# 冲击响应身份认证解决方案

# （ET99）



北京坚石诚信科技股份有限公司

**2008-6-10**

目前，网络上的身份认证手段主要有以下几种方法：用户名/密码、IC 卡、生物特征、动态口令、USB Key 等，这里介绍一种既简单又不失安全性的认证方式——冲击响应认证模式，这种认证模式是基于 USB Key 的。

USB Key 是一种 USB 接口的小巧的硬件设备，形状与我们常见的 U 盘没有什么两样。但它的内部结构不简单，它内置了 CPU、存储器、芯片操作系统（COS），可以存储用户的密钥，利用 USB Key 内置的密码算法实现对用户身份的认证。每一个 USB Key 都具有硬件 PIN 码保护，同时在硬件中会存储密钥，所以 PIN 码和硬件构成了用户使用 USB Key 的两个必要因素。用户只有同时取得了 USB Key 和用户 PIN 码，才可以登录系统。即使用户的 PIN 码被泄漏，只要用户持有的 USB Key 不被盗取，合法用户的身份就不会被仿冒；如果用户的 USB Key 遗失，拾到者由于不知道用户 PIN 码，也无法仿冒合法用户的身份。

USB Key 内置单向散列算法（MD5），预先在 USB Key 和服务器中存储一个证明用户身份的密钥，当需要在网络上验证用户身份时，先由客户端向服务器发出一个验证请求。服务器接到此请求后生成一个随机数回传给客户端 PC 上插着的 USB Key，此为“冲击”。USB Key 使用该随机数与存储在 USB Key 中的密钥进行 MD5 运算得到一个运算结果作为认证证据传送给服务器，此为“响应”。与此同时，服务器使用该随机数与存储在服务器数据库中的该客户密钥进行 MD5 运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客户端是一个合法用户。

下面以 ET99 USB Key 的 ASP 示例为例具体说明冲击响应的身份认证过程：

1、 欲使用 ET99USB Key 做冲击响应的身份认证首先需要设置 ET99USB Key 的属性，修改 PID 等。


“硬件 PID”：ET99 的产品标示，默认 8 个 F，通过种子码算法产生，种子即是在“PID 种子”中输入的。

“SO PIN 码”：管理员 PIN 码，开发商保存，可用于对 USER PIN 的解锁等，通过种子码算法产生，默认 16 个 F。

“USER PIN”：用户 PIN 码，字符限制“0-9，A-F”，外壳加密中需要验证，同时读写数据需要该 PIN 码验证通过，默认 16 个 F。

“新的 USER PIN 码”：用户根据自己的需要设置，注意字符的限制。

“PID 种子”：用于产生 PID 的种子，长度在 1-51 字节范围内。

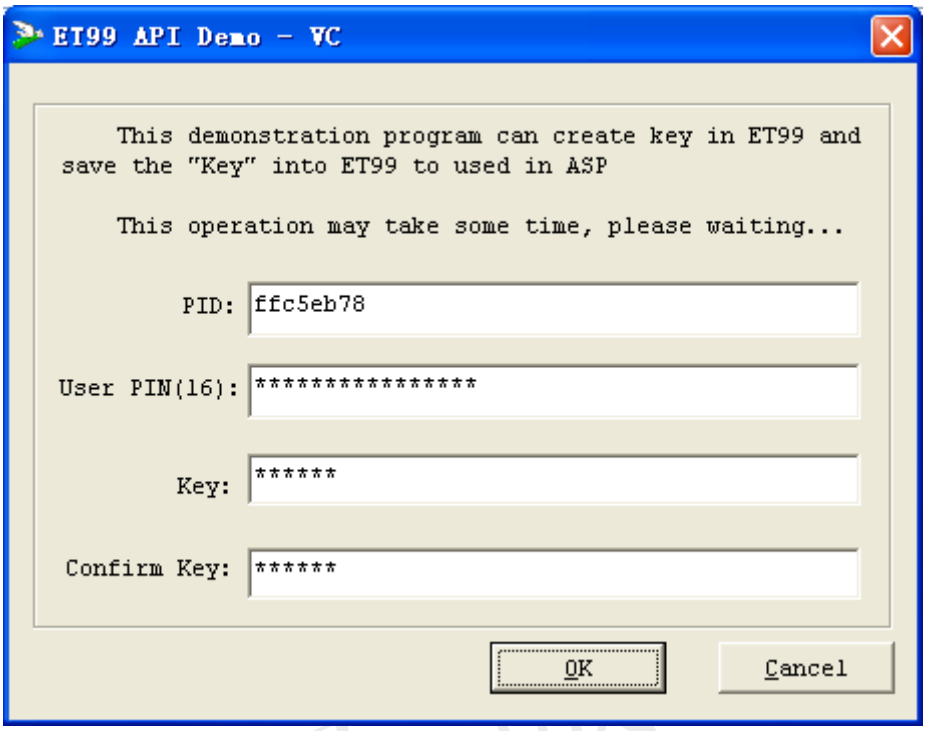
“SO PIN 种子”：用于产生 SO PIN 的种子，长度在 1-51 字节范围内。

