

I. Généralités

Un certificat auto-signé (self-signed certificate) est un type de certificat numérique qui est signé par la même entité par laquelle il est émis. En d'autres termes, l'émetteur et sujet sont identiques. Contrairement à un certificat signé par une autorité de certification, qui est une entité de confiance tierce, un certificat auto-signé ne dispose pas de cette vérification par un tiers. Un certificat auto signé est souvent utilisé pour les environnements de développement, des tests internes ou des applications privées où la confiance externe n'est pas requise. Comme ils ne sont pas signés par une autorité de certification reconnue, les navigateurs et autres systèmes de validation de certificats ne leur font pas automatiquement confiance.

Dans une architecture client-serveur, les certificats auto-signés ont des usages spécifiques, principalement dans des environnements de développement ou pour des systèmes internes où la sécurité et la confiance peuvent être gérées localement.

Lorsque le serveur et le client sont sur la même machine, la configuration est généralement plus simple car il n'y a pas besoin de gérer la distribution des certificats à plusieurs machines. Le client doit être configuré pour accepter le certificat auto-signé. Notons que les clés privées et les certificats sur la machine pour éviter toute compromission locale.

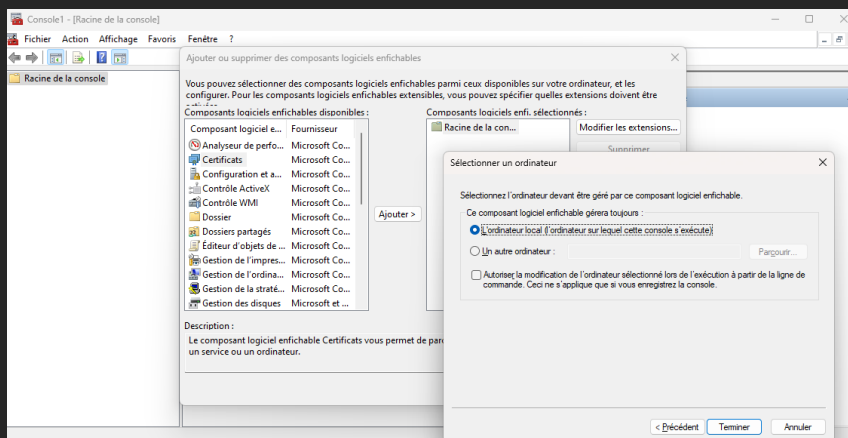
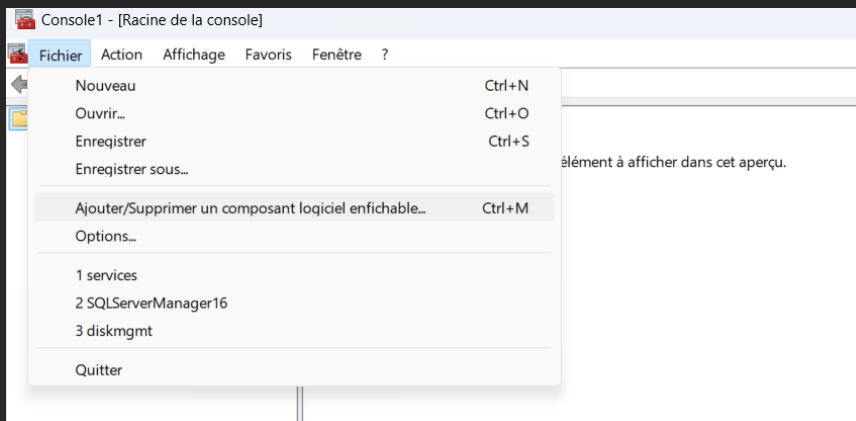
Lorsque le serveur et le client sont sur des machines différentes, le certificat auto-signé doit être distribué à toutes les machines clientes. Cela implique un processus manuel ou automatisé pour ajouter le certificat au magasin de certificats de confiance de chaque client. Chaque client doit être configuré pour faire confiance au certificat auto-signé à l'aide de processus spécifiques pour importer des certificats dans des magasins de certificats de confiance. Par ailleurs, La sécurité devient plus complexe car les communications passent par des réseaux externes. Il est crucial de protéger les clés privées et de s'assurer que le certificat n'est pas compromis pendant le transfert.

