在 SSH 中使用 RSA 和 DSA 认证（详解）

**思路整理：**  
一直没有理解公匙模式下的认证过程，这里总结一下公匙和秘匙的制作和安置方法。以下假设一台服务器Server和一台PC作为例子。  
首先，并不是在服务器上生成公匙和秘匙。因为很多关于RSA 和 DSA 认证协议的文章都使用Linux服务器作为道具，自然也就使用诸如 *ssh-keygen -t rsa* 之类的命令，而使得我总是误认为要先在Linux服务器上先生成公匙和秘匙。而真正的安置方法是：  
当从PC连接Server的时候，需要在PC上保存一对公匙和秘匙(这对公匙和秘匙可以用诸如PenguiNet之类的工具生成)，而只要把生成的公匙传到Server上即可。而往往在Server上，公匙是被放在 ~/.ssh/authorized\_keys 这个文件中。这个文件的设置可以在 **/etc/ssh/sshd\_config** 中找到。

AuthorizedKeysFile .ssh/authorized\_keys

那么当从一个Linux Client Server连接到另外一个Linux Server的时候，我们应该在 Linux Client Server 上生成一对秘匙(RSA时默认为 id\_rsa 和 id\_rsa.pub)，保存在 ~/.ssh/ 中， 这个设置可以在 **/etc/sshd/ssh\_config** 中设置：

# IdentityFile ~/.ssh/identity  
# IdentityFile ~/.ssh/id\_rsa  
# IdentityFile ~/.ssh/id\_dsa

这样我们也可以更好地理解 ssh\_config 和 sshd\_config 的区别了。

 **RAS/DSA认证安装过程(以 tenten 用户为例)：**   
(以下测试在最新的OpenSSH 4.2 下通过，在 OpenSSH\_3.9p1 下测试失败！)

**[root@domain ~]$su - tenten**  
**[tenten@domain ~]ssh-keygen -t rsa**  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/tenten/.ssh/id\_rsa):[Enter]  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/tenten/.ssh/id\_rsa.  
Your public key has been saved in /home/tenten/.ssh/id\_rsa.pub.  
The key fingerprint is:  
c7:93:83:c4:24:30:56:90:37:a0:eb:a7:5d:4c:8d:ea:1a: tenten@example.com

:::或者:::

**[tenten@kdx ~]$ ssh-keygen -t dsa**  
Generating public/private dsa key pair.  
Enter file in which to save the key (/home/tenten/.ssh/id\_dsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/tenten/.ssh/id\_dsa.  
Your public key has been saved in /home/tenten/.ssh/id\_dsa.pub.  
The key fingerprint is:  
a2:be:16:2e:66:e4:69:68:a0:eb:a7:5d:4c:8d:ea:1a:da:54:35:55:32:8e:e2 tenten@example.com

查看生成的文件：

[tenten@kdx ~]$ ls /home/tenten/.ssh/ -la  
total 28  
drwx------ 2 tenten tenten 4096 Oct 11 16:09 .  
drwx------ 3 tenten tenten 4096 Oct 9 16:50 ..  
-rw------- 1 tenten tenten 736 Oct 11 16:09 **id\_dsa**  
-rw-r--r-- 1 tenten tenten 612 Oct 11 16:09 **id\_dsa.pub**  
-rw------- 1 tenten tenten 951 Oct 11 16:03 **id\_rsa**  
-rw-r--r-- 1 tenten tenten 232 Oct 11 16:03 **id\_rsa.pub**  
-rw-r--r-- 1 tenten tenten 667 Oct 9 16:48 known\_hosts

设置 sshd\_config 文件，去除密码认证

# To disable tunneled clear text passwords, change to no here!  
**PasswordAuthentication no**

由于在 sshd\_config 文件里面，我们设置了以下内容：

#AuthorizedKeysFile .ssh/authorized\_keys

所以我们要把共匙重命名为 autherized\_keys

[root@domain .ssh]# mv id\_dsa.pub autherized\_keys

所以最终服务器端 ~/.ssh/ 目录下的内容为（注意authorized\_keys的权限为 644）

[tenten@domain .ssh]$ ls -la  
total 12  
drwx------ 2 tenten tenten 4096 Oct 11 19:57 .  
drwx------ 3 tenten tenten 4096 Oct 11 18:50 ..  
-rw-r--r-- 1 tenten tenten 232 Oct 11 19:46 authorized\_keys

 引申：   
在安装 openssh 的最后，输入 make install 命令后，会发现最后会生成 public/private key：

Generating public/private **rsa1** key pair.  
Your identification has been saved in /usr/local/etc/ssh\_host\_key.  
Your public key has been saved in /usr/local/etc/ssh\_host\_key.pub.  
The key fingerprint is:  
22:67:00:5f:82:87:ab:22:e7:8e:cd:bb:d2:07:98:57 root@example.com

Generating public/private **dsa** key pair.  
Your identification has been saved in /usr/local/etc/ssh\_host\_dsa\_key.  
Your public key has been saved in /usr/local/etc/ssh\_host\_dsa\_key.pub.  
The key fingerprint is:  
17:6c:d8:6f:31:db:bd:3c:66:81:86:12:13:a4:33:a3 root@example.com

Generating public/private **rsa** key pair.  
Your identification has been saved in /usr/local/etc/ssh\_host\_rsa\_key.  
Your public key has been saved in /usr/local/etc/ssh\_host\_rsa\_key.pub.  
The key fingerprint is:  
27:0e:16:41:f8:96:ed:93:b6:a8:61:74:fe:87:e2:91 root@example.com  
/usr/local/sbin/sshd -t -f /usr/local/etc/sshd\_config