Cryptographie

Mathis EVRARD
Yassine ACHCHAB
Jules MINIOT
Nohann AMAND-REGHAI

Sommaire

- Création certificats
- Monter un serveur web
- Authentification côté client
- Démonstration
- Algorithme de chiffrement

Création certificats

Création clé privé de l'autorité de certification

```
openssl gensra -des3 2048 > autoriteCertification.key
```

Création certificat d'autorité auto signé

```
openssl req -new -x509 -days 365 -key autoriteCertification.key > autoriteCertificatAutoSigne.crt
```

Création clé privé du serveur

```
openssl genrsa 2048 > serveur.key
```

Création certificat serveur

```
openssl req -new -key serveur.key > demandeSignatureCertificat.csr
```

Signature du certificat du serveur par la CA

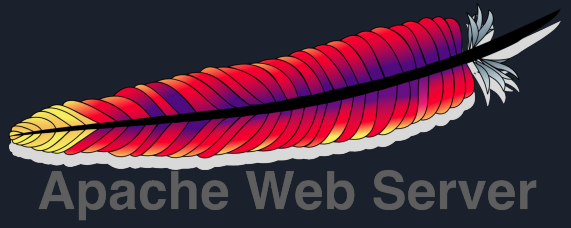
```
openssl x509 -req -in demandeSignatureCertificat.csr -out certificatSigne.crt
-CA autoriteCertificatAutoSigne.crt -CAkey autoriteCertification.key -CAcreateserial -CAserial ca.srl
```

Convertir un certificat au format DER

```
openssl x509 -in autoriteCertificatAutoSigne.crt -outform DER -out autoriteCertificatAutoSigne.der.crt
```

Monter un serveur web

- Apache2
- Configuration SSL
- Vérification certificat



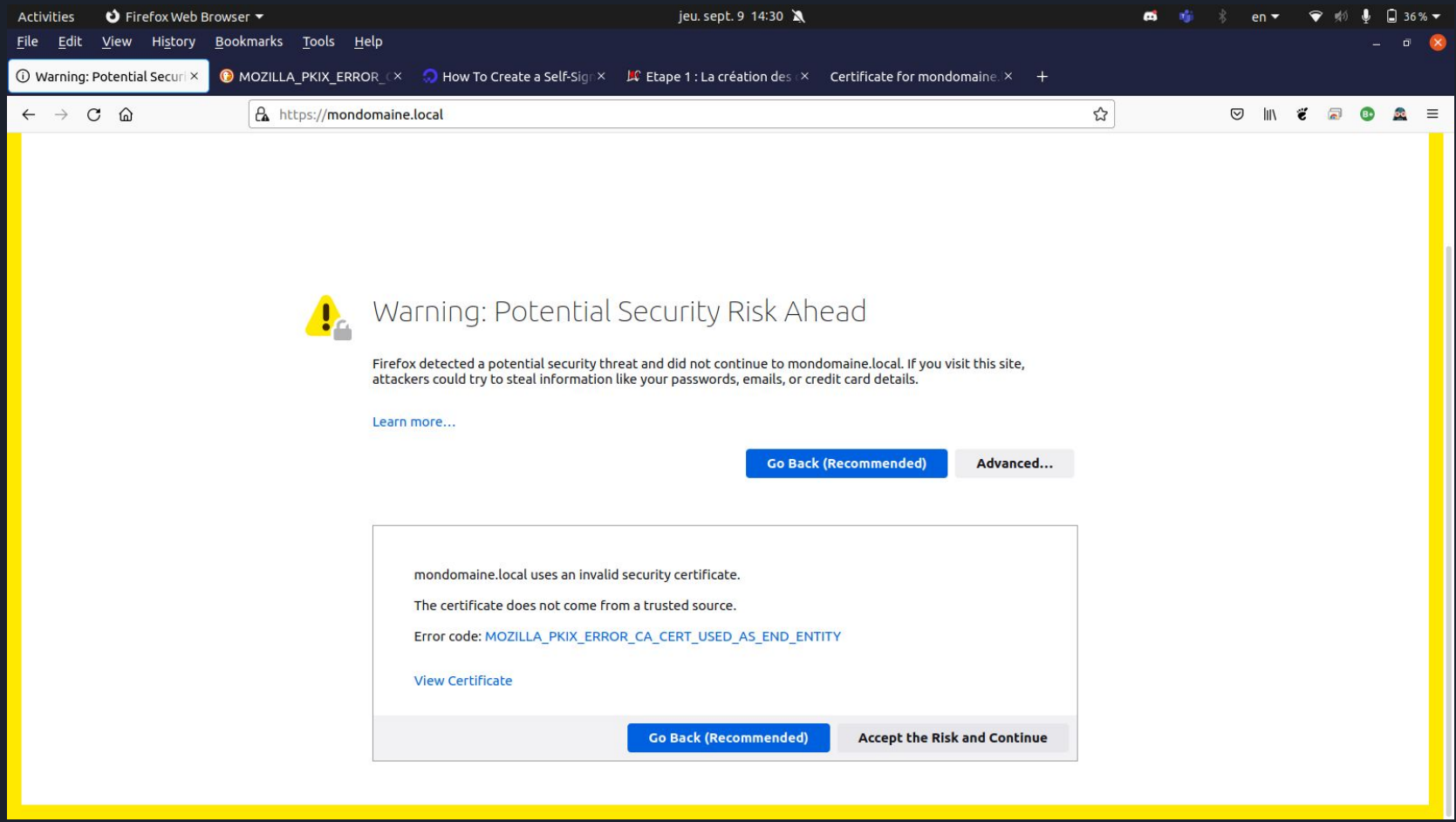
Serveur apache / Fichiers conf pour mettre SSL et HTTPS

```
nano 5.4                                        default-ssl.conf
lule mod_ssl.c>
  <VirtualHost _default_:443>
          ServerAdmin webmaster@localhost

          ServerName mondomaine.local


  #   A self-signed (snakeoil) certificate can be created by inst
  #   the ssl-cert package. See
  #   /usr/share/doc/apache2/README.Debian.gz for more info.
  #   If both key and certificate are stored in the same file, or
  #   SSLCertificateFile directive is needed.
  SSLCertificateFile      /etc/apache2/ssl/certificatSigne.crt
  SSLCertificateKeyFile /etc/apache2/ssl/serveur.key
```

