

# **ActivCard 动态口令身份认证系统**

---

## **Token One 令牌使用手册**



Version:2.0

北京启迅网安科技有限公司

[www.activcard.cn](http://www.activcard.cn)

2004 年 10 月

# 目 录

概 述.....	1
0.1 什么是动态口令.....	1
0.2 为什么需要使用动态口令.....	2
第一章 ActivCard 令牌介绍 .....	5
1.1 令牌外观.....	5
1.2 状态栏标志图例.....	6
1.3 操作提示信息.....	7
第二章 操作指南.....	8
2.1 第一次使用令牌.....	8
2.2 同步认证方式.....	10
2.3 挑战/应答认证方式.....	12
2.4 修改令牌 PIN 码 .....	14
2.5 解除令牌 PIN 码锁定 .....	16
2.6 令牌手工重同步操作.....	18



## 概 述

### 0.1 什么是动态口令

动态口令(Dynamic Password),又叫"一次性口令(OTP: One Time Password)",是由电子令牌(Token)等手持终端设备生成的,根据某种加密算法,产生的随某一个不断变化的参数(例如时间,事件等)不停地、没有重复变化的一种口令。是为了解决传统静态的、固定的口令和密码存在的无法解决的缺陷,而设计的一种密码体制,以保护用户的关键数据资源。

动态口令,也就是一次性口令的主要思路是:在登录过程中加入不确定因素,使每次登录过程中传送的信息都不相同,以提高登录过程安全性。例如,登录密码=MD5(用户名+密码+时间),系统接收到登录口令后做一个验算即可验证用户的合法性。

用以产生动态口令的因素选择方式大致有以下几种:

- **口令序列** 口令为一个单向的前后相关的序列,系统只用记录第 N 个口令。用户用第 N-1 个口令登录时,系统用单向算法算出第 N 个口令与自己保存的第 N 个口令匹配,以判断用户的合法性。由于 N 是有限的,用户登录 N 次后必须重新初始化口令序列。
- **挑战/回答** 用户要求登录时,系统产生一个随机数发送给用户。用户用某种单向算法将自己的秘密口令和随机数混合起来发送给系统,系统用同样的方法做验算即可验证用户身份。
- **时间同步** 以用户登录时间作为随机因素。这种方式对双方的时间准确度要求较高,一般采取以分钟为时间单位的折中办法。
- **事件同步** 这种方法以挑战/回答方式为基础,将单向的前后相关序列作为系统的挑战信息,以节省用户每次输入挑战信息的麻烦。但当用户的挑战序列与服务器产生偏差后,需要重新同步。

动态口令的生成设备有以下几种:



- **Token Card (令牌卡)** 用类似计算器的小卡片计算一次性口令。对于挑战/回答方式, 该卡片配备有数字按键, 便于输入挑战值; 对于时间/事件同步方式, 该卡片每隔一段时间就会重新计算口令; 有时还会将卡片作成钥匙链式的形状, 某些卡片还带有 PIN 保护装置。
- **Soft Token (软件令牌)** 用软件代替硬件, 某些软件还能够限定用户登录的地点。
- **IC 卡** 在 IC 卡上存储用户的秘密信息, 这样用户在登录时就不用记忆自己的秘密口令了

#### 动态口令的认证方法和原理

当令牌或其他终端设备持有者将令牌中计算出来的某一时刻的口令输入计算机的登录窗口时, 在计算机(网络)另一端的认证服务器软件会根据相同的算法和同样的要素计算出这一时刻对应于该令牌的认证口令, 这个口令用来与令牌产生的口令比对, 进行身份认证, 对比相同, 则通过认证; 对比不同, 则不能通过认证。

于是由动态口令令牌和计算机(网络)上的认证服务器软件就构成了一个用户身份鉴别的认证系统, 这是一种基于时间同步的认证系统。

## 0.2 为什么需要使用动态口令

在现实生活中, 我们个人的身份主要是通过各种证件来确认的, 比如: 身份证、户口本等。计算机世界与现实世界非常相似, 各种计算资源(如: 文件、数据库、应用系统)也需要认证机制的保护, 确保这些资源被应该使用的人使用。在大多数情况下, 认证机制与认证和记账也紧密结合在一起。

