

ADCS - Signer les certificats



Difficulté : Intermédiaire

Notions : CA, certificats, sécurité, https

I. Introduction

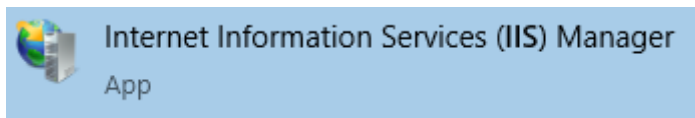
Cette procédure a pour but d'expliquer le processus de certification à travers la CA d'entreprise.

II. Créer une requête

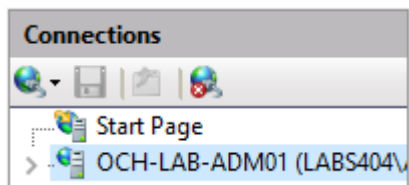
2.1 Déprécié - à travers IIS

Déprécié : Depuis 2022, il faut impérativement faire figurer en plus du CNAME, les attributs 'Alternates names'. Ce que le format utilisé par l'assistant IIS ne fait pas.

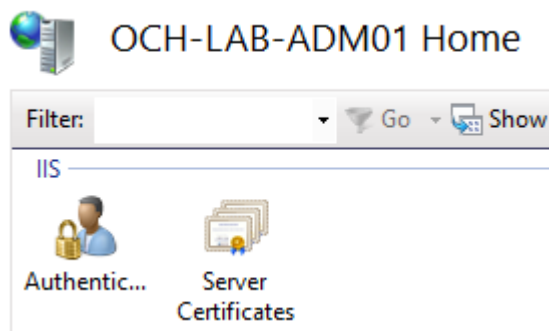
Ouvrir la console IIS :



Sélectionner le serveur

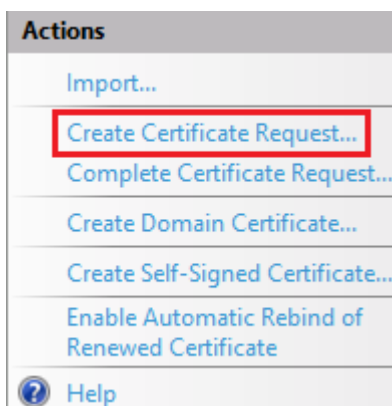


Double cliquer sur '*certificates*'



4Méthode 1 : générer un CSR

Cliquer sur '*Create certificate Request...*'



Dans la fenêtre suivante, entrer les attributs désirés et faire '**Next**'.

Request Certificate



Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	remoteapp01.labs404.fr
Organization:	LABS404
Organizational unit:	IT Dept.
City/locality	Saint Christophe sur Guiers
State/province:	Rhone-Alpes
Country/region:	FR

Previous

Next

Finish

Cancel

Choisir le Provider et la longueur de la clé (conseillé '**2048**') et faire '**Next**'.

Request Certificate ? X

 **Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Microsoft RSA SChannel Cryptographic Provider ▼

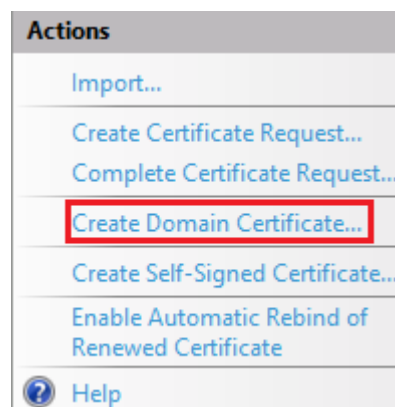
Bit length:

2048 ▼

Previous Next Finish Cancel

Choisir le chemin vers lequel exporter le .csr et faire '**Finish**'.

Sélectionner '**Create Domain Certificate...**'.



Dans la fenêtre suivante, entrer les attributs désirés et faire '**Next**'.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	remoteapp01.labs404.fr
Organization:	LABS404
Organizational unit:	IT Dept.
City/locality	Saint Christophe sur Guiers
State/province:	Rhone-Alpes
Country/region:	FR

Previous Next Finish Cancel

Sélectionner la CA qui devra signer le certificat, Entrer un nom pour le certificat et faire '*Finish*'.

Select Certification Authority

Select a certificate authority you want to use:

Certificate Authority	Computer
labs404-OCH-LAB-ADCS01-CA	och-lab-adcs01.labs404.fr
labs404-OCH-LAB-ADCS01-CA-1	och-lab-adcs01.labs404.fr

Create Certificate

 **Online Certification Authority**

Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.

Specify Online Certification Authority:

labs404-OCH-LAB-ADCS01-CA-1\och-lab-adcs01.labs404.fr

Select...

Example: CertificateAuthorityName\ServerName

Friendly name:

och-lab-rds01_2023_Cert

Previous

Next

Finish

Cancel

L'avantage de cette seconde methode est que le certificat est directement généré et installé sur le serveur.

Tout est automatisé.



