

# HTTPS

Version 1.0.1

Niveau requis : 5/7



## *Mise en place de la sécurisation HTTPS d'un site en localhost sous Windows avec WAMP*

## Sommaire

<b>I.</b>	<b>PREAMBULE.....</b>	<b>3</b>
I.I.	OBJET.....	3
I.II.	PREREQUIS .....	3
I.III.	VERSIONS DU DOCUMENT .....	3
I.IV.	DOCUMENTS DE REFERENCE .....	3
<b>II.</b>	<b>UN PEU DE THEORIE .....</b>	<b>3</b>
II.I.	PRINCIPE DE LA SECURISATION .....	3
II.II.	GESTION DES CERTIFICATS .....	4
II.II.1	<i>Principe de signature / autorité de certification .....</i>	<i>4</i>
II.II.2	<i>Exemple du site <a href="https://pequignat.eu">https://pequignat.eu</a> .....</i>	<i>4</i>
II.II.3	<i>Magasins de certificats sous windows .....</i>	<i>13</i>
II.III.	ECHANGES RESEAU .....	16
<b>III.</b>	<b>MISE EN ŒUVRE .....</b>	<b>17</b>
III.I.1	<i>Configuration de Wamp / Apache.....</i>	<i>17</i>
III.I.2	<i>Génération de la clef privée et clef publique .....</i>	<i>18</i>
III.I.3	<i>Configuration du Virtual Host en SSL .....</i>	<i>19</i>
III.I.4	<i>Tests.....</i>	<i>20</i>
<b>IV.</b>	<b>SOURCES D'INFORMATIONS.....</b>	<b>28</b>
<b>V.</b>	<b>FIN DU DOCUMENT .....</b>	<b>28</b>

## I. Préambule

### I.I. *Objet*

L'objet de ce document est de décrire comment à des fins de développement sur son Poste mettre la sécurisation SSL/TLS sous Wamp et le faire reconnaître comme site web de confiance : sans alerte de sécurité dans le navigateur.

### I.II. *Prérequis*

Le prérequis est d'avoir suivi préalablement le document de référence [R1] sur la mise en place d'un Hôte Virtuel sous Wamp.

### I.III. *Versions du document*

Version	Date	Auteur	Description
1.0.0	09/04/2022	Péquignat.eu	Création du document
1.0.1	08/10/2022	Péquignat.eu	Changement du nom de l'auteur

### I.IV. *Documents de référence*

#	Document	Version	Auteur(s)
[R1]	Mise en place d'un Hôte Virtuel sous Wamp	1.0.1	Péquignat.eu

## II. Un peu de théorie

### II.I. *Principe de la sécurisation*

Le principe de la sécurisation se base sur le cryptage à clef publique/clef secrète où la clef secrète sert à crypter et sécuriser les données transmises et la clef publique sert à décoder les données pour les rendre lisible.

Afin d'assurer que la donnée provient du bon endroit et non d'un usurpateur, il est nécessaire que d'une part la clef secrète ne peut être déduit de la clef publique car celle-ci est publique, et d'autre part que la clef publique soit bien reconnue de provenance fiable. C'est-à-dire que l'on fait confiance dans la clef publique.

Dans l'usage de l'utilisation des sites Internet, lorsque vous naviguer sur un site en HTTPS (bien avec le S de http), il y a une reconnaissance par le navigateur de la clef publique qui exploite un magasin d'autorités certifiante : C.A. (Certification Authority).

La plupart de navigateur sous Windows, exploite le magasin Windows qui stocke ces CA.

Dans certains sites, il est possible de vouloir Authentifier le client, c'est-à-dire votre navigateur ou votre application, dans ce cas, on dit que l'on est sur une double authentification. Votre client doit disposer d'un couple clef privé et clef publique qui celle-dernière est reconnaissable par le serveur pour que celui-ci accepte la connexion.

## II.II. *Gestion des certificats*

### II.II.1 **Principe de signature / autorité de certification**

Un certificat (clef publique), pour être reconnu doit être connu par une Autorité Certifiante (CA). Cette autorité peut déléguer la reconnaissance à des sous Autorité Intermédiaire.

Une Autorité Intermédiaire est donc aussi reconnue par l'Autorité Certifiante (CA). Pour reconnaître une autorité ou une clef publique, celle-ci est tamponné avec une signature numérique.

Aussi, la clef publique du serveur, auquel vous tentez d'accéder a une clef publique qui peut être signé par une Autorité Intermédiaire qui elle-même peut être signée par une Autorité Intermédiaire ou Racine.