目前各类计算资源主要靠固定口令的方式来保护。比如要使用一个 Windows 2000 系统, 首先必须在该 Windows 2000 系统上拥有一个账户和相应的口令。当登录 Windows 2000 时, 系统会要求输入账户和口令。在账户和口令被确认了以后, 就可以使用 Windows 2000 系统了。

### 传统固定、静态密码的缺陷

这种以固定口令为基础的认证方式存在很多问题, 最明显的是以下几种:



1. 网络数据流窃听（**Packet Sniffer**）：由于认证信息要通过网络传递，并且很多认证系统的口令是未经加密的明文，攻击者通过窃听网络数据，就很容易分辨出某种特定系统的认证数据，并提取出用户名和口令。

2. 认证信息截取/重放（**Record/Replay**）：有的系统会将认证信息进行简单加密后进行传输，如果攻击者无法用第一种方式推算出密码，可以使用截取/重放方式。

3. 字典攻击：由于多数用户习惯使用有意义的单词或数字作为密码，某些攻击者会使用字典中的单词来尝试用户的密码。所以大多数系统都建议用户在口令中加入特殊字符，以增加口令的安全性。

4. 暴力破解（**Brute Force**）：也称为穷举尝试，这是一种特殊的字典攻击，它使用字符串的全集作为字典。如果用户的密码较短，很容易被穷举出来，因而很多系统都建议用户使用长口令。

5. 窥探：攻击者利用与被攻击系统接近的机会，安装监视器或亲自窥探合法用户输入口令的过程，以得到口令。

6. 社交工程：攻击者冒充合法用户发送邮件或打电话给管理人员，以骗取用户口令。

7. 垃圾搜索：攻击者通过搜索被攻击者的废弃物，得到与攻击系统有关的信息，如果用户将口令写在纸上又随便丢弃，则很容易成为垃圾搜索的攻击对象。

虽然用户可以通过经常更换密码和增加密码长度来保证安全，但这同时也给用户带来了很大麻烦。一般情况下，用户不会在一个相对短的时间间隔内频繁地更换自己的口令，因此这种口令基本上是静态方式，而且口令在网上一般以明码传输，口令很容易因为被窃听、盗取和截获导致用户身份被盗用，因而这种静态口令不安全因素是网络系统普遍存在的隐患。据估计，对网络系统的非法入侵和攻击事件中，有六成源于对静态口令的攻击和突破，基于口令认证的身份鉴别的安全性成为网络安全中迫切需要解决的一个问题。

### 动态口令与传统的静态口令相比的优势

1. 动态性：用户的动态口令随设定的时间或事件等变量自动变化，无需人工干预，某一时刻的产生的动态口令不能在其他时刻使用。



2. 一次性：任一时刻产生的动态口令在其失效前只能被用户使用一次，否则，系统将视其为非法行为而报警。

3. 随机性：动态口令是随机生成、无规律的。即使本次口令被窃听成功，也难以由此猜出下次的口令。

4. 多重安全性：用户的动态口令令牌产生的动态口令与用户名、静态口令等多因素结合实现多重认证。即使电子令牌丢失，用户仍可在应急状态下利用用户名和静态口令进行用户身份认证。而其他非法持有者，单靠令牌无法实现登录及认证。

5. 通用性：用户操作的客户端无需增加任何软件，只需在提示输入动态口令时键入当时令牌上显示的口令。在认证服务器端，采用 PPP、RADIUS 等标准协议实现被访问对象与认证服务器的之间信息交换，可方便地在网络环境下实现身份认证。

6. 可管理性：统一的身份认证方式和动态口令生成方式，能大大减小在分发密码、支持服务、密码丢失、密码更改及身份管理等各个方面的开销和成本。

基于以上静态密码的缺陷和动态口令的优势，因此我们推荐客户在重要的计算机和数据资源上使用动态口令身份认证。

本使用手册描述了 **ActivCard One** 令牌的全部功能和可进行的操作菜单，并且列出了各种功能操作的步骤。

本手册可作最终用户的操作手册用于指导使用 **ActivCard One** 令牌。如有任何不能确定的问题，请联系您的系统管理员、系统集成商或者直接与我们联系。

启迅·北京	Tel:86-10-51299660	E-mail:sales@activcard.cn
启迅·深圳	Tel:86-755-61281330	E-mail:Shenzhen@activcard.cn
启迅·上海	Tel:86-21-28666799	E-mail:shanghai@activcard.cn