“请选择设置项”：用户根据自己的需要，选择需要修改的属性。

“设置”：设置完成点击设置按钮，提示设置成功。

用户需要记住“新的 SO PIN”和“新的硬件 PID”。

2、 设置完成之后，在 ET99USB Key 中设置密钥，该密钥仅用于计算，不可读取，这样的设计保证了密钥的安全。




“硬件 PID”：ET99 的产品标示，默认 8 个 F，通过种子码算法产生，种子即是在“PID 种子”中输入的。

“USER PIN”：用户 PIN 码，字符限制“0-9，A-F”，即是前面提到的硬件 PIN 码，默认 16 个 F。

“Key”：用于计算的密钥，此密钥不可读取，只能用于计算。

“Confirm Key”：再次输入密钥以确认。

“OK”：设置完成点击，提示成功可进行下面操作。


设置成功后会在相同目录下生成 user.txt 文件，用于存储用户信息和密钥，

该文本文件在 ASP Demo 测试中被模拟为服务器端数据库，开发商在实际开发过程中需要将用户信息和密钥写入到系统数据库中，以备验证时使用。

3、 因为 ET99USB Key 都是通过客户端脚本语言访问硬件，所以首先需要在客户端注册组件，注册方式可以选择手动注册、网页安装或者使用我们提供的一个 exe 安装。

4、 在 logon.asp 文件中，首先通过 FindToken、OpenToken 函数查找并打开 ET99，然后验证 PIN 码并获取 ET99 的硬件序列号，此序列号唯一，最后在调用硬件 MD5 函数完成客户端的计算。Logon.asp 详细代码如下:

```
chPid =TheForm.TokenPid.Value
tokencount = ET99.FindToken ( chPid )
If Err Then

    ShowErr "Not found ET99"
    ShowErr Digest
    Validate = false
    Exit function
 Else
ET99.OpenToken chPid,1
If Err then
    ShowErr "Open ET99 failed."
    Validate = false
    Exit function
End if
ET99.VerifyPIN 0, TheForm.UserPIN.Value
If Err Then
    ShowErr "Verify User PIN Failure!!!"
    Validate = false
    ET99.CloseToken
```

```
    Exit function
End If
dim results
results = "01234567890123456"
results = ET99.GetSN
If Err Then
    ShowErr "Get SN fail!"
    ET99.CloseToken
    Exit function
End If
If Not bErr Then
    Digest = ET99.MD5HMAC (1, <%
                Response.Write Chr(34)
                Response.Write RndData
                Response.Write Chr(34)
                %>, 20)
   If Err Then
      ShowErr "HashToken compute"
      Validate = false
      ET99.CloseToken
      Exit function
    End If
```

在硬件 MD5 计算中，第一个参数为密钥指示，“1”代表取第一个单元的密钥，在做身份认证时这个参数固定为“1”。第二个参数为待加密的数据，这里使用随机数，这样保证了每次验证的过程产生的散列结果都不相同，同时这个随机数也需要传送到服务器端参与计算。第三个参数为待加密数据的长度，这里即是随机数的长度。