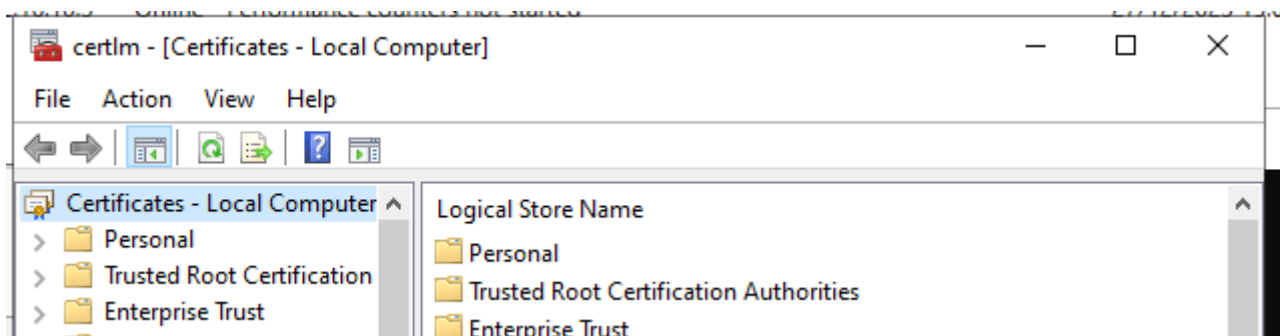
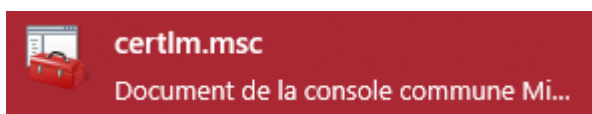
Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

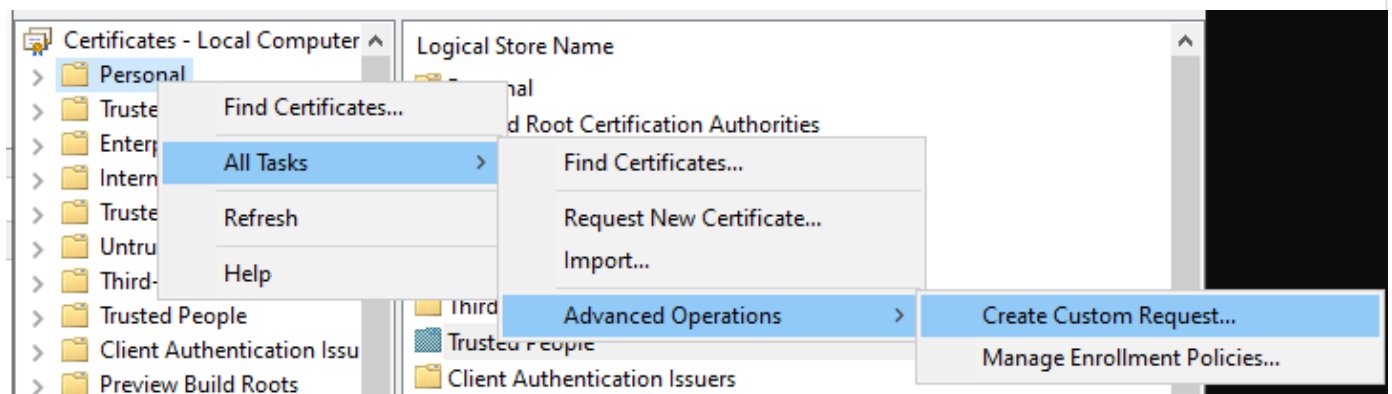
Filter:	Go	Show All	Group by:	No Grouping
Name	Issued To	Issued By	Expiration Date	Certificate Hash
och-lab-adm01.labs404.fr	och-lab-adm01.labs404.fr	labs404-OCH-LAB-ADCS01-C...	19/12/2025 21:57:26	933EDD37B45E0B78D32F
och-lab-adm01.labs404.fr	och-lab-adm01.labs404.fr	labs404-OCH-LAB-ADCS01-C...	19/12/2025 22:14:33	27C7BFBAC8CAAB5362f
och-lab-rds01_2023_Cert	remoteapp01.labs404.fr	labs404-OCH-LAB-ADCS01-C...	26/12/2025 15:44:25	5D0168AD43E4AA4F764!

2.2 à travers le gestionnaire de certificats windows

Lancer le gestionnaire de certificats en recherchant '**certlm.msc**'



Sur '**Personal**', faire clic droit puis '**All Tasks --> Advanced Operations --> Create Custom Request**'



Sur le premier écran, faire '**Next**'.

 Certificate Enrollment

Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network

You have credentials that can be used to verify your right to obtain the certificate

Next

Cancel

Si disponible, Choisir '**Active Directory Enrollment Policy**' sinon continuer sans et faire '**Next**'.

 Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator	
Active Directory Enrollment Policy	▼
Configured by you	
Add New	
Custom Request	
Proceed without enrollment policy	

Next

Cancel

Choisir le template '**Web Server**' ou celui qui sera nécessaire, faire '**Next**'.

Certificate Enrollment

Custom request

Choose an option from the list below and configure the certificate options as required.

Template: Web Server 

☐ Suppress default extensions

Request format: ☒ PKCS #10
☐ CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Next

Cancel

Déplier le template et cliquer sur '*Properties*'.

Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

Active Directory Enrollment Policy

☒ Web Server

i **STATUS:** Available

Details ^

The following options describe the uses and validity period that apply to this type of certificate:

Key usage:

Digital signature
 Key encipherment

Application policies: Server Authentication

Validity period (days): 730

Properties

Next

Cancel

Dans l'onglet '**General**', remplir le Nom du certificat.

Certificate Properties

General Subject Extensions Private Key

A friendly name and description will make it easier to identify and use a certificate.

Friendly name:

och-lab-adm01.labs404.fr

Description:

Dans l'onglet '**Subject**', renseigner toutes les informations nécessaires ainsi que **TOUS** les **Alternative name** nécessaires.

Choisir le type **DNS**.

Certificate Properties

General Subject Extensions Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type:
Organization unit

Add >

< Remove

Value:

CN= och-lab-adm01.labs404.fr
C=FR
L=SCSG
O=labs404
S=Rhone-Alpes
OU=IT Dept

Alternative name:

Type:
DNS

Add >

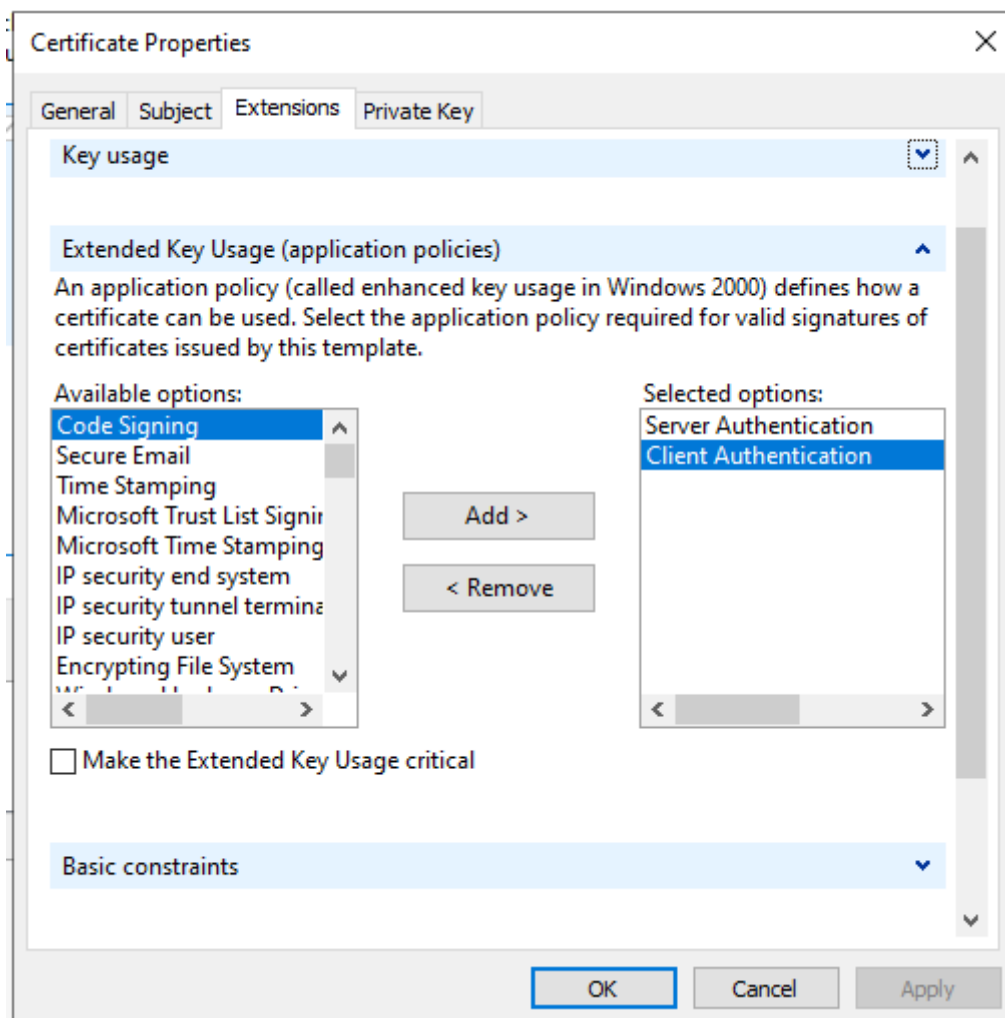
< Remove

Value:

