

- ▶ <http://slproweb.com/products/Win32OpenSSL.html>
- ▶ 1 – Se rendre dans le répertoire de d'apache
  - ▶ `cd C:\wamp\bin\apache\Apache2.2.22\bin`
- ▶ 2 - Générer le la clef privé
  - ▶ `openssl genrsa -aes256 -out private.key 2048`
- ▶ 3 – Supprimer la passphrase
  - ▶ `openssl rsa -in private.key -out private.key`
- ▶ 4 - Générer le certificat auto-signé
  - ▶ `openssl req -new -x509 -nodes -sha1 -key private.key -out certificat.crt -days 36500 -config C:\wamp\bin\apache\apache2.2.22\conf\openssl.cnf`
- ▶ 5 – Copier le certificat et la clef privée
  - ▶ `C:\wamp\bin\apache\Apache2.2.22\conf` et créez deux dossiers « cert » et « key ».
- ▶ Copier `certificat.crt` dans le dossier « cert »
- ▶ Copier `private.key` dans le dossier « key »

# Certificat SSL

Secure Socket Layer

# Réalisé par:

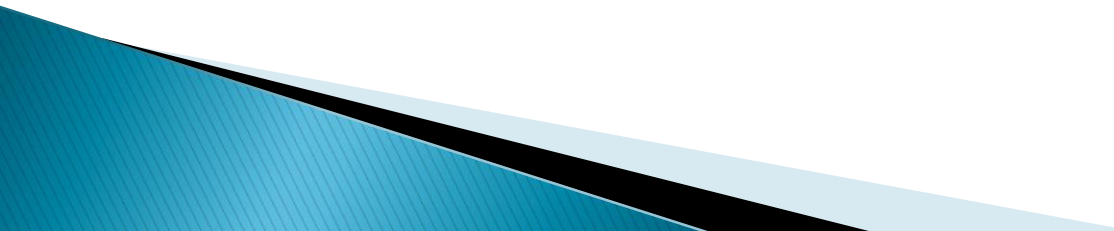
- ▶ SIDAOUI Abdelfahem



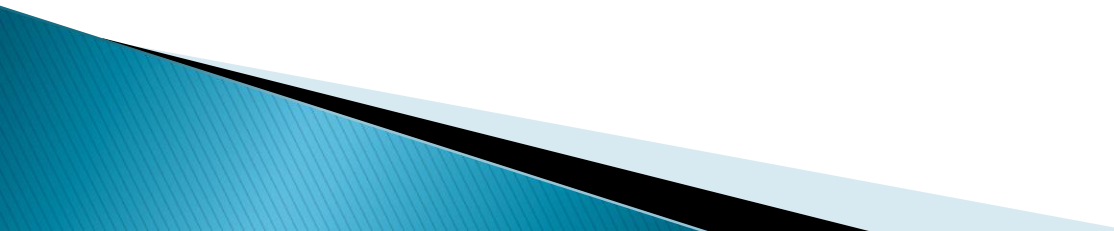
# SSL

- ▶ **SSL (Secure Socket Layer):** c'est un protocole de sécurisation conçu par Netscape qui se situe entre la couche transport (TCP) et les protocoles de la couche application.
- ▶ Il assure les services de sécurité suivantes : confidentialité, l'intégrité et l'authentification du serveur et du client.

# Qu'est-ce qu'une PKI ?

- ▶ PKI (Public Key Infrastructure) est un système de gestion des clefs publiques qui permet de gérer des listes importantes de clefs publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau.
  - ▶ Système permettant aux agents de reconnaître quelle clé publique appartient à qui.
- 

# Services principaux:

- ▶ Une infrastructure PKI fournit donc quatre services principaux:
    - ❖ fabrication de bi-clés.
    - ❖ certification de clé publique et publication de certificats.
    - ❖ Révocation de certificats.
    - ❖ Gestion la fonction de certification.
- 

# Composants d'une PKI :

- ❖ Autorité d'enregistrement (RA).
  - Vérifie l'identité du demandeur de certificat.
- ❖ Autorité de certification (CA).
  - Signe les certificats.
  - Signe les révocations de certificats.
  - Peut être la même que la RA.

# Composants d'une PKI :

- ❖ Autorité de dépôt (Repository) :
  - Maintient les certificats dans un répertoire public de certificats.
  - Maintient une liste de révocation de certificats (CRL) dans le répertoire des certificats.
  
