EeasyRSA

RootCA

apt install easy-rsa
mkdir /root-ca
cp –r /usr/share/easy-rsa/* /root-ca/
¨
./easyrsa init-pki
mv pki/vars.example pki/vars

nano pki/vars
set_var EASYRSA_DN "org"
set_var EASYRSA_REQ_COUNTRY "DK"
set_var EASYRSA_REQ_ORG "Lego APS"
set_var EASYRSA_REQ_CN "Lego APS Root CA"
(Set all other parameters to “”)
set_var EASYRSA_BATCH "yes"

./easyrsa build-ca nopass
cp /easyrsa/pki/ca.crt /ca/ca.crt
Verify: openssl x509 -in /ca/CA.crt -text –noout

SubCA

apt install easy-rsa
mkdir /sub-ca
cp –r /usr/share/easy-rsa/* /sub-ca/

./easyrsa init-pki
./easyrsa build-ca subca nopass

On root-ca: ./easyrsa import-req /sub-ca/pki/reqs/ca.req “Lego APS Intermediate CA”
On root-ca: ./easyrsa sign-req ca "Lego APS Intermediate CA"

cp /root-ca/easyrsa/pki/issued/”Lego APS Intermediate CA.crt” /sub-ca/pki/ca.crt

mv pki/vars.example pki/vars
nano pki/vars
set_var EASYRSA_AUTO_SAN 1

Chain

cat sub-ca.crt ca.crt > chain.pem

Remove all fields from the file other than the actual certificates.

Order:
1. Application

2. Sub
3. Root

cp chain.pem chain.crt

Trust

cp /ca/chain.crt /usr/local/share/ca-certificates/
update-ca-certificates

You also have to add the cert to the browser trust store.

Generate cert

On sub-ca: ./easyrsa gen-req <FQDN> nopass
On sub-ca: ./easyrsa sign-req server <FQDN>

cat /sub-ca/pki/issued/<FQDN>.crt chain.crt > fqdn.pem