

Rapport TP SSR

Sécuriser un serveur web apache en mode SSL

Réalisé Par :

- AZIZ Rezak
- MECHARBAT Lotfi Abdelkrim

Groupe : SIQ3

Année universitaire : 2020/2021

Dans un premier temps nous devons installer les outils suivants :

- TinyCA
- OpenSSL
- Xampp

I. Création d'un espace de Publication Web Apache :

- Création d'un répertoire de test delta :

```
root@debian:/opt/lampp/htdocs# mkdir delta
```

- Modification du fichier lampp/etc/httpd.conf

```
#DocumentRoot "/opt/lampp/htdocs"
DocumentRoot "/opt/lampp/htdocs/delta"

<Directory "/opt/lampp/htdocs/delta">
#<Directory "/opt/lampp/htdocs">
#
```

- Création d'une page web dans le répertoire delta

```
root@debian:/opt/lampp/htdocs/delta# nano index.html
root@debian:/opt/lampp/htdocs/delta# ls
index.html
```

- Relancer Apache

```
root@debian:/opt/lampp# ./lampp restart
Restarting XAMPP for Linux 8.0.3-0...
XAMPP: Stopping Apache...ok.
XAMPP: Stopping MySQL...ok.
XAMPP: Stopping ProFTPD...ok.
XAMPP: Starting Apache...ok.
XAMPP: Starting MySQL...ok.
XAMPP: Starting ProFTPD...ok.
root@debian:/opt/lampp#
```

- Tester le navigateur



Hello World From Rezak and Lotfi

II. Créer un répertoire pour la zone sécurisée :

- Création de répertoire secure et mettre une page html dedans

```

root@debian:/opt/lampp/htdocs/delta# mkdir secure
root@debian:/opt/lampp/htdocs/delta# cd secure
root@debian:/opt/lampp/htdocs/delta/secure# nano index.html

```

- Modification des fichiers de configuration

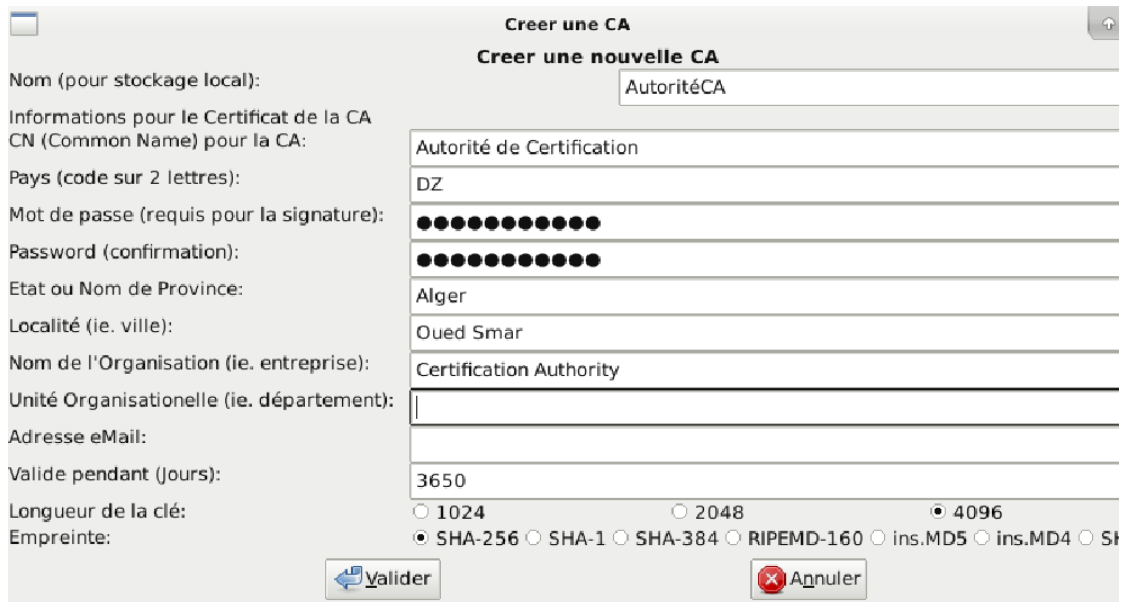
```

#DocumentRoot "/opt/lampp/htdocs"
DocumentRoot "/opt/lampp/htdocs/delta/secure"

