

Créer sa CA et signer ses certificats

Pour cela, on va se rendre dans un dossier isolé :

```
# mkdir /root/ca && cd /root/ca  
</bash>
```

puis on va créer l'organisation de dossier suivante:

```
<code bash>  
# mkdir certs crl newcerts private  
# chmod 700 private
```

Et on créer les fichiers de contrôle :

```
# touch index.txt  
# echo 1000 > serial
```

puis on créer le fichier :

[openssf.cfg](#)

```
[ ca ]  
# `man ca`  
default_ca = CA_default  
  
[ CA_default ]  
# Directory and file locations.  
dir                = /root/ca  
certs              = $dir/certs  
crl_dir            = $dir/crl  
new_certs_dir      = $dir/newcerts  
database           = $dir/index.txt  
serial             = $dir/serial  
RANDFILE           = $dir/private/.rand  
  
# The root key and root certificate.  
private_key        = $dir/private/ca.key.pem  
certificate        = $dir/certs/ca.cert.pem  
  
# For certificate revocation lists.  
crlnumber          = $dir/crlnumber  
crl                = $dir/crl/ca.crl.pem  
crl_extensions     = crl_ext  
default_crl_days   = 30  
  
# SHA-1 is deprecated, so use SHA-2 instead.  
default_md         = sha256
```

```
name_opt          = ca_default
cert_opt          = ca_default
default_days     = 375
preserve         = no

[ req ]
# Options for the `req` tool (`man req`).
default_bits     = 4096
distinguished_name = req_distinguished_name
string_mask      = utf8only

# SHA-1 is deprecated, so use SHA-2 instead.
default_md       = sha256

# Extension to add when the -x509 option is used.
x509_extensions  = v3_ca

[ req_distinguished_name ]
countryName          = Country Name (2 letter code)
stateOrProvinceName = State or Province Name
localityName         = Locality Name
#.organizationName  = Organization Name
organizationalUnitName = Organizational Unit Name
commonName           = Common Name
emailAddress         = Email Address

countryName_default      = FR
stateOrProvinceName_default = Deux-Sèvres
localityName_default     = Niort
#.organizationName_default = VirtIT
#organizationalUnitName_default =
emailAddress_default     = contact@virtit.fr

[ v3_ca ]
# Extensions for a typical CA (`man x509v3_config`).
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
```

From:
<https://wiki.virtit.fr/> - VirtIT

Permanent link:
https://wiki.virtit.fr/doku.php/kb:crypto:creer_ca?rev=1534974547

Last update: **2018/08/22 21:49**



