Chapitre 11 – Echanges sécurisés et authentifiés avec SSL

3. Configuration côté SSL.

▪ Le paquet openssl doit être déjà installé, vérifiez-le :

▪ L’emplacement du fichier de configuration openssl.cnf se situe dans le répertoire /etc/ssl. Vérifiez le contenu de ce dernier :

```
root@DS2: /etc/ssl#ls -l
total 36
drwxr-xr-x 2 root root     16384 12 mars  09:53 certs
-rw-r--r-- 1 root root     12332 27 oct.  15:16 openssl.cnf
drwx--x--- 2 root ssl-cert  4096 12 mars  09:53 private
```

▪ Copie sauvegarde du fichier /etc/ssl/openssl.cnf :

```
root@DS2: /etc/ssl#ls -l
total 52
drwxr-xr-x 2 root root     16384 12 mars  09:53 certs
-rw-r--r-- 1 root root     12332 27 oct.  15:16 openssl.cnf
-rw-r--r-- 1 root root     12332 12 avril 20:54 openssl.cnf.sauv
drwx--x--- 2 root ssl-cert  4096 12 mars  09:53 private
root@DS2: /etc/ssl#
```

3.1. Création d’une autorité de certification racine.

▪ Création de l’environnement du CA c’est-à-dire les répertoires qui hébergeront son certificat et ses divers fichiers (cf. fichier /etc/ssl/openssl.cnf ci-après) :

```
root@DS2: ~#cd /etc/ssl
root@DS2: /etc/ssl#mkdir /etc/ssl/CA
root@DS2: /etc/ssl#mkdir /etc/ssl/CA/certs /etc/ssl/CA/private /etc/ssl/CA/newcerts
root@DS2: /etc/ssl#ls -l /etc/ssl/CA
total 12
drwxr-xr-x 2 root root 4096 12 avril 20:57 certs
drwxr-xr-x 2 root root 4096 12 avril 20:57 newcerts
drwxr-xr-x 2 root root 4096 12 avril 20:57 private
root@DS2: /etc/ssl#
```

▪ Création des deux fichiers serial et index.txt destinés d'une part, à garder trace du dernier numéro de série utilisé par le CA (chaque certificat doit avoir un numéro de série distinct) et d'autre part, à garder trace des certificats générés :

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

▪ Modification du fichier de configuration /etc/ssl/openssl.cnf dans la partie [CA_default] :

```
  GNU nano 7.2                                                  /etc/ssl/openssl.cnf *


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

####################################################################
[ 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 = 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
```

▪ Spécification, dans le fichier openssl.cnf, de l'extension de la norme X.509

```
  GNU nano 7.2                                                  /etc/ssl/openssl.cnf
# subjectAltName=email:move

# Copy subject details
# issuerAltName=issuer:copy

# This is required for TSA certificates.
# extendedKeyUsage = critical,timeStamping

[ 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-exupery.fr

[ v3_ca ]
```

▪ Remplacement usr_cert par v3_req (x509_extensions). Par ailleurs, la CA qui signe la CSR et qui doit gérer ces extensions doit avoir copy_extensions = copy non commenté.

```
  GNU nano 7.2                                                  /etc/ssl/openssl.cnf
# OpenSSL may not work correctly which could lead to significant system
# problems including inability to remotely access the system.
# [default_sect]
# activate = 1


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

####################################################################
[ 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
```

▪ Génération de la clé privée du CA à l'aide de la commande genrsa d'OpenSSL :