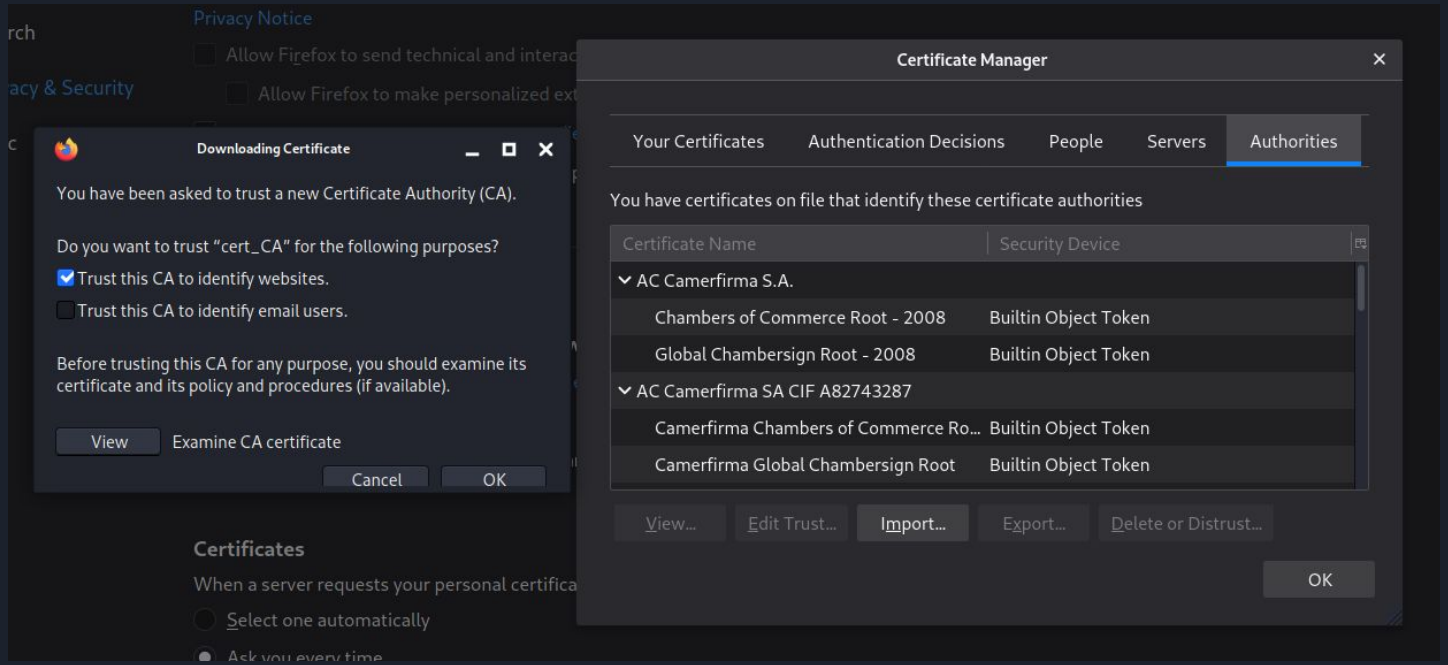
```
BrowserMatch "MSIE [2-6]" \
               nokeepalive ssl-unclean-shutdown \
               downgrade-1.0 force-response-1.0
```

