TP11 – Échanges sécurisés et authentifiés avec SSL

SAOU Rayan

Table des matières

Table des matières 1

1. Configuration côté SSL 2

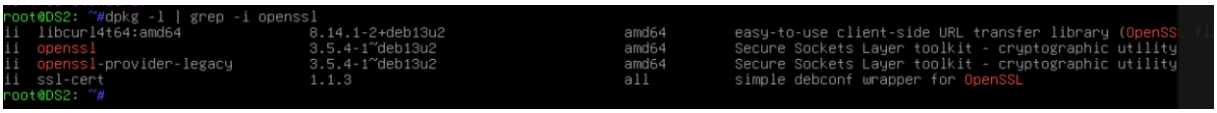
1.1 Création d'une autorité de certification racine 2

1.2 Création des clés et du certificat du serveur Web 6

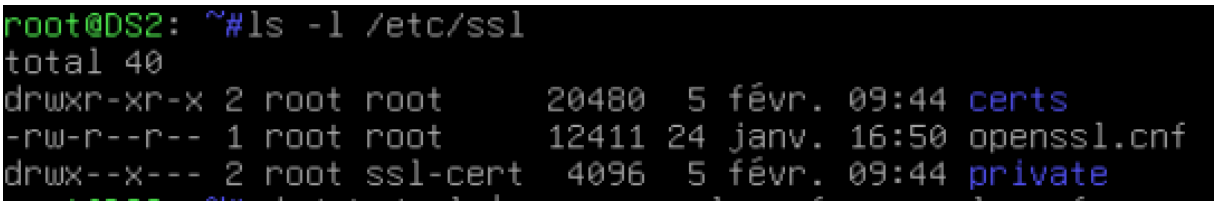
2. Configuration côté Apache 8

1. Configuration côté SSL

Nous vérifions si le paquet OpenSSL est déjà installé :



Nous vérifions le contenu du fichier de configuration OpenSSL situé dans /etc/ssl :



Nous en faisons une sauvegarde :

1.1 Création d'une autorité de certification racine

Nous créons l'environnement du CA :

```
root@DS2: /etc/ssl#mkdir CA
root@DS2: /etc/ssl#mkdir CA/certs
root@DS2: /etc/ssl#mkdir CA/private CA/newcerts
root@DS2: /etc/ssl#ls -l
total 60
drwxr-xr-x 5 root root      4096 28 avril 11:31 CA
drwxr-xr-x 2 root root     20480  5 févr. 09:44 certs
-rw-r--r-- 1 root root     12411 24 janv. 16:50 openssl.cnf
-rw-r--r-- 1 root root     12411 28 avril 11:10 openssl.cnf.sauv
drwx--x--- 2 root ssl-cert  4096  5 févr. 09:44 private
root@DS2: /etc/ssl#
```

Nous créons ensuite les deux fichiers serial et index.txt :

```
root@DS2: /etc/ssl#echo "01" > CA/serial
root@DS2: /etc/ssl#touch CA/index.txt
```

Nous modifions le fichier de configuration openssl.cnf :

```
[ 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
```

Nous spécifions dans le fichier de configuration, l'extension de la norme X509 :

```
[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = secu.sio-exupey.fr
```

Nous remplaçons usr_cert par v3_req :

```
####################################################################
[ 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
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem # The private key

x509_extensions = v3_req                # 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
```

Nous générons ensuite la clé privée du CA à l'aide de la commande genrsa :

```
root@DS2: /etc/ssl#openssl genrsa -out CA/private/cakey.pem 2048
```

Nous créons le certificat de l'autorité racine auto-signé :

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

Nous pouvons remarquer la présence des fichiers ***cakey.pem*** et ***cacert.pem***

```
root@DS2: ~#cd /etc/ssl/CA
root@DS2: /etc/ssl/CA#ls -l private/
total 4
-rw------- 1 root root 1704 28 avril 11:52 cakey.pem
root@DS2: /etc/ssl/CA#ls -l certs/
total 4
-rw-r--r-- 1 root root 1391 29 avril 08:52 cacert.pem
root@DS2: /etc/ssl/CA#
```