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

```
 GNU nano 7.2                                                    /etc/ssl/CA/private/cakey.pem
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDAM4U67PpQn07r
thmCzz/9//dXeW4a/LbiSibenxHptUPU11y9kCaN1zQnZMBC9dyHJ+pHoNfHGsLC
Dt4E10MS9o5dm6esPpubh2n/cni4gitcBln/dbzNO4jYjMiTZPXklKXurztxA20z
WrFDNoDw8eXYEc62LMmyHslftrti29JHbgUvdLJ9sp3uYSEQOg+CWBMR6LRiEK3N
JwHKS0NXVi65derUbVz98zhwKHV9lgNix/QIgjOYxYfmpidi0yEevEDse12vwM6U
Eoh16KMTsDNEp+m1FY6ctD7e4tONUMzxnZwKfrYLArKg5liExMGGEp3lLdVUcEOz
ZUpZoULVAgMBAAECggEAJagidxJVk8S2sXtu4aBp9QG4zABsWGjBizIEjhMD7zJ2
zQV58+EBkMJEg2Bbw/LIR4nEPs7uX+HoHR3NFY04ZMd+SqxTzG1CzxTXqXcb3GiS
hrfu25yNhnde3zCsHqbF/4g5P3vBLWoCs/BVsSnFVw/J3MzWX36EcPvTsAdNDPfV
zjuUkub89CJxtYw0UaIKuDgD3igVnBEkjBB+un01U2vb1sE59lzRJc/AmJQJRbnK
/KQFtJkixuniF3NRcKqjy4M+ytb+zFptyR3r9a48KQqPasfG0DpTyCn8w11pbyhy
trc8P7pN1VacrAhnEonIEfKLshOiDZz7LLSL6JMKiQKBgQD1Oiw+EfnJU9orhUAz
PvS7KwFU1mXjcJBfs0AxxTfgXK48GxwAMyRGojzDNij4s+0DHdvUYVFJmlqslKLo
yxm14BUW/KQAgIrLzDIWq2fIfSq+Hsg/+YSWSciKL4l/IktlcY4KZGYfrLM38/Bh
mXzcYuxpXT4/5hMT2GRzzTGe+QKBgQDIpQRa1LzU1b30DuJWpWWFa+8zsxxiCgEM
R2134d4h/vGhfcwbrIyrbAS5QYqoZn2eQ4Q/lI2HwbmdLJJ8e72d0pjSo8J/Mgwq
J/IMID/fEsa0CdKxImKZwu2Z7pn+1K5j9OybQRzO0WtqiJLfv4Qxe48VId2CCYP0
S0abPh5NvQKBgQDgXdtA5z19YMUKcJ5uxLkxzoUnVApg8AqIJP8lCma3VtTrlXon
DKOyJJonmZQfCLBf25/YTzoKd7likZQEHl9lsqJZJ8n9054qHKfvaeBI5YyH6q4Z
KniO8O8Uz62jroMBTULgqz9s15waI4zaH47ILZJUTMW5vQ3TaHdwJFu0MQKBgQC8
el7j4DFeEUa1y4GMeSQruB9kRl1kLxea7EIFulQLRUzAMcaZPHaL1RV+3PWeiWB5
Wd0SSL7GhxGQdr1IWIjfh2Ptgs2C5IWO2CVEhMrbBu1HVG7p3G4ZGIZP8lYQjsMe
vIXCteCU2x53XcHykxpfzTy0UjKdI8kjo864qBqZVQKBgQDIedyQRcv8ciQP8fZu
2KPdm0UFlwivGDIboVb08YYj/sEbMin89GcmJIvFf40GEuSrrz1h05Up9lXRuIOq
ftjgVSJXjgIzuUBgyH31SEs4s8BPNJ0OX+npJ9EN8DueIyHGiwEDM2YVL5tH2cmv
EDgDBV4+ZlFS0XJunLO75yrM1A==
-----END PRIVATE KEY-----
```

```
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 []:
root@DS2: #_
```

▪ Nous constatons la présence des fichiers cakey.pem et cacert.pem respectivement dans les répertoires /etc/ssl/CA/private et /etc/ssl/CA/certs :

```
root@DS2: ~#cd /etc/ssl/CA/private
root@DS2: /etc/ssl/CA/private#ls -l
total 4
-rw------- 1 root root 1708 12 avril 21:12 cakey.pem
root@DS2: /etc/ssl/CA/private#
```

```
root@DS2: ~#cd /etc/ssl/CA/certs
root@DS2: /etc/ssl/CA/certs#ls -l
total 4
-rw-r--r-- 1 root root 1391 12 avril 21:14 cacert.pem
root@DS2: /etc/ssl/CA/certs#
```

- Affichage du certificat racine à l'aide de la commande x509 d'OpenSSL :

