Võtmete genereerimine (RSA)

Genereeri 2048-bitine RSA privaatvõti
```
openssl genrsa -out KEY.pem 2048
```

Genereeri 4096-bitine RSA võti, krüpteeritud AES128-ga
```
openssl genrsa -out KEY.pem -aes128 4096
```

Võtme suurus peab olema käsu viimane argument. Krüpteerimisvalikud: -aes128, -aes192, -aes256, -des3

Võtmete genereerimine (Elliptiline kõver)

Genereeri EC võti otse (soovitatav kõver: P-384)
```
openssl genpkey -algorithm EC -pkeyopt ec_paramgen_curve:P-384 -out EC-KEY.pem
```

Genereeri EC parameetrite fail
```
openssl genpkey -genparam -algorithm EC -pkeyopt ec_paramgen_curve:secp384r1 -out EC-PARAM.pem
```

Vaata toetatud kõveraid
```
openssl ecparam -list_curves
```

Soovitatud kõverad: prime256v1 (P-256), secp384r1 (P-384), secp521r1 (P-521)

Sertifikaaditaotlused (CSR)

Loo CSR olemasoleva privaatvõtmega
```
openssl req -new -key KEY.pem -out CSR.pem
```

Loo CSR ja uus privaatvõti korraga
```
openssl req -new -newkey rsa:2048 -nodes -out CSR.pem -keyout KEY.pem
```

Määra subjekt käsureal (vältimaks interaktiivset küsitlust)
```
openssl req -new -key KEY.pem -out CSR.pem -subj "/CN=minu.ee/O=Firma/C=EE"
```

-nodes = privaatvõtit EI krüpteerita. -newkey rsa:2048 / ec:EC-PARAM.pem / dsa:DSA-PARAM.pem

Iseallkirjastatud sertifikaadid

Loo sertifikaat olemasoleva võtmega
```
openssl req -x509 -key KEY.pem -out CERT.pem -days 365
```

Loo sertifikaat ja uus võti korraga
```
openssl req -x509 -newkey rsa:2048 -nodes -out CERT.pem -keyout KEY.pem -days 365
```

-days N = sertifikaadi kehtivusaeg päevades (vaikimisi 30)

CA sertifikaadi allkirjastamine

Allkirjasta CSR oma CA sertifikaadiga
```
openssl x509 -req -in CSR.pem -CA ca.pem -CAkey ca-key.pem -CAcreateserial -out CERT.pem -days 365
```

-CAcreateserial loob seerianumbri faili automaatselt. Lisa -extfile ext.cnf laienduste jaoks.

Võtmete ja sertifikaatide vaatamine

Vaata RSA privaatvõtme sisu
```
openssl rsa -in KEY.pem -noout -text
```

Vaata mis tahes võtme sisu (RSA, DSA, EC)
```
openssl pkey -in KEY.pem -noout -text
```

Eralda ainult avalik võti
```
openssl pkey -in KEY.pem -pubout
```

Vaata x509 sertifikaadi sisu
```
openssl x509 -in CERT.pem -noout -text
```

Vaata CSR sisu
```
openssl req -in CSR.pem -noout -text
```

Sertifikaadist konkreetse info eraldamine

Kehtivusajad
```
openssl x509 -in CERT.pem -noout -dates
```

Väljaandja ja subjekt
```
openssl x509 -in CERT.pem -noout -issuer -subject
```

Seerianumber
```
openssl x509 -in CERT.pem -noout -serial
```

SAN (Subject Alternative Name) laiendus
```
openssl x509 -in CERT.pem -noout -ext subjectAltName
```

Muud: -modulus, -pubkey, -ocsp_uri, -startdate, -enddate, -fingerprint

Kontrollimine ja valideerimine

Kontrolli, kas võti ja sertifikaat sobivad kokku (võrdle modulust)
```
openssl x509 -in CERT.pem -noout -modulus | openssl md5
```
```
openssl rsa  -in KEY.pem  -noout -modulus | openssl md5
```

Kui md5 väärtused on samad, siis võti ja sertifikaat sobivad kokku.

