Création d'un certificat CA racine autosigné

Instructions sur la façon de créer un certificat CA racine autosigné pour signer des certificats CA intermédiaires.

1. Préparez un répertoire pour l'autorité de certification racine où est stockée la clé privée du certificat racine.

   mkdir rootCA
   mkdir rootCA/{certs,db}
   touch rootCA/db/db
   touch rootCA/db/db.attr

   aller dans le répertoire rootCA

2. Créez un fichier de configuration root-csr.conf qui contient les lignes suivantes :

   [req]
   encrypt_key = no
   utf8 = yes
   string_mask = utf8only
   prompt=no
   distinguished_name = root_dn
   x509_extensions = extensions
   [root_dn]
   # Nom de pays (code à 2 lettres)
   countryName = FR
   # Nom de localité (par exemple, ville)
   localityName = Aubiere
   # Nom d'organisation (par exemple, entreprise)
   #0.organizationName = Example Corp
   organizationName = AAA- ….
   # Nom de certificat
   commonName = Autorite certification racine
   [extensions]
   keyUsage = critical,keyCertSign,cRLSign
   basicConstraints = critical,CA:TRUE
   subjectKeyIdentifier = hash

   Conseil: Pour en savoir plus sur les paramètres de configuration disponibles, reportez-vous aux pages man OpenSSL (par exemple, man req) et consultez le fichier type openssl.cnf de votre installation (par exemple, /etc/pki/tls/openssl.cnf sous CentOS).

3. Exécutez la commande suivante pour créer une nouvelle clé racine et un certificat racine autosigné :

   openssl req -x509 -sha256 -days 3650 -newkey rsa:3072 \
   -config root-csr.conf -keyout rootCA.key -out rootCA.crt

4. Exécutez la commande suivante pour vérifier les informations contenues dans le certificat créé :

   openssl x509 -in rootCA.crt -text -noout

Création d'un certificat CA intermédiaire pour créer d'autres certificats

Vous devez créer un certificat intermédiaire signé via le certificat racine afin de pouvoir signer les certificats pour le serveur qui héberge le portail Web ou autres serveurs internes.

Suivez ces instructions pour créer une requête de signature de certificat, puis utilisez le certificat racine et sa clé pour signer le certificat intermédiaire dans la requête.

1. Préparez un répertoire pour l'autorité de certification intermédiaire où est stockée la clé privée du certificat CA.

   ```
   mkdir CA
   mkdir CA/{certs,db}
   touch CA/db/db
   touch CA/db/db.attr
   ```

2. Créez un fichier de configuration CA-csr.conf qui contient les lignes suivantes :

   ```
   [ req ]
   encrypt_key = no
   default_bits = 2048
   default_md = sha256
   utf8 = yes
   string_mask = utf8only
   prompt = no
   distinguished_name = ca_dn
   [ ca_dn ]
   0.organizationName = "a completer"
   organizationalUnitName = "a completer"
   commonName = "a completer"
   ```

3. Exécutez la commande suivante pour créer une requête de signature de certificat avec la nouvelle clé privée :

   openssl req -new -config CA-csr.conf -out CA.csr -keyout CA.key

4. Créez un fichier de configuration rootCA.conf qui contient les lignes suivantes :

```
[ ca ]
default_ca = the_ca
[ the_ca ]
dir = ./rootCA
private_key = $dir/rootCA.key
certificate = $dir/rootCA.crt
new_certs_dir = $dir/certs
serial = $dir/db/crt.srl
database = $dir/db/db
default_md = sha256
policy = policy_any
email_in_dn = no
[ policy_any ]
domainComponent = optional
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = optional
emailAddress = optional
[ ca_ext ]
keyUsage = critical,keyCertSign,cRLSign
basicConstraints = critical,CA:true
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always
```

    - Les certificats signés avec le certificat racine doivent se référer à sa liste de révocation de certificats (CRL).
5. Exécutez la commande suivante pour signer le certificat dans la requête à l'aide du certificat racine :

   ```
   openssl ca -config rootCA.conf -days 365 -create_serial \
   -in CA.csr -out CA.crt -extensions ca_ext -notext
   ```

    - Utilisez l'option Extensions pour sélectionner la section appropriée du fichier de configuration.
6. Reliez les certificats de façon à créer la chaîne de certificats dans un fichier unique :

   ```
   cat CA/CA.crt rootCA/rootCA.crt >CA/CA.pem
   ```

Vous disposez désormais du nouveau certificat CA intermédiaire et de sa clé privée stockée dans le répertoire CA.!!!

Création d'un certificat d'entité finale pour le serveur Web

Instructions sur la façon de créer le certificat pour le serveur qui héberge le portail Web. Le certificat d'entité finale est signé via le certificat CA intermédiaire qui a été lui-même signé à l'aide du certificat racine.

Suivez ces instructions pour créer une requête de signature de certificat, puis utilisez le certificat CA intermédiaire et sa clé pour signer le certificat d'entité finale dans la requête.

1. Créez une clé pour votre serveur web et son fichier de requête

   ```
   openssl genrsa -out server.key 2048
   openssl req -new -key server.key -out server.csr
   ```

2. Créez un nouveau fichier de configuration CA.conf qui contient les lignes suivantes :

   ```
   [ ca ]
   default_ca = the_ca
   [ the_ca ]
   dir = ./CA
   private_key = $dir/private/CA.key
   certificate = $dir/CA.crt
   new_certs_dir = $dir/certs
   serial = $dir/db/crt.srl
   database = $dir/db/db
   unique_subject = no
   default_md = sha256
   policy = any_pol
   email_in_dn = no
   copy_extensions = copy
   [ any_pol ]
   domainComponent = optional
   countryName = optional
   stateOrProvinceName = optional
   localityName = optional
   organizationName = optional
   organizationalUnitName = optional
   commonName = optional
   emailAddress = optional
   [ leaf_ext ]
   keyUsage = critical,digitalSignature,keyEncipherment
   basicConstraints = CA:false
   extendedKeyUsage = serverAuth,clientAuth
   subjectKeyIdentifier = hash
   authorityKeyIdentifier = keyid:always
   ```

[ca_ext]
keyUsage = critical,keyCertSign,cRLSign
basicConstraints = critical,CA:true,pathlen:0
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always

- Les certificats signés avec le certificat racine doivent se référer à sa liste de révocation de certificats (CRL).

3. Exécutez la commande suivante pour signer le certificat du serveur dans la requête à l'aide du certificat CA intermédiaire :

   openssl ca -config CA.conf -days 365 -create_serial \
   -in server.csr -out server.crt -extensions leaf_ext -notext

   - Utilisez l'option Extensions pour sélectionner la section appropriée du fichier de configuration.

Vous disposez désormais du nouveau fichier de certificat du serveur server.crt et de sa clé privée server.key dans le répertoire actuel.

Exécutez la commande suivante pour vérifier les informations contenues dans le certificat :

openssl x509 -in server.crt -text -noout

Attendre l'explication

mettre le certificat dans firefox

Onglet paramètres, vie privée et sécurité

Tout en bas : certificats

➔ Afficher les certificats
- Autorité
  - Importer
    On importe les 2 certificats (root et intermédiaire) -> fichier CA.pem

Dans le fichier ssl.conf, mettre le certificat server, signé par la clé intermédiaire.

Cela ne fonctionne pas …

Utilisation du San (Subject Alt Name) au lieu du CN

Ajouter : subjectAltName = DNS: nom_machine dans la section [leaf_ext]