- ❖ Autorité de recouvrement :
  - Protège certaines clés privées pour récupération ultérieure.



# Installer un certificat SSL sous WAMP

- ▶ Installer un certificat SSL sous un serveur  
Wamp est relativement simple et ne prend que quelques minutes, nous allons donc voir ici comment générer un certificat Auto-signé avec OpenSSL et comment l'installer.
- ▶ **NB:** cette manipulation ne pourra remplacer un vrai **certificat acheté** auprès d'une autorité de certification.

# Installer un certificat SSL sous WAMP

- ▶ Une remarque avant de commencer, selon votre version d'**Apache** les chemins vers les différents fichiers/dossiers peuvent changer. Cette documentation a été écrite avec **Apache2.2.22**.
- ▶ Les premières étapes sont des commandes DOS, la première chose est donc d'ouvrir une invite de commande (Démarrer -> Exécuter -> cmd -> OK).

# Installer un certificat SSL sous WAMP

## 1 – Se rendre dans le répertoire d'apache

✓ `cd C:\wamp\bin\apache\Apache2.2.22\bin`

## 2 – Générer le la clef privé

On va commencer par générer la clé privée, elle se trouvera dans le fichier « `private.key` » ici le chiffage est de 2048bits.

✓ `openssl genrsa -aes256 -out private.key 2048`

# Installer un certificat SSL sous WAMP

- Si vous rencontrez l'erreur « L'ordinal 296 .... SSLEAY32.dll » :



# Installer un certificat SSL sous WAMP

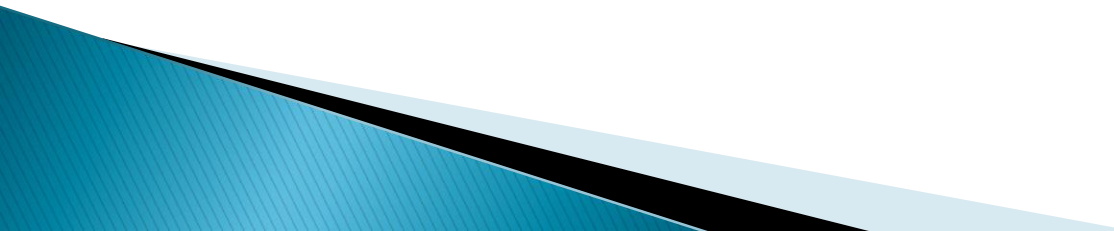
La solution est de se rendre sur cette page :

<http://slproweb.com/products/Win32OpenSSL.html> et de télécharger **Win32 OpenSSL**

**v1.0.0m Light** une fois installé il faut se déplacer dans le répertoire/sous-répertoires d'installation afin de copier les fichiers suivants :

- \* ssleay32.dll
- \* libeay32.dll
- \* openssl.exe

# Installer un certificat SSL sous WAMP

- ✓ Pour les coller dans le dossier  
C:\wamp\bin\apache\Apache2.2.22\bin (en confirmant les remplacements).
  - ✓ Le problème devrait alors être corrigé et la commande précédente s'exécuter correctement.
- 

# Installer un certificat SSL sous WAMP

## 3 – Supprimer la passphrase

On va libérer la clé privée de la « passphrase » qui la protège.

✓ `openssl rsa -in private.key -out private.key`

## 4 – Générer le certificat auto-signé

Nous allons ici générer le certificat auto-signé qui servira à certifier la connexion et à en chiffrer les échanges.

# Installer un certificat SSL sous WAMP

Ici le certificat sera valide 100 ans, remplacez donc 36500 par le nombre de jours de validité du certificat. Ensuite l'invite de commande vous demandera quelques informations libres à vous de les saisir. Notre certificat portera le nom : « certificat.crt »

✓ `openssl req -new -x509 -nodes -sha1 -key private.key -out certificat.crt -days 36500 -Config C:\wamp\bin\apache\apache2.2.22\conf\openssl.cnf`