```

III. Créer les certificats et les clés

- Création de certificat de CA




Tiny CA Management 0.7.5 - AutoriteCA

CA Preferences Aide

CA Certificats Clés Requêtes de certification

Informations CA

Empreinte Numérique (MD5): 9C:DB:F2:88:64:BF:59:60:BD:78:CA:43:C8:D8:76:41
 Empreinte Numérique (SHA1): 14:FF:59:71:53:85:C0:DD:F1:5E:D2:C1:87:90:6B:AF:53:EF:BC:61
 Fingerprint (SHA256): A7:BB:7A:D4:E1:89:44:BC:9E:AD:DC:78:49:11:CF:A4:73:A6:D7:36:11:95:4A:9D:D8:40:55:75:

Unité Organisationnelle (OU) Certification Authority	Date de Création Apr 23 23:02:41 2021
	Date d'Expiration Apr 21 23:02:41 2031
	Algorithme de Clé Publique rsaEncryption
	Algorithme de Signature sha256WithRSAEncryption

- Création des dossiers des clés et certificats

```
root@debian:/opt/lampp/etc# mkdir delta
root@debian:/opt/lampp/etc# mkdir delta/cles delta/certifs
```

- Création du certificat du serveur

Créer Requête

Créer une nouvelle requête de certificat

Nom commun (ie. votre Nom, votre adresse eMail ou le Nom du serveur): serveur

Adresse eMail:

Mot de passe (protrège votre Clé privée): ●●●●●●●●●●

Password (confirmation): ●●●●●●●●●●

Pays (code sur 2 lettres): DZ

Etat ou Nom de Province: Alger

Localité (ie. ville): Oued Smar

Nom de l'Organisation (ie. entreprise): Certification Authority

Unité Organisationnelle (ie. département): Certification Authority

Longueur de la clé: ☐ 2048 ☐ 1024 ☒ 4096

Empreinte: ☐ RIPEMD-160 ☒ SHA-256 ☐ SHA-384 ☐ ins.MD5 ☐ SHA-512 ☐ SHA-1 ☐ ir

Algorithme: ☒ RSA ☐ DSA



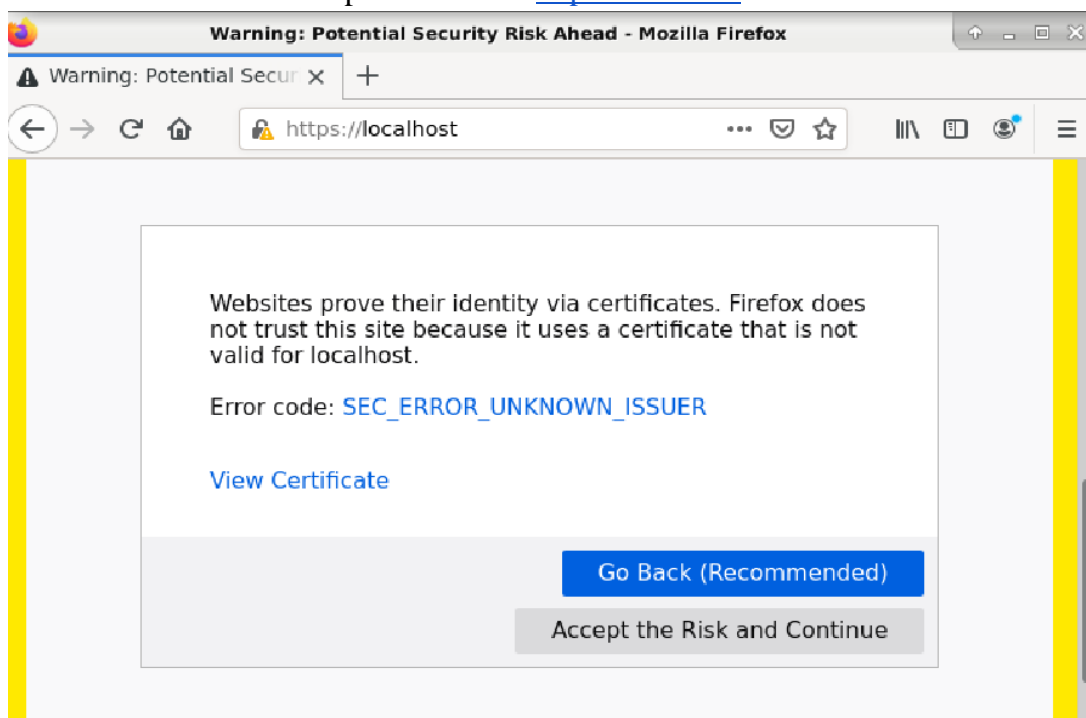
- Modification des fichiers de configuration

