

L'objectif ici est de sécuriser l'accès à votre site web, ici l'exemple porte sur GLPI, mais vous pouvez faire cela pour n'importe quel site web hébergé sur votre serveur Apache.

Le mode chiffré de HTTP (HTTPS) repose sur l'utilisation d'algorithmes asymétriques. Le serveur conserve secrètement sa clef privée et diffuse le plus largement possible sa clef publique. Ainsi, il peut prouver son identité, car il possède la clef privée associée à cette clef publique. Seule la clef privée peut chiffrer un message déchiffré par la clef publique. Ceci repose sur deux hypothèses fortes :

- Secret de la clef privée : l'algorithme prouve que l'émetteur possède bien la clef privée. Si celle-ci a été dérobée, alors le message est soit légitime, soit émis par celui qui a dérobé la clef.
- Identification de la clef publique : Il faut aussi être sûr que la clef publique est bien celle du serveur. Sinon, il est possible d'établir une communication sécurisée avec un autre site, qui pourra soit mettre en place une version alternative du site, soit simplement écouter la communication légitime.

Pour assurer le secret de la clef privée, il convient d'utiliser un serveur raisonnablement sécurisé (mis à jour des correctifs).

Étape 1 : Activez le module SSL d'apache2

- ✓ Pour faire en sorte que le glpi réponde à : <https://www.glpi.local> avec un DNS local de référence

```
#a2enmod ssl
```

- ✓ Modifiez les fichiers de conf de l'accès au site **glpi**, si besoin copiez les fichiers par défaut et modifiez les comme suit :

```
#cp /etc/apache2/sites-available/default-ssl.conf glpi-ssl.conf
#cp /etc/apache2/sites-available/000-default.conf glpi.conf
```

```
#nano /etc/apache2/sites-available/glpi.conf
```

```
<VirtualHost *:80>
    ServerName glpi.local
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/glpi

#rediriger sur https    DirectoryIndex glpi.html
    Redirect permanent / https://glpi.local/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory /var/www/glpi>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

```
#nano /etc/apache2/sites-available/glpi-ssl.conf
```

```
<IfModule mod_ssl.c>
    <VirtualHost *:443>
        ServerName glpi.local
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/glpi
        <Directory /var/www/glpi>
            Options Indexes FollowSymLinks
            AllowOverride All
            Require all granted
        </Directory>
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
#FICHIERS certificat et clé à créer voir plus loin
        SSLCertificateFile /opt/ca/glpi.crt
        SSLCertificateKeyFile /opt/ca/glpi.key
        <FilesMatch "\.(cgi|sh|html|php)$">
            SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
            SSLOptions +StdEnvVars
        </Directory>
    </VirtualHost>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Quelques explications :

VirtualHost : permet d'ajouter un hôte virtuel (notre nouveau site) ;

*:80 : valable quelle que soit l'adresse IP et utilise le port 80 ;

ServerAdmin : l'e-mail du webmestre ;

DocumentRoot : le répertoire local qui contient le site ;

ServerName : le nom entré dans le navigateur ;

Log(s) : les fichiers de logs qui peuvent être distincts pour chaque

site.

SSLCertificateFile /opt/ca/glpi.crt : lien avec le certificat de l'autorité de certification à importer sur le client puis auto-certifié

SSLCertificateKeyFile /opt/ca/glpi.key : Lien avec la clé privé du site

- ✓ Désactivez les sites par défaut et activez les sites glpi :

```
#a2disssite default-ssl.conf
#a2disssite 000-default.conf
#a2ensite glpi.conf
#a2ensite glpi-ssl.conf
```

Étape 2 : créer l'autorité de certification les clés et certificats nécessaires pour chiffrer la communication

Les paramètres du certificats autosigné :

clef privé glpi :

Les nouveaux paramètres sont :

- glpi.key : la cle privé de glpi

-in glpi.csr : la demande de certificat ;

-out glpi.crt : le certificat créé ;

-CA ca.crt : le certificat de l'autorité de certification ;

-CAkey ca.key : la clef privée de l'autorité de certification ;

-CAcreateserial -CAserial ca.srl : il faut créer et utiliser un numéro de série qui sera incrémenté à chaque nouvelle utilisation, la création n'est faite qu'une fois.

