Aime Florian
BTS SIO1

Chapitre 11 – Echanges sécurisés et authentifiés avec SSL

1. Configuration côté SSL

On s'assure premièrement que le paquet **openssl** est installé sur **DS2** :

```
root@DS2:~#dpkg -l | grep -i openssl
ii  libcurl4:amd64               7.64.0-4+deb10u2                amd64        easy-to-use clien
t-side URL transfer library (OpenSSL flavour)
ii  openssl                      1.1.1d-0+deb10u5                amd64        Secure Sockets La
yer toolkit - cryptographic utility
ii  ssl-cert                     1.0.39                          all          simple debconf wr
apper for OpenSSL
```

Le fichier ***openssl.cnf*** se trouve dans le dossier ***/etc/ssl/*** :

```
root@DS2:~#cd /etc/ssl
root@DS2:/etc/ssl#ls -l
total 32
drwxr-xr-x 2 root root     16384 mars  31 19:22 certs
-rw-r--r-- 1 root root     11118 févr. 16 23:08 openssl.cnf
drwx--x--- 2 root ssl-cert  4096 mars  31 19:22 private
```

On crée une sauvegarde du fichier :

```
root@DS2:/etc/ssl#cp openssl.cnf openssl.cnf.sauv
root@DS2:/etc/ssl#ls -l
total 44
drwxr-xr-x 2 root root     16384 mars  31 19:22 certs
-rw-r--r-- 1 root root     11118 févr. 16 23:08 openssl.cnf
-rw-r--r-- 1 root root     11118 avril 12 18:36 openssl.cnf.sauv
drwx--x--- 2 root ssl-cert  4096 mars  31 19:22 private
root@DS2:/etc/ssl#
```

1.1. Création d'une autorité de certification racine.

Création de l'environnement du CA, il stockera son certificats et ses fichiers :

```
root@DS2:/etc/ssl#mkdir /etc/ssl/CA
root@DS2:/etc/ssl#mkdir /etc/ssl/CA/certs
root@DS2:/etc/ssl#mkdir /etc/ssl/CA/private
root@DS2:/etc/ssl#mkdir /etc/ssl/CA/newcerts
root@DS2:/etc/ssl#ls -l CA/
total 12
drwxr-xr-x 2 root root 4096 avril 12 18:41 certs
drwxr-xr-x 2 root root 4096 avril 12 18:41 newcerts
drwxr-xr-x 2 root root 4096 avril 12 18:41 private
root@DS2:/etc/ssl#
```

On crée les deux fichiers ***serial*** et ***index.txt*** destinés à :

- garder trace du dernier numéro de série utilisé par le CA (chaque certificat doit avoir un numéro de série distinct)
- garder trace des certificats générés

```
root@DS2:/etc/ssl#echo "1" > /etc/ssl/CA/serial
root@DS2:/etc/ssl#touch /etc/ssl/CA/index.txt
root@DS2:/etc/ssl#ls CA/
certs  index.txt  newcerts  private  serial
root@DS2:/etc/ssl#_
```

On modifie le fichier de configuration ***/etc/ssl/openssl.cnf*** dans la partie **[CA_default]** (directives **dir** et **certificate**) :

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

dir             = /etc/ssl/CA           # 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/cacert.pem # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
```

Génération de la paire de clés publique/privée du CA à l'aide de la commande ***genrsa*** d'OpenSSL :

```
root@DS2:~#openssl genrsa -out /etc/ssl/CA/private/cakey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.....................+++++
e is 65537 (0x010001)
root@DS2:~#
```

On crée le certificat de l'autorité racine auto-signé à l'aide de la commande ***req -x509*** d'OpenSSL :

```
root@DS2:~#openssl req -new -x509 -key /etc/ssl/CA/private/cakey.pem -out /etc/ssl/CA/certs/cacert.p
em -days 3650
```

```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Saint-Raphaël
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sio-exupery
Organizational Unit Name (eg, section) []:bts sio
Common Name (e.g. server FQDN or YOUR name) []:DS2.sio-exupery.fr
Email Address []:
```

Les fichiers ***cakey.pem*** et ***cacert.pem*** sont bien présents dans les répertoires ***/etc/ssl/CA/private*** et ***/etc/ssl/CA/certs*** :

