Client Setup

1 - Abstract

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

- Host Certificate
- Client Certificate

If one would like to use only one certificate, execute the corresponding subtask.

Configuration paths

There are two different options to tell the ssh daemon about the certificate: `'user based'` (recommended) or `'global'`

- `'user based'`: The certificate is valid for one specific user on the client.

```
SSH_CERTIFICATES=$HOME/.ssh/netdef
SSH_CONFIG=$HOME/.ssh/config
SSH_KNOWNHOSTS=$HOME/.ssh/known_hosts
```

- `'global'`: The certificate is valid for each user on the client.

```
SSH_CERTIFICATES=/etc/ssh/netdef
SSH_CONFIG=/etc/ssh/ssh_config
SSH_KNOWNHOSTS=/etc/ssh/ssh_known_hosts
```

2 - Client Certificate

Step 1 - Sign client's public key

The instructions how to singed a clients public key can be found here.

The CA provides a zip file where all signed keys are stored.

```
helloworld-1234567890-1-cert.pub
helloworld-1234567890-2-cert.pub
...
helloworld-1234567890-N-cert.pub
```

Step 2 - Copy all certificates to netdef folder

Copy all certificates that can be found in the provided tar file to the folder `'$SSH_CERTIFICATES'`.

```
mkdir -p $SSH_CERTIFICATES
cp *cert.pub $SSH_CERTIFICATES
```

Step 3 - Edit the config file

Add the following lines to `'$SSH_CONFIG'`. The name of the certificate as well as `'$SSH_CERTIFICATES'` must be replaced with the correct file name and the correct path to the folder respectively.

```
Host *.netdef.org
        CertificateFile `$SSH_CERTIFICATES`/helloworld-1234567890-1-cert.pub
        CertificateFile `$SSH_CERTIFICATES`/helloworld-1234567890-2-cert.pub
        ...
        CertificateFile `$SSH_CERTIFICATES`/helloworld-1234567890-N-cert.pub
```