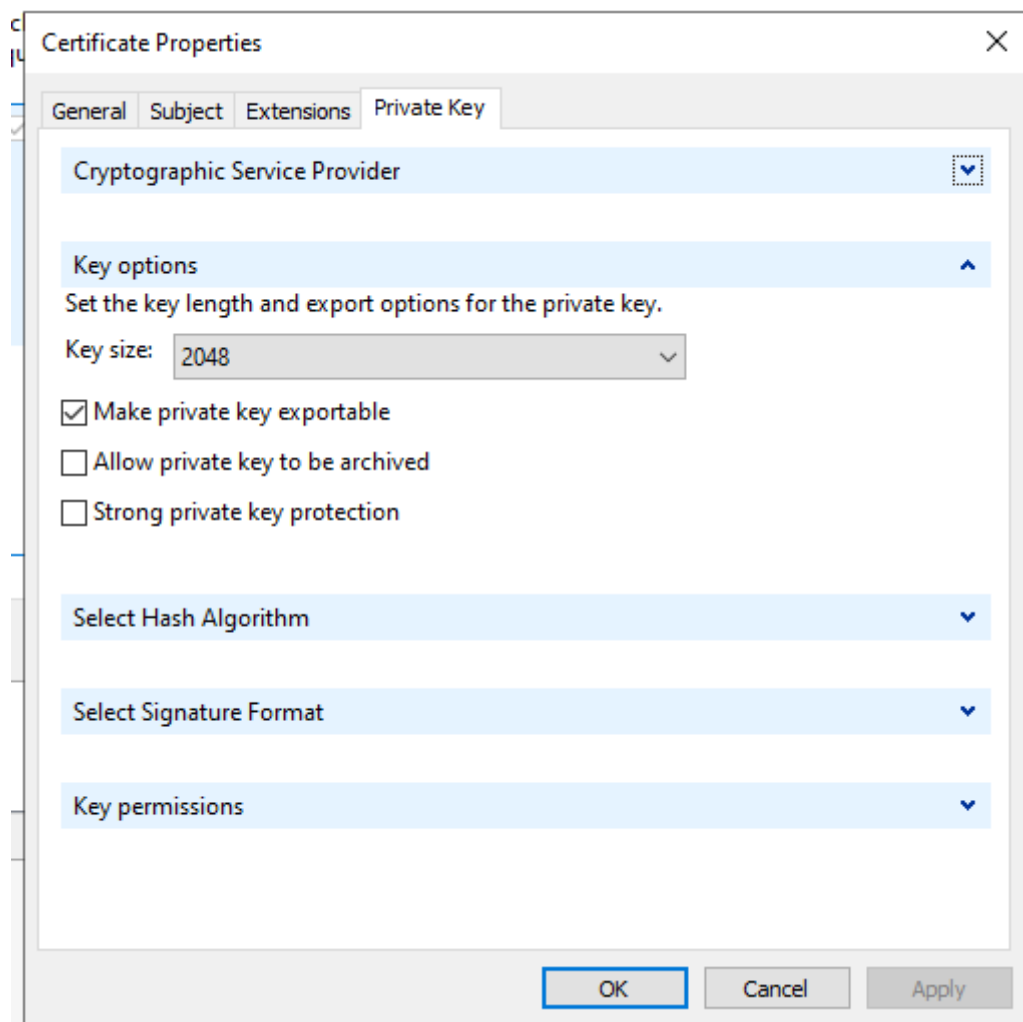
DNS
och-lab-adm01.labs404.fr

OK Cancel Apply

Dans l'onglet '**extensions**', déplier, '**Extended Key Usage**' et ajouter '**Server Authentication**' et '**Client Authentication**'



Enfin, dans l'onglet '**Private Key**', marquer la clé comme exportable.



Cela permettra, une fois le certificat installé, d'exporter le package en tant que .pfx

2.3 en powershell

Utiliser la commande suivante :

```
certreq -?
```

Selon le scenario, les arguments changeront.

III. Valider la requête en web

Prérequis : Pour pouvoir signer les certificats en web, il faut que le composant web de la CA soit installé.

Se connecter à la CA : normalement ***http(s)://<fqdn.de.la.ca>/certsrv***

Entrer ses identifiants.

Sign in to access this site

Authorization required by http://och-lab-adcs01
Your connection to this site is not secure

Username

Password

Choisir '***Request a certificate***'.

Microsoft Active Directory Certificate Services — labs404-0CH-LAB-ADCS01-CA-1Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Puis '***advanced certificate request***',

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

Ensuite,

1. Coller le contenu du CSR, Incluant les lignes BEGIN et END
2. Sélectionner le type de certificat voulu
3. Cliquer sur '**submit**'

Microsoft Active Directory Certificate Services – labs404-OCH-LAB-ADCS01-CA-1

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

IWz7Igi64vHps7v+ZW/UvH819pvhRuT8cjDgRHxPfZh12gaKBv6i1Y8NHfheHC8xQh3YhNOT9y6BhvoRvtZ7A=-----END CERTIFICATE REQUEST-----

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

Après un peu d'attente, si le compte était un compte habilité, la réponse reviens.

Attention : Sinon, il faudra aller signer la demande dans le gestionnaire de la CA.

Choisir le format et cliquer sur '**Download Certificate**'

Microsoft Active Directory Certificate Services – labs404-OCH-LAB-ADCS01-CA-1

Certificate Issued

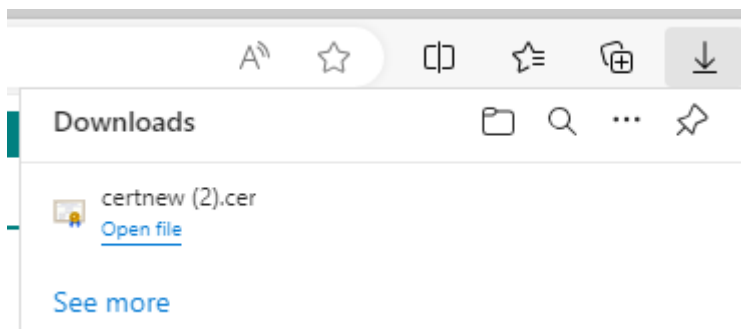
The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

