2.2 - Opret Certificate signing request (CSR) på Proxmox

2_2 – Opret Certificate Signing Request (CSR) på Proxmox

Information

Formålet med denne øvelse er at oprette en **Certificate Signing Request (CSR)** på Proxmox-hosten.

CSR'en indeholder oplysninger om serverens identitet og anvendes senere af den interne Root CA til at udstede et servercertifikat til Proxmox Web GUI.

Den private nøgle, som oprettes i denne øvelse, tilhører Proxmox og må ikke forlades systemet.

Deløvelser

1 Opret mappe til certifikatfiler

```
mkdir -p /root/certs
cd /root/certs
```

---

2 Generér privat nøgle til Proxmox

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

Denne private nøgle anvendes senere sammen med det signerede certifikat og skal forblive på Proxmox-hosten.

---

3 Opret Certificate Signing Request (CSR)

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

Når du bliver spurgt under oprettelsen: - **Common Name (CN)** → `proxmox.local` (eller det hostname, der anvendes til adgang)

Common Name skal svare til det navn, som senere bruges til at tilgå Proxmox Web GUI.

---

4 Opret Subject Alternative Name (SAN)-konfiguration

Moderne browsere kræver **SAN-felter** i certifikater. Common Name alene er ikke tilstrækkelig.

```
cat > san.cnf <<EOF
subjectAltName = DNS:proxmox.local,IP:192.168.1.50
EOF
```

Tilpas DNS-navn og IP-adresse, så de matcher din Proxmox-installation.

---

5 Overfør CSR og SAN-fil til Windows (CA-miljø)

```
scp proxmox.csr san.cnf youruser@windows-ip:/C:/proxmoxCA/
```

Disse filer anvendes i næste øvelse, hvor certifikatet signeres af den interne Root CA.

Når denne øvelse er gennemført, er Proxmox-hosten klar med: - en privat servernøgle - en CSR - en SAN-konfiguration

I næste øvelse (2_3) signeres certifikatet på Windows ved hjælp af den interne Root CA.

Last update: 2026-03-20 13:58:28