Verifitseeri sertifikaat CA sertifikaadiga
```
openssl verify -CAfile ca.pem CERT.pem
```

Kontrolli sertifikaadi ahelat
```
openssl verify -CAfile ca.pem -untrusted intermediate.pem CERT.pem
```

TLS ühenduse testimine

Ühenda serveriga ja kuva sertifikaat
```
openssl s_client -connect server.ee:443 -showcerts
```

Testi konkreetset TLS versiooni
```
openssl s_client -connect server.ee:443 -tls1_3
```

Kuva ainult sertifikaadi ahel
```
openssl s_client -connect server.ee:443 2>/dev/null | openssl x509 -noout -text
```

OpenSSL Spikker — Failivormingud ja teisendamine

Failivormingud

PEM	Base64 kodeeritud, -----BEGIN...-----, kõige levinum
DER	Binaarne formaat, kompaktne, Java/Windows
PFX/P12	PKCS#12, võti + sertifikaat ühes failis, parooliga kaitstud
JKS	Java KeyStore, ainult Java rakendused (keytool)

Faili vormingu kontrollimine

Kontrolli, kas fail on PEM formaadis
```
openssl x509 -in FAIL
```

Kontrolli, kas fail on DER formaadis
```
openssl x509 -in FAIL -inform DER
```

Kontrolli, kas fail on PFX/P12 formaadis
```
openssl pkcs12 -in FAIL -nodes
```

Võtmefailide kontrollimiseks kasuta openssl pkey sama süntaksiga.

Teisendamine: PEM <=> DER

PEM → DER
```
openssl x509 -in CERT.pem -outform DER -out CERT.der
```

DER → PEM
```
openssl x509 -in CERT.der -inform DER -out CERT.pem
```

Teisendamine: PEM <=> PFX/P12

PEM → PFX (sertifikaat + võti)
```
openssl pkcs12 -export -in CERT.pem -inkey KEY.pem -out FAIL.pfx
```

PEM → PFX (ainult sertifikaadid, ilma võtmeta)
```
openssl pkcs12 -in CERTS.pem -nokeys -export -out CERTS.pfx
```

PFX → PEM (kõik)
```
openssl pkcs12 -in FAIL.pfx -out KOIK.pem -nodes
```

PFX → ainult privaatvõti
```
openssl pkcs12 -in FAIL.pfx -out KEY.pem -nodes -nocerts
```

PFX → ainult kliendisertifikaat
```
openssl pkcs12 -in FAIL.pfx -out CERT.pem -clcerts -nokeys
```

-cacerts = ainult CA sertifikaadid. -clcerts = ainult lõppolemi sertifikaat.

Kasulikud kombinatsioonid

Loo CA + serveri sertifikaat ühe skriptiga
```
# 1. Loo CA võti ja sertifikaat

openssl req -x509 -newkey rsa:4096 -nodes \
  -keyout ca-key.pem -out ca.pem -days 3650 \
  -subj "/CN=Minu CA/O=Labor/C=EE"

# 2. Loo serveri võti ja CSR

openssl req -new -newkey rsa:2048 -nodes \
  -keyout server-key.pem -out server.csr \
  -subj "/CN=server.labor.ee"

# 3. Allkirjasta CSR CA sertifikaadiga

openssl x509 -req -in server.csr \
  -CA ca.pem -CAkey ca-key.pem -CAcreateserial \
  -out server.pem -days 365
```

Räsimine ja krüpteerimine

Faili SHA256 räsi
```
openssl dgst -sha256 fail.txt
```

Faili krüpteerimine AES-256-CBC-ga
```
openssl enc -aes-256-cbc -salt -in fail.txt -out fail.enc
```

Faili dekrüpteerimine
```
openssl enc -d -aes-256-cbc -in fail.enc -out fail.txt
```

Juhusliku parooli genereerimine (32 baiti, base64)
```
openssl rand -base64 32
```

Kiirviide: peamised alavaldkonnad

`genrsa / genpkey`	Võtmete genereerimine
`req`	CSR loomine, iseallkirjastatud sertifikaadid
`x509`	Sertifikaatide vaatamine, teisendamine, allkirjastamine
`pkey / rsa / ec`	Võtmefailide vaatamine ja teisendamine
`pkcs12`	PFX/P12 failide loomine ja avamine
`s_client`	TLS ühenduse testimine
`verify`	Sertifikaadi ahela valideerimine
`dgst`	Räsifunktsioonid (SHA256, SHA384, ...)
`enc`	Sümmeetriline krüpteerimine/dekrüpteerimine
`rand`	Juhuslike andmete genereerimine

Nõuanded

- openssl version -a — vaata OpenSSL versiooni ja konfiguratsioonifaili asukohta
- openssl list -cipher-algorithms — loetelu toetatud šifritest
- openssl list -digest-commands — loetelu toetatud räsialgoritmidest
- Kasuta alati -noout, kui ei taha näha kodeeritud (PEM) väljundit