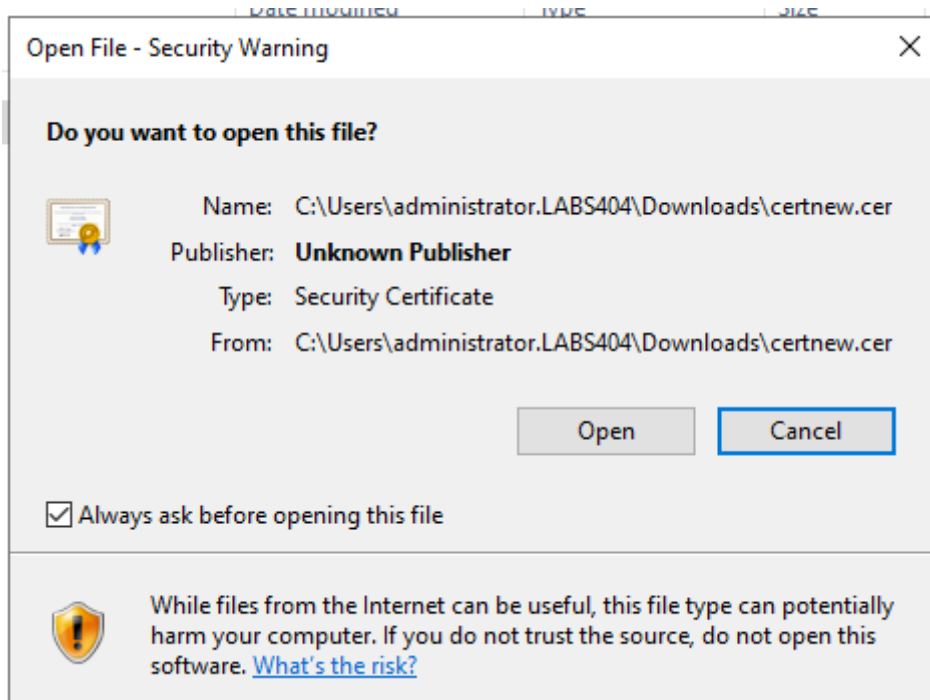
[Download certificate chain](#)



