Atitit 流行的密码安全机制二次密码以及otp一次性密码

OTP全称叫One-time Password,也称动态口令，是根据专门的算法每隔60秒生成一个与时间相关的、不可预测的随机数字组合，每个口令只能使用一次，每天可以产生43200个密码，其中被广泛关注的当属深圳市海月通信技术有限公司独立研发的手机动态口令。

**目录**

[简介](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp01)[传统静态密码的缺点](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp02)[OTP身份认证系统组成](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp03)[1.动态口令认证服务器群](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp03_a)[2.动态口令管理服务站点](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp03_b)[动态口令认证系统特点](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp04)[应用范围](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp05)[一次性可编程芯片](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp06)[OTP](http://www.seamoon.com.cn/one_time_password_baike04.asp" \l "otp07)

**简介**

动态口令是一种安全便捷的帐号防盗技术，可以有效保护交易和登录的认证安全，采用动态口令就无需定期更换密码，安全省心，这是这项技术的一个额外价值，对企事业内部应用尤其有用。动态令牌即是用来生成动态口令终端。

**传统静态密码的缺点**

相比较动态口令认证方式，静态口令认证缺点如下：  
　　（1） 为了便于记忆，用户多选择有特征作为密码，所有静态口令相比动态口令而言，容易被猜测和破解；  
　　（2） 黑客可以从网上或电话线上截获静态密码，如果是非加密方式传输，用户认证信息可被轻易获取；  
　　（3） 内部工作人员可通过合法授权取得用户密码而非法使用；　  
　　静态口令根本上不能确定用户的身份，其结果是，个人可以轻松地伪造一个假身份或者盗用一个已有使用者的身份，给企业造成巨大的经济和声誉损

在业务中，为安全起见，常常需要二次验证。其流程一般为，密码验证之后，需要再次输入一个一次性的密码（一般为位数较短的数字），才能完成验证。二次验证一般需要同时验证设备的唯一性。

从验证方式上看，二次验证可以通过短信验证或 APP 验证（Google Authenticator）。对于短信验证，优点是操作方便，不需安装额外的 APP；缺点是实时性较差，依赖短信，有被窃听的风险。APP 方式正好相反。

OTP 一般分为计次使用（HOTP）以及计时使用（TOTP）两种，计次使用的 OTP 产出后，可在不限时间内使用；计时使用的 OTP 则可设定密码有效时间，从 30 秒到两分钟不等，而 OTP 在进行认证之后即废弃不用，下次认证必须使用新的密码，增加了试图不经授权存取有限制资源的难度[1](http://wulfric.me/2014/09/design-of-sms-verification/" \l "fn:1" \o "维基：一次性密码 ↩)。

Google Authenticator 的二次验证也是使用的 OTP。其核心原理是：服务器和客户端（一般是Google Authenticatorapp）保存同一份密钥，客户端根据该密钥和当前时间戳计算得到 6 位数字，发到服务器，服务器根据同样的算法得到 6 位数字。做比较之后判断客户端传来的数字是否合法。详述如下[2](http://wulfric.me/2014/09/design-of-sms-verification/" \l "fn:2" \o "Google账户两步验证的工作原理 ↩)：

## 2FA (Two Factor Authentication/雙因素身份驗證) 與 One Time Password （一次性密碼）

在2FA (Two Factor Authentication/雙因素身份驗證）中， SaaS (Software as a Service) 通常需要使用手機等裝置才能獲得密碼以外的其他身份驗證。現今，每個人都有手機，通常手機不與別人共用。這意味著手機也可以用來識別一個人。因此，在2FA中，裝置將產生OTP （One Time Password/一次性密碼) 以識別該裝置屬於該使用者，並且SaaS (Software as a Service)將允許使用者使用該一次性密碼登入。在2FA 中的OTP通常每隔一定的秒數例如每30秒產生一次密碼。一次性密碼將透過使用安裝在裝置中的安全令牌(security token)生成。

## 裝置驗證和無密碼(Passwordless)登入

今天，大多數人不會共用他們的個人電腦， 這意味著員工的個人電腦也可以用來識別這個人。裝置認證是透過使用裝置中安裝的證書數據(Certificate Data)來認證對SaaS (Software as a Service) 的存取。只要使用者使用的裝置被授權， 使用者就可以從任何地方使用他們擁有的裝置存取雲端服務。並且， 如果裝置可以代表一個人， 那麼可以使用裝置來認證一個人， 這樣就可以提供無密碼登入。在無密碼登入時， 裝置將成為登入身份證明， 使用者不需額外輸入密碼。由於沒有密碼， 所以沒有密碼被破解的風險， 使用者也不需要記住密碼。

# [信息安全] 4.一次性密码 && 身份认证三要素

2018-01-19阅读 4610

在信息安全领域，一般把****Cryptography****称为****密码****，而把****Password****称为****口令****。日常用户的认知中，以及我们开发人员沟通过程中，绝大多数被称作密码的东西其实都是Password（口令），而不是真正意义上的密码。本文保持这种语义，采用密码来代指Password，而当密码和口令同时出现时，用英文表示以示区分。