## 第一章 ActivCard Token One 令牌介绍

### 1.1 令牌外观

ActivCard(ActivIdentity)公司的 Token One v2.0 令牌产品大小为标准信用卡大小，尺寸为：82mm x 52mm x 5mm，外观与计算器非常相似。重量 25 克，机身轻薄，便于携带。

令牌正面按功能划分为二个部分：显示屏幕区域(LCD),功能键盘区域(10 个数字键和 2 个功能键)。请见下图(图 1-1):



图 1-1 ActivCard 令牌示意图

功能键盘用来输入保护令牌的 PIN 码，调出菜单以及显示其他辅助功能。

功能键盘区有十个数字键，一个  键作为调出菜单和退格/删除键，一个  键作为令牌开/关机键以及确认(回车)键。



显示屏幕区域显示由令牌产生的动态口令、其他相关功能提示以及结果；

显示屏幕又分为二行，上部小图标显示的是令牌的状态信息；下部大字体显示的是令牌的菜单、动态口令以及文字提示信息。请见下图(图 1-2)：

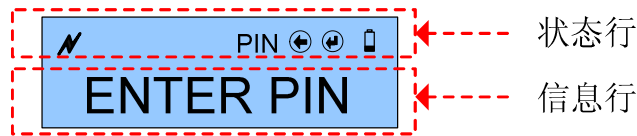


图 1-2 LCD 显示信息示意图

### 1.2 状态栏标志图例

图标	描述
	无线通信状态 令牌正在与初始化设备(ActivCoupler)通信中
CHAL	挑战数等待状态 令牌等待输入挑战码(挑战/应答模式)
INIT	初始化状态 手动初始化准备就绪或者正在进行中
STAT	辅助信息显示状态 查看令牌管理参数(令牌 SN 号、内部时钟、口令产生计数器等)
PIN	PIN 码修改状态 此状态提示 PIN 码修改准备就绪或者正在进行中
	辅助功能键(兼回退键)可用状态 提示可按  键进入功能菜单，并且此键兼具回退/删除功能
	确认状态 提示可按  键进入某具体功能或关闭令牌电源
	提示电池电量不足并尽快更换 已使用令牌内部应急后备电池，如不更换电池将导致令牌损坏



## 1.3 操作提示信息

信息	描述
ENTER PIN	开机时提示输入 PIN 码
CHANGE PIN	提示修改 PIN 码
NEW PIN	提示输入新的 PIN 码
CONFIRM	提示再次输入新的 PIN 码，以便确认
COMPLETE	完成(修改 PIN 码、令牌解锁等操作成功后提示)
VIEW SN	菜单选项-提示是否查看令牌 SN 号(令牌序列号)
VIEW CLOCK	菜单选项-提示是否查看令牌内部时钟参数值
VIEW COUNT	菜单选项-提示是否查看令牌内部动态口令累计生成计数器值
LOCKED	提示令牌已经由于连续输错 PIN 码次数达到上限而被锁住，此时不要试图重试 PIN 码，需要联系系统管理员帮助解锁
ERROR	提示 PIN 码输入不正确
LAST TRY	提示只能最后一次允许输入 PIN 码 如果此时 PIN 码输入仍不正确，令牌将会自动被锁住
CHANGE BAT	提示必须更换电池 在更换电池以前，令牌的其他功能都将无法使用
WAIT	提示令牌在输入一个错误的 PIN 码后被临时锁定



## 第二章 操作指南

用户在第一次领到令牌的时候，会随同令牌领到一个由系统管理员为分配令牌分配的一个初始 PIN 码。令牌设置 PIN 码的必要性在于，只有知道这个 PIN 码的人，才可以通过这个令牌产生真正的动态口令。以保证即使令牌万一丢失、被盗后，不至于被他人冒用。令牌的 PIN 码有最大的错误尝试次数限制，如果连续输入错误的 PIN 码次数达到上限后，令牌将会被自行锁住，这个时候必须联系系统管理员才能解锁。