```
root@DS2:~#ls -l /etc/ssl/CA/certs/
total 4
-rw-r--r-- 1 root root 1399 avril 12 18:54 cacert.pem
root@DS2:~#ls -l /etc/ssl/CA/private/
total 4
-rw------- 1 root root 1679 avril 12 18:49 cakey.pem
root@DS2:~#_
```

On affiche le certificat racine à l'aide de la commande ***x509*** d'OpenSSL :

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5d:97:78:f4:98:0d:10:2f:25:cd:b7:96:27:33:4d:29:ba:76:66:6c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = FR, ST = France, L = Saint-Rapha\C3\83\C2\AB1, O = sio-exupery, OU = bts sio, CN
 = DS2.sio-exupery.fr
        Validity
            Not Before: Apr 12 16:54:51 2021 GMT
            Not After : Apr 10 16:54:51 2031 GMT
        Subject: C = FR, ST = France, L = Saint-Rapha\C3\83\C2\AB1, O = sio-exupery, OU = bts sio, C
N = DS2.sio-exupery.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b1:f0:45:ee:df:c4:e6:9b:0b:0b:5e:f5:c4:50:
                    6e:83:10:1b:0e:e4:2c:07:f6:7f:08:88:42:1b:87:
                    cf:38:b6:ec:84:4f:a8:ee:81:ca:40:14:2a:73:9c:
                    2a:df:cf:0d:2c:51:1a:ce:ad:1c:e0:55:7c:d9:01:
                    72:f3:df:fd:de:f3:cf:30:d3:94:b0:1d:a2:23:1d:
                    6c:c6:99:4b:92:31:7f:97:4c:f2:41:95:47:c5:9f:
                    c9:7e:8b:d5:ad:d4:76:4a:a8:f0:73:b1:d8:e9:98:
                    c7:9c:73:a3:dc:bc:a8:83:15:77:24:9e:85:dd:56:
                    47:97:0d:98:1f:dc:6e:33:4f:bb:1a:be:74:f7:b9:
                    41:45:b8:25:5c:61:15:44:21:3a:6d:3e:51:89:7f:
                    43:b0:61:d3:52:82:f3:54:1e:58:36:5a:cb:98:22:
                    0d:09:35:0c:67:37:e2:28:f8:0d:62:61:ed:81:d9:
                    fc:3f:2f:22:ce:5a:52:a0:c0:99:63:42:33:7c:a0:
                    8f:4a:e0:0c:e9:40:88:dc:96:ba:4e:d2:9a:28:f7:
                    33:28:51:73:67:bb:17:6d:dc:77:d1:30:7f:76:b5:
                    1f:a8:0d:a0:c9:e9:03:65:d9:3b:a0:f7:fd:91:cd:
                    39:10:45:87:66:a3:0d:0f:08:65:68:1e:9d:a2:88:
                    ab:19
                Exponent: 65537 (0x10001)
--Plus--
```

1.2. Création des clés et du certificat du serveur Web

Génération d'une paire de clés publique/privée pour le serveur Web (***/etc/ssl/private***) :

```
root@DS2:~#openssl genrsa -out /etc/ssl/private/web.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.......................+++++
...........+++++
e is 65537 (0x010001)
```

On génère une demande de signature de certificat (requête de certification CSR) à l'aide de la commande req d'OpenSSL :

```
root@DS2:~#openssl req -new -key /etc/ssl/private/web.key -out /etc/ssl/certs/webds2.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]:France
Locality Name (eg, city) []:Saint-Raphaël
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sio-exupery
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:secu.sio-exupery.fr
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@DS2:~#
```

On signe la requête en tant que CA à l'aide de la commande ca d'OpenSSL :

```
root@DS2:~#openssl ca -in /etc/ssl/certs/webds2.csr -config /etc/ssl/openssl.cnf
Using configuration from /etc/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Apr 12 17:18:05 2021 GMT
            Not After : Apr 12 17:18:05 2022 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = France
            organizationName          = sio-exupery
            commonName                = secu.sio-exupery.fr
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                19:97:10:46:C4:90:8D:0E:A9:CC:5E:BC:4E:01:7C:EE:12:BA:F2:14
            X509v3 Authority Key Identifier:
                keyid:79:A4:99:63:93:3C:29:C0:E7:60:97:5F:86:37:E7:C0:FE:BB:89:01

Certificate is to be certified until Apr 12 17:18:05 2022 GMT (365 days)
Sign the certificate? [y/n]:y_
```