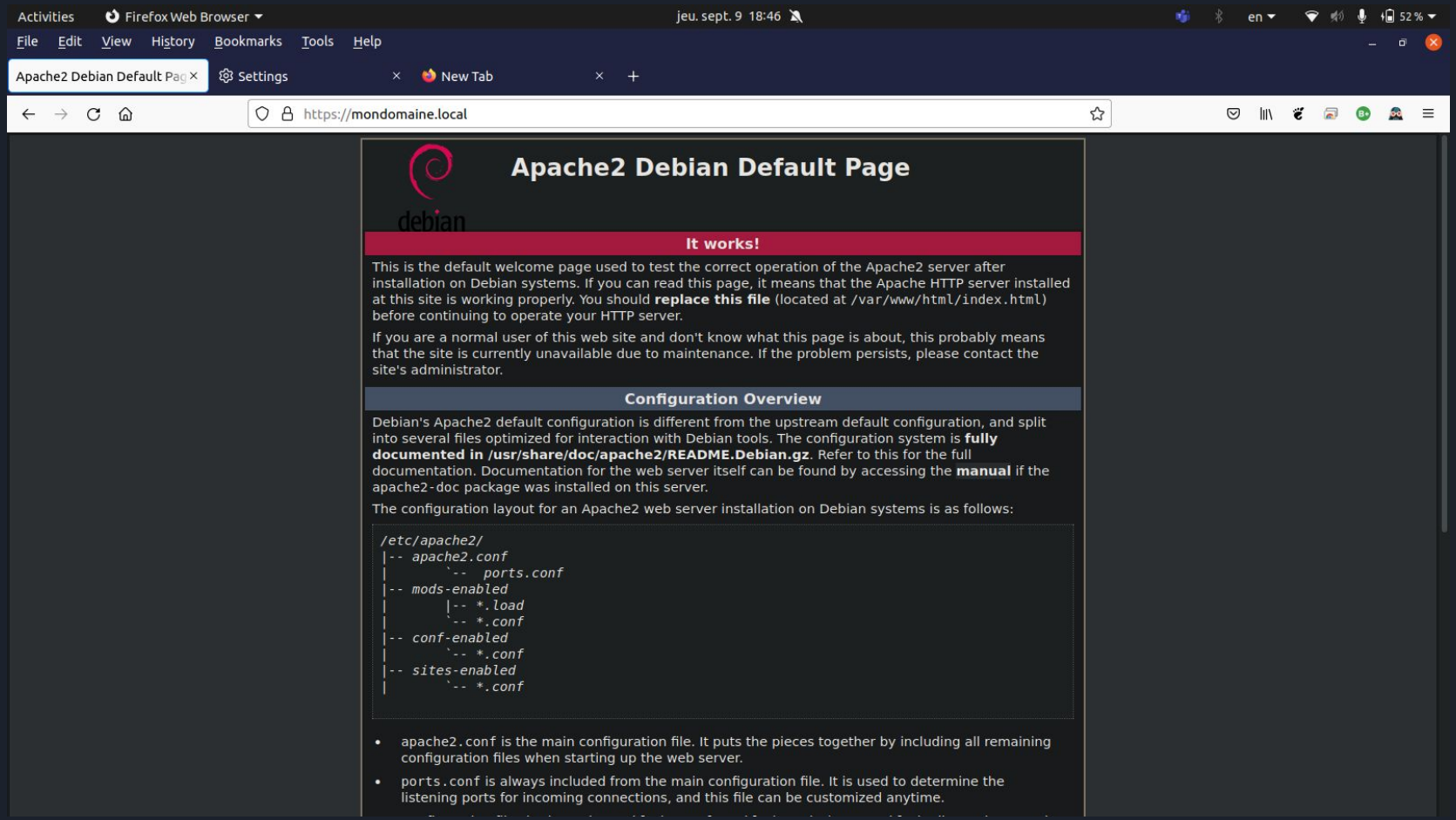
```
Redirect "/" "https://mondomaine.local/"
```