L'Autorité Racine est signée par elle-même. On dit que le CA est Auto-Signée (self-signed).

### II.II.2 **Exemple du site <https://pequignat.eu>**

Aller avec votre navigateur <https://pequignat.eu>

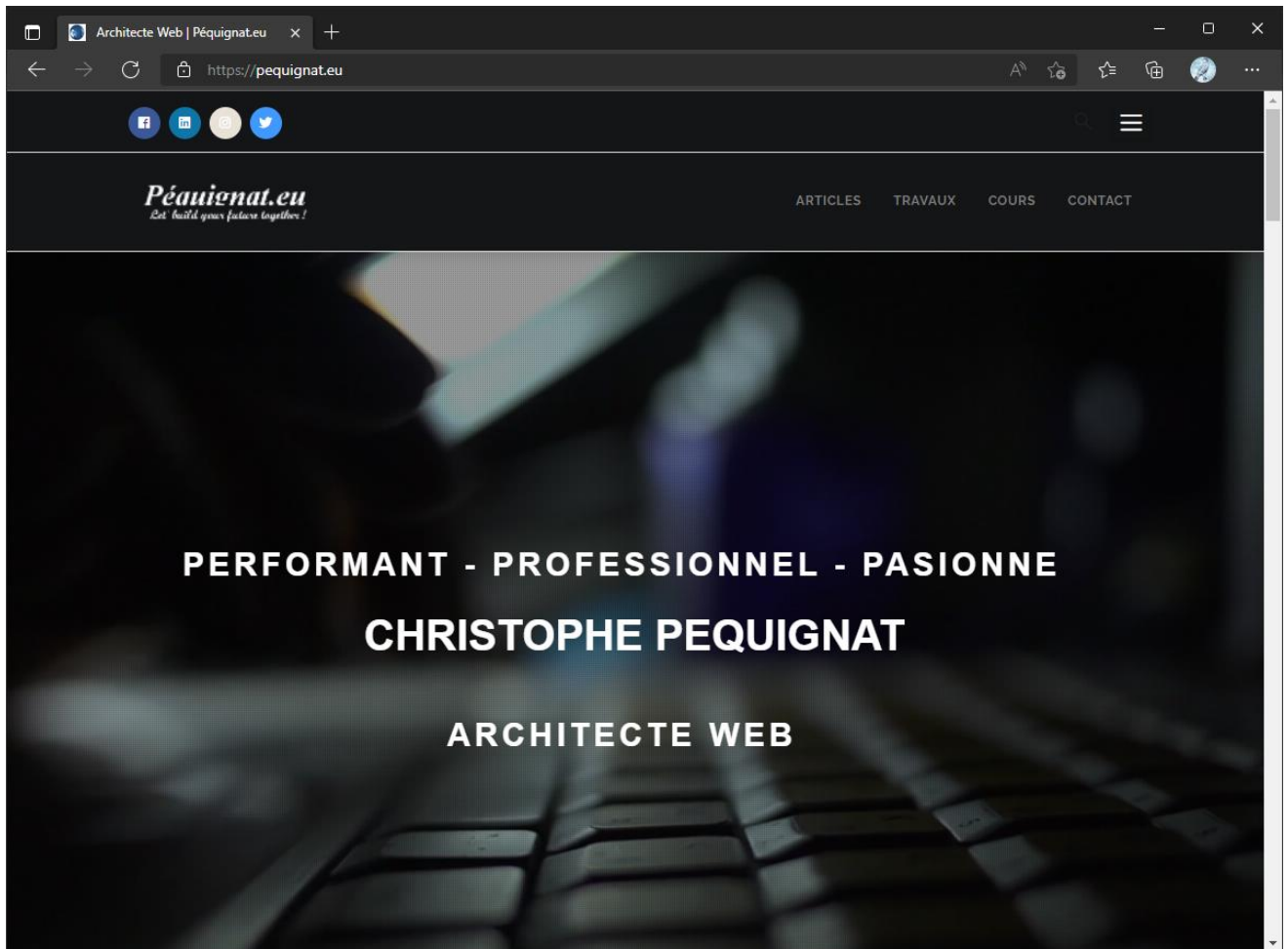
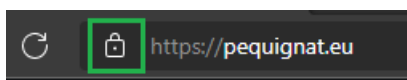