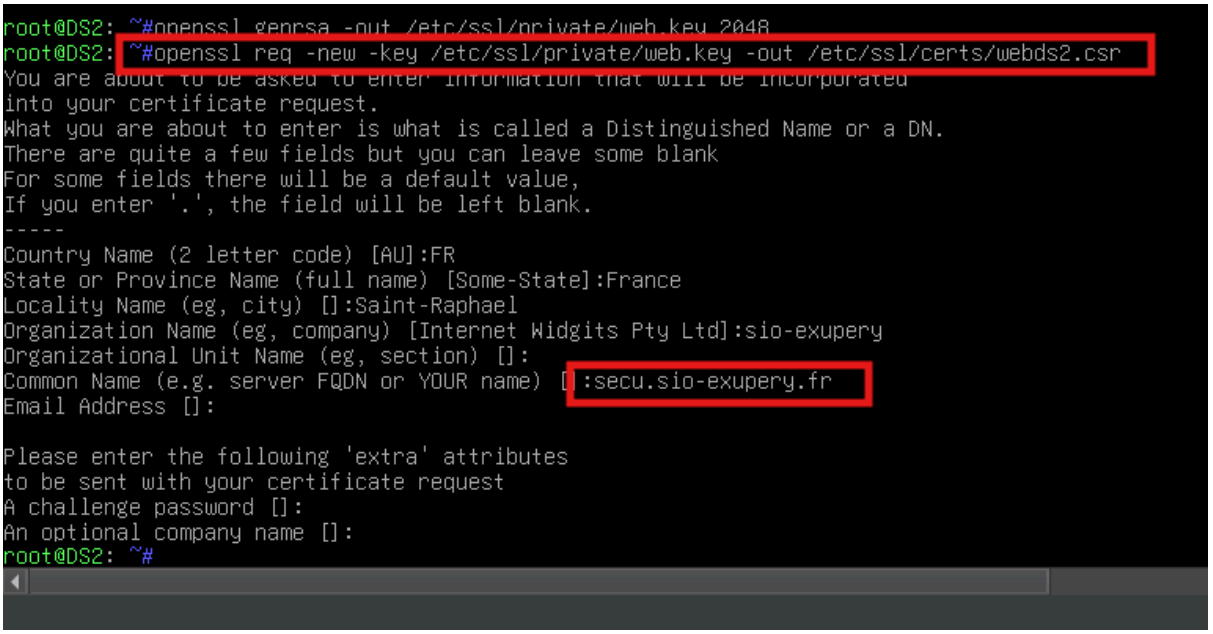
```
root@DS2: ~#openssl x509 -in /etc/ssl/CA/certs/cacert.pem -text | more
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            67:b2:6c:11:60:23:d7:de:f1:47:c3:4b:a2:48:ee:d6:f7:8d:df:15
        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 12 19:14:29 2025 GMT
            Not After : Apr 10 19:14:29 2035 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:c0:33:85:3a:ec:fa:50:9f:4e:eb:b6:19:82:cf:
                    3f:fd:ff:f7:57:79:6e:1a:fc:b6:e2:4a:26:de:9f:
                    11:e9:b5:43:d4:d7:5c:bd:90:26:8d:d7:34:27:64:
                    c0:42:f5:dc:87:27:ea:47:a0:d7:c7:1a:c2:c2:0e:
                    de:04:d7:43:12:f6:8e:5d:9b:a7:ac:3e:9b:9b:87:
                    69:ff:72:78:b8:82:2b:5c:06:59:ff:75:bc:cd:3b:
                    88:d8:8c:c8:93:64:f5:e4:94:a5:ee:af:3b:71:03:
                    6d:33:5a:b1:43:36:80:f0:f1:e5:d8:11:ce:b6:2c:
                    c9:b2:1e:c9:5f:b6:bb:62:db:d2:47:6e:05:2f:74:
                    b2:7d:b2:9d:ee:61:21:10:3a:0f:82:58:13:11:e8:
                    b4:62:10:ad:cd:27:01:ca:4b:43:57:56:2e:b9:75:
                    ea:d4:6d:5c:fd:f3:38:70:28:75:7d:96:03:62:c7:
                    f4:08:82:33:98:c5:87:e6:a6:27:62:d3:21:1e:bc:
                    40:ec:7b:5d:af:c0:ce:94:12:88:65:e8:a3:13:b0:
                    33:44:a7:e9:b5:15:8e:9c:b4:3e:de:e2:d3:8d:50:
                    cc:f1:9d:9c:0a:7e:b6:0b:02:b2:a0:e6:58:84:c4:
                    c1:86:12:9d:e5:2d:d5:54:70:43:b3:65:4a:59:a1:
                    42:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                7C:8E:2E:34:01:45:9A:3E:C6:FC:D1:A1:6F:9C:60:EE:8C:C0:BA:C2
            X509v3 Authority Key Identifier:
                7C:8E:2E:34:01:45:9A:3E:C6:FC:D1:A1:6F:9C:60:EE:8C:C0:BA:C2
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        9b:8e:6b:0b:1f:3a:b7:e8:f7:6a:20:22:bc:b3:0b:bc:de:4d:
        1c:9f:d3:d0:d4:a7:3b:e8:13:44:e0:e5:73:84:11:c5:72:9b:
        6a:5f:98:9a:4e:f7:c5:52:e9:da:2c:39:5d:c5:ff:c5:78:94:
        bb:9b:19:99:c1:ea:07:f2:1b:70:8f:d6:c4:3f:be:bb:c1:24:
        ce:f3:b7:21:01:d9:84:d9:ba:6f:c8:ae:55:81:ed:04:85:16:
        7b:fc:85:fa:61:16:9c:0b:f4:bf:99:c7:8a:83:8f:08:df:b8:
--Plus--
```

