

SSH Single Sign On

User *user1* on host *SRV1* gains access *SRV2* (with *user2* identity) without interactive user/password authentication using the key-pair based authentication, as follows:

1. *user1* generates a pair of RSA keys on *SRV1*:

```
[user1@SRV1 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user1/.ssh/id_rsa):
Created directory '/home/user1/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user1/.ssh/id_rsa.
Your public key has been saved in /home/user1/.ssh/id_rsa.pub.
The key fingerprint is:
41:68:f1:9e:a2:9c:d3:fe:d4:b3:40:8d:a0:0c:a6:53 user1@SRV1
[user1@SRV1 ~]$
```

2. *user1* adds its *SRV1* public key (*~/.ssh/id_rsa.pub*) to the authorized keys (*~/.ssh/authorized_keys*) on *users2*'s home on *SRV2*:

```
[user1@SRV1 ~]$ cat ~/.ssh/id_rsa.pub | ssh user2@SRV2 'cat >>
~/.ssh/authorized_keys'
Password:
[user1@SRV1 ~]$
```

3. *user1* logs on *SRV2* with *user2* identity without password request

```
[user1@SRV1 ~]$ ssh user2@SRV2
Last login: Tue Dec 19 22:51:24 2006 from x
Sun Microsystems Inc. SunOS 5.10 Generic January 2005
$
```