# **0. OTP一次性密码**

OTP是One Time Password的简写，即一次性密码。在平时生活中，我们接触一次性密码的场景非常多，比如在登录账号、找回密码，更改密码和转账操作等等这些场景，其中一些常用到的方式有：

1. 手机[短信](https://cloud.tencent.com/product/sms?from=10680" \t "https://cloud.tencent.com/developer/article/_blank)+短信验证码；
2. 邮件+邮件验证码；
3. 认证器软件+验证码，比如Microsoft Authenticator App，Google Authenticator App等等；
4. 硬件+验证码：比如网银的电子密码器；

这些场景的流程一般都是在用户提供了账号+密码的基础上，让用户再提供一个一次性的验证码来提供一层额外的安全防护。通常情况下，这个验证码是一个6-8位的数字，只能使用一次或者仅在很短的时间内可用（比如5分钟以内）。

# **1. HOTP基于消息认证码的一次性密码**

HOTP是HMAC-Based One Time Password的缩写，即是基于HMAC（基于Hash的[消息认证码](http://www.cnblogs.com/linianhui/p/security-based-toolbox.html" \l "auto_id_12" \t "https://cloud.tencent.com/developer/article/_blank)）实现的一次性密码。算法细节定义在RFC4226（[https://tools.ietf.org/html/rfc4226](https://tools.ietf.org/html/rfc4226" \t "https://cloud.tencent.com/developer/article/_blank)），算法公式为： HOTP(Key,Counter)  ，拆开是 Truncate(HMAC-SHA-1(Key,Counter)) 。

1. Key：密钥；
2. Counter：一个计数器；
3. HMAC-SHA-1：基于SHA1的HMAC算法的一个函数，返回MAC的值，MAC是一个20bytes（160bits）的字节数组；
4. Truncate：一个截取数字的函数，以3中的MAC为参数，按照指定规则，得到一个6位或者8位数字（位数太多的话不方便用户输入，太少的话又容易被暴力猜测到）

# **3. 身份认证三要素**

首先解释下什么是身份认证？其实很简单，就是让对方相信你就是你。那么如何让对方相信你就是你呢？按照你能提供的信息的等级来划分，大致有如下三种信息可以证明你就是你自己：

1. 你所知道的信息：比如我们最广泛使用的“****用户名+密码****”，因为只有你自己知道“****用户名+密码****”这个信息组合，那么当你把这个组合提供给我的时候，我就可以相信你就是你。
2. 你所拥有的信息：假如你的“用户名+密码”泄露给了第三方，这个时候你就会有被第三方冒充的危险了。怎么办呢，再进一步提供一个只有****你自己拥有的信息****，即可防止被第三方冒充的危险。
3. 你所独有的信息：再假设一下，你拥有的信息也被泄露给了第三方，这个时候你又会面临被冒充的危险。再进一步，提供一个只有****你自己所独有的的信息****，比如你的指纹，虹膜，面部特征等等。

## **3.1 2SV 两步验证（Two Steps Verification）**

两步验证现在是一个再加强认证安全方面广泛使用的一个解决方案。比如Google的2SV（[https://www.google.com/landing/2step/](https://www.google.com/landing/2step/" \t "https://cloud.tencent.com/developer/article/_blank)），Microsoft的2SV（[https://support.microsoft.com/zh-cn/help/12408/microsoft-account-about-two-step-verification](https://support.microsoft.com/zh-cn/help/12408/microsoft-account-about-two-step-verification" \t "https://cloud.tencent.com/developer/article/_blank)）等等，通常的做法是当用户输入了"****用户名+密码****"的基础上，会让用户再提供一个****一次性密码****（以短信、邮件，或者动态密码生成器app的方式发放给用户）。再有比如在一些服务中需要用户额外设置的安全问题，比如“你的出生地在哪？”等等此类。

## **3.2 2FA双因素认证（Two Factor Authentication）**

2SV有个孪生兄弟2FA（双因素认证：Two Factor Authentication），那么关于2SV和2FA有什么区别呢，比如让用户在“****用户名+密码****”的基础上提供的额外的****一次性密码****，关于这个****一次性密码****到底是属于“****你所知道的信息****”还是“****你所拥有的信息****”呢？并没有明显的区分界限，有兴趣的可以看看这里的讨论：https://security.stackexchange.com/questions/41939/two-step-vs-two-factor-authentication-is-there-a-difference 。 如果你觉得这个一次性密码属于“****你所知道的信息****”，那么你可以认为它是2SV；如果你觉得这个一次性密码属于“****你所拥有的信息****”，那么你可以认为它是2FA。

总结来说，2FA就是使用了身份认证中的2个要素。

下面是身分認證的三種型態:

* What you know (你所知道的資訊，例如帳號、密碼...)
* What you have (你所擁有的物件，例如金鑰、憑證...)
* What you are (你本身擁有的屬性，例如指紋、掌形、靜脈、五官特徵...)