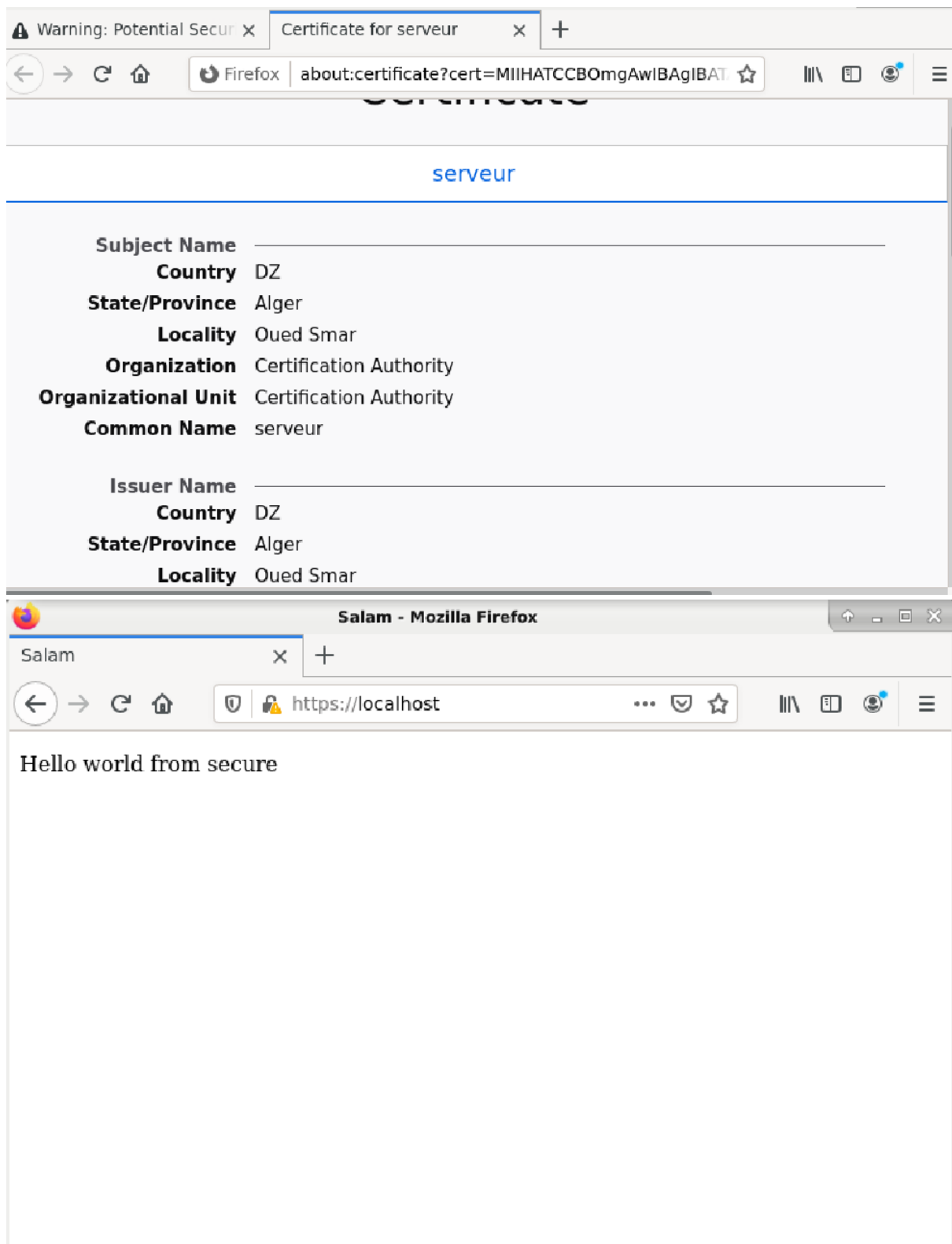
```
#SSLCertificateFile "/opt/lampp/etc/ssl.crt/server.crt"
SSLCertificateFile "/opt/lampp/etc/delta/certifs/serveurcert.pem"

#SSLCertificateKeyFile "/opt/lampp/etc/ssl.key/server.key"
SSLCertificateKeyFile "/opt/lampp/etc/delta/cles/serveurkey.pem"
```