Nous affichons le certificat racine à l'aide de la commande x509 OpenSSL :

```
root@DS2: /etc/ssl/CA#openssl x509 -in certs/cacert.pem -text | more
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            50:bb:0b:6f:d9:94:8a:e3:7f:95:fe:af:73:16:73:29:fa:57:84:a1
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FR, ST=France, L=Saint-Raphael, O=sio-exupery, OU=BTS SIO, CN=DS2.sio-exupery.fr
        Validity
            Not Before: Apr 29 06:52:36 2026 GMT
            Not After : Apr 26 06:52:36 2036 GMT
        Subject: C=FR, ST=France, L=Saint-Raphael, O=sio-exupery, OU=BTS SIO, CN=DS2.sio-exupery.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:32:11:7f:e7:e9:92:df:f4:f0:2c:d3:0d:56:
                    be:5d:77:0b:ba:b3:ab:24:c5:70:b5:7f:20:d0:d2:
                    fb:3a:89:e3:4b:fc:cb:e4:9f:17:36:44:d0:ff:d7:
                    d5:09:dc:c9:a7:6a:ab:3a:b1:0b:22:6a:6e:6f:b8:
                    91:ed:69:1a:75:ee:56:aa:c9:08:03:4c:19:5c:2b:
                    5e:0a:28:7c:53:12:90:e0:c4:b7:96:3a:3c:d8:6b:
                    da:60:52:a2:ff:3e:90:3f:88:d5:d3:79:2d:1d:e2:
                    6b:63:ce:8f:08:38:75:a8:15:e8:07:d6:f5:58:ff:
                    c6:e6:64:6b:20:82:6c:75:47:cb:50:08:68:5b:28:
                    f6:55:a3:f2:9c:0e:8f:5b:00:f3:34:16:f7:46:d5:
                    d7:2e:08:23:b5:27:f3:67:d2:4b:30:b0:65:d4:0e:
                    d8:ab:3e:c1:49:70:b3:cd:54:1b:0e:f0:d3:22:e0:
                    8f:27:f6:40:d4:56:f4:b0:8d:5e:7a:9c:a8:01:c0:
                    70:f9:b3:f3:6d:db:1c:77:8a:b1:be:40:c3:00:7b:
                    1d:c8:29:4e:a5:30:48:fc:a1:ac:e8:af:12:e6:d5:
                    a0:f7:0d:71:d9:4e:46:f5:eb:b6:81:f4:6c:2a:f8:
                    47:a6:0a:40:76:22:2c:8d:85:a8:dc:ba:3f:40:a6:
                    8d:95
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                65:C8:7C:26:EE:4A:86:E5:91:48:46:51:39:3E:0A:EE:C4:ED:DB:E1
            X509v3 Authority Key Identifier:
                65:C8:7C:26:EE:4A:86:E5:91:48:46:51:39:3E:0A:EE:C4:ED:DB:E1
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        03:e4:bd:80:3e:2e:dc:e1:4e:1e:db:9e:73:44:f9:fc:4b:31:
        0f:c6:c4:6a:a8:b1:80:e2:e3:23:a8:66:76:d5:1a:d9:42:82:
        5f:d1:76:ef:59:c2:af:45:86:49:10:d0:22:de:5c:7b:20:d5:
        56:1a:77:dd:52:ec:13:11:da:10:da:ad:c1:73:d4:a5:fd:03:
        f6:d8:3b:60:86:df:cc:c6:cf:07:d0:67:f4:1d:a7:2e:ed:9d:
        7e:f0:39:6d:d3:e5:c3:cb:59:26:aa:69:f4:98:6b:f0:61:00:
```

```
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUULsLb9mUiuN/lf6vcxZzKfpXhKEwDQYJKoZIhvcNAQEL
BQAwezELMAkGA1UEBhMCRlIxDzANBgNVBAgMBkZyYW5jZTEWMBQGA1UEBwwNU2Fp
bnQtUmFwaGFlbDEUMBIGA1UECgwLc2lvLWV4dXBlcnkxEDAOBgNVBAsMB0JUUyBT
SU8xGzAZBgNVBAMMEkRTMi5zaW8tZXh1cGVyeS5mcjAeFw0yNjA0MjkwNjUyMzZa
Fw0zNjA0MjYwNjUyMzZaMHsxCzAJBgNVBAYTAkZSMQ8wDQYDVQQIDAZGcmFuY2Ux
FjAUBgNVBAcMDVNhaW50LVJhcGhhZWwxFDASBgNVBAoMC3Npby1leHVwZXJ5MRAw
DgYDVQQLDAdCVFMgU0lPMRswGQYDVQQDDBJEUzIuc2lvLWV4dXBlcnkuZnIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCxMhF/5+mS3/TwLNMNVr5ddwu6
s6skxXC1fyDQ0vs6ieNL/Mvknxc2RND/19UJ3Mmnaqs6sQsiam5vuJHtaRp17laq
yQgDTBlcK14KKHxTEpDgxLeWOjzYa9pgUqL/PpA/iNXTeS0d4mtjzo8IOHWoFegH
1vVY/8bmZGsggmx1R8tQCGhbKPZVo/KcDo9bAPM0FvdG1dcuCCO1J/Nn0kswsGXU
DtirPsFJcLPNVBsO8NMi4I8n9kDUVvSwjV56nKgBwHD5s/Nt2xx3irG+QMMAex3I
KU6lMEj8oazorxLm1aD3DXHZTkb167aB9Gwq+EemCkB2IiyNhajcuj9Apo2VAgMB
AAGjUzBRMB0GA1UdDgQWBBRlyHwm7kqG5ZFIRlE5PgruxO3b4TAfBgNVHSMEGDAW
gBRlyHwm7kqG5ZFIRlE5PgruxO3b4TAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4IBAQAD5L2APi7c4U4e255zRPn8SzEPxsRqqLGA4uMjqGZ21RrZQoJf
0XbvWcKvRYZJENAi3lx7INVWGnfdUuwTEdoQ2q3Bc9Sl/QP22Dtght/Mxs8H0Gf0
Hacu7Z1+8Dlt0+XDy1kmqmn0mGvwYQAULk42Q70nGY+gqqs8GxB8PaY13g3gbYHJ
PzONddgcsnfx2wxIMRDTmBYjbFjuivMpIvxj4UOOXlPQ+DhxUOGP05xctHE2bxpC
nJGcdnePsVVkJ54tJJmKwg5dEvLe1UslygOxV+DvpMZW4/9+GIuudM5ymCcKj/b4
ANQimLpjXDP/+X57gToQdQ5UAK3ejMz/2rdh
-----END CERTIFICATE-----
root@DS2: /etc/ssl/CA#_
```