Contenu de ***index.txt*** et ***serial*** :

```
root@DS2:~#more /etc/ssl/CA/index.txt
V       220412171805Z           01      unknown /C=FR/ST=France/O=sio-exupery/CN=secu.sio-exupery.fr
root@DS2:~#more /etc/ssl/CA/serial
02
root@DS2:~#
```

Le certificat SSL ***01.pem*** est présent dans le répertoire ***/etc/ssl/CA/newcerts*** :

```
root@DS2:~#ls -l /etc/ssl/CA/newcerts
total 8
-rw-r--r-- 1 root root 4526 avril 12 19:18 01.pem
```

Enfin, on crée , à l'aide de **VIM**, le certificat SSL ***secu.sio-exupery.fr.crt*** obtenu à partir du fichier ***01.pem*** en conservant les lignes depuis **BEGIN CERTIFICATE** jusqu'à **END CERTIFICATE** :

```
-----BEGIN CERTIFICATE-----
MIIDxjCCAq6gAwIBAgIBATANBgkqhkiG9w0BAQsFADB+MQswCQYDVQQGEwJGUjEP
MA0GA1UECAwGRnJhbmNlMRkwFwYDVQQHDBBTYWludC1SYXBoYcODwqtsMRQwEgYD
VQQKDAtzaW8tZXh1cGVyeTEQMA4GA1UECwwHYnRzIHNpbzEbMBkGA1UEAwwSRFMy
LnNpby1leHVwZXJ5LmZyMB4XDTIxMDQxMjE3MTgwNVoXDTIyMDQxMjE3MTgwNVow
UjELMAkGA1UEBhMCRlIxDzANBgNVBAgMBkZyYW5jZTEUMBIGA1UECgwLc2lvLWV4
dXBlcnkxHDAaBgNVBAMME3NlY3Uuc2lvLWV4dXBlcnkuZnIwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCzuiBz2Va2AOz4pLUjCK9gC2wCCN/HeiUIxuuO
wHsuXixSEf7qKE4AtEs9ZIbQPY7yZf694KT5m/rDQiipwD4xTPZ6jS+ldxqPvLVW
vHtKZCd42WrBJq4SiL7b1gNv73KrhhCO8+fFRCbnCvUUat4ZOOck4YBOLd8WDGxU
byWP13x3poMyVYxqM5X9wydI4GQSGG2s7PXTEKk+XNJj3NtOY6wiPHYuFYxFThgv
I3HnMvAkJWx28y41BSS/f4kG+hgolVbcOdWefMw/MINzVygui+muIKx8FdBHdZuY
LUugO1FtGoo7m/b2EI5fR2f8R9en81tsfxwh6y58j/4FFseZAgMBAAGjezB5MAkG
A1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TUOwgR2VuZXJhdGVkIENlcnRp
ZmljYXRlMBOGA1UdDgQWBBQZlxBGxJCNDqnMXrxOAXzuErryFDAfBgNVHSMEGDAW
gBR5pJljkzwpwOdgl1+GN+fA/ruJATANBgkqhkiG9w0BAQsFAAOCAQEAeD63RTrM
2YUSFu49hE1BwcjX7+37qFEurmOPDp6bWzSsl6WDZyMPkEhXRGy7aU2F7Pf7xeuA
ADd8lXRPmUQi1Amsi/JpEShi2rA2ce3lpMzHJKrkquDlJThYB9JATkZTDVl4jlzG
lBJNe2AnRpMKdnowutTMtz1b7gMipVq8PLi0aWRJgF59c99PQ+/9yNKaj+KD+QdT
esCmO3dA6yvl4hSnmM4ac2vDj79WB8qB9ffJtTNA9kSt755NMOacjF9moN9uljj2
Du4OVu1EXsoCSOSxjAiQoaeQvJ2TswsQ/wcoCD2YMOFv54VzoO32EnyjwyP4omit
i/rFtd8AHRHV7g==
-----END CERTIFICATE-----
~
~
~
~
~
~
~
~
~
~
~
~
~
                                                                1,1           Tout
```