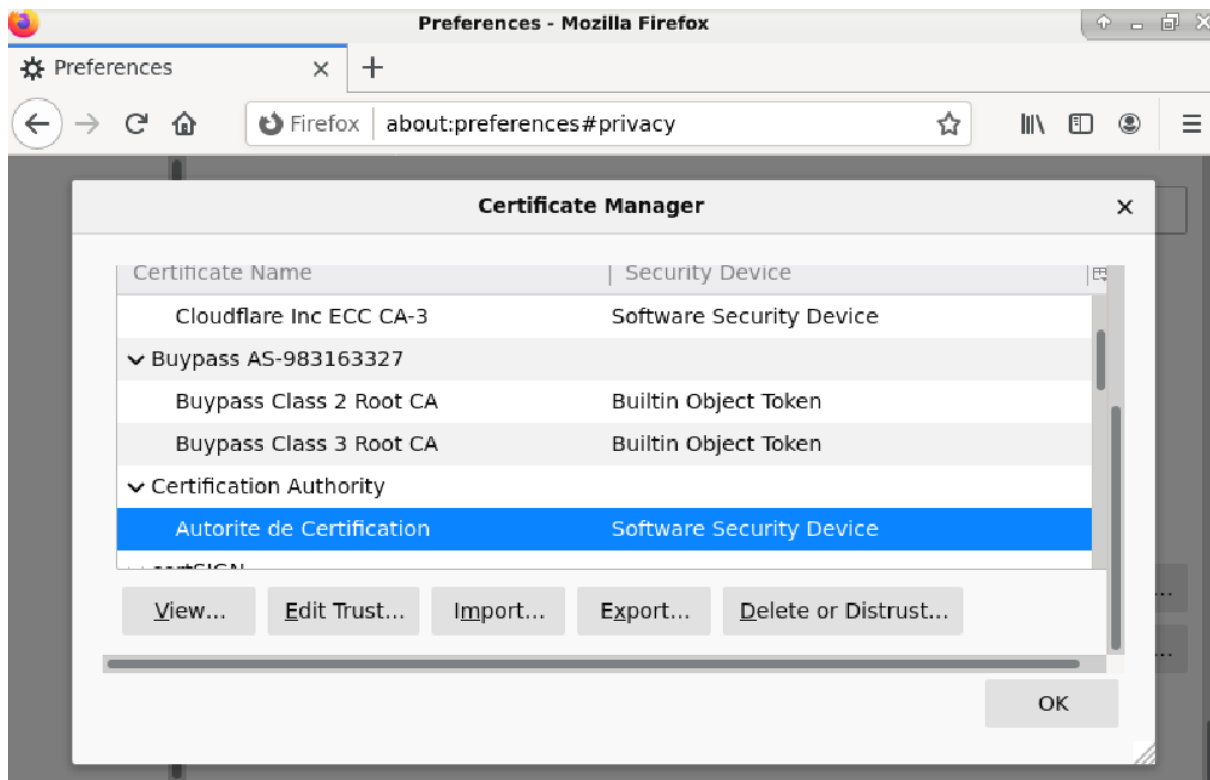
IV. Les Tests :