**注意：**切勿自行尝试解锁，因为解锁码输入错误次数达到上限时，令牌将会自毁。

### 2.1 第一次使用令牌


令牌第一次使用时，系统可能会设定令牌为第一次使用必须修改 PIN 码，以此来加强令牌的安全性。

如何确定令牌是否设定第一次使用时必须修改 PIN 码呢？请参照以下步骤：

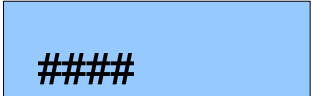
1 请按“ON”键打开令牌电源




屏幕提示：请输入 PIN 码



2 输入随令牌发放的 PIN 码，假设为“8888”



如果 PIN 码输入错误，屏幕会提示错误  
此时令牌会自动关机，请重新回到第一步。





- 3 输入正确的 PIN 码后，如果令牌显示如下图中任一个所示(此图数字为示例，实际使用中显示数字与本图不同)，则说明令牌无须修改 PIN 码，可以正常使用。



如果需要自行修改 PIN 码，请参照“2.4 修改令牌 PIN 码”一节操作指南

- 4 如果输入正确的 PIN 码后，令牌屏幕显示“NEW PIN”字样，则说明第一次使用必须修改 PIN 码。此时请输入您设定的新 PIN 码。注意：因令牌有弱 PIN 检测功能，像“1111”、“1234”这种过于简单的 PIN 码是无效的。



- 5 输入新 PIN 码后，按“ON”键。

要求确认新 PIN 码。



- 6 再次输入相同的新 PIN 码后，按“ON”键。



此时令牌将自动关闭。再次开机就可以正常使用了。



提示：在输入数字时， 键可以用来回退/删除一个字符。



## 2.2 同步认证方式

同步认证方式产生一个一次性的口令。这个动态口令只是把原来系统使用的静态（固定）的口令改换成由令牌产生的，一次性有效的动态口令。其他整个业务流程无需任何改变。

用户只要在需要登录系统的时候，使用手中持有的令牌产生一个口令即可。产生的密码只能使用一次。令牌产生的密码是一次有效的，该口令在通过系统认证过后就立即作废。不再重复使用了。

下述步骤指导您如何产生一个动态口令：

- 1 请按“ON”键打开令牌电源



屏幕提示：请输入 PIN 码

ENTER PIN

- 2 输入您的 PIN 码

####

ERROR

如果 PIN 码输入错误，屏幕会提示错误  
此时令牌会自动关机，请重新回到第一步。

- 3 输入正确的 PIN 码后，如果令牌显示如下图中所示等待输入状态，说明您的令牌开启了“挑战/应答”方式的认证功能，请按“ON”键跳过这个功能。

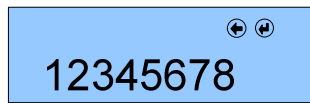
CHAL

如果您的系统有“挑战/应答”方式的认证应用，请参见“2.3 挑战/应答认证方式”。

如果您的令牌不是这种显示，则会直接进入第四步。




- 4 如果您的令牌屏幕上显示如下图类似的一串数字，那么这就是动态口令(此图数字为示例，实际使用中显示数字与本图不同)



注意：令牌在若干秒内如果没有按键，将会自动关机。如果需要这个密码延长显示时间，只需随意按动 0-9 中的任意一个数字键。  
此时按“ON”键则立即关机；  
按“MENU”键就会进入辅助功能菜单状态。

第四步产生的“12345678”就是动态口令，每次使用，此数字串都会不相同。



如果不小心误操作，用“”键回退试一下。如果还无法解除误操作，则几十秒不要按任何按键，令牌会自动关机。关机后请重新从第一步开始操作。




### 2.3 挑战/应答认证方式

挑战/应答认证方式也叫异步认证方式。是动态口令身份认证的一种方式，此种认证方式比同步方式操作相对繁琐，实现相对复杂，所以较少被采用，一般用于对安全性要求更高的场合，比如登陆网上银行等，需要附加认证的情形。


