

# 鼎信高科动态口令显示卡 - 口令安全策略的考虑

---

公司名称：北京鼎信高科信息技术有限公司

公司地址：北京市海淀区上地信息路 11 号

彩虹大厦北楼 306 室

邮政编码：100085

联系电话：010-62963695

传 真：010-62960847

网 站：[www.topsensetech.com](http://www.topsensetech.com)

今天，随着整个网络的普及和信息化建设的加速，网络已经成为日常工作和生活中越来越密不可分的组分。网络之所以能够成为人类社会所日益倚重的工具，主要在于它的高效性和开放性，人们可以自由地在网络上进行信息交换。但是随着各种网络应用的推广，在各种信息沟通和虚拟生活中，需要确认使用者的身份，因此也就产生了各种应用系统中对身份认证和确认过程。网络中籍此来确认使用者的身份并授予他们必要的使用权限和信息资源。特别是电子商务和网络银行应用的普及，使得网络中的身份显得更加重要，为此也就产生了各种身份认证和保护的技术和手段。

身份认证是信息安全的重要组成部分，它是保护信息系统安全的第一道大门。只有通过身份认证系统的帮助，才能按照不同的使用者身份进行资源管理。才能将非法访问拒之门外。

电子商务和电子银行无疑是对用于使用者身份最为关注，但是在现代网络社会中，各种各样的虚拟身份都需要保护，比如我们的博客、BBS帐号，企业电子邮箱密码等等。最传统的保护方式就是使用用户名、口令。这种方式在身份的概念引入应用系统时就已经存在，现在也是使用最为广泛的身份保护方式，但是随着信黑客手法的层出不穷，网络嗅探器、键盘记录器、crack工具等等，甚至新出的社会工程学的口令骗取方式等等，在这些攻击方式的面前，用户名+口令的身份认证方式显得脆弱不堪。

为此我们需要一种方便、可靠、安全的身份保护方式：动态口令认证。

与传统的口令管理系统不同，基于动态口令的强化认证可以实现低成本、高安全的有效结合，使得对于口令的管理变的异常方便。同时，其事实安全性与理论体系完整的其他认证体系相比丝毫不弱。

# 目 录

<b>第 1 章</b>	<b>简介</b> .....	<b>1</b>
<b>第 2 章</b>	<b>动态口令的组成和使用原理</b> .....	<b>3</b>
2.1	动态口令认证系统硬件组成 .....	3
2.2	动态口令的工作逻辑 .....	4
2.3	动态口令认证方式和原理 .....	5
2.1.1	时间同步认证.....	5
2.1.2	事件同步认证.....	7
<b>第 3 章</b>	<b>动态口令卡成本优势</b> .....	<b>8</b>
3.1	购置成本 .....	8
3.2	分发成本 .....	9
3.3	管理成本 .....	9
3.4	总结-全部拥有成本.....	10
<b>第 4 章</b>	<b>安全的效应 – 底线</b> .....	<b>12</b>
4.1	适宜的安全性.....	12
4.2	口令作为一种安全机制 .....	12
4.3	强化身份认证以增强安全性 .....	14
4.4	动态口令认证安全性分析 .....	14
4.4.1	普通口令技术的缺点 .....	14
4.4.2	PKI 身份认证体系 .....	16
4.5	总结 .....	17
<b>第 5 章</b>	<b>强化安全的回报</b> .....	<b>18</b>
5.1	鼎信高科动态口令卡 .....	18
5.2	增加业务收益.....	19
5.3	降低成本 .....	20
5.4	符合安全监管规定 .....	21
5.5	弱化风险 .....	21
5.6	结论 .....	21
<b>第 6 章</b>	<b>附录-OTP 的原理和算法</b> .....	<b>22</b>
6.1	系统构成 .....	22
6.2	工作原理 .....	23
6.3	工作流程 .....	24
6.4	IETF RFC 4226 HOTP 算法简介 .....	25

## Chapter

# 1

## 第1章 简介

身份认证技术分为：常规的“口令”代码认证、动态口令认证、生物技术(指纹、虹膜、面容等)认证、通过第三方发放的数字证书(CA)认证等。其中常规的“口令”代码认证是计算机系统的早期身份认证产品，因其“口令”的静态特性和重复使用性，存在易窃取、易猜测、易破解等安全缺陷，是一种弱身份认证系统，只能用于安全等级要求较低的信息系统。动态口令认证、生物技术认证和数字证书认证是强身份认证系统，可用于政府、金融、企业等重要信息系统的安全认证。

针对静态口令认证的缺陷，80年代初，美国科学家 Leslie Lamport 首次提出了利用散列函数产生一次性口令的思想，即用户每次登录系统时所使用的口令是不同的，且一次有效。1991年贝尔通信研究中心(Bell core)用 DES 加密算法首次研制出了基于一次性口令思想的挑战/应答式动态口令身份认证系统 S/KEY。之后，更安全的基于 MD4 和 MD5 散列算法的动态口令认证系统也开发出来。

随着越来越多的传统业务转移到了网上，许多企业正在关注和评估比传统的固定密码保护方式更为强化的网络登录安全性的管理方法。然而，采用强化身份认证来取代普通的口令/帐号认证方案需要考虑到一些必要的因素，其中包括：要适合用户本身的使用需求（可用性，便于携带和多功能于一体），要适合公司本身的使用需求（安全的强度，互操作性和集成性，应用范围/系统大小的可定