2. Configuration côté Apache

Pour que le protocole **SSL** puisse fonctionner avec le Serveur **HTTP Apache 2**, il faut activer le ***module ssl***, installé normalement d'office, avec la commande ***a2enmod ssl*** :

```
root@DS2:~#a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certifica
tes.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@DS2:~#
```

ssl.conf, le fichier de configuration du module, se trouve dans ***/etc/apache2/mods-enabled/*** ainsi que la directive de chargement **ssl.load**.

```
lrwxrwxrwx 1 root root 36 avril 12 19:29 socache_shmcb.load -> ../mods-available/socache_shmcb.load
lrwxrwxrwx 1 root root 26 avril 12 19:29 ssl.conf -> ../mods-available/ssl.conf
lrwxrwxrwx 1 root root 26 avril 12 19:29 ssl.load -> ../mods-available/ssl.load
lrwxrwxrwx 1 root root 29 mars  31 19:22 status.conf -> ../mods-available/status.conf
lrwxrwxrwx 1 root root 29 mars  31 19:22 status.load -> ../mods-available/status.load
root@DS2:~#
```

Le serveur **Apache** doit disposer de sa clé privée et de son certificat qui contiendra sa clé publique. Afin de lui préciser les clés et certificat **SSL** à utiliser, on ajoute les lignes **SSLCertificateFile** et **SSLCertificateKeyFile** (***/etc/apache2/mods-enabled/ssl.conf)*** :

```
 GNU nano 3.2                    /etc/apache2/mods-enabled/ssl.conf                    Modifié

        # the CPU cost, and did not override SSLCipherSuite in a way that puts
        # insecure ciphers first.
        # Default: Off
        #SSLHonorCipherOrder on

        #   The protocols to enable.
        #   Available values: all, SSLv3, TLSv1, TLSv1.1, TLSv1.2
        #   SSL v2  is no longer supported
        SSLProtocol all -SSLv3

        #   Allow insecure renegotiation with clients which do not yet support the
        #   secure renegotiation protocol. Default: Off
        #SSLInsecureRenegotiation on

        #   Whether to forbid non-SNI clients to access name based virtual hosts.
        #   Default: Off
        #SSLStrictSNIVHostCheck On

SSLCertificateFile /etc/ssl/certs/secu.sio-exupery.fr.crt
SSLCertificateKeyFile /etc/ssl/private/web.key

</IfModule>
```

Apache n'écoutait que le port 80 du protocole **HTTP**. Il écoute également le port **HTTPS** 443 dans la mesure où le module **SSL** est activé (directive ***Listen 443***).

```
root@DS2:~#cat /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
```

On modifie le fichier ***/etc/apache2/sites-enabled/sites-sio.conf*** pour la partie concernant l'hôte virtuel par l'IP :