- ✓ Créez un répertoire pour stocker ces fichiers et création d'une clef privée pour l'autorité de certification :

Nous allons devenir une autorité de certification, signer la nouvelle clef pour glpi, puis nous connecter à nouveau avec notre navigateur. Il faut générer une clef privée pour l'autorité de certification. Cette clef peut être protégée par une phrase de passe, c'est même recommandé. Nous générons une clef RSA de longueur 4096.

```
root@SIO1-GLPI-CG:~#mkdir /opt/ca
root@SIO1-GLPI-CG:~#cd /opt/ca
root@SIO1-GLPI-CG:/opt/ca# openssl genrsa -des3 4096 > ca.key
```

Generating RSA private key, 4096 bit long modulus (2 primes)

.....+++++

.....+++++

e is 65537 (0x010001)

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

- ✓ Maintenant qu'on a la clé, on va générer le **root certificate (certificat racine)**, créez ensuite le certificat de l'autorité qui sera importé par le navigateur :

```
root@SIO1-GLPI-CG:/opt/ca# openssl req -x509 -new -nodes -key ca.key -sha256 -days
10000 -out ca.pem
```

Ici, vous générez le certificat pour une durée de 10.000 jours pour être tranquille une bonne fois pour tout en interne.

Au moment de la génération, il est demandé la passphrase de la clé précédente.

Un certain nombre de questions sont posées, y répondre comme mis en exemple ici :

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) [AU]:FR
State or Province Name (full name) [Some-State]:Bretagne
Locality Name (eg, city) []:Lannion
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FLD
Organizational Unit Name (eg, section) []:Local
Common Name (e.g. server FQDN or YOUR name) []:www.glpi.local
Email Address []:webmaster@localhost

Les options de la commande openssl :

req : demande de chiffrement de certificat ;
-new : génère une nouvelle demande de certificat ;
-x509 : génère un certificat autosigné ;
-days 10000 : durée de validité du certificat ;
-nodes : ne crypte pas la clef privée ;
-out /etc/ssl/localcerts/geronimo.pem : le fichier de certificat ;
-keyout /etc/ssl/localcerts/geronimo.key : le fichier de la clef privée.

- ✓ Dans le cas où vous auriez besoin d'un fichier .crt (au lieu du .pem), exécutez cette commande :
root@SIO-CG-pfwiki /opt/ca# openssl x509 -in ca.pem -inform PEM -out ca.crt
- ✓ créez ensuite une clé privée pour le site **glpi** :

```
root@SIO1-GLPI-CG:/opt/ca#openssl genrsa 4096 > glpi.key
```

Generating RSA private key, 4096 bit long modulus (2 primes)

```
.....++  
++  
.....++++  
e is 65537 (0x010001)
```

- ✓ Ensuite, il faut préparer une demande de certificat (CSR(Certificate Signing Request)) cette demande doit être envoyée à l'autorité de certification :

```
root@SIO1-GLPI-CG:/opt/ca# openssl req -new -key glpi.key > glpi.csr
```

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) [AU]:FR
State or Province Name (full name) [Some-State]:Bretagne
Locality Name (eg, city) []:Lannion
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FLD
Organizational Unit Name (eg, section) []:Local
Common Name (e.g. server FQDN or YOUR name) []:www.glpi.local
Email Address []:webmaster@localhost

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:Btssio2017

An optional company name []:FLD

- ✓ Enfin, l'autorité signe la clef du serveur :
On va créer un fichier de configuration pour le sous-domaine concerné, pour cela créez le fichier glpi.ext, ainsi complété :
root@SIO1-GLPI-CG:/opt/ca# glpi.ext

```
authorityKeyIdentifier=keyid,issuer  
basicConstraints=CA:FALSE  
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment  
subjectAltName = @alt_names  
[alt_names]  
#DNS.1=FQDN  
DNS.1 = www.glpi.local
```

- ✓ On va maintenant signer le certificat avec notre CA, pour une validité de 10.000 jours :

```
root@SIO1-GLPI-CG:/opt/ca# openssl x509 -req -in glpi.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out glpi.crt -days 10000 -sha256 -extfile glpi.ext
```

Signature ok

subject=C = FR, ST = Bretagne, L = Lannion, O = FLD, OU = Local, CN = www.glpi.local, emailAddress = webmaster@localhost
Getting CA Private Key