制性和未来的适应性)。同时在任何大的技术投资中，价格总是需要被考虑的一个因素。

鼎信高科动态口令支持系统就是一个增强身份认证安全性的支撑平台，其中包括口令卡、管理系统、接口系统三大组件，通过接口系统和管理系统的配合，可以和用户现存的身份认证系统做很好的结合起来。用户通过口令卡获取一次性认证密钥，密钥由硬件电路根据复杂的安全算法逻辑生成，使用一次后即告作废，即使这一次通讯的口令被窃取，那么下一次使用时已经失效。通过这种认证机制使得用户口令变得“飘忽不定”，难以琢磨，除非黑客对高强度的算法进行破解，这无论从时间复杂度还是多次获取译码样本的难度来说都较传统的认证方式困难的多。

本白皮书通过详细的技术细节介绍和对比分析说明动态口令体系的安全性和易用性。

**Chapter**  
**2**

## 第2章 动态口令的组成和使用原理

在本章中，结合动态口令体系的三大部分（口令卡、管理系统、接口系统）给出介绍并分析在实际的网络应用部署中带给我们的好处。

### 2.1 动态口令认证系统硬件组成

动态口令认证一般有两种应用模式，其一，一个完成的动态口令认证系统除了动态口令认证自己的三个部分外，还需要和传统的（或用户已经在使用的）认证系统相结合，成为一个统一的整体；其二，单纯依靠动态口令系统进行认证的应用方式。这种应用方式中，“接口系统”可以独立的完成一次性口令和用户身份的认证。在这两种应用方式中，方式一的应用最为普遍，安全性也相对较高，这就是安全行业经常称呼的“双因素认证”认证方式。



图 2.1 动态口令卡（动态口令生成器）硬件

动态口令认证卡一般有两种形态，一种是独立的硬件令牌卡（图 2.1 左），

一种是集成在普通信用卡内部的超薄型动态口令卡（图 2.1 右）。两种硬件实际的工作原理是完全相同的，只不过采用的材料和加工工艺不同。而对于集成在信用卡内部的产品形态，即可以当作普通的银行卡、磁卡使用，也可以作为独立的动态口令生成器使用，由于其携带轻便，功能统一，所示在国外已经逐渐流行起来。

口令卡是整个动态口令认证系统中唯一需要额外增加的硬件部分，其他的各个组成部分都可以是软件的形态进行安装配置。

## 2.2 动态口令的工作逻辑

动态口令系统对于单位内部的应用认证系统并不会做太多的变化，仅仅是对原来的口令部分进行“延长”。用户原有的用户身份基本可以保持不变，仅需要进行部分使用习惯的调整。

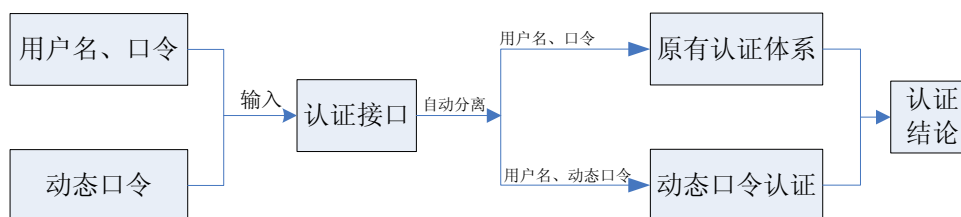


图 2.2 动态口令认证与原始认证系统的结合逻辑

图 2.2 给出了动态口令认证体系和原有的传统认证体系的关系，从这张图中可以看出，在通用的用户名、口令认证体系中增加动态口令认证并不是非常复杂。仅仅在原有的认证体系中“嵌入”一个动态口令认证的“认证接口”即可。这个“接口”可以将用户输入的口令、动态口令进行分离，分离后通过各自的认证确认过程获得结论后进行归并。在一些新建的应用中，动态口令可以直接和用户名、口令认证的传统体系结合而无需分离进行独立的认证，这样对于身份的管理会更加方便。但是其逻辑结构和图 2.2 是一致的。

由动态口令的工作逻辑图可以看到，一个标准的动态口令体系无论是新建系

统还是升级系统，其结构中相对传统认证主要多出了三个部分，这三个部分分别对应着动态口令认证体系的三个主要功能模块。如表格 2.1:

**表格 2.1: 动态口令三组件**

模块名称	形态	说明
动态口令生成	硬件	即 Token、口令卡等
认证接口	软件	兼容各种认证系统
管理系统	软件	动态口令的注册、注销、认证过程控制

在图 2.2 中表示的是动态口令的工作逻辑，也就是说，在普通安全认证的基础上通过认证接口将用户通过传统认证界面输入的信息“分流”成两个独立的认证组分，其中上边的流程就是传统的用户名、口令认证过程，而下边部分就是基于动态口令硬件设备的“一次性口令”验证部分。

## 2.3 动态口令认证方式和原理

动态口令也称一次性口令 (One-time Password)。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 (two factor): 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 (Time Synchronous) 认证技术、基于事件同步 (Event Synchronous) 认证技术和挑战/应答方式的非同 (Challenge/Response Asynchronous) 认证技术。

### 2.1.1 时间同步认证

基于时间同步认证的方式是把时间作为双因子中的变动因子，一般以一个固定的周期 (秒/分) 为变化单位。所谓“同步”是指用户口令卡和认证服务器所产生的口令在时间上必须同步。这里的时间同步方法不是用精确计时或通讯同步技术，而是用“滑动窗口”技术。