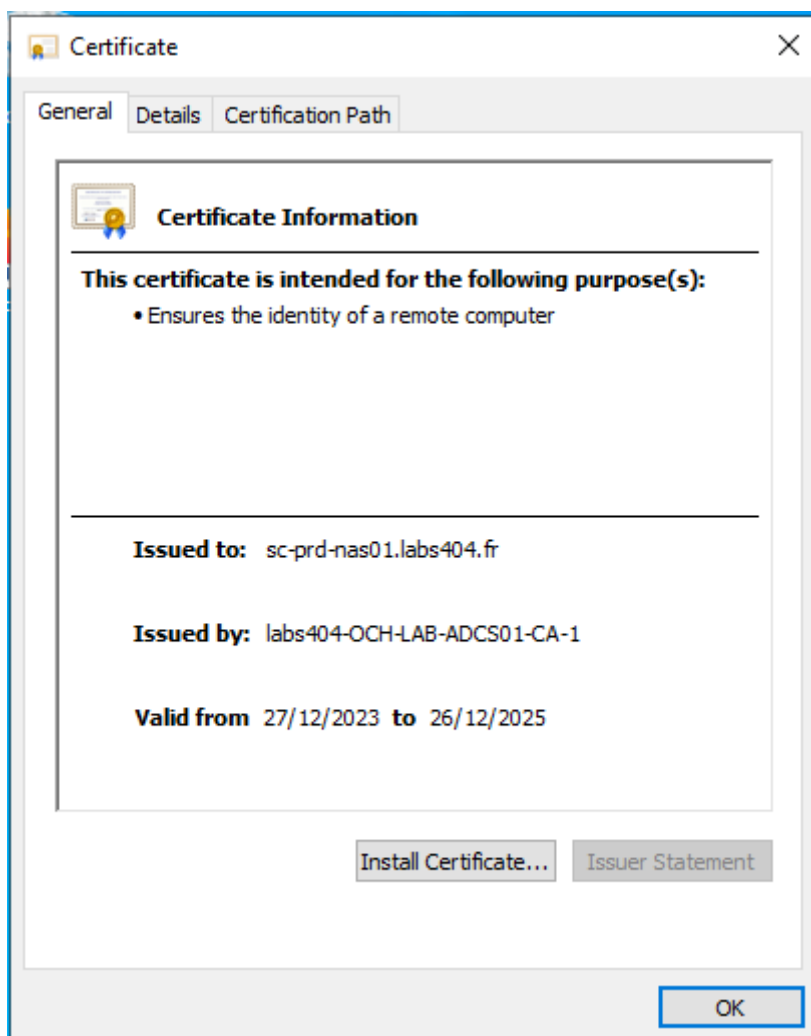
IV. Installer le certificat

4.1 Avec l'import windows

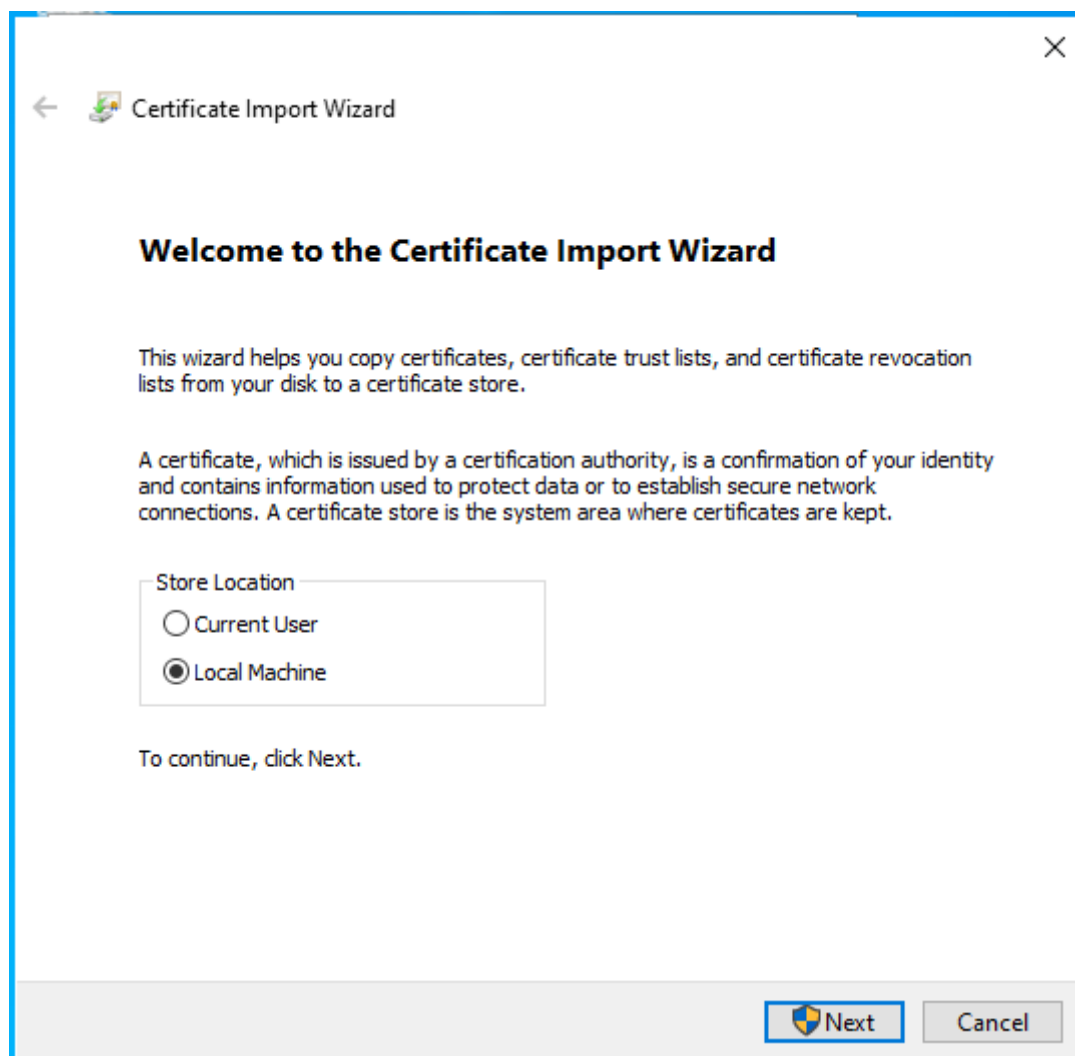
Double-cliquer sur le certificat à importer.



