**Public Key Authentication**

For example: id\_dsa.pub, id\_dsa…

### Host Authentication

Host authentication is used to check if the host is correct or not. It can’t be used to configuring logins without passwords like Public Key Authentication.

[root@localhost .ssh]# ssh root@192.168.100.101

The authenticity of host '192.168.100.101 (192.168.100.101)' can't be established.

ECDSA key fingerprint is 42:c5:02:f7:ae:bb:85:8b:a9:c9:85:be:62:39:9b:0d.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.100.101' (ECDSA) to the list of known hosts.

root@192.168.100.101's password:

The authenticity of host '192.168.100.101 (192.168.100.101)' can't be established.

ECDSA key fingerprint is 42:c5:02:f7:ae:bb:85:8b:a9:c9:85:be:62:39:9b:0d.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.100.101' (ECDSA) to the list of known hosts.

Above red text is host authentication.

After confirming host authentication, you still have to input password.

To make sure that a user is not attacked by a man-in-the-middle attack, he is asked to check the fingerprint of the host key of the server when logging in the first time. As users typically do not check the fingerprints and just type in yes, it may also be a good idea to distribute the host public keys from the server to the clients. This is done in a similar manner as for public keys of the user in the previous section.

The host public keys are stored in /etc/ssh/ssh\_host\_dsa\_key.pub and /etc/ssh/ssh\_host\_rsa\_key.pub on the server. Each one contains a line begining with the type (ssh-dss or ssh-rsa), followed by the key (long ASCII string) and followed by the user who created the key (root@example or something else), e.g., for the DSA key:

#### File: /etc/ssh/ssh\_host\_dsa\_key.pub

ssh-dss AAAAB3Nz..nIwO4v0= root@example

To make the host known to the client, append its public key to /etc/ssh/ssh\_known\_hosts on the clients. The lines in that file have the following format consisting of a comma-separated list of hostname and IP of the server, the key type and the public key (again only one line!):

#### Excerpt: /etc/ssh/ssh\_known\_hosts

example,223.1.2.1 ssh-dss AAAAB3Nz..nIwO4v0=