Figure 1 - Site <https://pequignat.eu>

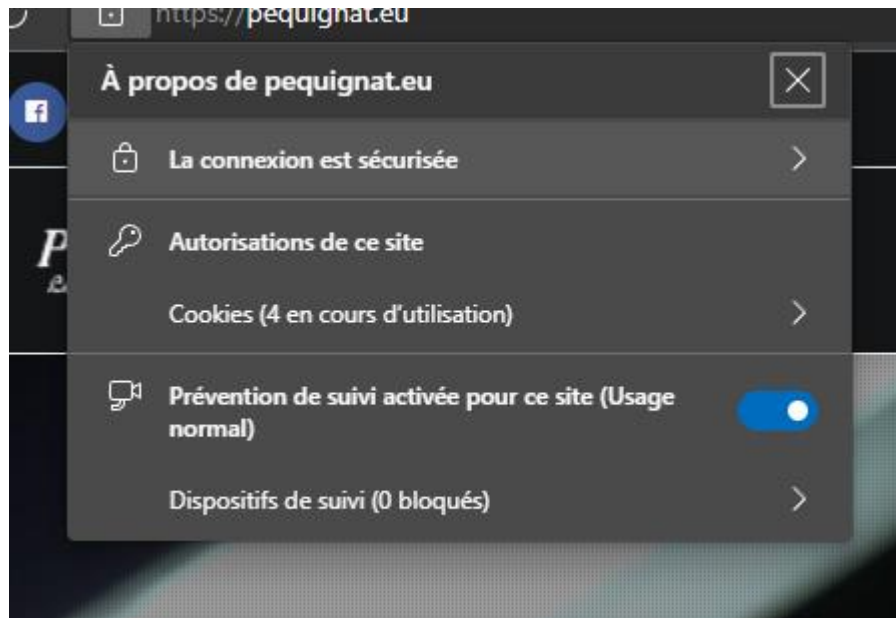
Vous accéder au site sans avoir d'alerte de sécurité.

Vous pouvez voir qu'il y a un cadenas verrouillé sur à gauche de l'URL :

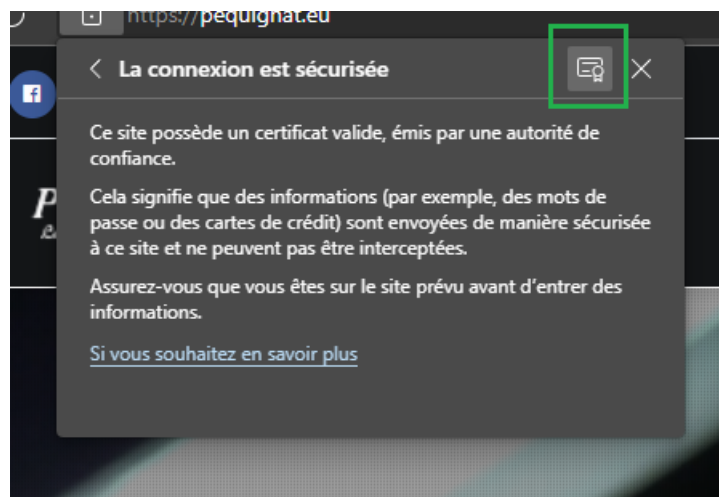


Nous allons voir les détails.

