Connexion en SSH

Sur un VM Debian qui nous sert de serveur. On se connecte en SSH :

```
C:\Users\NJ-Ghost>ssh pki@10.40.0.5
pki@10.40.0.5's password:
Permission denied, please try again.
pki@10.40.0.5's password:
Linux SRVM-PKI 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pki@SRVM-PKI:~$ su
Mot de passe :
root@SRVM-PKI:/home/pki#
```

Préparation

Nous allons créer la structure des répertoires, qui servira à accueillir les différents fichiers nécessaires au bon fonctionnement de la PKI. Nous allons donc rentrer les commandes suivantes :

```
root@SRVM-PKI:/home/pki# mkdir -p /etc/pki/{certs,crl,newcerts,private}
root@SRVM-PKI:/home/pki# chmod 700 /etc/pki/private
root@SRVM-PKI:/home/pki# touch /etc/pki/index.txt
root@SRVM-PKI:/home/pki# nano /etc/pki/serial
```

Puis dans le fichier précédemment surligné, **Ajouter** 1000 :

```
  GNU nano 7.2                                          /etc/pki/serial *
1000
```

Configuration du fichier

Nous allons copier le fichier de configuration par défaut de OpenSSL pour ensuite le modifier :

```
root@SRVM-PKI:/home/pki# cp /etc/ssl/openssl.cnf /etc/pki/openssl.cnf
root@SRVM-PKI:/home/pki# nano /etc/pki/openssl.cnf
```

```
[ ca ]
default_ca      = CA_default            # The default ca section

####################################################################
[ CA_default ]

dir             = /etc/pki              # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/certs/ca.crt     # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/ca.key   # The private key
RANDFILE        = $dir/private/.rand    # Fichier aléatoire
x509_extensions = usr_cert              # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default            # Subject Name options
cert_opt        = ca_default            # Certificate field options

# Extension copying option: use with caution.
# copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.
# crl_extensions        = crl_ext

default_days    = 365                   # how long to certify for
default_crl_days= 30                    # how long before next CRL
default_md      = sha256                # use public key default MD
preserve        = no                    # keep passed DN ordering

# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
policy          = policy_match
```

```
[ req ]
default_bits            = 2048
default_keyfile         = /etc/pki/private/ca.key
distinguished_name      = req_distinguished_name
attributes              = req_attributes
x509_extensions         = v3_ca                 # The extensions to add to the self signed cert
```

A cette étape on ne modifie uniquement **_default** ou on l'ajoute si celui n'est pas présent :

```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = FR
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = PACA

localityName                    = Locality Name (eg, city)
localityName_default            = Avignon
0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = ITWay

# we can do this but it is not needed normally :-)
#1.organizationName             = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = IT
#organizationalUnitName_default =

commonName                      = Common Name (e.g. server FQDN or YOUR name)
commonName_max                  = 64
commonName_default              = ITWay

emailAddress                    = Email Address
emailAddress_max                = 64
emailAddress_default            = contact@itway.local
# SET-ex3                       = SET extension number 3
```

Créer la clé privée et le certificat de l'Autorité de Certification

On génère une clé privée pour l'AC avec la commande suivante, dont il faudra entrer une phrase de pass, par exemple : BTSSIO!

```
root@SRVM-PKI:/home/pki# openssl genrsa -aes256 -out /etc/pki/private/ca.key 4096
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Puis entrer cette ligne de commande :

```
root@SRVM-PKI:/home/pki# chmod 400 /etc/pki/private/ca.key
```

Par la suite on créer un certificat pour l' AC qui est valable selon la durée que l'on lui donne, ici par ex : 3650 jours soit 10 ans :

```
root@SRVM-PKI:/home/pki# openssl req -new -x509 -days 3650 -key /etc/pki/private/ca.key -sha256 -out /etc/pki/certs/ca.crt -config /etc/pki/openssl.cnf
```

Par la suite on vous demande de rentrer la phrase de pass créée précédemment. Une fois celle-ci rentrée, si le fichier configuré précédemment a été saisi correctement, les paramètres par default apparaitrons, il suffira de faire entrer.