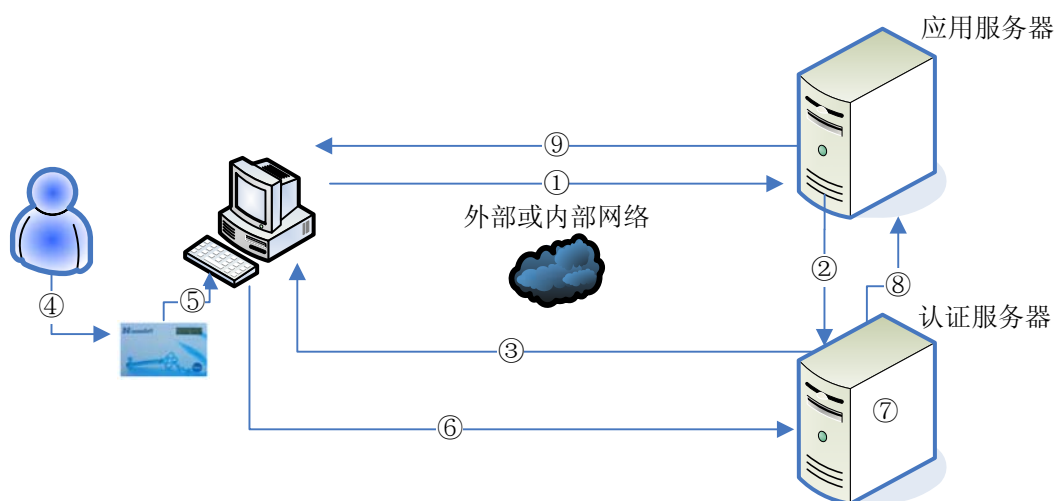


图 2.3 为客户终端访问系统时，基于时间同步的认证过程。

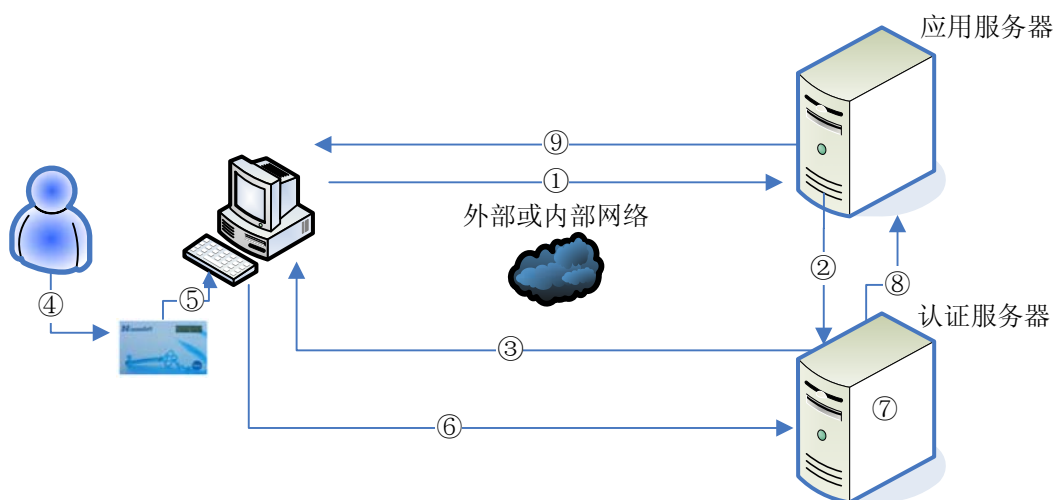


图 2.3 动态口令卡（动态口令生成器）硬件

1. 客户向应用服务器发出应用登录请求；
2. 应用服务器向认证服务器发出对客户身份合法性和真实性的认证请求；
3. 客户终端弹出身份认证对话框；
4. 客户从动态口令卡上获取动态口令码；
5. 客户将用户名、口令和动态口令键入终端的身份认证对话框；
6. 客户终端将用户名、口令和动态口令通过网络传输给认证服务器；
7. 认证服务器首先进行原始的用户名、口令认证，通过后，再调本地存储的用户信息，产生与用户信息、时间相关的随机序列，并与客户输入的

动态口令进行比对，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. 应用服务器将结果告知客户终端，并决定是否提供相应服务。

注：简单应用时可能应用服务器和认证服务器会合二为一。

### 2.1.2 事件同步认证

事件同步认证是把变动的数字序列（事件序列）作为动态口令产生双因子中的变动因子，与用户自己的初始密钥共同运算产生动态口令码。这种模式下的同步是指每次认证时，认证服务器与口令卡保持相同的事件序列。如果用户使用时，因操作失误多产生了几组口令出现不同步，服务器会自动同步到目前使用的口令，一旦一个口令被使用过后，在口令序列中所有这个口令之前的口令都会失效。其认证过程与时间同步认证相同。

**Chapter**  
**3**

## 第3章 动态口令卡成本优势

在评估任何一项用户身份认证技术时——不论是静态密码口令，动态口令，数字证书还是生物识别技术，都需要准确地了解其真实的全部拥有成本，这不仅包括购置成本，也包括日后应用时的分发和管理费用。

### 3.1 购置成本

传统的静态密码管理系统在所有主要的身份认证系统中，其购置成本最低，甚至是近于零，因为其经常是内嵌于操作系统，或者由通信工具和商务应用软件“免费”提供，同时传统的静态密码管理系统不要求终端用户购买任何特定的硬件和软件设备。

与之不同，强化认证技术要求购置一个服务器软件，并为每一个终端使用者配备一个硬件安全设备，如动态口令卡/数字证书卡/生物识别卡等。

然而，购置成本仅仅是总体拥有成本中的一项，其他的还包括分发成本和管理成本。

动态口令卡已在世界上经过多年的应用，产品成熟，使用方便，密码随机产生，并一次性使用，保证了用户登录的安全性。

数字证书卡通常为内置用户数字证书的 USB 卡，需要插到用户的电脑上使

用。生物识别，包括指纹识别等技术，也得到了越来越多地应用，但这些强化安全认证技术所使用的终端硬件成本相比动态口令卡都要更高一些。

### 3.2 分发成本

不同的身份认证技术其分发成本是完全不同的。对于传统的静态密码口令方式，用户要获得一个账号/密码可能需要填写一套申请表格，如果相关信息是要保护的及有价值的，公司需要专门的流程来处理及批准这样的申请，经理审核通过客户的申请，然后由 IT 部门为这个用户建立一个账户，一次性的用户开通过程通常要花费 15 到 20 分钟的人工时间，这样就产生了分发成本，即人工的费用。