# Installer un certificat SSL sous WAMP

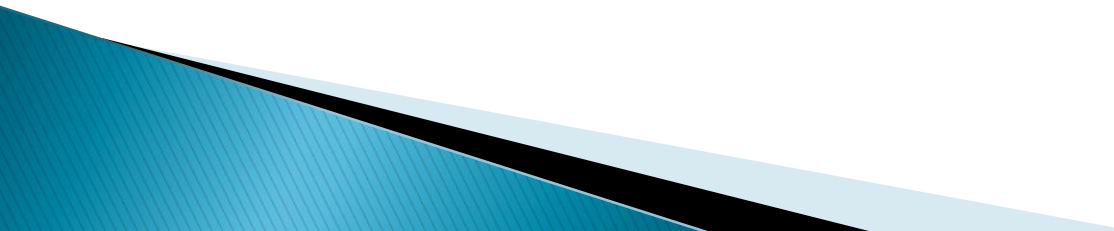
## 5 – Copier le certificat et la clef privée

- ▶ Maintenant que notre certificat et notre clef privée sont générés il nous faut les stocker sur le serveur. Pour ce faire rendez-vous dans le dossier `C:\wamp\bin\apache\Apache2.2.22\ conf`, et créez deux dossiers « cert » et « key ».
- ✓ Copier `certificat.crt` dans le dossier « cert »
- ✓ Copier `private.key` dans le dossier « key »

# Installer un certificat SSL sous WAMP

## 6 – Édition des fichiers de configurations

Afin d'installer notre certificat, nous devons éditer trois fichiers de configuration, les deux premiers permettront d'activer **SSL** pour **Apache** et **PHP** et le troisième permettra d'installer le certificat sur le serveur.



# Installer un certificat SSL sous WAMP

Editer C:\wamp\bin\apache\Apache2.2.22\conf\httpd.conf

Dé-commenter les lignes (enlever le « # ») suivantes :

- ✓ LoadModule ssl\_module modules/mod\_ssl.so  
et
- ✓ Include conf/extra/httpd-ssl.conf

# Installer un certificat SSL sous WAMP

Editer C:\wamp\bin\php\php5.3.8\php.ini

Dé-commenter la ligne (enlever le « ; »)  
suivante :

✓ extension=php\_openssl.dll

# Installer un certificat SSL sous WAMP

Editer C:\wamp\bin\apache\Apache2.2.22\conf\extra\httpd-ssl.conf

Rechercher ligne: <VirtualHost\_default\_:443>

- ✓ Remplacer la ligne « DocumentRoot ... » par :  
DocumentRoot "c:/wamp/www/"
- ✓ Remplacer la ligne « ServerName ... » par :  
ServerName localhost:443

# Installer un certificat SSL sous WAMP

- ✓ Remplacer la ligne « ErrorLog ... » par :  
ErrorLog  
"c:/wamp/bin/apache/Apache2.2.22/logs/ssl\_error.log«
- ✓ Remplacer la ligne « TransferLog ... » par :  
TransferLog  
"c:/wamp/bin/apache/Apache2.2.22/logs/ssl\_access.log"

# Installer un certificat SSL sous WAMP

- ✓ Remplacer la ligne « SSLCertificateFile ... » par  
SSLCertificateFile  
"c:/wamp/bin/apache/Apache2.2.22/conf/cert/certificat.crt "
- ✓ Remplacer la ligne « SSLCertificateKeyFile ... »  
par : SSLCertificateKeyFile  
"c:/wamp/bin/apache/Apache2.2.22/conf/key/private.key"

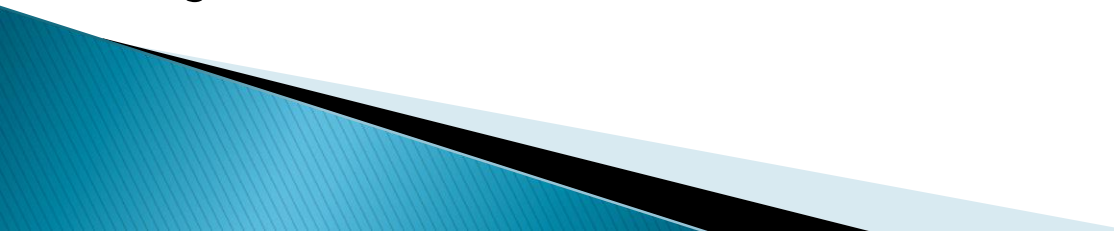
# Installer un certificat SSL sous WAMP

- ✓ Remplacer la ligne « <Directory ...> » par :  
`<Directory "c:/wamp/www/">`
- ✓ Remplacer la ligne « CustomLog ... » par :  
`CustomLog`  
`"C:/wamp/bin/apache/Apache2.2.22/logs/ss`  
`l_request.log" \`