在資訊安全中，較安全的身分認證方法一般會要求在上面三種型態中，選擇兩樣的組合來進行驗證，則稱為雙因素認證(2-Factor Authentication)。  
而 PKI 或 OTP 的方法，可以說是「What you have」的代表。PKI 又有分軟體檔案式的 PKI Token 或硬體式的 PKI Token。後者硬體式的 Token 相對上是比較安全的。  
硬體式的 PKI，如 金融IC卡、自然人憑證(儲存於IC卡中)、USB Token 等都是常見的應用。我們嘗試從下面四個面相來比較 PKI 與 OTP 的優缺點。

安全性 –  
OTP tokens 相對 PKI 而言比較不安全。因為 OTP 的本質仍然是以密碼為基礎。相對於 USB 或 SmartCard，本質上完全是「Something you have」，有唯一性，如果憑證被偷的話，是很明確的。

使用方便性 –  
OTP tokens 由於需要讀取上面顯示的一次性密碼然後以鍵盤輸入，所以仍然有點麻煩。USB Token 插上即可，是最簡單的。而 SmartCard、IC卡則需要額外的讀卡機，對有些使用者而言不是很熟悉的操作方式。

可攜性 –  
OTP 型式的 Token 由於不需要與電腦界接，可以獨立運作，所以可攜性最廣泛。不只用電腦連線時可以使用，使用電話存取網銀也可以用、甚至連 ATM 也可以用。  
USB token 體積小攜帶方便，幾乎現代看得到的電腦都支援，但仍然需要界接，有些情況還需要裝驅動程式才能讀取。  
Smartcards 需要額外的讀卡機與驅動程式，相對而言比較不便。

應用彈性-  
OTP tokens 只能用於認證用途，無法攜帶任何的憑證於其上，所以不容易做到數位簽章、加密與不可否認性等數位憑證的應用。因此 USB Token 以及 SmartCards 可以提供更多的功能選擇。

## 获取密码的方法

[编辑](https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/javascript:;)

### 文字短信

由于文字短信是很普及可以接触到的技术，成为了动态密码传递的方式中最常见的一种方式。但由于移动网络传递短信时的安全性问题，这种方式对于[中间人攻击](https://baike.baidu.com/item/%E4%B8%AD%E9%97%B4%E4%BA%BA%E6%94%BB%E5%87%BB" \t "https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/_blank)的抗性较低。

### 智能手机

对于有成本考量但希望获取较高安全性的公司，会规划使用在智能手机上安装移动应用程序产生动态密码。

### 特殊载具

追求更高的安全性而可以接受较高的成本时，会使用独立的载具存放产生动态密码所需的密钥，避免被[中间人攻击](https://baike.baidu.com/item/%E4%B8%AD%E9%97%B4%E4%BA%BA%E6%94%BB%E5%87%BB" \t "https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/_blank)（文字短信）或是被透过移动设备的系统漏洞而获取密钥（智能手机）。因为载具独立而内置配有电池，因此会有寿命与回收的问题。

另外有折衷的方案是类似[YubiKey](https://baike.baidu.com/item/YubiKey" \t "https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/_blank)使用USB供电，透过模拟USB键盘输入的方式，但由于与计算机有实体接触，安全性在严格的考量下不会与完全隔离的方案相同。

### 网页服务

### 纸张

在某些国家的在线银行系统会采用预印的方式提供一次性的密码。

## 优势

[编辑](https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/javascript:;)

动态密码的解决方案有以下几个优点：

解决用户在密码的记忆与保存上的困难性。

由于密码只能使用一次，而且因为是动态产生，所以不可预测，也只有一次的使用有效性，可以大为提升使用的安全程度。

基于这些优点，有越来越多的银行金融业甚至是游戏业使用OTP解决方案，来提升保护其用户的安全性。

## 挑选动态密码技术

[编辑](https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/javascript:;)

以下供您参考，为组织选择适合的[动态密码](https://baike.baidu.com/item/%E5%8A%A8%E6%80%81%E5%AF%86%E7%A0%81/3621186" \t "https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/_blank)，同时支持两种密码器混合使用。

|  |  |  |
| --- | --- | --- |
|  | **硬件令牌** | **短信密码** |
| **安全性** | 最高 | 较高 |
| **便捷性** | 高 | 最高 |
| **表现形式** | 硬件，随身携带 | 发送手机短信 |
| **移动办公** | 100%解决方案 | 需[短信网关](https://baike.baidu.com/item/%E7%9F%AD%E4%BF%A1%E7%BD%91%E5%85%B3/10179707" \t "https://baike.baidu.com/item/%E4%B8%80%E6%AC%A1%E6%80%A7%E5%AF%86%E7%A0%81/_blank)支持 |
| **实时性** | 高 | 较高（依赖网关速率） |

短信认证核心优点是费用低，无需携带、无需更换。　硬件令牌核心优点是在产品质量可靠情况下可以在任何地方进行