1.2 Création des clés et du certificat du serveur Web

Nous générons une paire de clés publique privée pour le serveur Web :

```
root@DS2: /etc/ssl/CA#openssl genrsa -out /etc/ssl/private/web.key 2048
root@DS2: /etc/ssl/CA#
```

Nous générons ensuite une demande de signature du certificat à l'aide de la commande req d'OpenSSL :

```
root@DS2: /etc/ssl/CA#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-Raphael
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: /etc/ssl/CA#_
```

Nous signons ensuite la requête en tant que CA avec 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 29 07:15:05 2026 GMT
            Not After : Apr 29 07:15:05 2027 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = France
            organizationName          = sio-exupery
            commonName                = secu.sio-exupery.fr
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:secu.sio-exupery.fr
Certificate is to be certified until Apr 29 07:15:05 2027 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y_
```

Une fois signé, nous affichons le contenu des fichier ***index.txt*** et ***serial*** :

```
root@DS2: ~#cat /etc/ssl/CA/index.txt
V       270429071505Z           01      unknown /C=FR/ST=France/O=sio-exupery/CN=secu.sio-exupery.fr
root@DS2: ~#cat /etc/ssl/CA/serial
02
```

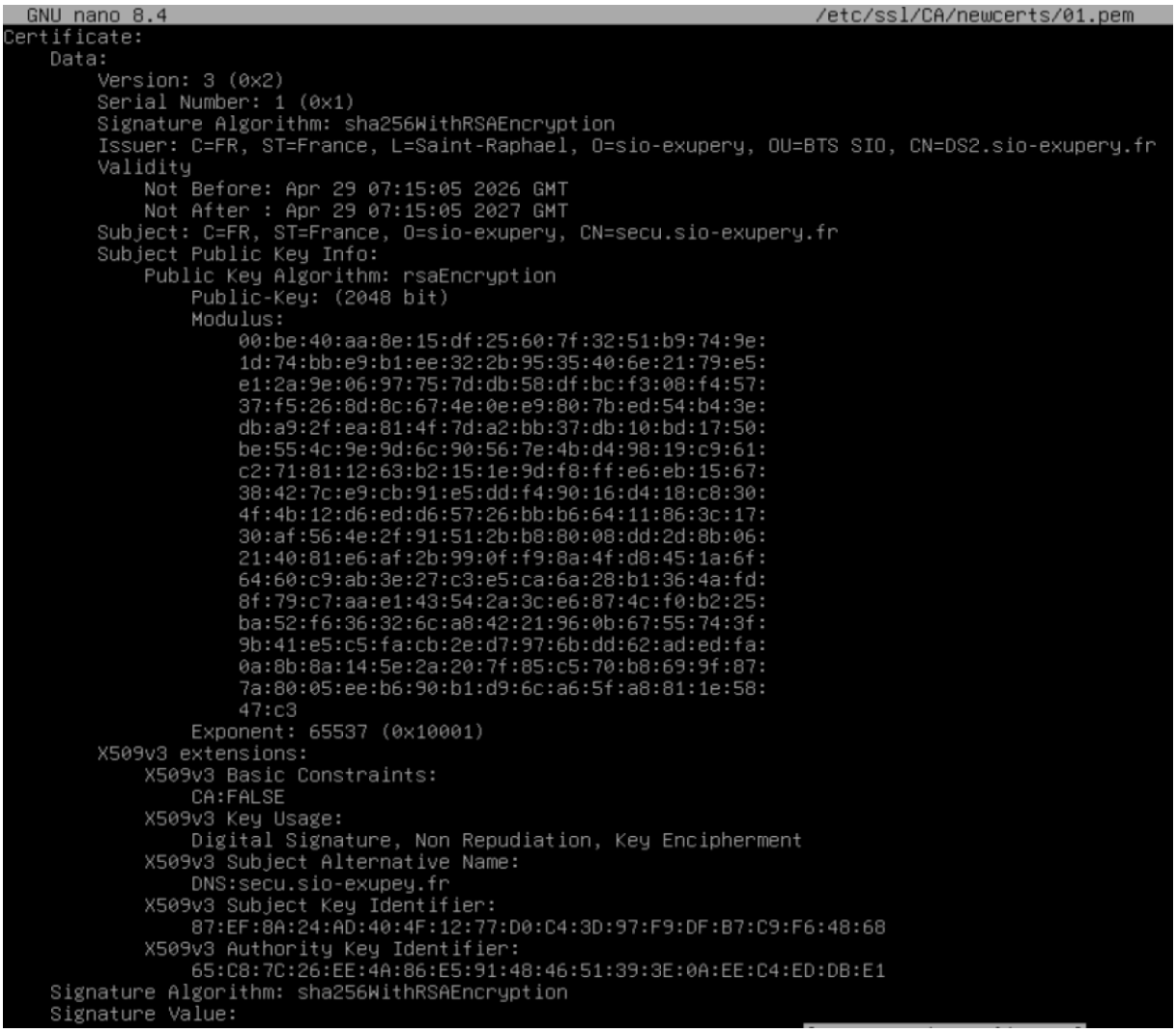
Nous vérifions aussi la présence du certificat SSL ***01.pem*** :