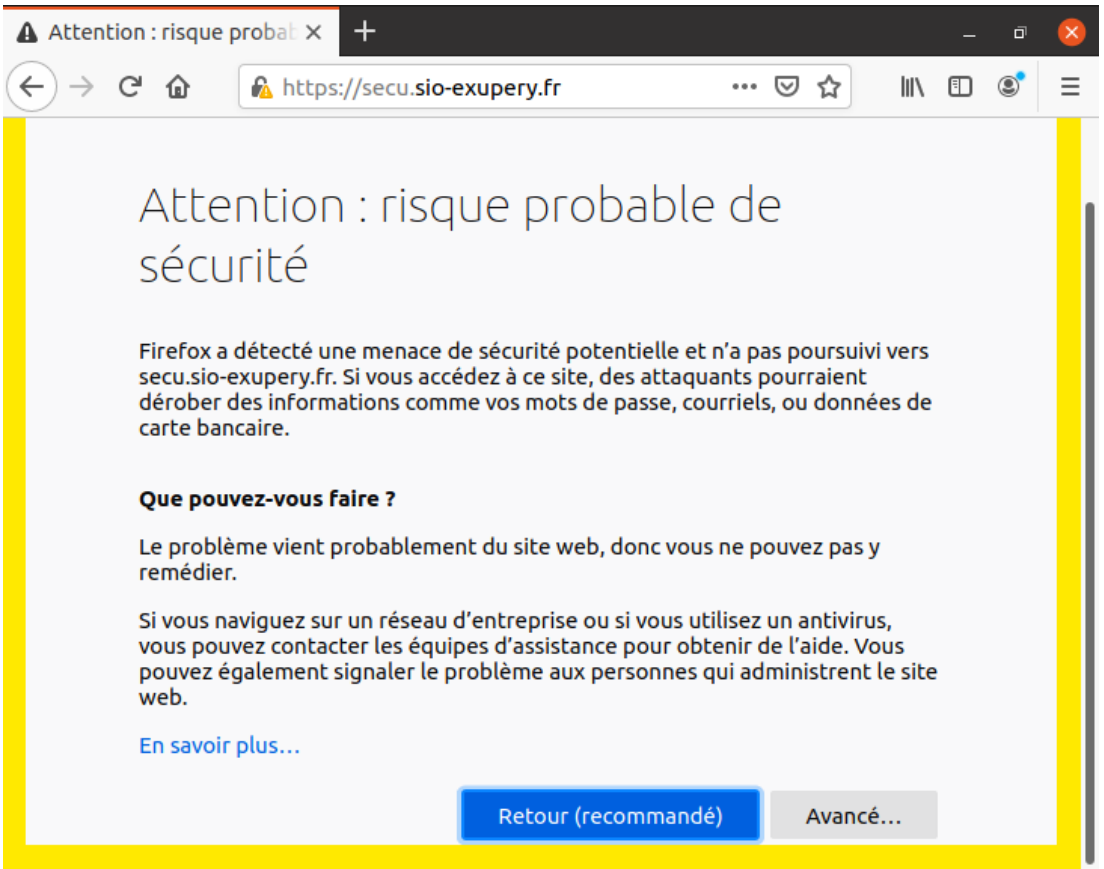
```
  GNU nano 3.2                  /etc/apache2/sites-enabled/sites-sio.conf

<VirtualHost 192.168.2.9:443>
        ServerName secu.sio-exupery.fr:443
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/secu
        ErrorLog /var/www/html/secu/logs/error.log
        CustomLog /var/www/html/secu/logs/access.log combined
        SSLEngine on
        LogLevel info
</VirtualHost>
```

On relance Apache puis on saisit la commande ***ss -ntl4*** afin d'afficher les connexions TCP actives ainsi que les ports d'écoute :

```
root@DS2:~#ss -ntl4
State       Recv-Q      Send-Q           Local Address:Port           Peer Address:Port
LISTEN      0           80                   127.0.0.1:3306                0.0.0.0:*
LISTEN      0           10                 192.168.2.9:53                  0.0.0.0:*
LISTEN      0           10                 192.168.2.1:53                  0.0.0.0:*
LISTEN      0           10                   127.0.0.1:53                  0.0.0.0:*
LISTEN      0           32                     0.0.0.0:21                  0.0.0.0:*
LISTEN      0           128                    0.0.0.0:22                  0.0.0.0:*
LISTEN      0           128                  127.0.0.1:953                 0.0.0.0:*
root@DS2:~#_
```