- ✓ Redémarrez apache :

```
# systemctl restart apache2
```

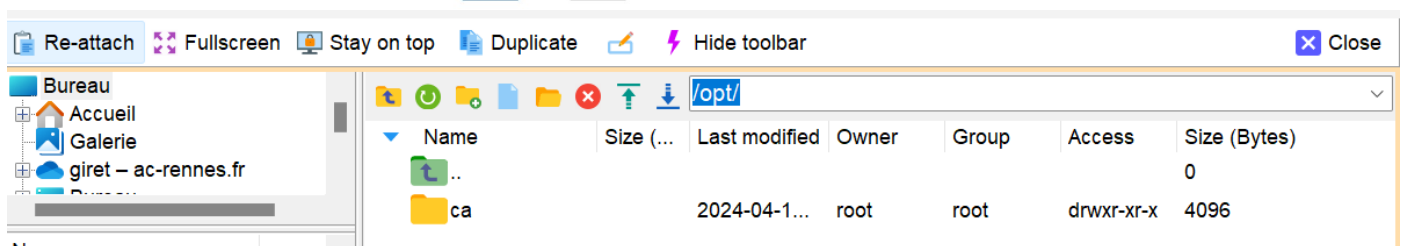
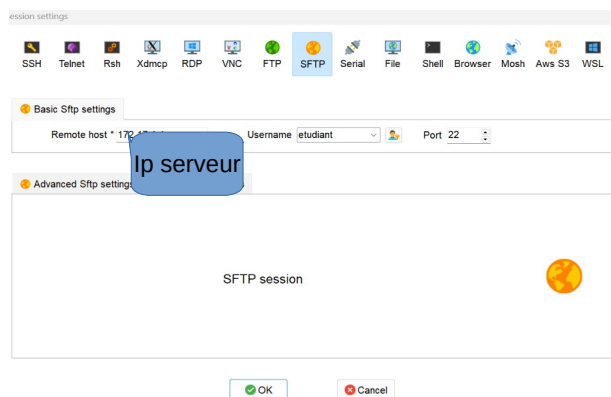
- ✓ Modifiez le fichier hosts sur votre pc, puisqu'un lien doit être fait entre un FQDN et le certificat :
sur une machine linux

```
#/etc/hosts
```

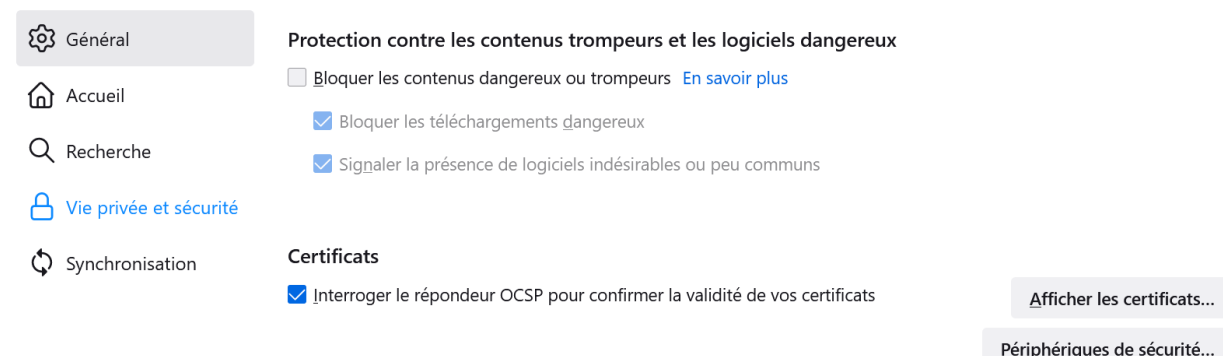
sur une machine windows 10 à ouvrir dans le bloc note en administrateur sur le client :