对于动态口令卡/数字证书卡等其他的身分认证方式，也同样需要相关的人工处理过程，并带来相应的分发成本。

### 3.3 管理成本

一个用户身份认证系统在日常的使用中可能会发生各种各样的问题，比如如果发生了用户账号/密码遗忘或者被盗用的情况时，就需要花费公司的资源来处理和解决问题。这种日常管理和维护一个认证系统的应用开销，就是管理成本，也是更值得考虑的一种成本。

当问题发生时，通常会产生两种费用。一个是用于解决问题时的资源消耗，另一个是相关人员生产力的损耗。

后勤和技术服务人员需要花费时间和精力以解决一般的与有关认证的问题。这些人会打电话并使用公司安全设备以分析问题和解决问题。同时，受影响用户的时间可能遭受损失，这样相应的工资和福利也损耗了。

此外，在这个过程中，所有的相关人员的生产力都有所损失。当一名雇员是在全力投入去解决一个身份认证的问题时，其并没有创造额外的价值，故而生

产力也会损失大约相应时段工资的数额。

企业可以自行根据以上分析去评估这个成本的具体数额，大概估计每次问题产生的费用总额=50 元。

那么一个典型用户忘记密码并寻求帮助的次数是怎样的呢？通常一年之中，有很多情形可能会造成用户忘记其使用的口令。当用户有一段时间不使用密码，比如在经历主要的节日，休假或者旅行之后，用户很可能就忘记了一个密码。任何的密码变更，不管多么的不频繁，还会有许多用户忘记新的密码。如果这时用户有多个密码口令需要记忆，同时好的密码管理要求定期的更换密码，那么忘记密码所带来的高管理成本就不可避免了。一年之中，一个用户平均可能会数次忘记密码。跟据统计报道，保守估计平均每个用户每年会产生 3.8 次与密码有关的问题并寻求帮助。

这样，对于传统的静态账号/口令系统，一个用户一年由于遗忘密码而产生的管理成本估计为  $3.8 \times 50 = 190$  元。

忘记密码只是常见问题中的一个，现今，很多用户在非安全场所登录网络并使用密码，同时电脑木马病毒、网络黑客、网络陷阱等也严重威胁用户的信息和密码安全，由此而产生账号/口令被盗用的现象也屡见不鲜，而这些会给企业和用户带来更大的损失，更高的管理成本，严重的会威胁到业务发展。

对于强化安全登录系统，由于密码是动态产生并一次性使用的，而且其技术特点保证了其难于被盗用和假冒，因此就避免了高昂的管理成本。

### 3.4 总结-全部拥有成本

当比较强化安全认证系统和静态密码系统的成本时，重要的是，要不仅仅看购置成本，还需要看分发成本和管理成本。由以上分析，我们可以看到，传统的静态账号/口令系统反而可能是成本最高的身份认证系统！

表格 3.1 各种认证方式的成本分析

	传统静态帐号/密码	动态口令	数字证书	生物识别
购置成本	近于 0	一般	高	很高
分发成本	一般	一般	一般	一般
管理成本	高	低	低	低
安全性	一般，易受盗用	高	高	高
使用方式	手动输入	手动输入，联机自动输入	联机自动输入	联机自动输入

## Chapter

# 4

## 第4章 安全的效应 – 底线

在考虑采用一种密码系统的成本时，企业还必须要考虑安全性本身的问题。脆弱的安全性可导致敏感信息和资源暴露给非授权人员或者入侵者，从而造成直接和间接的损失。相应地，强化身份认证可带来新的业务机会，并产生新的或者增强的业务流。所以，要保证足够的安全性，这就是底线。

### 4.1 适宜的安全性

对于一个企业，在制订安全策略时，首先需要明确的是，其各种不同的业务需对应什么样的安全等级才是最适宜的，对不重要的数据或应用进行高强度的安全保护，和对于关键数据或资源不作保护或只作底等级的保护，这两者同样都是不明智的。把解决方案和安全需求相匹配起来是很重要的。

安全性遭到破坏所产生的影响，对于不同的公司来说是很不一样的，其评估需根据信息本身的价值、中断的业务量、系统的复杂性以及公司的市场地位而定。企业需要认真评估这些影响，以确定相应数据和业务的适当保护程度。

### 4.2 口令作为一种安全机制

口令通常被认为是一种较弱的身份认证方式。它们能够容易地被猜到，或者当用户键入个人信息的时候很容易被人从后面偷窥到。此外，有一些很容易取得

的工具可被用来截获用户用键盘输入并通过网络传输的密码文件。当密码被偷或者被破解时，受害者通常不知道他们的身份已经被盗，同时，盗窃者也通常不会被发现。

通过 2007 中国互联网络信息中心的调查报告，我们可以看出账号/口令被盗的比例较高，且很多盗用都是恶意的。

**表格 4.1 网民中网络安全问题发生的比率**

	比例
电脑感染病毒	90.8%
账号/个人信息被盗、被改	44.8%
网上遭到黑客攻击	26.7%
被仿冒网站欺骗	23.9%
都没有碰到过	2.5%
其他	1.2%