挑战/应答认证方式的流程为：远程认证服务器根据用户的令牌资料产生一个随机的数字串，即“挑战码”，用户得到这个挑战码后，需要把此码输入到令牌中去，令牌根据输入的“挑战码”生成一个“应答码”，然后用户再把此应答码输入登陆窗口，回传给远程认证服务器，远程认证服务器检查密码的正确性，来决定是否许可进入系统或执行操作。

下面我们假设远程认证服务器提示“654321”为本次认证的挑战码，参照以下步骤进行“挑战/应答”认证：



1 请按“ON”键打开令牌电源



屏幕提示：请输入 PIN 码



2 输入您的 PIN 码



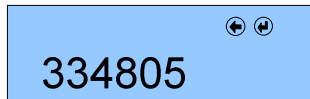
如果 PIN 码输入错误，屏幕会提示错误  
此时令牌会自动关机，请重新回到第一步。



- 3 输入正确的 PIN 码后，如果令牌显示如下图中所示等待输入状态，请通过令牌的数字键盘输入登陆窗口提示的挑战码：654321，并按“ON”键确认。



- 4 如果您的令牌屏幕上显示如下图类似的一串数字，那么这就是根据挑战码 654321 计算出来的“应答码” (此图数字为示例，实际使用中显示数字与本图不同)



注意：令牌将在若干秒内如果没有按键，会自动关机。如果需要这个密码延长显示时间，只需随意按动 0-9 中的任意一个数字键。

此时按“ON”键则立即关机；

按“MENU”键就会进入辅助功能菜单状态。




## 2.4 修改令牌 PIN 码

为了保证令牌不被他人冒用，强烈推荐设置一个不容易被猜解的 PIN 码并经常更换。


令牌在发放给用户使用的时候，系统管理员都做了 PIN 码长度的限制，一般来说都是 4 位或者 6 位。新设置的 PIN 码长度必须在限制的长度以内。否则令牌将无法正确地接受您修改的 PIN 码。

修改 PIN 码的步骤如下所示：


1 请按“ON”键打开令牌电源




屏幕提示：请输入 PIN 码



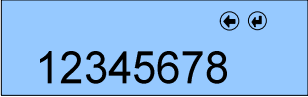
2 输入您的 PIN 码




如果 PIN 码输入错误，屏幕会提示错误  
此时令牌会自动关机，请重新回到第一步。



3 如输入正确的 PIN 码之后，先按照“2.2 同步认证方式”的操作方法，按“ON”键产生一个动态口令。



再按“MENU”键进入辅助功能菜单。





- 4 进入辅助功能菜单后，屏幕出现“CHANGE PIN”菜单。如果不是此菜单，请多按几次“MENU”键，直到循环菜单出现正确显示为止。



再按“ON”键进入菜单。



- 5 令牌屏幕显示“NEW PIN”字样。此时请输入您设定的新 PIN 码。注意：因令牌有弱 PIN 检测功能，像“1111”、“1234”这种过于简单的 PIN 码是无效的。同时，PIN 码的长度，要符合系统设置，否则都会不被接受。



6



输入新 PIN 码后，按“ON”键。



提示要求确认新 PIN 码。



7



再次输入相同的新 PIN 码后，按“ON”键。



PIN 码修改成功！此时令牌将自动关闭。再次开机就可以正常使用了。



## 2.5 解除令牌 PIN 码锁定

当用户使用令牌时，连续输入错误 PIN 码的次数达到系统设置的上限时(一般为 6 次)，令牌将会自动锁定。如果此时输入 PIN 码的提示由“ENTER PIN”变为“LAST TRY”时，说明只有最后一次机会输入 PIN 码，如果再输入错误将会启动令牌自动锁定功能。