II. Génération d'un certificat auto signé

1. Vérification de l'existence d'un certificat auto-signé

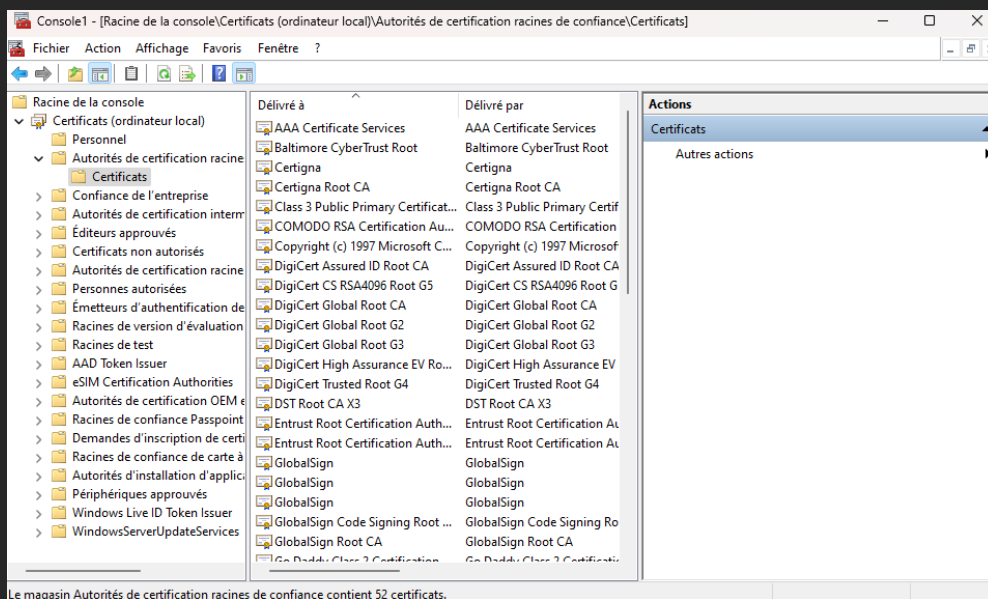
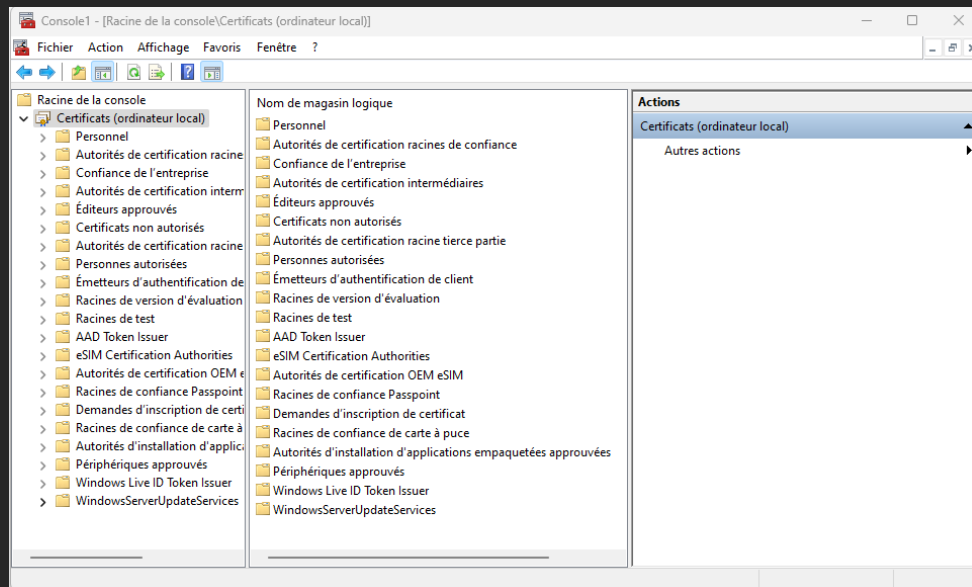
- a. Tapez **Win + R** pour ouvrir la boîte de dialogue *Exécuter*