- Relancer Apache et tester <https://localhost>

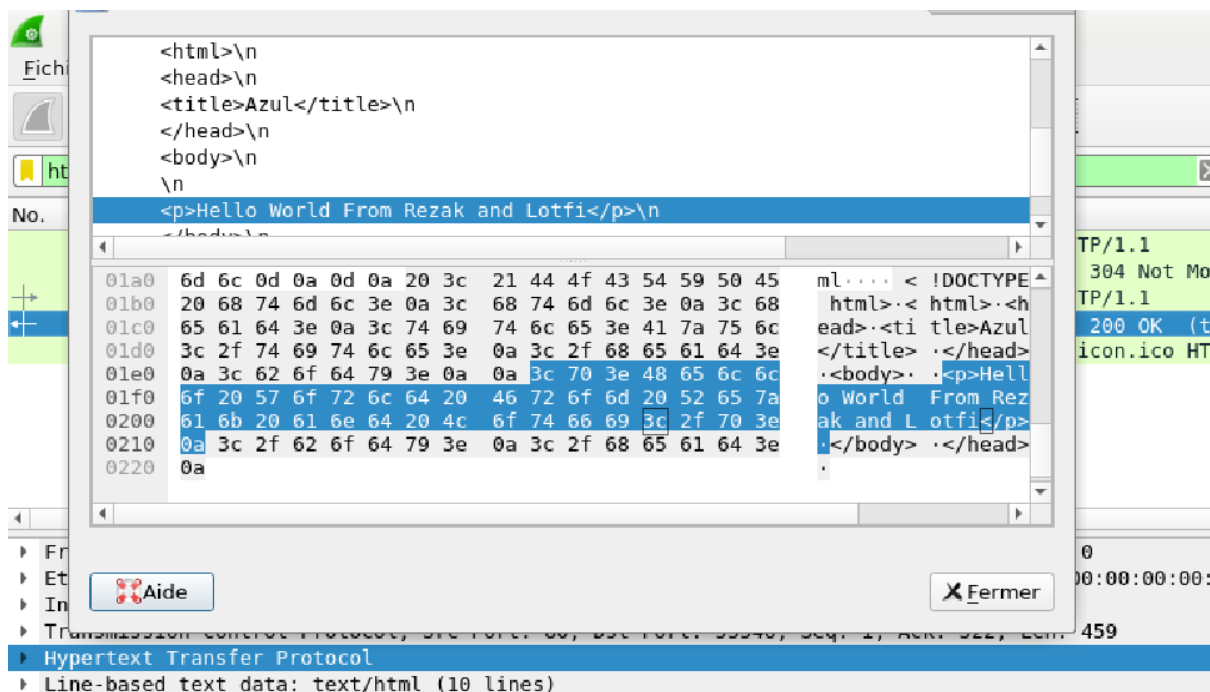




- Exporter le certificat du CA en utilisant tinyca2 et l'inclure dans le navigateur



V. Analyse et comparaison des échanges



Quand on utilise le protocole http pour accéder à notre serveur web, on voit que les communications se passent en clair.

3.007239164	::1	::1	TCP	86 53490 → 443 [ACK] Seq=1 Ack=1 Win=
3.008506501	::1	::1	TLSv1.3	603 Client Hello
3.008561488	::1	::1	TCP	86 443 → 53490 [ACK] Seq=1 Ack=518 Wi
3.017845740	::1	::1	TLSv1.3	2694 Server Hello, Change Cipher Spec,
3.017860309	::1	::1	TCP	74 53488 → 443 [RST] Seq=519 Win=0 Le
3.044202030	::1	::1	TCP	86 53490 → 443 [FIN, ACK] Seq=518 Ack
3.085516288	::1	::1	TCP	86 443 → 53490 [ACK] Seq=1 Ack=519 Wi
3.154180770	::1	::1	TLSv1.3	2694 Server Hello, Change Cipher Spec,
3.154196004	::1	::1	TCP	74 53490 → 443 [RST] Seq=519 Win=0 Le

Cependant dans le cas de https les communications sont chiffrés

VI. Ajouter un certificat Client

- Création d'un certificat client

Tiny CA Management 0.7.5 - AutoriteCA

CA, Preferences, Aide

Créer Requête

Créer une nouvelle requête de certificat

Nom commun (ie. votre Nom, votre adresse eMail ou le Nom du serveur): Client

Adresse eMail:

Mot de passe (protrège votre Clé privée): ●●●●●●●●●●

Password (confirmation): ●●●●●●●●●●

Pays (code sur 2 lettres): DZ

Etat ou Nom de Province: Alger

Localité (ie. ville): El harrach



Nom de l'Organisation (ie. entreprise): ETS LR

Unité Organisationelle (ie. département): Certification Authority

Longueur de la clé: ☐ 2048 ☒ 4096 ☐ 1024

Empreinte: ☐ SHA-1 ☐ ins.MD5 ☒ SHA-256 ☐ SHA-512 ☐ ins.MD4 ☐ RIPEMD-160 ☐ SH

Algorithme: ☒ RSA ☐ DSA

Export de Certificat

Export de Certificat dans un Fichier

Fichier: /opt/lampp/etc/delta/c 

Format d'Export:

