RSA-4096
SHA-512
NotAfter=50 years

C=<NRO>
O=<NRO name>
CN=eduroam-as-a-service <NRO> Server CA Root

private key

on CAT web server

kept offline

RSA-4096
SHA-512
NotAfter=**1.5 years**
EKU=serverAuth

C=<NRO>
O=<NRO name>
CN=auth.<nro>.hosted.eduroam.org

private key

on eaaS
RADIUS/EAP server

x ~ 200: one such structure for all NROs: AU, ..., LU, ... ZA

Notes:
* NRO's root CA is embedded with every installer
* NRO dependent server name is pinned with every installer

* corollary: once first client installer is "live" - no more changes to
  names and CA for given NRO

* still possible to do load-sharing and/or transfer of RADIUS/EAP
  to NROs:
  - "light": issue additional server cert with same CN to NRO for
    local EAP termination
  - "real": give root CA private key to NRO, for them to have
    control over EAP server certs
  - "exclusive": as in 'real', but afterwards OT deletes own copies of
    CA private key and server cert+key: NRO is on its own

Operational questions:
* do we need O= in the cert? NRO names change...
* 1.5 years validity to be discussed (chosen b/c clients never consult CRLs/OCSP
  anyway, so no revocation and thus should have short lifetime)