- Tapez *mmc* et appuyer sur *Entrée*
- Cliquez sur *Fichier*, puis sur *Ajouter/Supprimer un composant logiciel enfichable*
- Sélectionnez *Certificats*, puis *Ajouter*
- Sélectionnez *Compte d'ordinateur*, puis *Ordinateur local*



- La vérification des certificats auto-signés se fait en développant *Certificats (Ordinateur local)*, puis en sélectionnant *Personnel*, puis *Certificats*.
- Il est aussi possible de vérifier également dans *Autorités de certification racines de confiance*, puis *Certificats*, pour voir si un certificat auto-signé est enregistré là.

Certificat auto signé – Self-Signed Certificate



2. Génération d'un Certificat auto-signé avec PowerShell

- Tapez sur **Win + X**, puis sélectionnez **Windows PowerShell (Admin)** ou **Windows Terminal (Admin)**.
- Générez le Certificat Auto-signé

Ligne de commandes

```
New-SelfSignedCertificate -DnsName "ServerName" -CertStoreLocation  
"cert:\LocalMachine\My" -KeyLength 2048 -NotAfter (Get-Date).AddYears(1) -  
FriendlyName "My Self-Signed Certificate"
```

c. Exporter le Certificat et la Clé Privée (optionnel) PFX format :

Ligne de commandes

```
$cert = Get-ChildItem -Path cert:\LocalMachine\My | Where-Object { $_.Subject -like "*ServerName*" }

$password = ConvertTo-SecureString "YourPassword" -Force -AsPlainText

Export-PfxCertificate -Cert $cert -FilePath "C:\Path\To\YourCert.pfx" -Password $password
```

3. Génération d'un Certificat auto-signé avec OpenSSL

3.1. Installation d'OpenSSL

Télécharger & installer le full paquet sur le site suivant :

- Lien : <https://slproweb.com/products/Win32OpenSSL.html>
- Ouvrir un terminal et se placer le répertoire **bin** du dossier d'installation : *C:\Program Files\OpenSSL-Win64\bin*
- En cas de problème, ajouter dans les *variables d'environnements* du système le chemin d'accès vers le fichier de configuration

Win32/Win64 OpenSSL Screenshot

Download Win32/Win64 OpenSSL

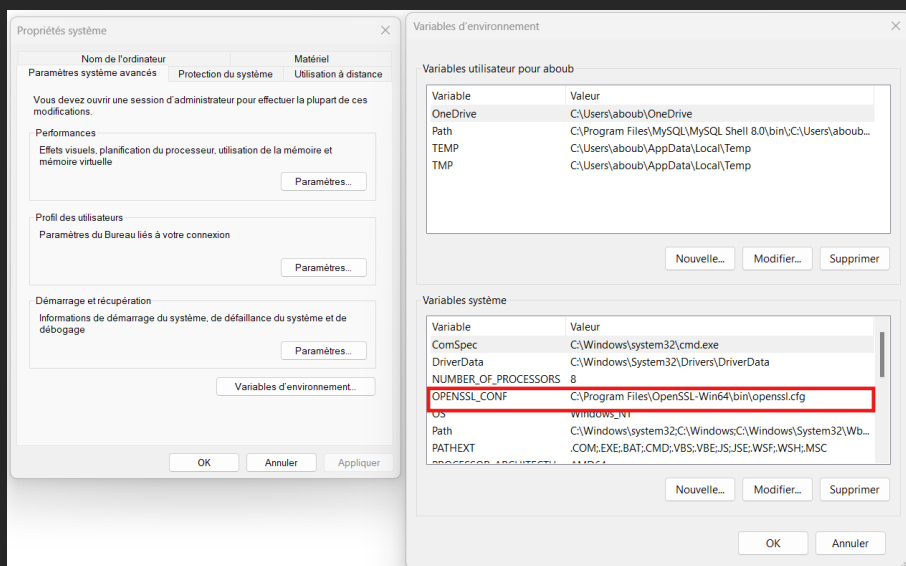
Download Win32/Win64 OpenSSL today using the links below!