每次输入正确 PIN 码时，PIN 码输入错误累计次数将清零。因此偶尔输错 PIN 码并不会造成累计次数增加而造成令牌自锁。

当令牌自动锁定后，用户可通过电话、网站等方式联系系统管理员进行远程解锁。

远程解锁步骤如下：

首先，打电话给动态口令系统管理员，当确认完用户身份后，系统管理员会要求用户报告令牌中产生的挑战解锁码(具体操作见下图)：

1 请按“ON”键打开令牌电源



屏幕提示：已被锁定。



2 请按“ON”键产生令牌解锁挑战码



向系统管理员报告令牌中产生的解锁挑战码数字串，等待系统管理员回应解锁码。此时可以按除“ON”键以外的其他任意键，延长数字显示时间，以免令牌自动关闭。



3 在输入系统管理员回应的令牌解锁码以前，请按“ON”键进入解锁码的



输入状态。



正确输入系统管理员回应的解锁码后，再按



“ON”键确认。

4 如果解锁失败，则提示“ERROR”，需要回到第一步重新开始解锁。



如果解锁码输入正确，令牌会显示“NEW PIN”，提示必须重设 PIN 码，以后的操作请参考“2.4 修改令牌 PIN 码”图示。



提示：在等待系统管理员回应解锁码的时候，如果等待时间较长，为了避免令牌自动关闭电源，用户可按一下除“ON”键以外的任意按键，到系统管理员开始回应解锁码前，用户先按“ON”键，再输入解锁码。



## 2.6 令牌手工重同步操作

用户使用令牌产生的动态口令在系统中进行动态口令身份验证，必须是采用相同的令牌信息。而令牌每次认证操作完成后，或时间改变后，令牌里和系统中的信息也会随之变化。

正常时，认证服务器可以与令牌同样随时间的变化和成功的认证操作而改变保存在系统中的相应的令牌信息。但是事实上有时候可能发生这些情况：用户不断产生密码，但并不完成系统的登陆认证操作；或者令牌的内部时钟不准确；或者系统的认证服务器时钟不准确等等，就会造成用户手持的令牌与服务器端信息的不同步。

ActivCard 的认证系统已经充分考虑到了这种情况的发生，应采用相应技术，允许动态口令的生成累计次数和时钟在安全范围内存在一定偏离。只要在系统许可的偏离范围内，可以正常完成认证，并且系统能够在正常认证流程完成后，自动同步令牌和系统的相关信息。但是如果一旦偏离值超出许可的范围以后，则必须要通过电话、网络的方式和系统管理员联系，手动完成令牌信息的同步操作。

ActivCard 动态口令身份认证系统默认的偏离许可范围是：


累计产生口令次数 30 次以内

内部时钟偏移值 23 小时以内

令牌的重同步工作非常简单，不需要用户繁琐操作，只需从令牌中读取相关信息，通过电话、网络等方式告之系统管理员即可。有时，系统管理员只需要部分信息，就可以完成令牌重同步工作。

以下是令牌重同步工作中取得相关信息的操作步骤：

1 请按“ON”键打开令牌电源



屏幕提示：请输入 PIN 码

ENTER PIN



- 2 输入随令牌发放的 PIN 码，假设为“8888”



如果 PIN 码输入错误，屏幕会提示错误  
此时令牌会自动关机，请重新回到第一步。



- 3 如输入正确的 PIN 码之后，先按照“2.2 同步认证方式”的操作方法，按“ON”键产生一个动态口令。



再按“MENU”键进入辅助功能菜单。



- 4 进入辅助功能菜单以后，按“MENU”  键数次，直到令牌显示

“VIEW SN”后， 按“ON”  键，会出现令牌的序列号，按“MENU”键返回辅助功能菜单。



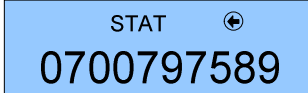
如果系统管理员不需要此信息，请跳过此步操作。


令牌的序列号可以在令牌背面的信息条中看到。





5 进入辅助功能菜单以后，按“MENU”  键数次，直到令牌显示

“VIEW CLOCK”后， 按“ON”  键，会出现令牌的内部时钟数字串，按“MENU”键返回辅助功能菜单。



STAT   
0700797589

6 进入辅助功能菜单以后，按“MENU”  键数次，直到令牌显示

“VIEW COUNT”后  ，按“ON”  键，会出现令牌产生密码的累积次数，按“MENU”键返回辅助功能菜单。



STAT   
0000004335