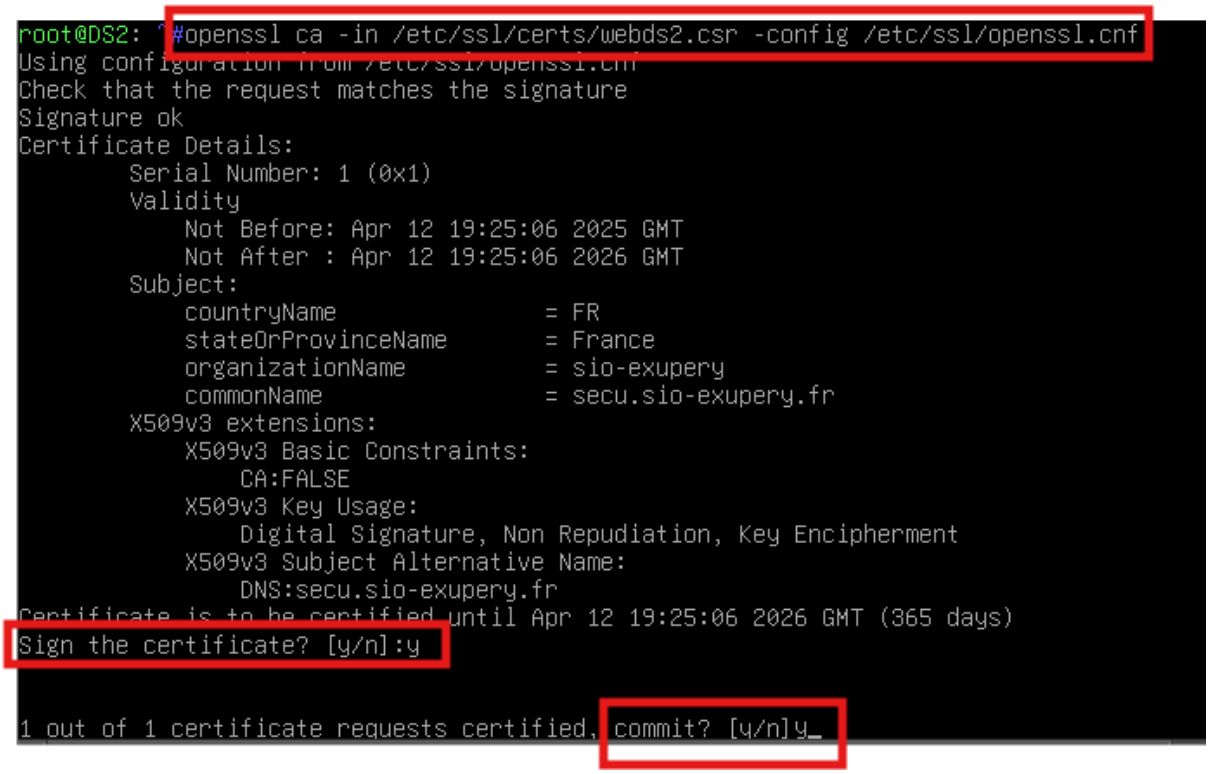
```
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUZ7JsEWAj197xR8NLokju1veN3xUwDQYJKoZIhvcNAQEL
BQAwezELMAkGA1UEBhMCRlIxDzANBgNVBAgMBkZyYW5jZTEWMBQGA1UEBwwNU2Fp
bnQtUmFwaGFlbDEUMBIGA1UECgwLc2lvLWV4dXBlcnkxEDAOBgNVBAsMB2J0cyBz
aW8xGzAZBgNVBAMMEkRTMi5zaW8tZXh1cGVyeS5mcjAeFw0yNTA0MTIxOTE0Mjla
Fw0zNTA0MTAxOTE0MjlaMHsxCzAJBgNVBAYTAkZSMQ8wDQYDVQQIDAZGcmFuY2Ux
FjAUBgNVBAcMDVNhaW50LVJhcGhhZWwxFDASBgNVBAoMC3Npby1leHVwZXJ5MRAw
DgYDVQQLDAdidHMgc2lvMRswGQYDVQQDDBJEUzIuc2lvLWV4dXBlcnkuZnIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAM4U67PpQn07rthmCzz9//dX
eW4a/LbiSibenxHptUPU11y9kCaN1zQnZMBC9dyHJ+pHoNfHGsLCDt4E10MS9o5d
m6esPpubh2n/cni4gitcBln/dbzNO4jYjMiTZPXklKXurztxA20zWrFDNoDw8eXY
Ec62LMmyHslftrti29JHbgUvdLJ9sp3uYSEQOg+CWBMR6LRiEK3NJwHKS0NXVi65
derUbVz98zhwKHV9lgNix/QIgjOYxYfmpidi0yEevEDse12vwM6UEohl6KMTsDNE
p+m1FY6ctD7e4tONUMzxnZwKfrYLArKg5liExMGGEp3lLdVUcEOzZUpZoULVAgMB
AAGjUzBRMB0GA1UdDgQWBBR8ji40AUWaPsb80aFvnGDujMC6wjAfBgNVHSMEGDAW
gBR8ji40AUWaPsb80aFvnGDujMC6wjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4IBAQCbjmsLHzq36PdqICK8swu83k0cn9PQ1Kc76BNE4OVzhBHFcptq
X5iaTvfFUunaLDldxf/FeJS7mxmZweoH8htwj9bEP767wSTO87chAdmE2bpvyK5V
ge0EhRZ7/IX6YRacC/S/mceKg48I37hYUt23jexbZwdVYeIF4tOziYspOqAkllS2
gRmwXIBBpO3JV3xHSw5RE+JcfZTyrwI3HJchw7eRp/bs7FJEwDo93pF2fqhQltJa
3aFKGJQLWBGCz5QoDgwVK0KnhYLmuJpNVGLtsmR6/hqqlgMpWWSINYkbSuOLM3c0
TCeV3Cp2hTtDxjsXZht+I7pmaWYx6zTpuFOA
-----END CERTIFICATE-----
```