```
root@DS2: ~#ls -l /etc/ssl/CA/newcerts/
total 8
-rw-r--r-- 1 root root 4606 29 avril 09:15 01.pem
```

Enfin, nous créons le certificat SSL ***secu.sio-exupery.fr.crt*** :

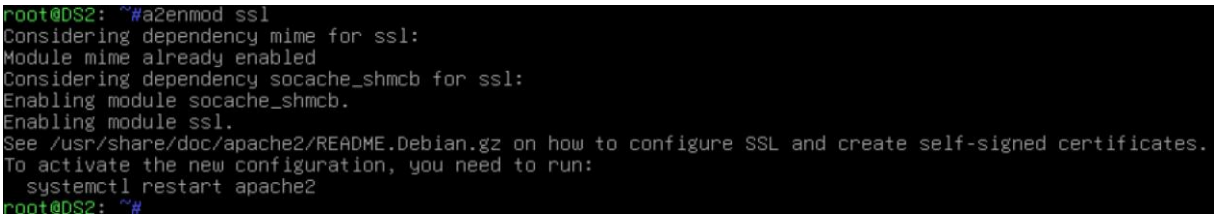
```
root@DS2: ~#cat /etc/ssl/CA/newcerts/01.pem > /etc/ssl/certs/secu.sio-exupery.fr.crt
```

Nous consultons ensuite le fichier :



2. Configuration côté Apache

Nous activons le module SSL avec la commande ***a2enmod ssl :***



Nous vérifions que le fichier de configuration ssl.conf se trouve dans /etc/apache2/mods-enabled/ :

```
root@DS2: ~#ls -l /etc/apache2/mods-enabled/ | tail -5
lrwxrwxrwx 1 root root 36 29 avril 09:39 socache_shmcb.load -> ../mods-available/socache_shmcb.load
lrwxrwxrwx 1 root root 26 29 avril 09:39 ssl.conf -> ../mods-available/ssl.conf
lrwxrwxrwx 1 root root 26 29 avril 09:39 ssl.load -> ../mods-available/ssl.load
lrwxrwxrwx 1 root root 29  5 févr. 09:45 status.conf -> ../mods-available/status.conf
lrwxrwxrwx 1 root root 29  5 févr. 09:45 status.load -> ../mods-available/status.load
```

Nous ajoutons les directives à la fin du fichier /etc/apache2/mods-enabled/ssl.conf :

```
#   The protocols to enable.
#   Available values: all, SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
#   SSL v2  is no longer supported
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1

#   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

# Warning: Session Tickets require regular restarting of the server!
# Make sure you do this (e.g. via logrotate) before changing this setting!
SSLSessionTickets off

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

Nous consultons les ports écoutés par Apache :

