

深信服 SSL VPN 结合金笛短信猫认证

深信服提供的金笛短信猫，可看作由五部分组成：短信猫主体、天线、电源适配器、SIM 卡、串口线。图 1 所示为短信猫和天线两部分，图 2 所示为电源接口和串口线接口；图 3 所示为天线和 SIM 卡插槽，其中天线是可以拧下来的。



图 1



图 2



图 3

SSL VPN 设备上有 COM1、COM2 两个串口，我选择将短信猫接在 COM1 口上（当然接 COM2 口也可以）。

在简单了解了金笛短信猫之后，我们再去看看 SSL VPN 设备的配置。

在【SSL VPN 设置】-【基础配置】-【短信认证配置】下启用短信认证，如图 4 所示。其他都可如图 4 所示进行设置，“SCSM 号码”是你使用的 SIM 卡那家运营商提供的短信服务接入号，请联系您所使用 SIM 卡的当地运营商；“短信使用的串口”提供的选择项有“串口 0”和“串口 1”，而我们接的是 COM1 口，所以选择“串口 0”；如果接的是 COM2 口，那就要选择“串口 1”了。

>>短信认证管理

启用短信认证

短信模块设置

启用内置短信模块
 启用外置短信模块

短信认证配置

短信验证码有效时间: 10 分钟(1 - 1440) 短信密码有效时间以分钟为单位

自定义短信: SSLVPN短信验证码为: 自定义信息将显示在发给用户的短信上,不超过32个字符,中文占2个字符

短信网关配置

发送方式: 短信猫

SMSC号码: 8613044556677 SMSC为当地移动的短信服务号码,如:861380****500,监听端口号是短信服务器监听端口号

短信猫波频率: 9600

短信使用的串口: 串口0

图 4

要对用户启用短信认证，还要在用户信息栏输入其手机号，选择“私有用户”（短信只能发给一个人，公有用户那谁收），选一种主要认证方式，辅助认证选“短信”，如图 5 所示。

>>新建/编辑用户信息

名称:	dagongzai	
描述:		- 请输入用户描述信息!
密码:	●●●●●●●●	
确认密码:	●●●●●●●●	
手机号码:	18612345678	
数字证书信息:		生成证书
免驱DKEY认证:	生成免驱DKEY认证信息	
绑定虚拟IP:		
分组:	默认用户组	▼

继承用户组属性

认证方法 其它属性 组策略

用户类型: 公共用户 私有用户

主要认证组合方式: 与 或

主要认证:

- 用户名/密码
- 数字证书/DKEY认证
- 外部认证
 - 选择外部认证服务器:
 -

辅助认证:

- 硬件特征码
- 短信
- 令牌认证
 - 选择令牌认证服务器:
 -

图 5

接下来，我们再来看看短信认证如何使用。前提：如图 5 所示，主要认证我们已经选择为“用户名/密码”认证。

登录SSL VPN

用户名

密码

[手动安装组件](#)

其它登录方式：[证书登录](#) 或 [USB-Key登录](#)

图 6

如图 6 所示，输入用户名、密码进行完主要认证之后，就弹出图 7 所示的界面，几秒钟之后，你号码为“18612345678”的手机就会收到短信，短信中包含一个 6 位数字密码。输入此密码，点击“提交”，认证通过，即可进入资源界面。

短信的内容大致为你设置的“自定义短息内容”+“6 位数字密码”，此处大概为“SSL VPN 短信验证密码为：863721”这样一条内容，信息来自短信猫内插的那张 SIM 卡。

多说一点，如果短信密码的时效尚未过期，你下次登录还可以使用，如图 8 所示。那时效是多久呢？和图 4 中的设置有关，我设置的是 10 分钟，可调节的时间范围为 1 分钟到 1 天。

如果没有收到短信，可点击“重新获取”。

校验码

图 7

校验码

您的短信验证码仍在有效期内。

图 8