3.2. Création des clés et du certificat du serveur Web. ▪ Génération d'une paire de clés publique/privée pour le serveur Web (répertoire /etc/ssl/private) :

▪ Génération d'une demande de signature de certificat (requête de certification CSR) à l'aide de la commande req d'OpenSSL. Attention, l'information Common Name doit correspondre à l'URL qui sera saisi depuis le navigateur Web (secu.sio-exupery.fr en l'occurrence) :



▪ Signature de la requête en tant que CA à l'aide de la commande ca d'OpenSSL. Répondez y à la question « Sign the certificate ? » et répondez également y pour l'écriture du certificat certifié dans la base de données SSL :



▪ Affichage du contenu des fichiers index.txt et serial :

▪ Nous vérifions la présence du certificat SSL 01.pem dans le répertoire /etc/ssl/CA/newcerts :

▪ Nous créons le certificat SSL secu.sio-exupery.fr.crt obtenu à partir du fichier 01.pem. Ce certificat est à placer dans le répertoire /etc/ssl/certs/ du serveur Web DS2 :

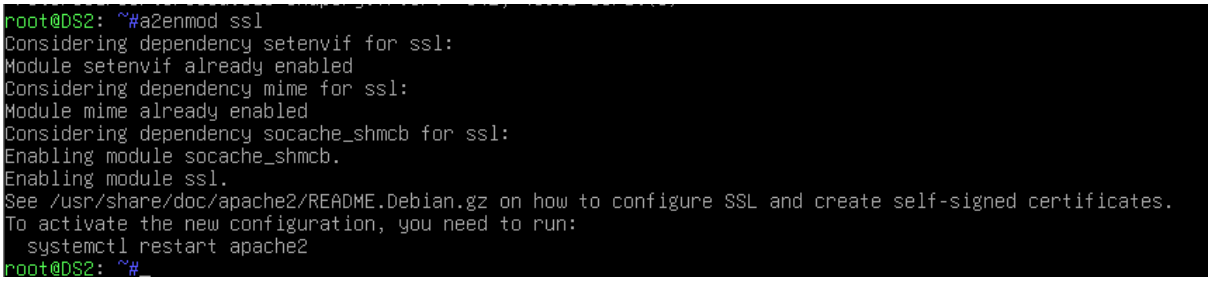
```
root@DS2: ~#cat /etc/ssl/CA/newcerts/01.pem > /etc/ssl/certs/secu.sio-exupery.fr.crt
root@DS2: ~#_
```