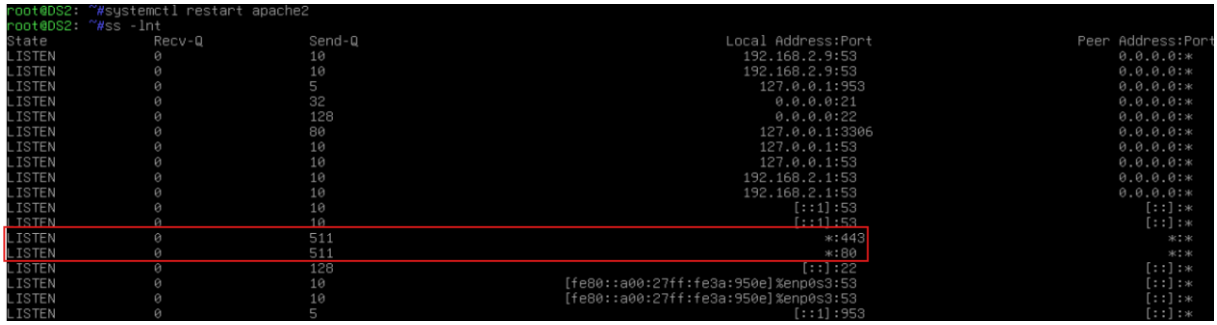
```
root@DS2: ~#cat /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

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

Nous modifions le port concertant les VirtualHosts :

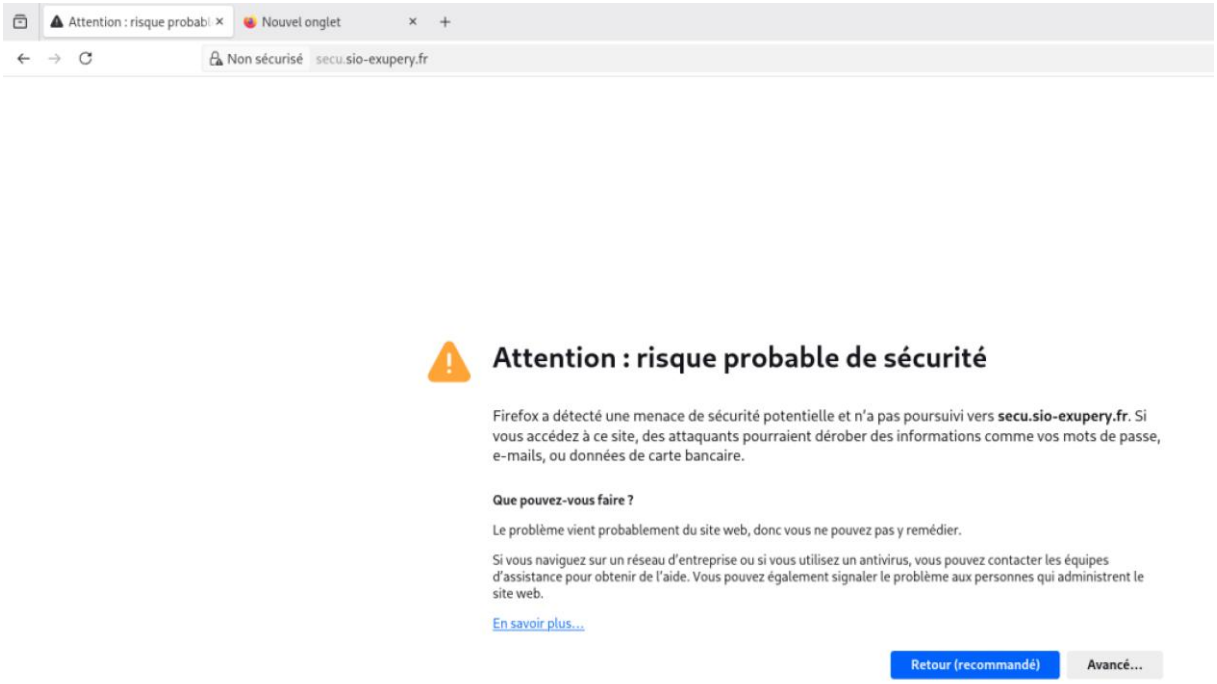
```
  GNU nano 8.4                                    /etc/apache2/sites-enabled/sites-sio.conf
<VirtualHost 192.168.2.9:443>
        ServerName secu.sio-exupery.fr:443_
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/secu
        ErrorLog /var/www/html/secu/logs/error.log
        CustomLog /var/www/html/secu/logs/access.log combined
        SSLEngine on
        LogLevel info