3. Test du serveur Web sécurisé depuis un client

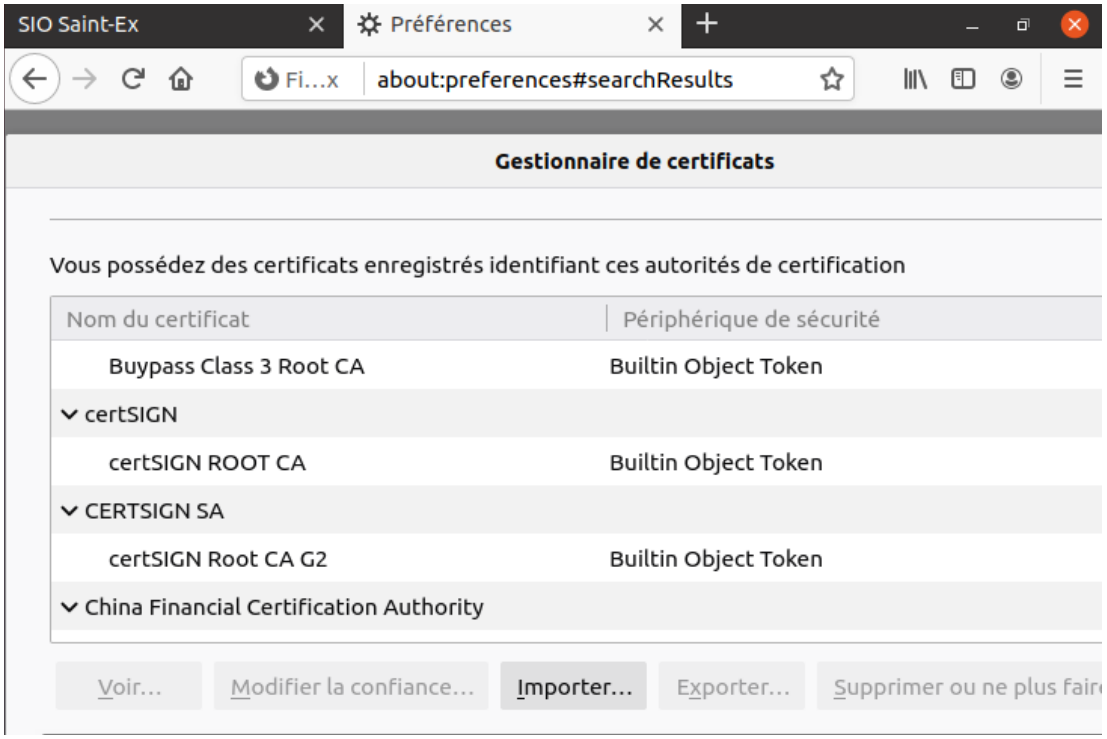
Sur **UD1**, on se rend sur ***https://secu.sio-exupery.fr***, mais le navigateur ne connaît pas l'autorité de certification :