Nous consultons le fichier à l'aide de VIM :

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        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 12 19:25:06 2025 GMT
            Not After : Apr 12 19:25:06 2026 GMT
        Subject: C=FR, ST=France, O=sio-exupery, CN=secu.sio-exupery.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e4:15:07:22:02:3b:2e:48:e6:73:56:96:14:10:
                    93:c7:ec:41:d4:0c:eb:97:44:e6:64:d1:d3:2c:f3:
                    80:9d:e6:d0:31:30:32:f7:07:cb:59:d3:dc:e1:1e:
                    d4:81:84:0e:df:f4:34:56:a5:f8:ec:93:23:a9:d4:
                    c9:e3:02:33:4c:fe:14:87:1e:f9:a4:74:e3:39:7c:
                    de:6a:33:35:87:a8:65:c6:71:5d:b3:a2:43:eb:17:
                    f4:7a:9e:0a:c0:aa:59:1d:5e:2e:cc:a8:b8:d4:b1:
                    ec:47:c8:fb:0f:47:92:2a:ca:47:8c:b9:0a:89:21:
                    2d:c7:9d:c1:e4:9c:7c:b9:78:b7:c5:43:2f:d9:a4:
                    9c:bd:59:7d:4b:6e:a1:f5:b9:c5:40:d1:7f:1e:76:
                    72:87:00:39:26:d5:b8:00:23:a0:40:68:9a:d7:80:
                    8d:4e:58:c8:74:02:29:f2:af:35:d5:ca:45:a4:a1:
                    ed:82:88:75:d8:d0:21:33:9d:e5:65:d2:3e:8d:56:
                    5a:87:05:51:6b:bc:90:f6:0d:a0:f6:0c:38:80:9c:
                    9d:12:0c:53:9d:ae:ca:61:28:b3:01:62:da:ed:36:
                    ea:38:6c:52:6e:05:67:c3:81:61:78:f5:29:c9:18:
                    e6:67:d3:5e:5c:29:ff:67:5b:22:7d:92:8c:3c:f6:
                    f3:87
                Exponent: 65537 (0x10001)
        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
            X509v3 Subject Key Identifier:
                E9:7E:97:DF:4A:6F:B7:E4:28:41:0D:CC:EC:67:8C:6E:6D:F6:82:27
            X509v3 Authority Key Identifier:
                7C:8E:2E:34:01:45:9A:3E:C6:FC:D1:A1:6F:9C:60:EE:8C:C0:BA:C2
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        35:89:3f:d6:d1:fd:8b:9d:79:38:69:88:f6:70:16:19:e8:b5:
        40:27:37:44:d8:8e:88:4b:2f:62:a4:ca:a0:38:81:d9:32:87:
        78:16:34:2a:22:53:9b:31:e6:fd:20:63:37:d1:fb:d6:30:38:
"/etc/ssl/certs/secu.sio-exupery.fr.crt" 84L, 4607B
```

4. Configuration côté Apache.

▪ Nous activons le module ssl, installé normalement d'office, avec la commande a2enmod ssl :



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

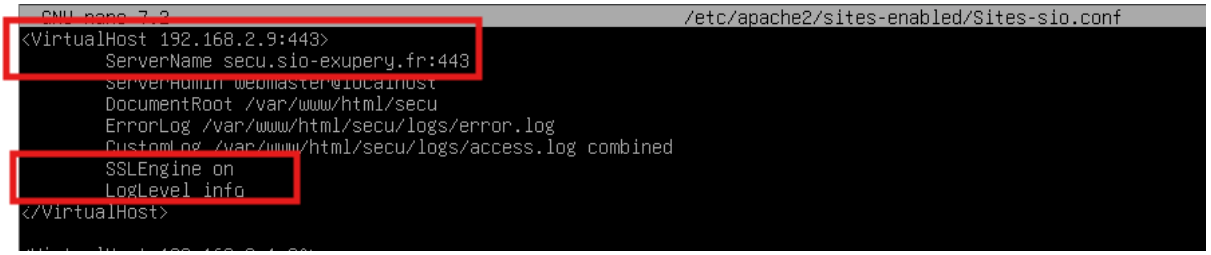
▪ Ajoutez les lignes SSLCertificateFile et SSLCertificateKeyFile juste avant la directive du fichier /etc/apache2/mods-enabled/ssl.conf :