</VirtualHost>
```

La directive SSLEngine permet d'activer le moteur SSL qui permet le chiffrage des échanges entre client et serveur :

Nous relançons le service Apache puis saisissons la commande ss -lnt afin d'afficher les connexions TCP :



Nous testons depuis DD1, depuis un navigateur l'url secu.sio-exupery.fr :

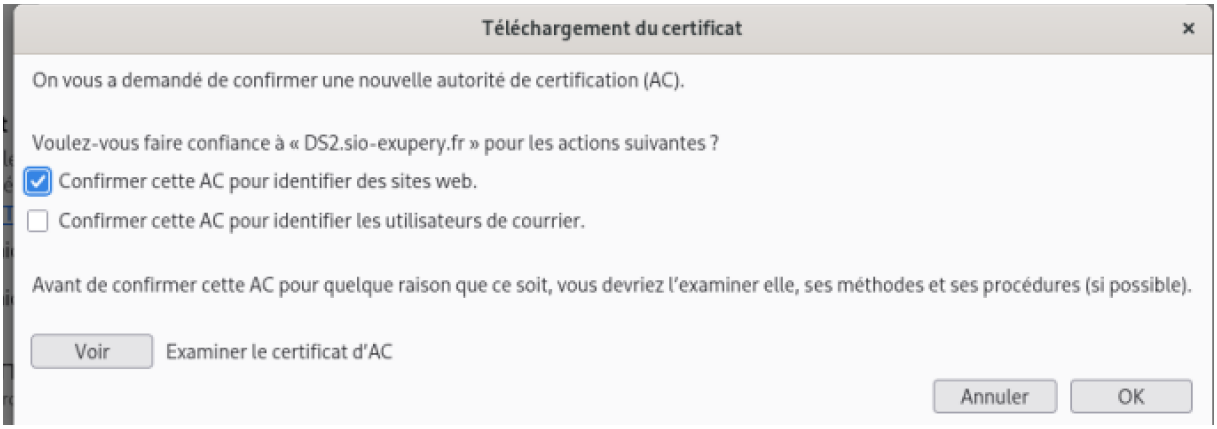


Le navigateur affiche donc un message d'erreur car le certificat à été signée par une autorité de certification non reconnue, nous poursuivons sur la page :

Depuis DD1, nous transférons le certificat de notre autorité de certification vers le répertoire personnel sio :