Demande du certificat



Installation du certificat dans le navigateur



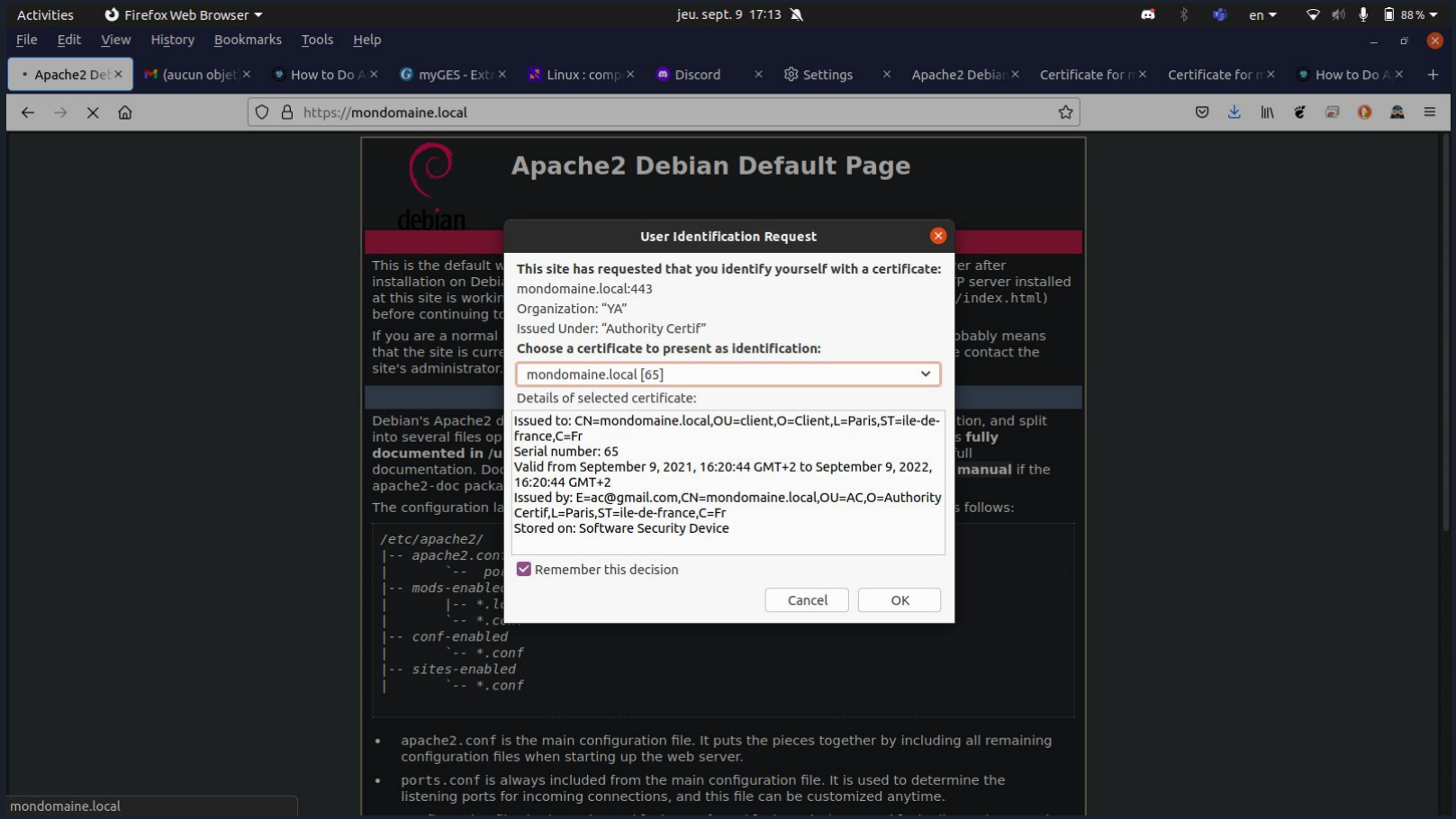

Activities
Firefox Web Browser
jeu. sept. 9 18:46
en
52 %
File Edit View History Bookmarks Tools Help
Apache2 Debian Default Pag
Settings
New Tab
https://mondomaine.local
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Authentification côté client

```
#   Client Authentication (Type):
#   Client certificate verification type and depth.  Types are
#   none, optional, require and optional_no_ca.  Depth is a
#   number which specifies how deeply to verify the certificate
#   issuer chain before deciding the certificate is not valid.
SSLVerifyClient require
SSLVerifyDepth  10
SSLCACertificateFile /etc/apache2/ssl/autoriteCertificatAutoSigne.crt
```

```
Création clé privé client:
        openssl genrsa 2048 > client.key

Création certificat client:
        openssl req -new -key client.key > certificatClient.csr

Signature certificat client pars CA:
        openssl x509 -req -in certificaClient.csr -out certificatClientSigne.crt
        -CA autoriteCertificatAutoSigne.crt -CAkey autoriteCertification.key -CAcreateserial -CA serial ca.srl

Regroupe clé et certificat client dans un packet p12:
        openssl pkcs12 -export -inkey client.key -in certificatClientSigne.crt -out clientSigne.p12
```

Demande certificat client



Démonstration

Algorithme de chiffrement

- Présentation
- Démonstration

Merci