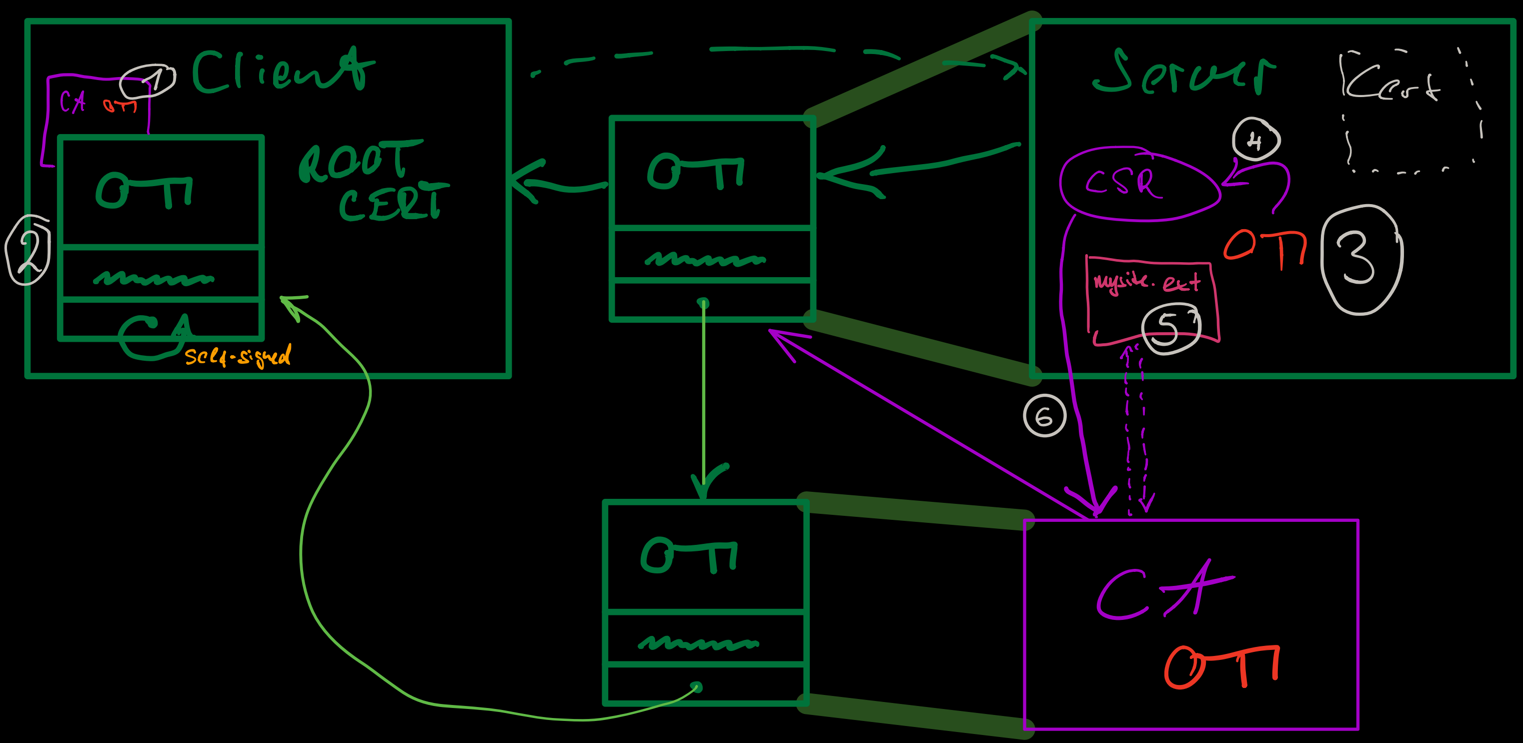
HTTPS



Setup https locally

- create own root CA:
  - Create private key (1)

```
openssl genrsa -des3
    -out myCA.key 2048
```

(do not omit passwd)

  - create root certificate (2)

```
openssl req -x509 -new -nodes
    -key myCA.key -sha256 -days 1825
```

```
-out myCA.pem
```

- deploy it to all machines
  - System (OS trust store)

    ```
    sudo mkdir /usr/local/share/ca-certificates/extra
    sudo cp myCA.pem —√/myCA.cert.crt
    sudo update-ca-certificates
    ```

  - Browser

    ~> do not make use of OS trust store, they use their own

    ```
    cert8.db
    cert9.db
    ```

    → see deploy script

- create CA-signed certificate for the site
  - create private key ③

    ```
    openssl genrsa -out mysite.key 2048
    ```

  - create CSR ④

    ```
    openssl req -new -key mysite.key -out mysite.csr
    ```

  - create mysite.ext ⑤

- Create signed certificate ⑥

```
openssl x509 -req -in mysite.csr -CA myCA.pem
    -CAkey myCA.key -CAcreateserial
    -out mysite.crt -days 825 -sha256
    -extfile mysite.ext
```