```
root@DD1:~# scp root@192.168.2.1:/etc/ssl/CA/certs/cacert.pem /home/sio
The authenticity of host '192.168.2.1 (192.168.2.1)' can't be established.
ED25519 key fingerprint is SHA256:aHcZvWbmN8w5TLu5z6+xNN5tiHSkt9wIUaOfrNJNMWw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.1' (ED25519) to the list of known hosts.
root@192.168.2.1's password:
Permission denied, please try again.
root@192.168.2.1's password:
cacert.pem                                    100% 1391   123.7KB/s   00:00
root@DD1:~#
```

Nous importons ensuite dans Firefox, le certificat dans le magasin de certificats du navigateur :



Certificat

DS2.sio-exupery.fr

Nom du sujet

Pays	FR
État / Province	France
Localité	Saint-Raphael
Organisation	sio-exupery
Unité organisationnelle	BTS SIO
Nom courant	DS2.sio-exupery.fr

Nom de l'émetteur

Pays	FR
État / Province	France
Localité	Saint-Raphael
Organisation	sio-exupery
Unité organisationnelle	BTS SIO
Nom courant	DS2.sio-exupery.fr

Validité

Pas avant	Wed, 29 Apr 2026 06:52:36 GMT
Pas après	Sat, 26 Apr 2036 06:52:36 GMT

Informations sur la clé publique

Algorithme	RSA
Taille de la clé	2048
Exposant	65537
Module	B1:32:11:7F:E7:E9:92:DF:F4:F0:2C:D3:0D:56:BE:5D:77:0B:BA:B3:AB:24:C5:70…

Nom du certificat	Périphérique de sécurité
sio-exupery	
DS2.sio-exupery.fr	Sécurité personnelle
SSL Corporation	
SSL.com Client ECC Root CA 2022	Builtin Object Token
SSL.com Root Certification Authority RSA	Builtin Object Token
SSL.com TLS RSA Root CA 2022	Builtin Object Token

Nous pouvons donc constater que le site secu.sio-exupery.fr apparaît avec un cadenas :