、“成功值”（currsucc）、“漂移值”（currdft）。其中令牌号和密钥都可以用字符串形式，成功值和漂移值接口中要用到 uint64（BigInteger）和 int 类型。

（2） 在系统的用户表中增加一个存“令牌号”的字段，存储与用户绑定的令牌号。

用户在登录时，输入用户名和 OTP 传给服务器端。服务器通过用户名到用户表中得到“令牌号”，再通过这个“令牌号”到令牌表中得到“密钥”，“成功值”和“漂移值”，带入到接口中进行认证或同步，认证或同步成功后将返回的值写回数据库中保存。认证或同步失败时，不要将这两个值写回数据库。

服务器接口开发模式

这种模式下，需要安装 OTP 厂商提供的服务器软件，安装 OTP 服务器软件的机器就是 OTP 认证服务器。可以在服务器端调用服务器接口，或者在 web 服务器机器上调用代理接口将 OTP 集成到应用系统中。

服务器接口是指应用系统直接调用这个接口，接口直接调用数据库取得需要的数据，完成认证，如下所示：

代理接口是指通过认证代理，认证代理再将认证信息传给服务器进行认证，如下所示：

综上，可以认为认证服务器是在服务器接口基础上封装好的有图形操作界面的软件。代理接口是在使用到负载均衡时会采用的手段，一个代理会根据优先级设置查找多个认证服务器，一个服务器也可以按照优先级设置接收多个认证代理的请求。坚石诚信的 OTP 认证服务器软件采用了多种优化措施，以及多进程/多线程的高效处理，每秒钟能够完成 3300 次以上的认证。就目前实际情况而言，不超过千万级别的用户，都是没有必要做负载均衡的。

在这种模式下，需要数据库中按照 OTP 厂商定义的表结构创建数据库表，在调用接口中的 API 函数前，都需要先与数据库进行连接。集成过程如下：

（1） 安装 OTP 认证服务器软件，包括 OTP 认证服务和 OTP 管理工具。
（2） 在 OTP 管理工具中创建数据库及符合 OTP 厂商定义的数据库表。
（3） 在应用系统中调用服务器接口 API 或者代理接口 API 完成认证。

服务器代理模式

该模式主要是针对一些具体应用而设计，不需要进行 API 接口开发就可以完成集成。由于其关联的东西较多，且软件界面都会有 OTP 厂商的标识，相对而言灵活性较差。这些具体应用一般包括：IIS/Apache 网站保护、VPN Radius 登录保护、Windows 登录保护、Linux 登录保护、Citrix 远程登录保护、OWA 登录保护等。集成过程如下：

（1） 安装 OTP 认证服务器软件，包括 OTP 认证服务和 OTP 管理工具。
（2） 根据不同的应用，安装对应的认证代理安装包。
（3） 在应用中配置 OTP 认证保护。

下面我们用一个表格来对比一下上述三种集成的特点：

	核心接口开发	服务器接口开发	服务器代理
集成工作量	1—2 天	1 周	1 周
API 接口调用	2 个接口	服务器：70 个接口 代理：20 个接口	不需开发
手机/短信令牌	支持	支持	支持
认证级别	千万级用户	千万级用户	千万级用户
灵活性	根据实际情况全部灵活调整	根据实际情况部分可调整	调整需订制

费用	免费	有偿使用（一般报价几万）	有偿使用（一般报价几万）
支持语言	C，Java 等各种支持 DLL/SO 调用的开发语言	C，Java 等各种支持 DLL/SO 调用的开发语言	无开发
支持系统	Windows 全系列、Linux 全系列、Unix、Solaris、FreeBSD	Windows 全系列、Linux 全系列、Unix、Solaris、FreeBSD	Windows 全系列、Linux 全系列、Unix、Solaris、FreeBSD