☒ PEM (Certificat)

☐ DER (Certificat)

☐ PKCS#12 (Certificat & Clé)

☐ Zip (Certificat & Clé)

☐ Tar (Certificat & Clé)

☐ TXT (Certificat)

Inclure la Clé (PEM)

☐ Oui ☒ Non

Inclure l'empreinte digitale (PEM)

☐ Oui ☒ Non

Export de la Clé

Export de Clé dans un Fichier

Fichier: /opt/lampp/etc/delta/c 

Format d'Export:

☒ PEM (Clé)

☐ DER (Clé sans Mot de passe)

☐ PKCS#12 (Certificat & Clé)

☐ Zip (Certificat & Clé)

☐ Tar (Certificat & Clé)

Sans Mot de passe (PEM/PKCS#12)

☒ Oui ☐ Non

Inclure le Certificat (PEM)

☐ Oui ☒ Non

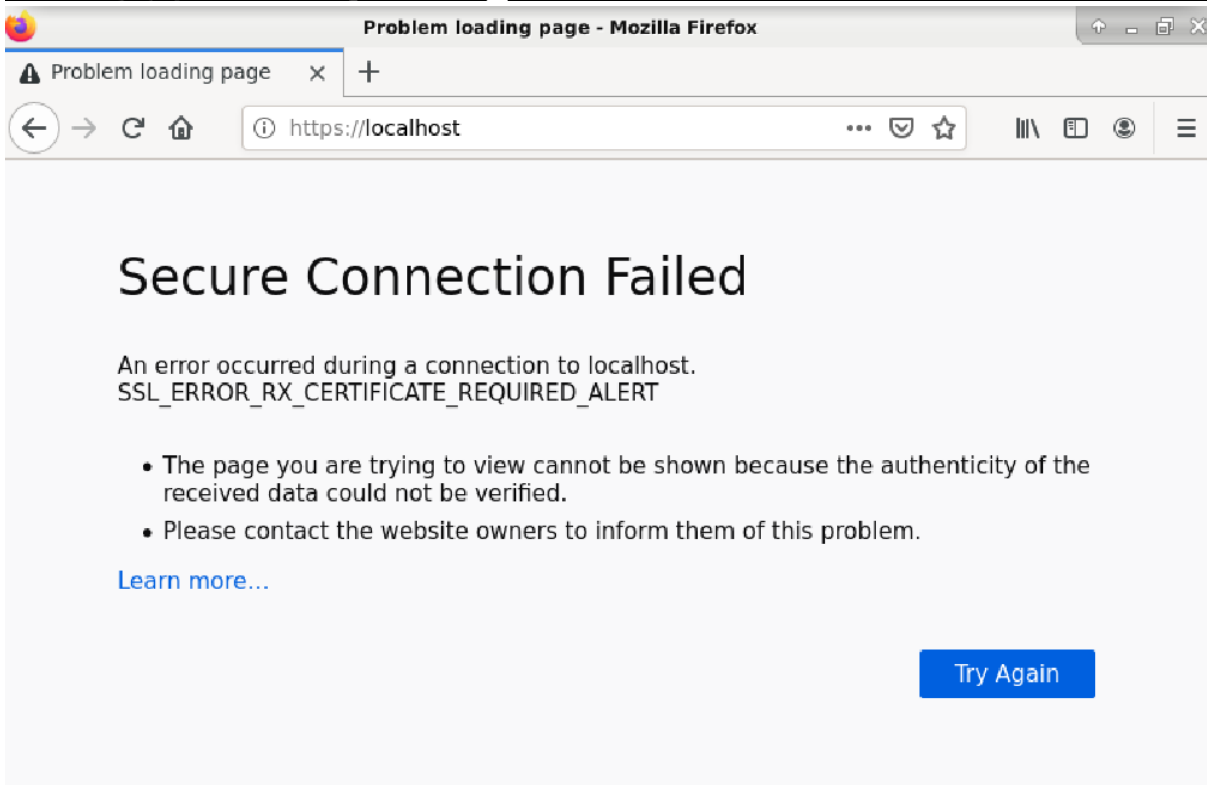
- Modification de Apache

```
#SSLCACertificatePath "/opt/lampp/etc/ssl.crt"
#SSLCACertificateFile "/opt/lampp/etc/ssl.crt/ca-bundle.crt"
SSLCACertificatePath "/opt/lampp/etc/delta/certifs"
SSLCACertificateFile "/opt/lampp/etc/delta/certifs/cacert.pem"

#SSLVerifyClient require
#SSLVerifyDepth 10
SSLVerifyClient require
SSLVerifyDepth 2
```