**表格 4.2 网民 2007 年下半年网络安全问题发生的频次**

	0 次	1 至 2 次	3 至 5 次	5 次以上
电脑感染病毒的次数	3.6%	37.0%	23.7%	35.8%
账号/个人信息被盗、被改的次数	16.3%	63.2%	13.1%	7.4%
网上遭到黑客攻击的次数	18.8%	47.8%	13.8%	19.6%
被仿冒网站欺骗的次数	12.4%	53.7%	16.1%	17.7%

**表格 4.3 网民发生帐号或密码被盗的场所**

	比例
网吧	56.5%
家里（包括亲戚朋友家）	37.1%
工作场所	24.7%
学校	17.5%
公共场所（图书馆/机场/咖啡厅等）	15.5%
其他	2.5%

**表格 4.4 发生网民帐号或个人信息被盗改的诱因**

	比例
MSN/QQ/E-mail/网游等帐号被破解	75.9%
回复含虚假和诱惑信息的欺诈电子邮件，帐户/密码等个人信息被骗	23.7%
访问假冒网上银行、网上证券、电子商务等网站，用户帐号密码被骗填入	16.8%

其他	9.4%
不知道	5.1%

### 4.3 强化身份认证以增强安全性

强化身份认证技术比传统的静态密码更安全可靠。用户通过结合他所知道的一样事物--一个密码，和一个他所拥有的事物—一个鼎信高科动态口令卡，来共同完成登录身份认证过程。在这个系统中，如果不同时拥有个人口令密码和动态口令卡，就不可能仿冒他人进行登录。第四章中会有更多有关鼎信高科动态口令卡的介绍，它通过安全算法在用户登录时即时动态产生登录密码，从而保证了用户安全登录受保护的资源。

### 4.4 动态口令认证安全性分析

动态口令认证被普遍认为是一种非常安全的认证方式，国外发达国家已经将之广泛的应用到电子交易和网上银行的用户身份鉴别之中。

#### 4.4.1 普通口令技术的缺点

可重用口令认证是目前使用最为广泛的系统登录认证方式，或许人们已经对她太熟悉，所以列举起她的缺点来简直如数家珍。这里是其主要的几种缺陷：

- **直接窥视** 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。对于后者，根本不需要特别的技术或设备，只要眼睛不是近视得太夸张，需要的仅是静悄悄的站在您的身后，就可以轻松实施攻击。
- **网络嗅探** 有时候口令需要通过网络传输，但是很多鉴别系统的口令是未经加密的明文，攻击者只要通过窃听网络数据，就很容易获取鉴别所需的用户名和口令。目前网络中可以随意下载到网络口令截获工具，可以方便的截获到电子邮箱、远程桌面、web 登录等口令信息。

- **重放攻击** 有的系统会将认证信息进行简单加密后进行传输，攻击者虽然无法通过嗅探器截获明文认证信息，但却可以首先截取加密后的口令然后将其重放，从而利用这种方式进行有效的攻击。目前很多 Web 登录应用都是使用了 MD5 加密口令传输的方式，虽然口令信息是密文的，不过每次的加密结果都是一致的。所以这种认证方式也是非常不安全的。
- **字典破解** 由于多数用户习惯使用有意义的单词、数字（如生日）作为密码，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。
- **暴力破解** 这是一种特殊的字典破解方式，它使用字符串的组合全集作为字典，即穷举所有可能的口令空间。这需要很大的耐心和巨大的工作量以及一点运气。然而，若用户的密码较短，那么它很快就会被穷举出来，因而很多系统都建议用户使用长口令。
- **社会工程学** 攻击者冒充管理人员发送邮件或打电话给合法用户，比如“我是某某单位的系统管理员，现在需要更新所有用户的密码，请将您原来使用的口令告诉我。”这种情况下，许多经验不足的用户会毫不犹豫地将其口令奉上。
- **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。有文章报道说，当今的商业间谍流行以清洁工人的身份来搜集情报，一方面清洁工人不太引起人们的注意，同时工作起来特顺手。

虽然管理员用尽了方法要求普通用户增强其口令设置，但是大部分的用户还是用自己的简单编码来作为口令，更有甚者为了符合系统的口令复杂度要求，又不至于遗忘，直接将口令写在纸条上放在键盘下方。

动态口令卡的使用可以充分规避以上所有的攻击方式。由于口令是一次性的，一旦使用过后将不在有效，所以黑客除了直接盗取动态口令卡外，其它攻击方式都将失效。

#### 4.4.2 PKI 身份认证体系

PKI 身份认证体系是一种公认安全性非常高的身份认证方式，在大多数用户甚至专业技术人员心目中，这时身份认证的“终极”解决方案。似乎使用了 PKI 身份认证体系就可以确保安全不失，这里我们先从安全的基本原理开始分析。

我们知道，PKI 之所以称之为理论安全体系，主要的原因在于他是一种非对称密钥的加解密方式，这些加解密使用的“密钥对”都是以证书的形式存在。加密者即便得到对方的公钥，也无法对其解密的信息进行解密（需要私钥解密）。为此，在密钥的交换过程中可以确保自己的“城池不失”。同时，标准的 PKI 体系里边拥有强大而完善的证书管理体系。并对证书进行签名等等一些列的保护机制。所以单单从理论上讲，PKI 证书认证体系的确“理论安全”的。

不过，作为最终用户，我们必须明白一个基本，而且是所有人都耳熟能详的安全原理：系统的整体安全性取决于其最薄弱的环节（木桶原理）。但是在实际应用中，这一原则往往会被忽视。

