Make Your Web great again

A. Konfigurasi dasar

B. Cerficate authority
Jika saya memiliki operasi system Linux maka langkah2 pengerjaan saya sbb:

Sudo apt install openssl
Buatkan direktorinya
mkdir -p /root/ca
cd /root/ca

Buat file yang diperlukan untuk CA
touch index.txt
echo 1000 > serial
kemudian membuat root CA certificate

openssl genrsa -aes256 -out private/cacert.key 2048

kemudian buat serfikat CA root yg ditanda tangani sendiri

openssl req -x509 -new -nodes -key private/cacert.key -sha256 -days 3650 -out cacert.pem

Saat diminta, masukkan informasi yang diperlukan.
Untuk memudahkan pembuatan sertifikat, buat berkas openssl.cnf di /root/ca dengan konten berikut.
cat <<EOF > /root/ca/openssl.cnf
[ca]
default_ca = CA_default

[CA_default]
dir = /root/ca
certs = \$dir/certs
crl_dir = \$dir/ca_crl
new_certs_dir = \$dir/newcerts
database = \$dir/index.txt
serial = \$dir/serial
RANDFILE = \$dir/private/.rand

private_key = \$dir/private/cacert.key

```
certificate       = \$dir/cacert.pem

crldays           = 365
policy            = policy_strict

[ policy_strict ]
countryName             = match
stateOrProvinceName     = optional
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits        = 2048
distinguished_name  = req_distinguished_name
string_mask         = utf8only

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = ID

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = East Java

localityName                    = Locality Name (eg, city)
localityName_default            = Surabaya

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = PT Sentra Vidya Utama

organizationalUnitName          = Organizational Unit Name (eg, section)

commonName                      = Common Name (e.g. server FQDN or YOUR name)

emailAddress                    = Email Address
emailAddress_default            =

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

[v3_ca]
basicConstraints = CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
keyUsage = digitalSignature, cRLSign, keyCertSign
EOF

Sekarang, mari kita buat sertifikat untuk situs web Anda. Untuk setiap situs web, kita akan membuat kunci pribadi, Permintaan Penandatanganan Sertifikat (CSR), lalu menandatangani CSR dengan CA Root Anda.

a. Sertifikat www.sevima.site
Buat kunci privat
openssl genrsa -out /root/ca/private/www.sevima.site.key 2048

Buat Permintaan Penandatanganan Sertifikat (CSR)
openssl req -new -key /root/ca/private/www.sevima.site.key -out /root/ca/www.sevima.site.csr -config /root/ca/openssl.cnf
Saat diminta detail CSR untuk www.sevima.site, pastikan Nama Umum (Common Name)-nya adalah www.sevima.site. Kolom lain dapat mewarisi pengaturan default di openssl.cnf.
Saat diminta detail CSR untuk www.sevima.site, pastikan Nama Umum adalah www.sevima.site. Kolom lain dapat mewarisi pengaturan default di openssl.cnf.

b. utara.sevima.site Sertifikat
Buat kunci privat
openssl genrsa -out /root/ca/private/utara.sevima.site.key 2048

Buat Permintaan Penandatanganan Sertifikat (CSR)
openssl req -new -key /root/ca/private/utara.sevima.site.key -out /root/ca/utara.sevima.site.csr -config /root/ca/openssl.cnf
Saat diminta detail CSR untuk utara.sevima.site, pastikan Nama Umum adalah utara.sevima.site.

Tandatangani CSR dengan CA Root Anda
openssl ca -batch -config /root/ca/openssl.cnf -extensions v3_req -days 365 -in /root/ca/utara.sevima.site.csr -out /root/ca/certs/utara.sevima.site.crt

C. timur.sevima.site Sertifikat

Tandatangani CSR dengan CA Root Anda

openssl genrsa -out /root/ca/private/timur.sevima.site.key 2048

Buat Permintaan Penandatanganan Sertifikat (CSR)

openssl req -new -key /root/ca/private/timur.sevima.site.key -out /root/ca/timur.sevima.site.csr -config /root/ca/openssl.cnf

Saat diminta rincian CSR untuk timur.sevima.site, pastikan Nama Umum adalah timur.sevima.site.

D. barat.sevima.site Sertifikat

Tandatangani CSR dengan CA Root Anda

openssl genrsa -out /root/ca/private/barat.sevima.site.key 2048

Buat Permintaan Penandatanganan Sertifikat (CSR)

openssl req -baru -kunci /root/ca/private/barat.sevima.site.key -out /root/ca/barat.sevima.site.csr -config /root/ca/openssl.cnf

Saat diminta rincian CSR untuk barat.sevima.site, pastikan Nama Umum adalah barat.sevima.site.

Tandatangani CSR dengan CA Root Anda

openssl ca -batch -config /root/ca/openssl.cnf -extensions v3_req -hari 365 -in /root/ca/barat.sevima.site.csr -out /root/ca/certs/barat.sevima.site.crt

C. Web Server