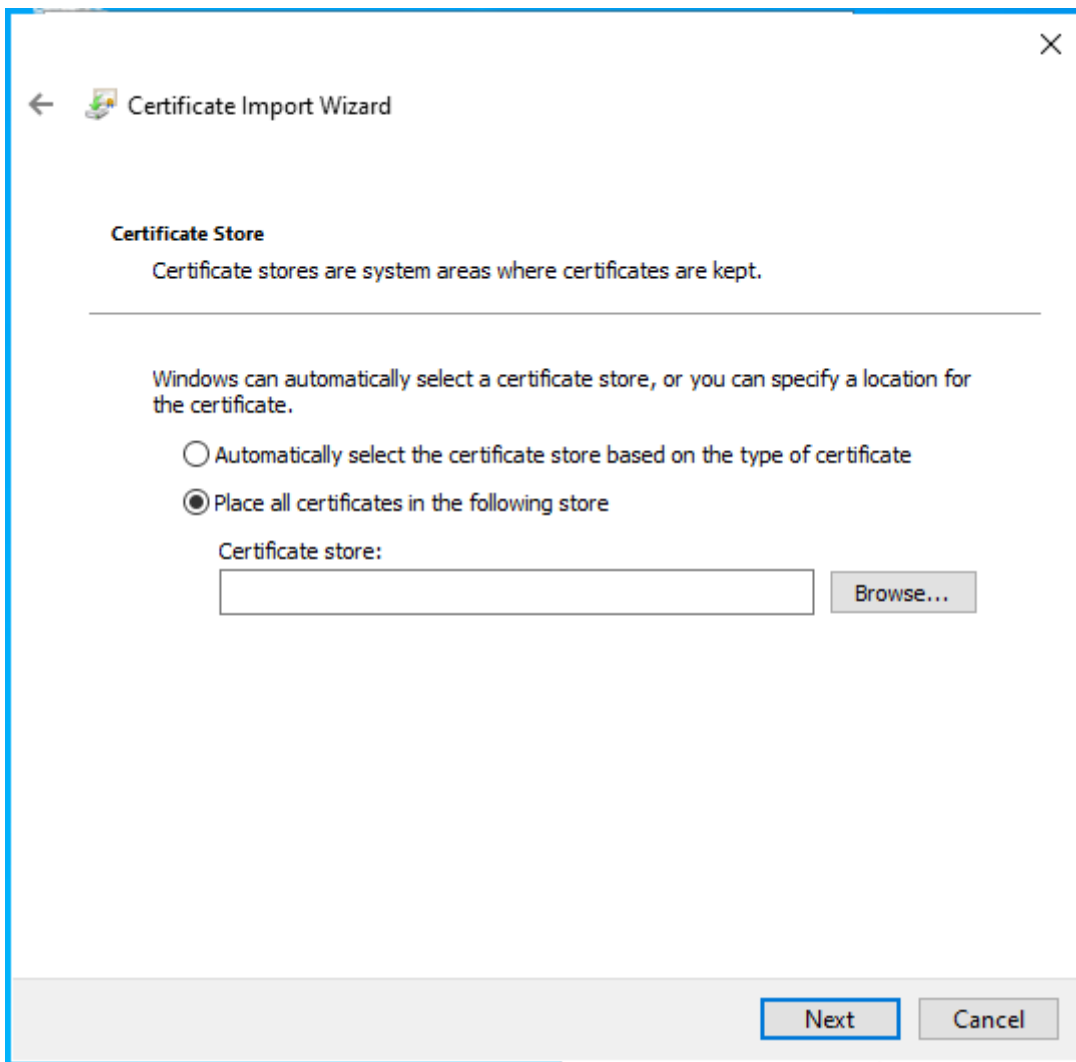
Vérifier les données, puis cliquer sur '*Install Certificate...*'



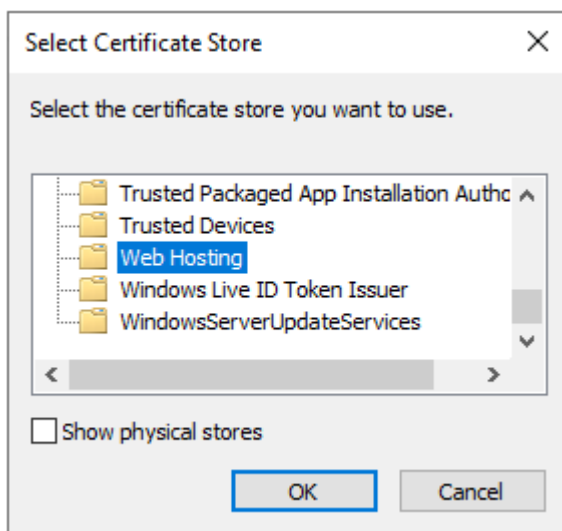
Ici, pour un certificat de serveur web, sélectionner '**Local Machine**' puis '**Next**'.