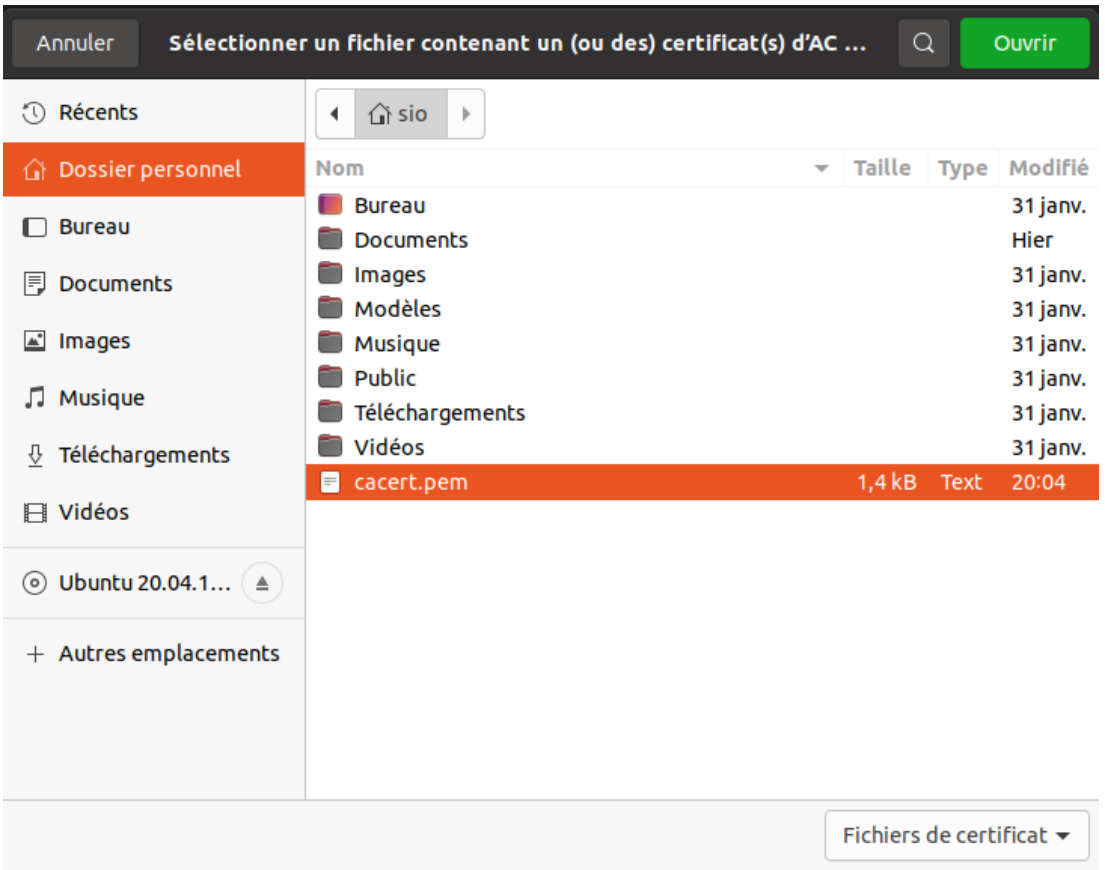


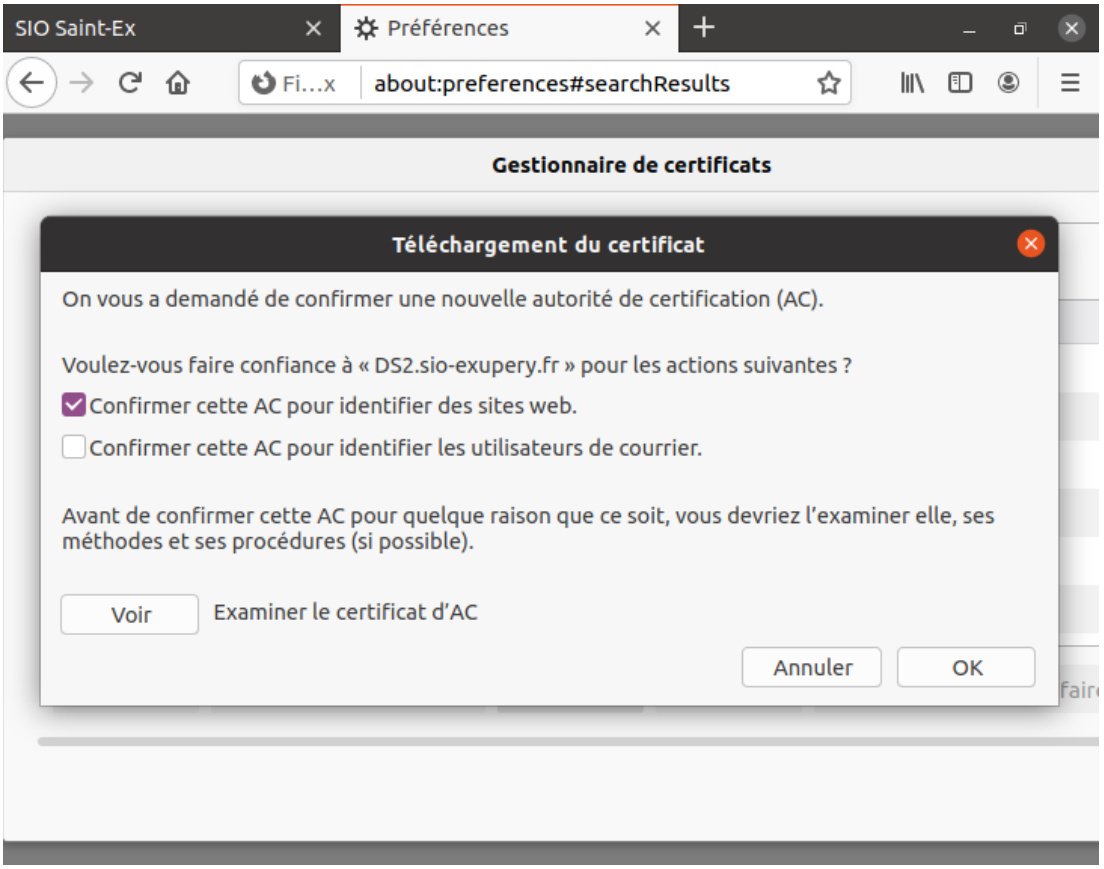
Depuis **UD1**, on transfère le certificat de l'autorité de certification vers le répertoire personnel de l'utilisateur sio :