```
  GNU nano 7.2                                        /etc/apache2/mods-enabled/ssl.conf
SSLSessionCacheTimeout  300

#   Semaphore:
#   Configure the path to the mutual exclusion semaphore the
#   SSL engine uses internally for inter-process synchronization.
#   (Disabled by default, the global Mutex directive consolidates by default
#   this)
#Mutex file:${APACHE_LOCK_DIR}/ssl_mutex ssl-cache


#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate. See the
#   ciphers(1) man page from the openssl package for list of all available
#   options.
#   Enable only secure ciphers:
SSLCipherSuite HIGH:!aNULL

# SSL server cipher order preference:
# Use server priorities for cipher algorithm choice.
# Clients may prefer lower grade encryption.  You should enable this
# option if you want to enforce stronger encryption, and can afford
# 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>_
```

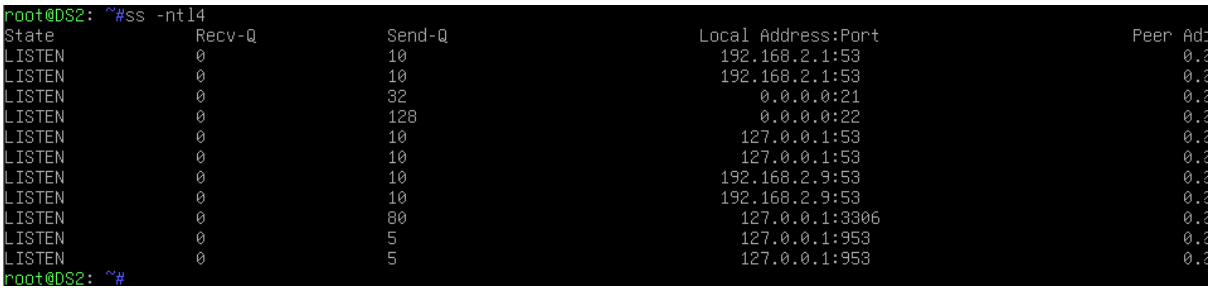
Affichage, pour voir cela, le fichier /etc/apache2/ports.conf/ports.conf :