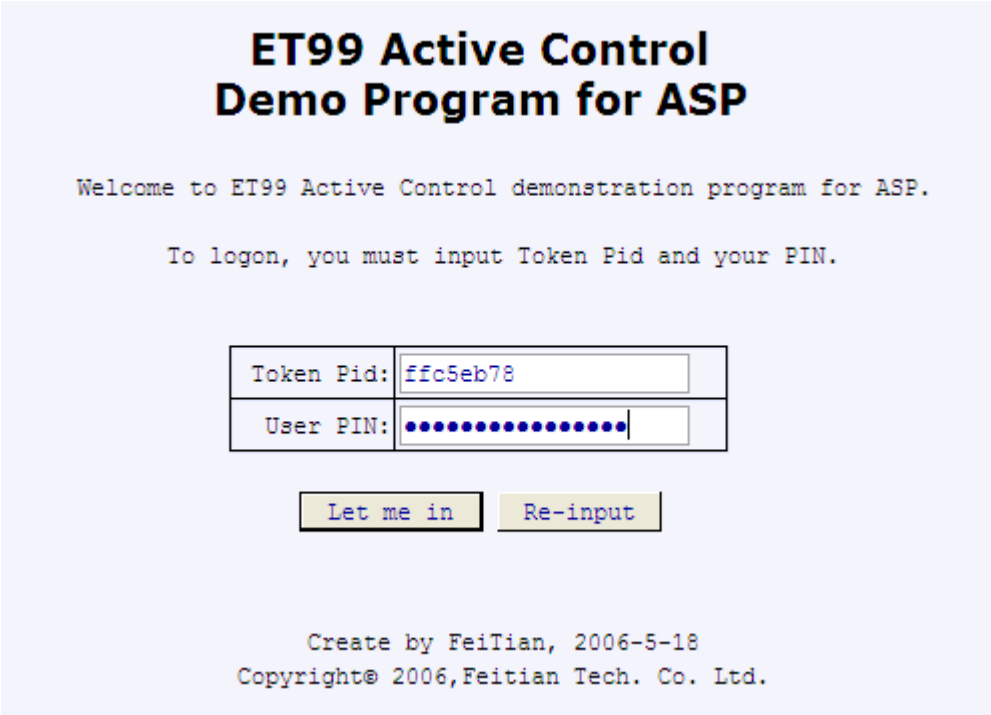
5、 在服务器端首先通过 CreateObject 方法创建一个对象实例，然后调

用软件 MD5 计算，产生服务器端的散列结果，这是将客户端计算传来的散列结果拿来做比较，如果结果相同，说明当前用户是合法的，如果不同，则说明用户不合法或者是密钥不正确。Verify.asp 实例代码如下:

```
If bErr = 0 Then
    Set S = Server.CreateObject("ET99_FULL.ET99Full.1")
    ServerDigest = S.Soft_MD5HMAC ( 1, RandomData,
PasswordInFile )
    ServerDigest = CStr(ServerDigest)
    If ServerDigest <> ClientDigest Then
        bErr = 4 'Password error.
    End If
    Set S = Nothing
End If
```

在软件实现 MD5 计算中，第一个参数是标志位，“0”表示 MD5 计算用于产生能够存储在 ET99 硬件中的密钥，“1”表示 MD5 计算用于产生服务器端散列结果，第二个参数“RandomData”即是待加密数据，参与 MD5 计算的随机数，第三个参数“PasswordInFile”存储在数据库中的密钥。

6、 使用坚石公司为您提供的 ASP Demo 测试冲击响应的身份认证。测试 ASP Demo 时需要预先安装 IIS 服务并建立虚拟目录。




该 ASP Demo 的登录页面如上图所示，登录验证的时候需要 USB Key 插在客户端，输入 PID 和 USER PIN（即硬件 PIN 码），点击“Let me in”，验证通过则会出现如下提示，说明登录用户合法。


如果客户端没有插 USB Key 或者密钥不正确等，登录系统，则会转到错误页面。