

## Setup password-less SSH

### Objective:

For some batch processing where multiple servers are accessed, a password less SSH between multiple source and target remote servers is needed. The available methods for authentication are: host-based authentication, public key authentication, challenge-response authentication, and password authentication. We will list steps for public authentication.

### Mechanics:

The idea is that each user creates a public/private key pair for authentication purposes. The server knows the public key, and only the user knows the private key. ssh implements public key authentication protocol automatically, using either the RSA or DSA algorithms. The OpenSSH SSH client supports SSH protocols 1 and 2. Protocol 2 is the default; with ssh falling back to protocol 1 if it detects protocol 2 is unsupported.

Both protocols support similar authentication methods, but protocol 2 is preferred since it provides additional mechanisms for confidentiality (the traffic is encrypted using AES, 3DES, low-fish, CAST128, or Arcfour) and integrity (hmac-md5, hmac-sha1, hmac-ripemd160). For our purposes we will assume that protocol 2 (default) is supported and available.

### Steps:

1. On the source server (A) command line run command (execute from \$HOME)
 

```
ssh-keygen
```
2. Produces key pair: id\_rsa. id\_rsa (private key) & id\_rsa.pub (public key)
3. id\_rsa is stored and id\_rsa.pub is stored in ~/.ssh/

```

[hpXsgn1.a11-3.com:/rhome/rms054/.ssh]$ ls -l
total 32
-rw-r--r-- 1 rms001 games 407 Mar 16 15:59 authorized_keys2
-rw-----1 rms001 games 1675 Mar 16 15:56 id_rsa
-rw-r--r--1 rms001 games 407 Mar 16 15:56 id_rsa.pub
-rw-r--r-- 1 rms001 games 1608 Mar 16 17:26 known_hosts
  
```

4. On remote (Target) server check if a file authorized\_keys exist in ~/.ssh. If not, then create it by doing
 

```
touch authorized_keys
```
5. Move the public key id\_rsa.pub to the target remote server (B) and save it in
 

```
~/.ssh/authorized_keys
```

  - Ensure that the transfer of keys does not have any line fee or new line characters

Now you can log on to the remote target server without providing a password from your source server.