File	Type	Description
Win64 OpenSSL v3.2.1 Light EXE MSI	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.2.1 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.3.1 EXE MSI	217MB Installer	Installs Win64 OpenSSL v3.3.1 (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.2.1 Light EXE MSI	4MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v3.2.1 (Only install this if you need 32-bit OpenSSL for Windows). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.3.1 EXE MSI	175MB Installer	Installs Win32 OpenSSL v3.3.1 (Only install this if you need 32-bit OpenSSL for Windows). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.3.1 Light for ARM (EXPERIMENTAL) EXE MSI	6MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.3.1 for ARM64 devices (Only install this VERY EXPERIMENTAL build if you want to try 64-bit OpenSSL for Windows on ARM processors). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.3.1 for ARM (EXPERIMENTAL) EXE MSI	170MB Installer	Installs Win64 OpenSSL v3.3.1 for ARM64 devices (Only install this VERY EXPERIMENTAL build if you want to try 64-bit OpenSSL for Windows on ARM processors). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.2.2 Light EXE MSI	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.2.2 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.2.2 EXE MSI	202MB Installer	Installs Win64 OpenSSL v3.2.2 (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.2.2 Light EXE MSI	4MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v3.2.2 (Only install this if you need 32-bit OpenSSL for Windows). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

```
Administrateur : Windows Poi x + - □ x
PS C:\Program Files\OpenSSL-Win64\bin> .\openssl.exe version
OpenSSL 3.3.1 4 Jun 2024 (Library: OpenSSL 3.3.1 4 Jun 2024)
PS C:\Program Files\OpenSSL-Win64\bin>
```

```
Administrateur : Windows Po...
PS C:\Program Files\OpenSSL-Win64\bin> .\openssl.exe version
OpenSSL 3.3.1 4 Jun 2024 (Library: OpenSSL 3.3.1 4 Jun 2024)
PS C:\Program Files\OpenSSL-Win64\bin> .\openssl.exe
help:

Standard commands
asn1parse          ca                ciphers           cmp
cms                crl              crl2pkcs7         dgst
dhparam            dsa             dsaparam          ec
ecparam            enc             engine            errstr
fipsinstall        gendsa          genpkey           genrsa
help              info            kdf               list
mac               nseq            ocs               passwd
pkcs12             pkcs7           pkcs8             pkey
pkeyparam          req             prime             rand
rehash            s_server        rsa               rsautl
s_client           speed           s_time            sess_id
smime             storeutl        spkac             srp
x509              ts              verify            version
```



3.2. Génération d'une clé privée

Commande à exécuter

Ligne de commandes

```
openssl.exe genrsa -out myprivate.key 2048
```

3.3. Création d'un CSR (Certificate Signing Request)

Création d'un certificat auto signé avec la clé privée tout juste créée :

Ligne de commandes

```
openssl.exe req -new -key myprivate.key -out myrequest.csr
```

3.4. Génération d'un certificat auto-signé et vérification du certificat

- Création d'un certificat

Ligne de commandes

```
openssl.exe x509 -req -days 365 -in myrequest.csr -signkey myprivate.key -out mycertificate.crt
```

- Vérification du certificat

Ligne de commandes

```
openssl.exe x509 -text -noout -in mycertificate.crt
```

```
sh Copier le code

# Generate private key
openssl genrsa -out myprivate.key 2048

# Create CSR
openssl req -new -key myprivate.key -out myrequest.csr

# Generate self-signed certificate
openssl x509 -req -days 365 -in myrequest.csr -signkey myprivate.key -out mycertificate.crt

# Verify certificate
openssl x509 -text -noout -in mycertificate.crt
```

Convertir au format PFX (optionnel)

Ligne de commandes

```
openssl.exe pkcs12 -export -out mycertificate.pfx -inkey myprivate.key -in mycertificate.crt
```

4. ISS

A faire

III. Exemple d'utilisation : SQL Server

SQL Server Management Studio est l'outil de gestion graphique de SQL Server qui permet de réaliser des tâches administratives et toutes les opérations de développement.

Il est possible de démarrer le serveur SQL Server en tant qu'application à l'aide de l'exécutable sqlservr.exe.