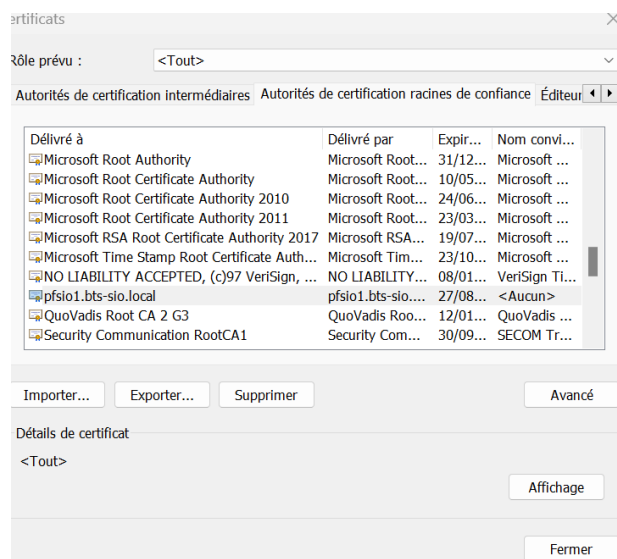
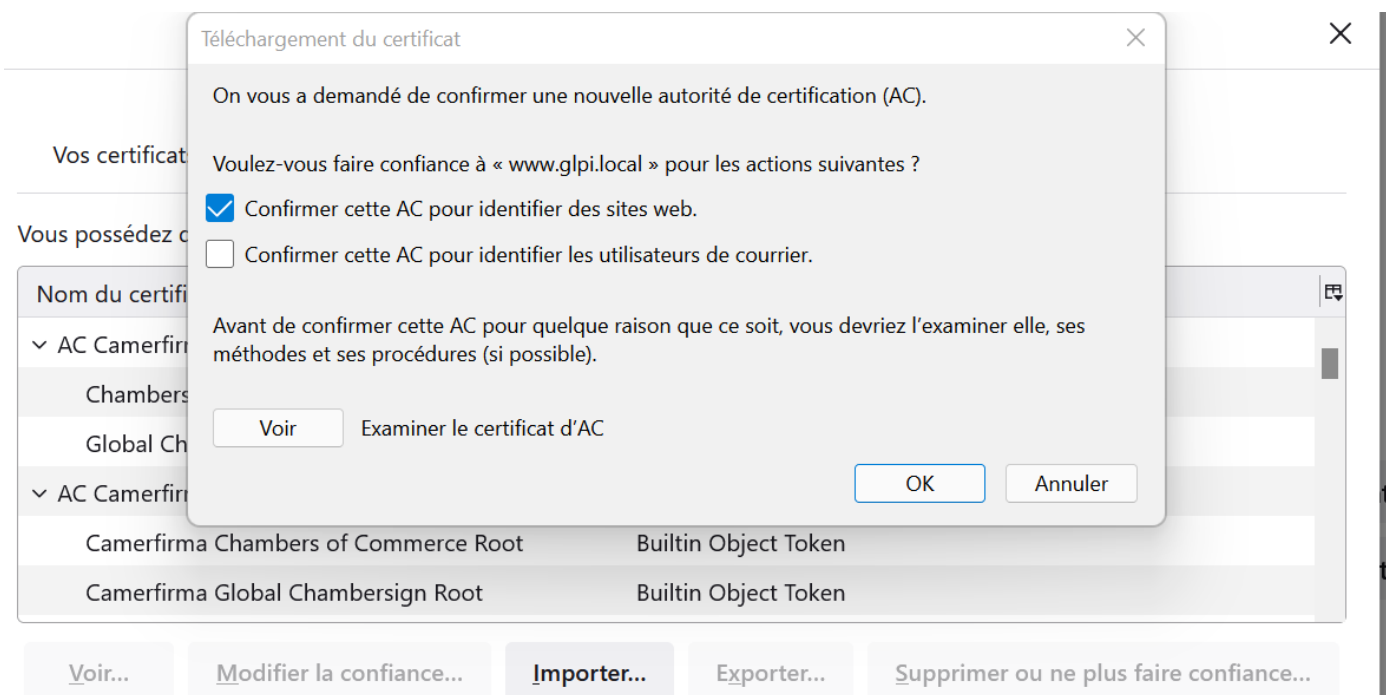
```
c:/Windows/System32/Drivers/etc/hosts#/etc/hosts
```

- ✓ Récupérer le certificat de l'autorité de certification sur le serveur web dans /opt/ca/ca.cert avec mobaxterm et copiez le sur le client puis importez ce certificat dans le navigateur non utile si l'autorité de certification est reconnue mais ici nous sommes auto-certifiés.



- ✓ Téléchargez le répertoire ca dans téléchargement et Installez le certificat dans le navigateur récupéré ca.crt sur le serveur avec mobaxterm et déposez le sur le client dans les autorités de certification racines de confiance.
Sur firefox par exemple :





Sur Opera

- ✓ Redémarrez le navigateur et Testez sur le client, dans le navigateur : <https://www.glpj.local> le cadenas est valide https fonctionnel

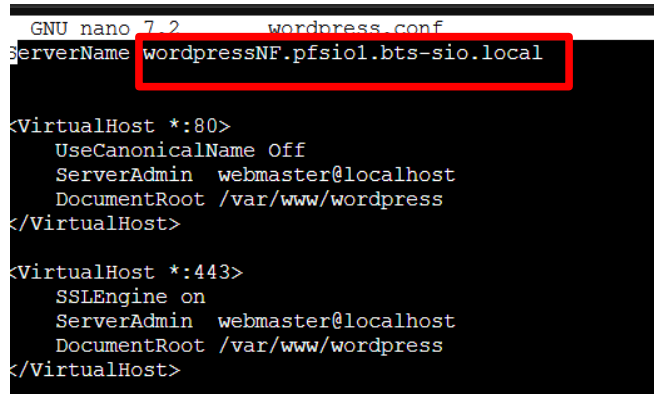
Ressources pour le portfolio (proxmox 172.17.0.23:8006 compte personnel AD sio)