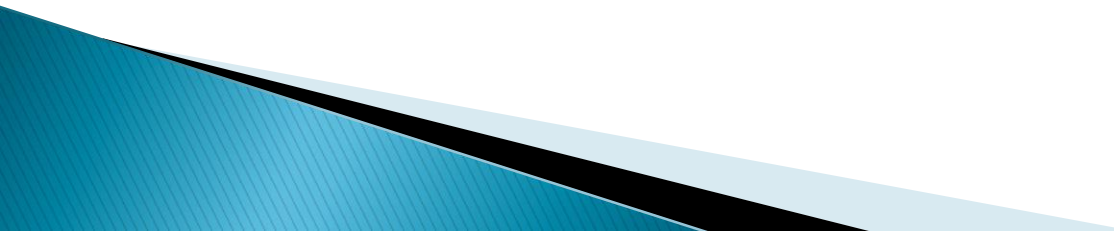


# Installer un certificat SSL sous WAMP

Voici quelques explication concernant les paramètres que l'on viens de modifier :

- ▶ **DocumentRoot** : définit le dossier racine du serveur
  - ▶ **ServerName** : définit le nom du serveur et son port d'écoute (443 étant le port SSL par défaut)
  - ▶ **ErrorLog** : définit l'emplacement du journal d'erreur
  - ▶ **TransferLog** : définit l'emplacement du journal des accès
- 

# Installer un certificat SSL sous WAMP

- ▶ **SSLCertificateFile** : définit l'emplacement du certificat
  - ▶ **SSLCertificateKeyFile** : définit l'emplacement de la clef privée
  - ▶ **<Directory ...>** : définit les propriétés sur dossier racine
  - ▶ **CustomLog** : définit l'emplacement du journal des requêtes
- 

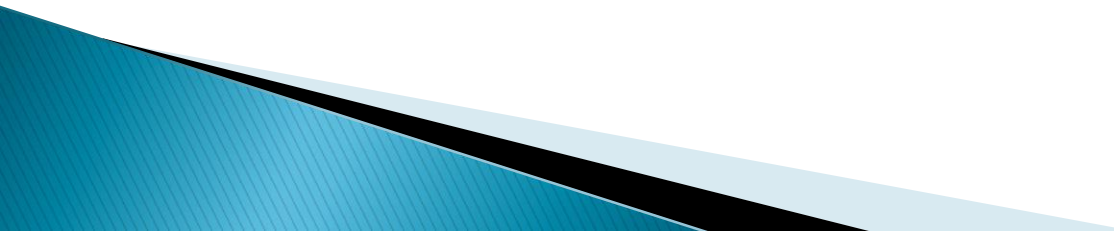
# Installer un certificat SSL sous WAMP

## 7 – Vérifier la configuration

Dans une invite de commande tapez la commande suivante:

✓ `httpd -t`

Ce dernier doit retourner « Syntax OK », si tel n'est pas le cas, il doit y avoir une erreur dans le fichier « `httpd-ssl.conf` », il faut donc retourner à l'étape précédente et vérifier la configuration.

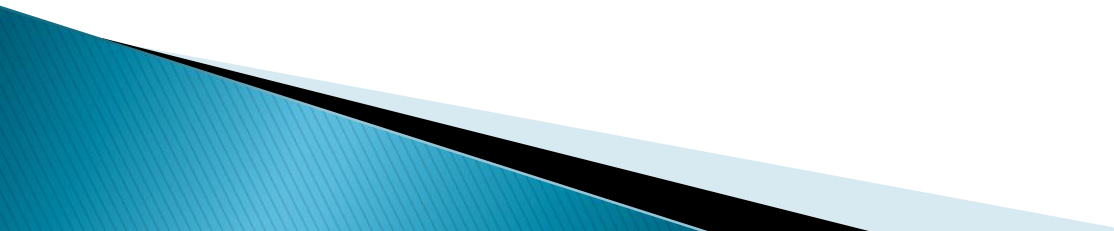


# Installer un certificat SSL sous WAMP

8 – Redémarrer Wamp

9 – L'accès à <https://localhost/> doit être possible

Le message suivant nous indique que la connexion n'est pas certifiée, il faut accepter les risques, c'est normal puisque notre certificat est auto-signé. Cette erreur n'apparaîtrait pas si le certificat aurait été acheté auprès d'une autorité de certification.



# Installer un certificat SSL sous WAMP



Voilà, le certificat est installé avec succès.

***Merci***  
***pour votre attention***