在研究黑客攻击技术的过程中，我们发现，这里也有一个基本的原理，那就是：永远不要认为自己的操作系统是安全的。换句话说，就是不要相信自己的操作系统不会被黑客攻破。

基于以上的两个原理，以及国内用户使用 PKI 认证体系时的使用习惯，我们可以非常简单的发现现有 PKI 证书认证体系的“短板”：证书的保存。

证书作为用户身份的最重要记录载体，无论我们使用什么样的证书保存方式，最终在认证的过程中都需要将之连接到计算机系统之中，我们称之为：接触式认证。这类认证证书即便保存在专用的硬件设备（USB-Key）中，也需要在认证过程中与计算机连接。否则认证根本无法进行。而一旦计算机操作系统被黑客所控制，那么我们也不用在期望证书的保存那么可靠。也就是说在这种情况下，黑客能够“克隆”用户证书的可行性并不低。

所以本文一直把 PKI 证书认证称之为“理论安全”。在实际应用中，往往会过分的依赖证书的可靠性。而动态口令认证方式所依赖的“一次性”口令，是一种非接触式的认证，虽然一次使用的口令可以被截获，只要黑客不能破解动态口令卡中的口令生成算法，或者盗取动态口令卡，那么，无论黑客如何控制我们的计算机，对于身份认证的安全性，他们仍然是无力撼动。

## 4.5 总结

当然还有很多其他的增强身份认证方式，不过，如果考虑到其身份认证要素的抗“克隆”能力，动态口令（一次性口令）认证无疑是安全的选择。

**Chapter**

**5**

## 第5章 强化安全的回报

通过实施鼎信高科动态口令卡强化身份认证系统，企业通常可以实现 4 个方面的业务好处：增加收入，降低成本，增进规范符合和弱化风险。

### 5.1 鼎信高科动态口令卡

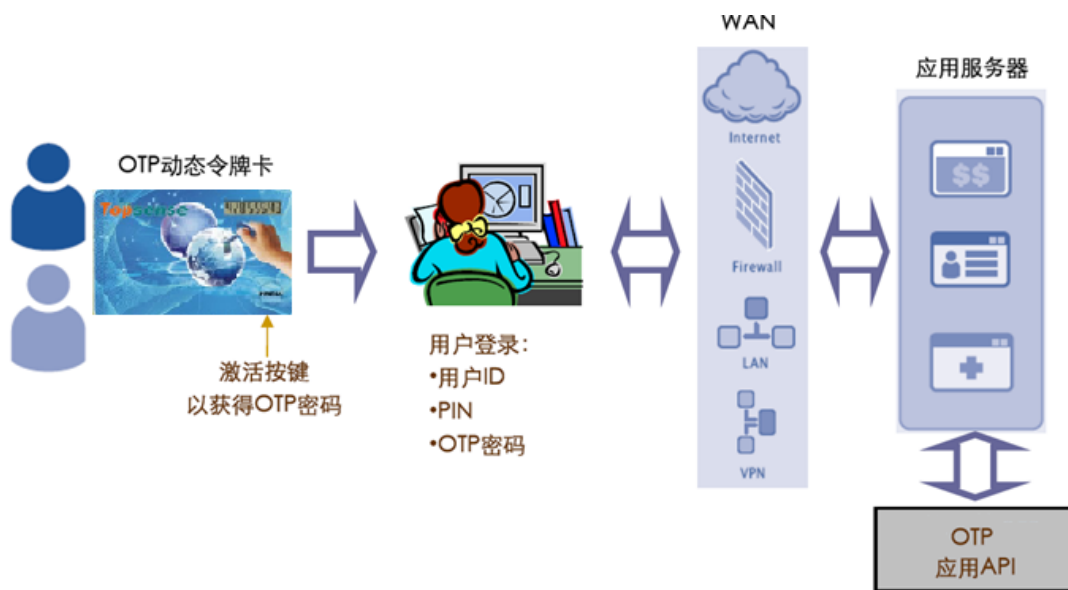


图 5.1 动态口令卡（动态口令生成器）硬件

鼎信高科动态口令卡为一个符合 ISO7816 标准的信用卡形式的动态密码卡，其所采用的强化安全认证技术区别于传统静态密码的关键之处在于：用户必须提供强大得多的身份证明才能通过登录认证。通常需要采用多重身份证明（因子）

来作为安全保障，因子越多越安全，静态密码只提供了一个因子，故被认为是最不安全的。

鼎信高科动态口令卡提供双因子认证，用户登录时首先需要输入一个他的个人密码（他知道的事物），然后按提示按动动态口令卡（他拥有的事物）上的按键以产生一个动态密码，这个密码会显示在显示器上，用户将其输入，在服务器端确认无误后，即可获得登录。动态密码卡采用基于 160 位 SHA-1 的 IETF RFC 4226 HOTP 算法（或者您自己的特定算法），由其产生的密码的安全性已经过业界的广泛验证，且密码是动态、一次性使用的，故保证了登录不可能被他人仿冒和盗用。

### 产品特性

- 尺寸：85.6×54×0.83 mm, 兼容于 ISO 7816 标准；
- 基于 160 位 SHA-1 的 IETF RFC 4226 HOTP 算法或者您自己的算法；
- 柔性 LCD 显示：绿色/白色，最大 8 位显示（可以根据需要定制显示位数和大小），超宽视角，可选双稳态显示屏；
- 电池寿命：事件模式（5 年），时间模式（3 年）；
- 可以根据客户要求订制卡的外表图案，如商标或其他个性化图案。

### 芯片特性

- CPU 芯片：具有 RTC 模块，同时支持时间同步和事件同步的单芯片；
- 也可以使用客户提供的芯片和固件。特别是在已经有了 Token 业务，仅仅需要为客户带来新的信用卡 Token 产品特性。

## 5.2 增加业务收益

互联网为企业提供了极好的开展电子商务的机会和平台。通过扩展到新的客户群，企业能够更快的发展其业务并且获得比以前更高的收益。但是，或许最能

够阻碍企业发挥并实现这种技术潜力的因素就是安全性——更确切的说就是用户认证。任何在线环境中，在开展业务之前，建立起和用户之间的相互信任是很关键的。首先通过认证用户的身份，你才能确信你的客户就是他们说他们自己是的那一个，并且确保他们不能否认任何已经执行的交易。

