

Host Setup

- [1 - Abstract](#)
- [2 - Client Certificate](#)
 - [Step 1 - Verify client certificates](#)
 - [Step 2 - Principals](#)
 - [Step 3 - Restart the SSH daemon](#)

1 - Abstract

As there are two different types of certificates, there are two individual tasks to setup a host.

- Host Certificate
- Client Certificate

Here at NetDEF we only use Client Certificates.

2 - Client Certificate

To setup the client certificate, the public key of the certificate authority is needed. There are three public keys called 'yubikey1.pub', 'yubikey2.pub' and 'yubikey3.pub'.

Step 1 - Verify client certificates

Add the following lines to the file '/etc/ssh/sshd_config' to tell the SSH daemon about the public key to verify client certificates. The host trusts all certificates the are signed by our CA.

```
### User CA certificate
TrustedUserCAKeys /etc/ssh/yubikey1.pub
TrustedUserCAKeys /etc/ssh/yubikey2.pub
TrustedUserCAKeys /etc/ssh/yubikey3.pub
```



Copy the public keys to the specified location.

Step 2 - Principals

Next we configure the hosts to accept only certain principals. To do so, add this line to '/etc/ssh/sshd_config'

```
### Auth Principals
AuthorizedPrincipalsFile /etc/ssh/auth_principals/%u
```

Then we need to populate the principals file. For each user we need to create a file.

```
mkdir -p /etc/ssh/auth_principals
echo -e 'host.netdef.org\nroot-everywhere' > /etc/ssh/auth_principals/root
```

This allows to all users to login as root that have either host.netdef.org or root-everywhere specified in the list of principals within their certificate.

You can control access to any other local user by creating the corresponding files under '/etc/ssh/auth_principals'.

Step 3 - Restart the SSH daemon