- Relancer et tester

```
root@debian:/opt/lampp# nano etc/extra/httpd-ssl.conf
root@debian:/opt/lampp# ./lampp restart
Restarting XAMPP for Linux 8.0.3-0...
XAMPP: Stopping Apache...ok.
XAMPP: Stopping MySQL...ok.
XAMPP: Starting Apache...already running.
XAMPP: Starting MySQL...ok.
```



Problem loading page - Mozilla Firefox

Problem loading page x +

← → ↻ 🏠 ⓘ https://localhost ... 📄 🔄 ☰

Secure Connection Failed

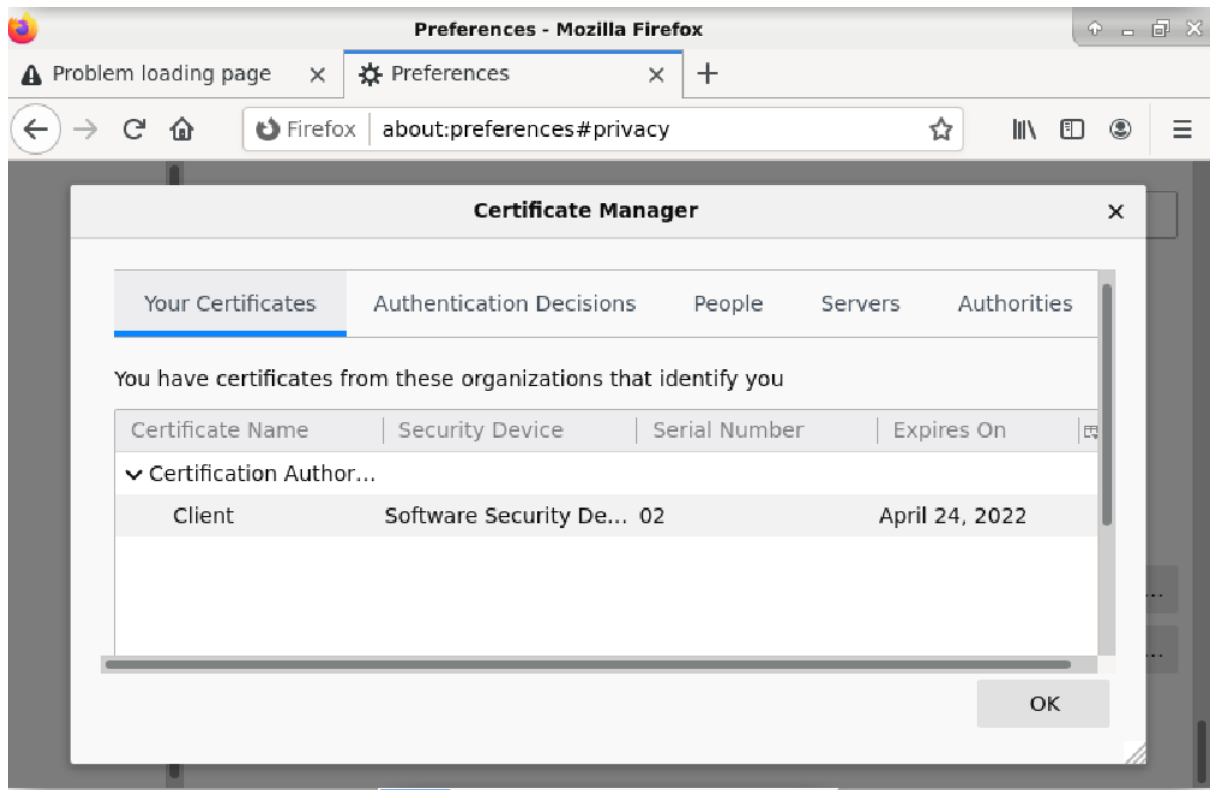
An error occurred during a connection to localhost.
SSL_ERROR_RX_CERTIFICATE_REQUIRED_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

[Learn more...](#)

Try Again

- Ajouter le certificat dans le client



- Relancer apache et tester