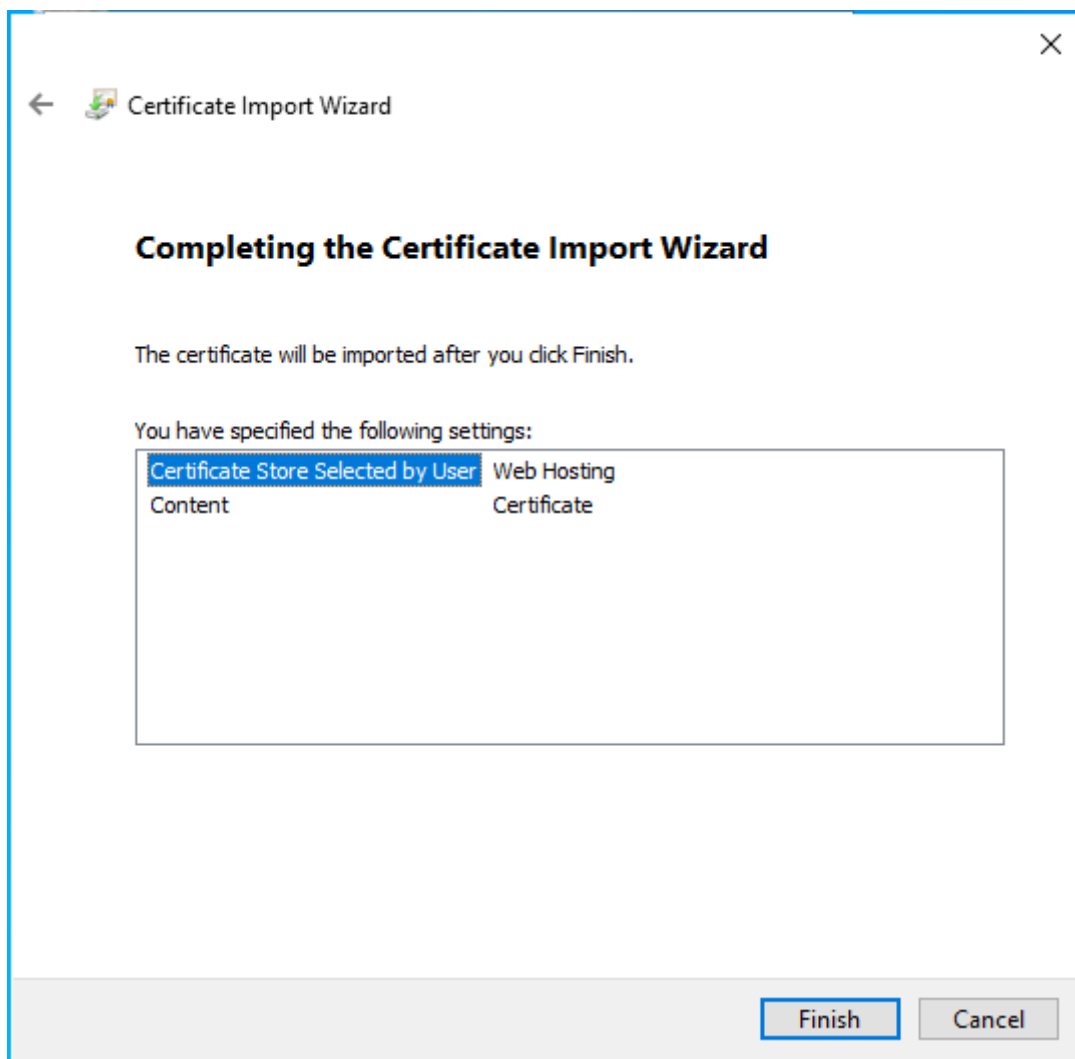
Cocher '**Place all certificates in the following store**' puis cliquer sur '**browse**'.



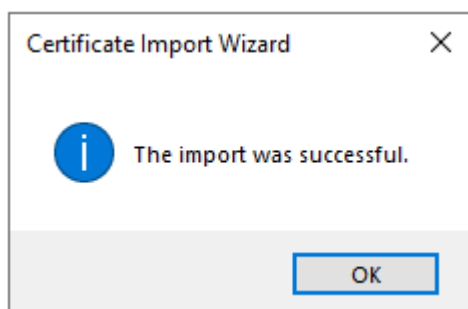
Sélectionner le magasin approprié (ici '**Web Hosting**'). Puis valider en cliquant '**OK**'



Faire '**Next**' puis '**Finish**'.

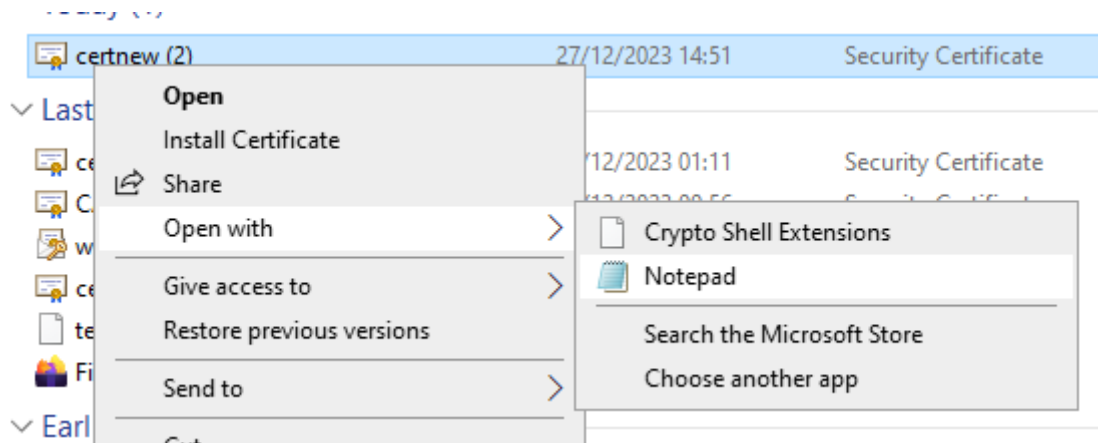


Le message de confirmation apparaît.



4.2 En récupérant le contenu du Certificat

Si besoin, ouvrir le certificat



Et récupérer le contenu en copier/coller

```
certnew (2) - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIF9zCCBN+gAwIBAgITIAAAAAZ382Sq00DryQAAAAAABjANBgkqhkiG9w0BAQsF
ADBTMRIwEAYKCZImiZPyLQBGRYCNIXFzAVBgoJkiaJk/IsZAEZFgdSYWJzNDA0
MSQwIgYDVQQDEtsYWJzNDA0LU9DSC1MQUITtQURDUzAxLUNBLTEwHhcNMjMxMjI3
-----
```

Il faudra ensuite suivre la procédure de votre équipement pour importer celui-ci.

Revision #2

Created 2026-07-30 08:23:02 UTC by Olivier

Updated 2026-07-30 08:25:35 UTC by Olivier