我们已经看到，传统的静态密码是一种较弱的用户身份认证方式，企业不应该完全信任基于此的用户身份。通过采用鼎信高科动态口令卡这样的强化用户认证技术，企业可以实现可信赖的电子商务安全性，并实现其营业收入额的增长。

### 可扩展及定制选项

- 照片 ID，磁条，智能卡以及射频模块均可以为多功能或者全功能卡应用而进行选择性的添加；
- 添加非接触式门禁控制能力（HID 和 MIFARE 兼容）以能够进行物理访问控制。

## 5.3 降低成本

电子商务应用可以是企业将很多复杂、花费人力的内部业务流程电子化并放到网上，比如：订单处理，人力资源系统，表格处理，及很多人力密集型的业务程序都已经自动化，由此可以提高企业效率并降低成本。

作为商业基础设施的至关重要的组成部分，要在用户接触到这些重要业务流程之前首先确认其身份。一个强化身份认证系统能够为用户提供一个有保障的认证方法，从而使企业安心实现其电子商务应用，并带来成本的节省。

鼎信高科动态口令卡采用了工业标准的双因子认证算法并在用户接触到关键数据和应用之前对用户进行身份识别认证，比如当登录：

- 银行账户，网络游戏账号，股票帐号等；

- VPNs & WLANs or Intranets & extranets 或者其他网络资源；
- 安全的 E-mail 或者传信应用；
- Microsoft® Windows® 桌面或者其他操作系统；
- 网络服务器或者其他服务器应用。

## 5.4 符合安全监管规定

对于个人隐私权的关注，政府机构和工业组织已经制定了立法和规范，以强制企业要严格按照标准去保护个人信息数据。达不到这些标准的规定，就可能导致企业遭受重大罚款。而且，用户和合作伙伴也可能会拒绝和这样的公司进行业务来往。通过在用户接触到关键资源之前对其进行强化的身份认证，可以使企业符合监管的规定。

## 5.5 弱化风险

一个广泛公开化的网络漏洞可以造成损失的积累。现在每天我们都能看到有关网络安全遭到威胁或者破坏的报道，而随着越来越多的有价值信息移到了网上，以及越来越多的交易在网上执行，风险还在不断地增加。强化身份认证能在用户登录敏感信息和应用之前对其认证，从而帮助企业弱化了风险。

## 5.6 结论

很明显，传统静态账号/密码并不是真正完全免费的，有许多隐藏的成本——包括管理费用——在评估总拥有成本时经常被忽略。另外，很重要的，脆弱的安全等级常导致代价昂贵安全漏洞，同时更强的安全性能增加收入机会。

鼎信高科的动态口令卡可以提供强大用户身份认证保障，并且使用方便，成本较低。

## Chapter

## 6

## 第6章 附录-OTP 的原理和算法

### 6.1 系统构成

动态口令系统通常是由用户端硬件（即动态口令卡），服务器端的安全认证软件以及应用程序的接口三部分组成。

**动态口令卡**中通过运行同步信任认证算法产生一次性使用的动态口令，口令无法预测和跟踪，从而使得用户口令既无法被盗用，又避免了静态口令经常变换所带来的问题。

**安全认证服务器**的作用是通过与应用系统服务器通过局域网相连，控制所有远程用户对网络和业务应用的登录，提供全面的认证、授权和管理服务。其中主要组成包括：

- 系统运行-- 通过运行与动态口令卡中相同安全认证算法，实现动态口令的认证授权，并记录详细的运行日志，实现与应用程序接口的连接。
- 用户管理-- 完成动态口令卡的发卡、删除、冻结及解冻；完成动态口令卡用户的基本信息查询。
- 数据库-- 存储用户信息、卡信息、管理员信息、系统设置、运行日志等系统信息，其中用户数据、密钥等保密信息以加密方式存储。

**应用程序接口**提供与特定应用系统的接口，以为其用户的登录提供认证服

务。比如：Radius 方式远程访问，VPN 远程访问，Windows 域认证等。

## 6.2 工作原理

鼎信高科动态口令卡内嵌有柔性 PCB，电池和显示器，PCB 上配有微处理器 MCU、时钟等电子元器件，每个口令卡的芯片中内置有唯一的用户密钥和唯一的电子序列号。对于时间同步模式，卡中的时钟计数器（T）每隔 1 分钟用用户密钥与 ID 号自动运算加密算法，加密时钟计数器 T 得出一个 6-8 位的字符串显示在液晶显示器上，并保存在内存中，每一分钟刷新一次。目前标准的算法为基于 160 位 HMAC-SHA-1 的 IETF RFC 4226 HOTP 算法，加密运算不可逆，即使动态口令被别人知晓，也无法倒推出用户的密钥。

此 6-8 位信息被输入并送到安全认证服务器，安全认证服务器根据客户 ID 从用户数据库中调出该用户的用户密钥、卡初始化时间  $t$  和电子序列号，用用户密钥和电子序列号将接收到的口令进行脱密变换，将脱密得到的时间参数与系统时间进行比较，考虑通信延迟及时钟误差作出接受或拒绝的判定。