Pour appliquer ceci au portfolios remplacer:

-le domaine **glpi.local** par le domaine **pfsio1.bts-sio.local**

-le FQDN : www.glpi.local par votre FQDN, exemple : **wordpressNF.pfsio1.bts-sio.local**

Vous trouvez votre FQDN dans le fichier de configuration de votre site, exemple : **wordpress.conf** qui se trouve dans **/etc/apache2/sites-available/**



```
GNU nano 7.2 wordpress.conf
ServerName wordpressNF.pfsio1.bts-sio.local

<VirtualHost *:80>
    UseCanonicalName Off
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/wordpress
</VirtualHost>

<VirtualHost *:443>
    SSLEngine on
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/wordpress
</VirtualHost>
```

Pour prendre à distance votre portfolio utilisez votre ip, exemple :ssh etudiant@ipcontainer
passer en su -

Les 2 fichiers glpi-ssl.conf et glpi-ssl.conf sont réunis dans le même fichier, complétez donc le fichier **wordpress.conf**

```
<VirtualHost *:80>
#    UseCanonicalName Off
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/wordpress
    Redirect permanent / https://pfCG.pfsio1.bts-sio.local/
</VirtualHost>

<VirtualHost *:443>
    SSLEngine on
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/wordpress
    SSLCertificateFile /opt/ca/pfCG.crt
    SSLCertificateKeyFile /opt/ca/pfCG.key
</VirtualHost>

<Directory /var/www/wordpress>
    Options +FollowSymLinks
    Options -Indexes
    AllowOverride All
    order allow,deny
    allow from all
</Directory>
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>
```

Les réponses aux questions pour l'autorité :

```
root@SIO-CG-pfwiki /opt/ca# openssl req -x509 -new -nodes -key ca.key -sha256 -days 10000 -out ca.pem
```

Enter pass phrase for 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) [AU]:FR

State or Province Name (full name) [Some-State]:Bretagne
Locality Name (eg, city) []:Lannion
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FLD
Organizational Unit Name (eg, section) []:bts-sio
Common Name (e.g. server FQDN or YOUR name) []:pfsio1.bts-sio.local
Email Address []:webmaster@localhost

```
root@SIO-CG-pfwiki /opt/ca# openssl genrsa 4096 > pfcg.key  
root@SIO-CG-pfwiki /opt/ca# openssl req -new -key pfcg.key > pfcg.csr
```

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) [AU]:FR  
State or Province Name (full name) [Some-State]:Bretagne  
Locality Name (eg, city) []:Lannion  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FLD  
Organizational Unit Name (eg, section) []:pfsio1.bts-sio  
Common Name (e.g. server FQDN or YOUR name) []:pfCG.pfsio1.bts-sio.local  
Email Address []:webmaster@localhost
```

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:Btssio2017
An optional company name []:

```
root@SIO-CG-pfwiki /opt/ca# nano pfcg.ext  
authorityKeyIdentifier=keyid,issuer  
basicConstraints=CA:FALSE  
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment  
subjectAltName = @alt_names  
[alt_names]  
#DNS.1=FQDN  
DNS.1 = pfCG.pfsio1.bts-sio.local
```

```
root@SIO-CG-pfwiki /opt/ca# openssl x509 -req -in pfcg.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out pfcg.crt -days 10000  
-sha256 -extfile pfcg.ext  
Certificate request self-signature ok  
subject=C = FR, ST = Bretagne, L = Lannion, O = FLD, OU = pfsio1.bts-sio, CN = pfCG.pfsio1.bts-sio.local, emailAddress =  
webmaster@localhost  
Enter pass phrase for ca.key:
```

Après intégration de l'autorité de certification dans le navigateur :



Afficher le certificat : pfCG.pfsio1.bts-sio.local

Généralités

Détails

Émis pour

Nom commun (CN)	pfCG.pfsio1.bts-sio.local
Organisation (O)	FLD
Unité d'organisation (OU)	pfsio1.bts-sio

Émis par

Nom commun (CN)	pfsio1.bts-sio.local
Organisation (O)	FLD
Unité d'organisation (OU)	bts-sio

Durée de validité

Émis le	mercredi 10 avril 2024 à 14:20:27
Expire le	dimanche 27 août 2051 à 14:20:27

Empreintes SHA-256

Certificat	8bce65cb9dd89f21bf7836a771424f0944f29aef10207e7c63f73c265c657256
Clé publique	58a569fc4b1674f1a5010b3fbf914e7aa181809e21c0a6b7247e7e89263c6750