```
Enter pass phrase for /etc/pki/private/ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:
State or Province Name (full name) [PACA]:
Locality Name (eg, city) [Avignon]:
Organization Name (eg, company) [ITWay]:
Organizational Unit Name (eg, section) [IT]:
Common Name (e.g. server FQDN or YOUR name) [ITWay]:
Email Address [contact@itway.local]:
```

Création de certificats pour les clients et les serveurs

On va se placer dans **/etc/pki/newcerts/** puis entrer la commande suivante afin de créer une clé privée pour un client ou un serveur, ICI GLPI :

```
root@SRVM-PKI:/etc/pki/newcerts# openssl genrsa -out glpi.key 2048
```

Ensuite on créer une requête de signature (CSR) pour le certificat client :

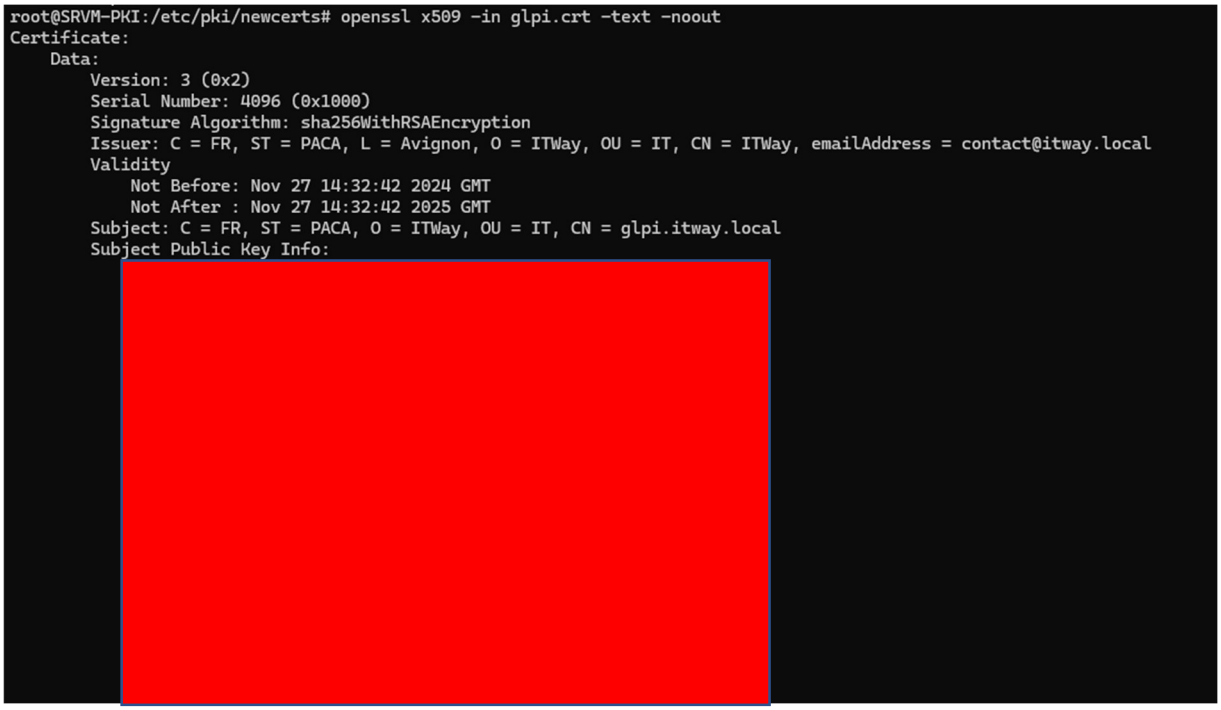
```
root@SRVM-PKI:/etc/pki/newcerts# openssl req -new -key glpi.key -out glpi.csr -subj "/C=FR/ST=PACA/L=Avignon/O=ITWay/OU=IT/CN=glpi.itway.local"
```

Par la suite on va signer le certificat client avec l'AC, il vous faudra rentrer la phrase de pass. Puis le certificat qui vient d'être généré serra détaillé. Il faudra le valider.

```
root@SRVM-PKI:/etc/pki/newcerts# openssl ca -config /etc/pki/openssl.cnf -in glpi.csr -out glpi.crt -days 365
Using configuration from /etc/pki/openssl.cnf
Enter pass phrase for /etc/pki/private/ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 27 14:32:42 2024 GMT
            Not After : Nov 27 14:32:42 2025 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = PACA
            organizationName          = ITWay
            organizationalUnitName    = IT
            commonName                = glpi.itway.local
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                13:07:10:D4:66:87:32:87:A2:1E:8F:81:A0:CF:52:52:75:3B:6E:35
            X509v3 Authority Key Identifier:
                AB:11:E2:62:E9:5D:DF:70:75:7D:A1:BE:BA:3C:00:EC:C8:D9:6B:05
Certificate is to be certified until Nov 27 14:32:42 2025 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
```

On procède à la vérification du certificat généré :



Test et validation

On vérifie la validité du certificat :

Pour trouver la clé, il faut aller dans le dossier où se trouve la clé :