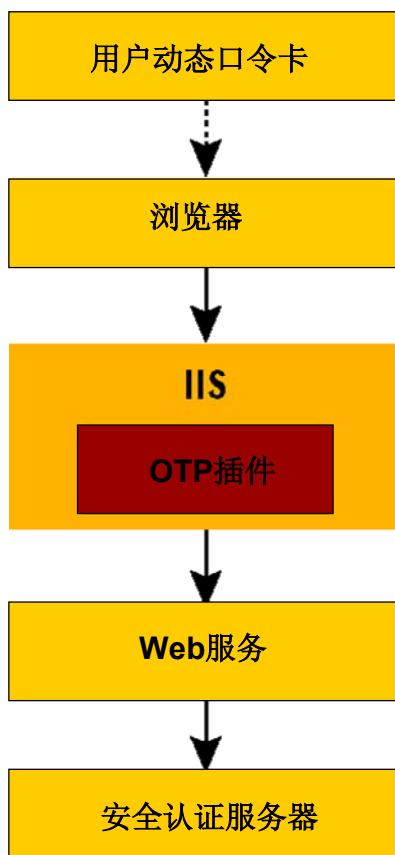


图 4.1 一次性密码解决方案组件

图 4.1 为一 Windows 系统下的网络身份认证示例图：当收到 Web 浏览器提示时，用户需要键入 OTP 值并单击“提交”按钮进行身份验证。OTP 插件模块从 IIS 得到通知，并且随后调用 Web 服务来检验身份验证请求。Web 服务在 SQL Server 表中查找用户的密钥和计数器值、检验 OTP 计算，并响应身份验证为成功还是失败。

### 6.3 工作流程

用户使用鼎信高科动态口令卡登录时工作流程如下：

- 1) 用户打开系统登录界面。
- 2) 输入用户识别码。

- 3) 用户取出动态口令卡，按下卡上按钮，产生一动态密码在液晶屏上显示。
- 4) 将动态口令输入。
- 5) 输入的信息被传送到后台服务器，后台服务器将用户识别码和动态口令传送到安全认证服务器。
- 6) 安全认证服务器根据用户识别码，从用户数据库中调出对应该用户的密钥。
- 7) 安全认证服务器使用与动态口令卡同样的认证算法对用户进行验证，并将验证结果返回给后台服务器。
- 8) 后台服务器将验证结果返回给用户，并根据验证结果赋予客户相应的权限，从而完成一次认证过程。

## 6.4 IETF RFC 4226 HOTP 算法简介

RFC 4226 HOTP 的全称为基于 HMAC 的一次口令算法，是国际 OATH(Open AuTHentication)标准化组织支持的用于动态口令的安全算法。

密钥哈希消息身份验证代码 (HMAC) 是基于密钥的一种加密哈希。HMAC 接受任意消息和密钥，并将消息映射成固定长度的摘要值（如 20 字节），从而确保只有具有相同密钥的人才能从相同的消息生成相同的摘要值。

基于哈希的 OTP 解决方案有两个输入值：密钥和计数器值。通常 OTP 的长度为 6-8 位数字，目前随机密钥通常为 256 位，即 32 字节。特定用户（或从技术角度讲，具有特定密钥的用户）每次进行身份验证尝试时，计数值都会增加。OTP 解决方案的安全性依赖于永不重复使用的计数值；这一点由 OTP 服务器保证。实际使用时，基于事件模式的计数值是 64 位无符号整数。另一种部署方法是使用与服务器之间的时间同步。

HMAC-OTP 的首个计算步骤是接受计数值，并将其编码为 HMAC 计算的输入消息。实际使用时，消息是设为计数器值的 8 字节缓冲区。下一计算步骤

是使用用户密钥计算上述消息的 HMAC。图 4.2 描述了这一流程

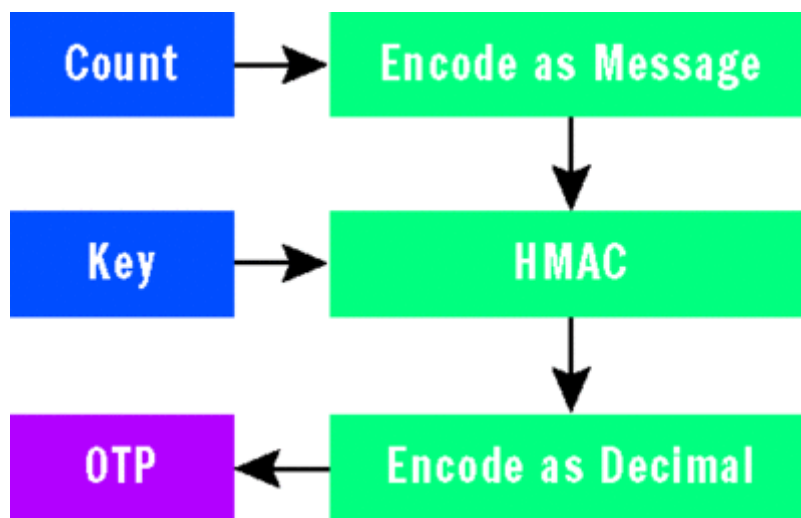


图 4.2 一次性密码流程

随后，通过对 20 字节的 HMAC 结果进行十进制编码，从而将此结果转换为 OTP 值，并显示在用户动态口令卡的显示屏上。

在终端上完成计算 OTP 值的过程后，同样需要在认证服务器上进行同样的算法计算，以完成认证过程。如图 4.1 中所示，身份验证 Web 服务 - 身份验证 Web 服务负责执行实际的 OTP 身份验证，其方法是确定提供的 OTP 值是否表明命名用户已拥有密钥。首先加载与身份验证请求中指定的用户名相对应的 SQL Server 数据库行，如果 SQL Server 无法找到匹配行，该方法将返回 false。

如果在 SQL Server 数据库中找到相应用户名，该方法将把以下数据项传给本机 OTP 产生算法函数：请求中指定的 OTP 值、用户密钥（从 SQL Server 中检索得到）以及计数器值（也从 SQL Server 中检索得到），进而完成认证计算。