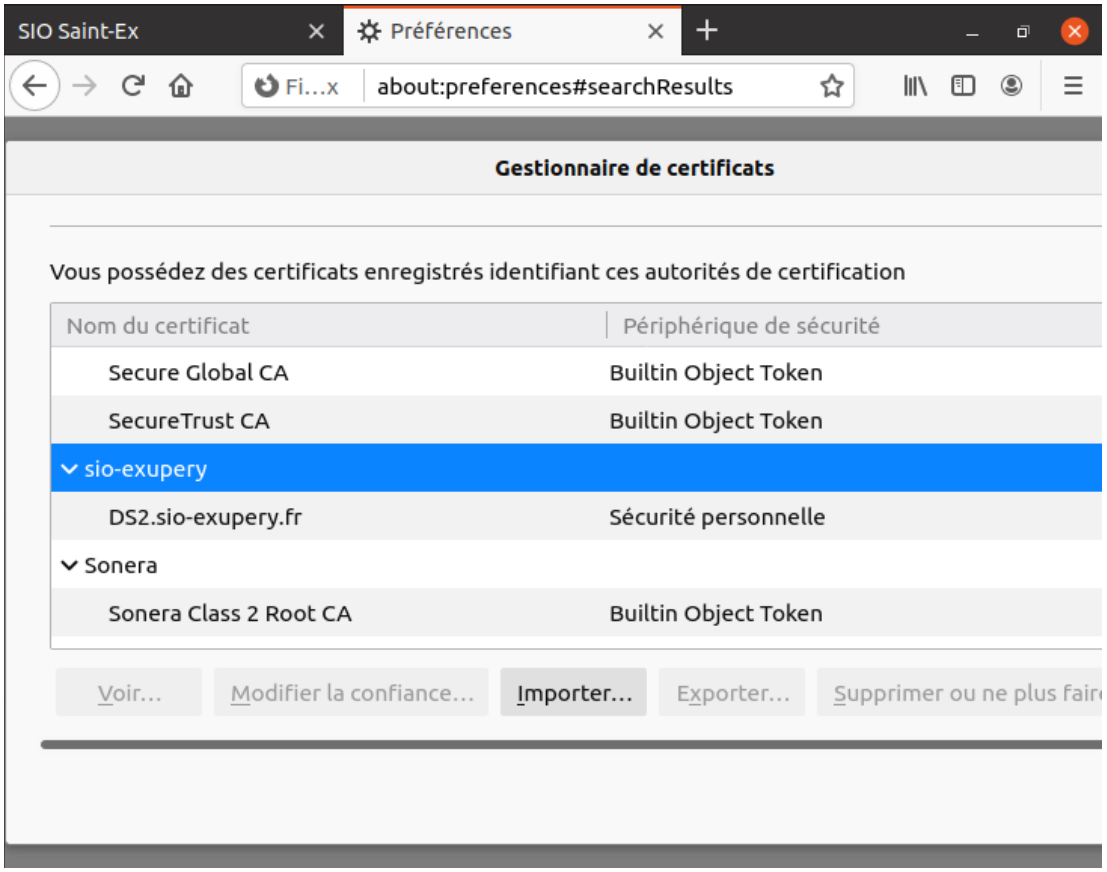
```
sio@UD1:~$ scp root@192.168.2.1:/etc/ssl/CA/certs/cacert.pem /home/sio
root@192.168.2.1's password:
cacert.pem                                    100% 1399   884.0KB/s   00:00
sio@UD1:~$
```

On importe le certificat dans le magasin de certificats du navigateur Firefox :






SIO Saint-Ex
Préférences
Fi…x
about:preferences#searchResults
Gestionnaire de certificats
Téléchargement du certificat
On vous a demandé de confirmer une nouvelle autorité de certification (AC).
Voulez-vous faire confiance à « DS2.sio-exupery.fr » pour les actions suivantes ?
Confirmer cette AC pour identifier des sites web.
Confirmer cette AC pour identifier les utilisateurs de courrier.
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).
Voir
Examiner le certificat d'AC
Annuler
OK


SIO Saint-Ex
Préférences
Fi…x
about:preferences#searchResults
Gestionnaire de certificats
Vous possédez des certificats enregistrés identifiant ces autorités de certification
Nom du certificat
Périphérique de sécurité
Secure Global CA
Builtin Object Token
SecureTrust CA
Builtin Object Token
sio-exupery
DS2.sio-exupery.fr
Sécurité personnelle
Sonera
Sonera Class 2 Root CA
Builtin Object Token
Voir…
Modifier la confiance…
Importer…
Exporter…
Supprimer ou ne plus fair

La page apparaît avec le cadenas indiquant une connexion sécurisée :