```
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>
root@DS2: ~#_
```

▪ Modification du contenu du fichier /etc/apache2/sites-available/sites-sio.conf pour la partie concernant l'hôte virtuel par l'IP :

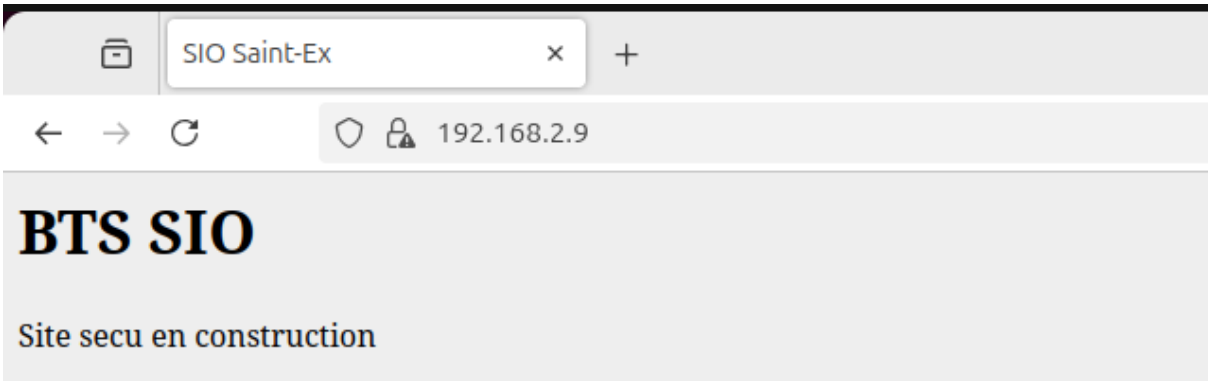


▪ Relancement du service Apache puis saisissez la commande ss -ntl4 afin d'affichez les connexions TCP actives ainsi que les ports d'écoute :



5. Test du serveur Web sécurisé depuis un client.

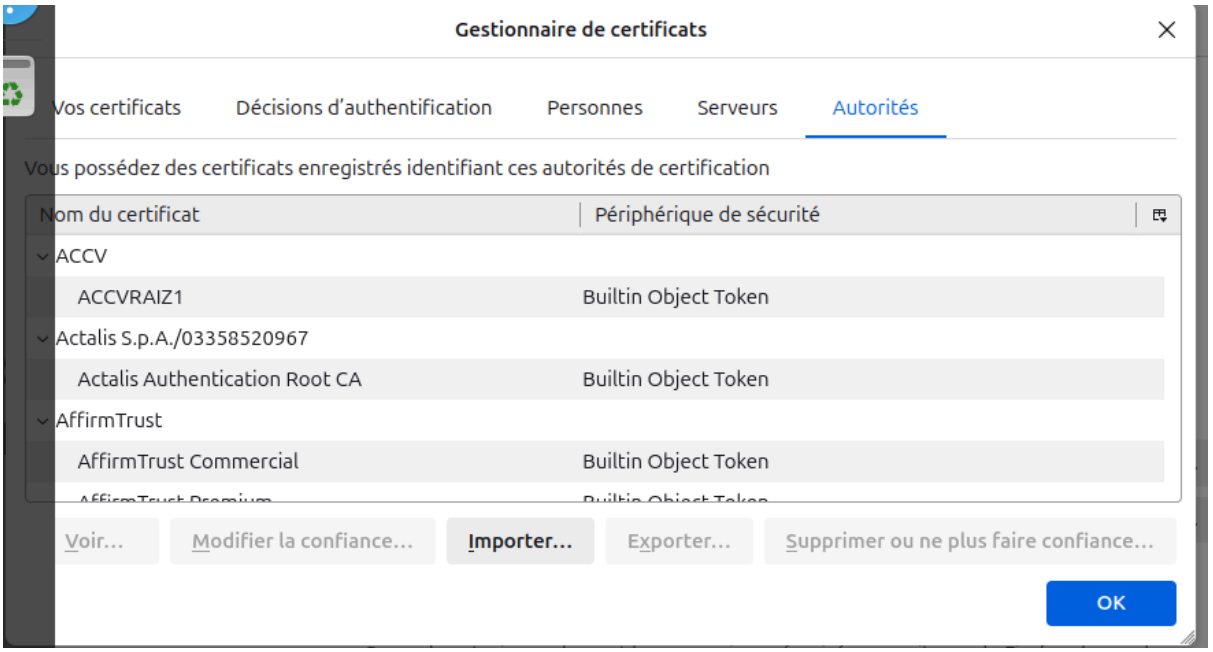
▪ Lancez, dans un navigateur sur le client UD1, l'URL https://secu.sio-exupery.fr. Cela provoque la demande d'acceptation du certificat car le navigateur ne trouve pas une autorité de certification reconnue (et pour cause : vous l'avez vous-même signé). Cliquez évidemment sur le lien Poursuivre sur cette page.



▪ Depuis la machine UD1, nous transférons le certificat de notre autorité de certification vers le répertoire personnel de l'utilisateur sio :

```
nicolasmtru@UD1:~$ sudo scp root@192.168.2.1:/etc/ssl/CA/certs/cacert.pem /home/
sio
[sudo] Mot de passe de nicolasmtru :
The authenticity of host '192.168.2.1 (192.168.2.1)' can't be established.
ED25519 key fingerprint is SHA256:QpRomLcdLXaYYh+7ZH6RVx8XbsP1M99O4NwUnnFTigE.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
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:
cacert.pem                                    100% 1391    33.9KB/s   00:00
nicolasmtru@UD1:~$
```

▪ Nous importons le certificat dans le magasin de certificats du navigateur Firefox (Paramètres / Vie privée et sécurité / Certificats / Afficher les certificats). Modifiez si besoin l'extension du certificat (mv cacert.pem cacert.crt)



Le reste ne s'affiche pas/ ne fonctionne pas une fois que je clique sur importer le certificat ssl "cacert"