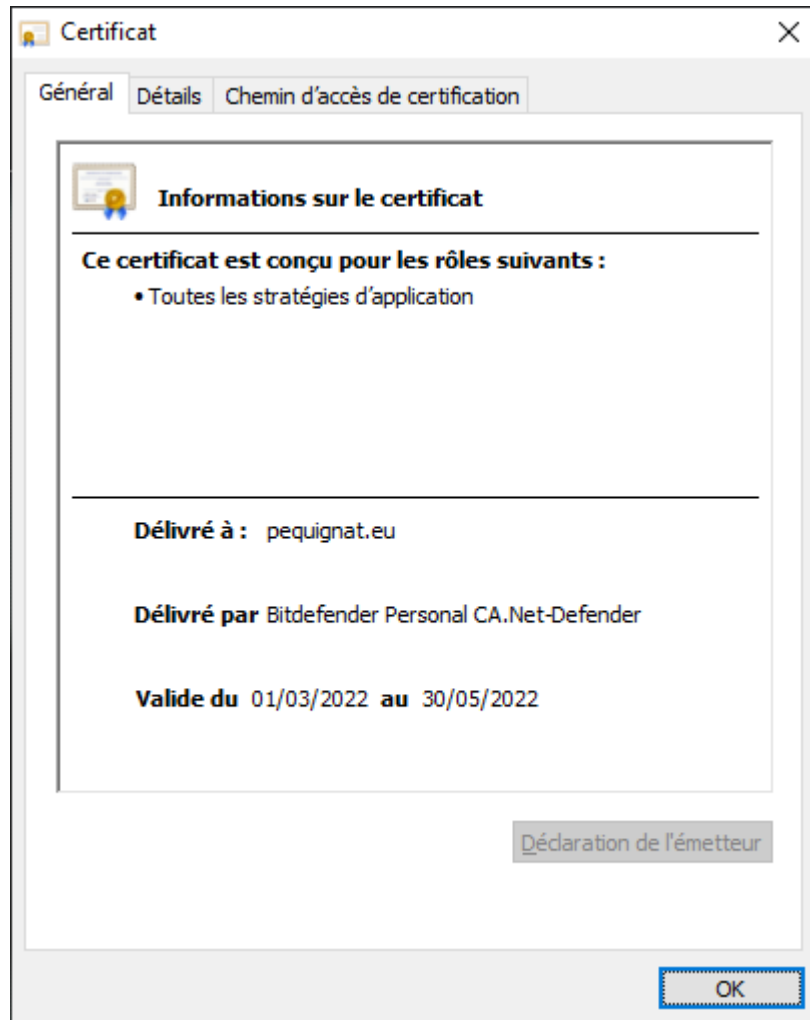
Cliquer dessus.



Cliquer sur « La connexion est sécurisée »

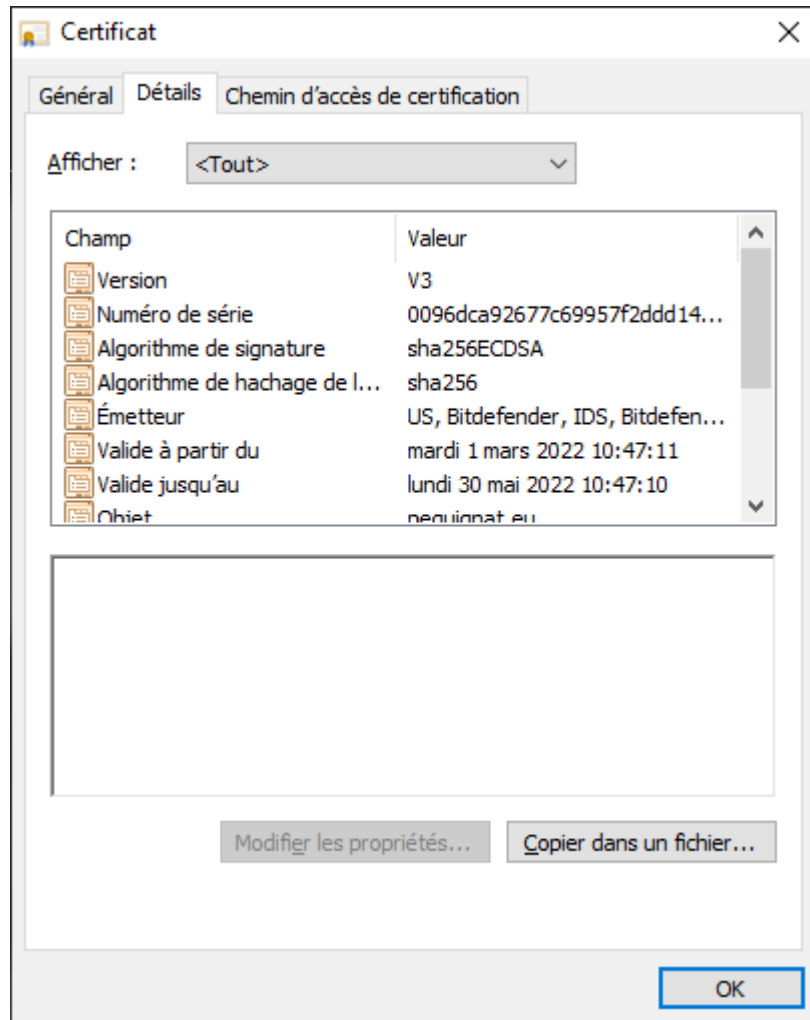


Cliquer ensuite sur la carte d'identité du certificat.



Vous pouvez voir que le site possède un certificat reconnu qui est délivré par « Bitdefender Personal CA.Net-Defender ».

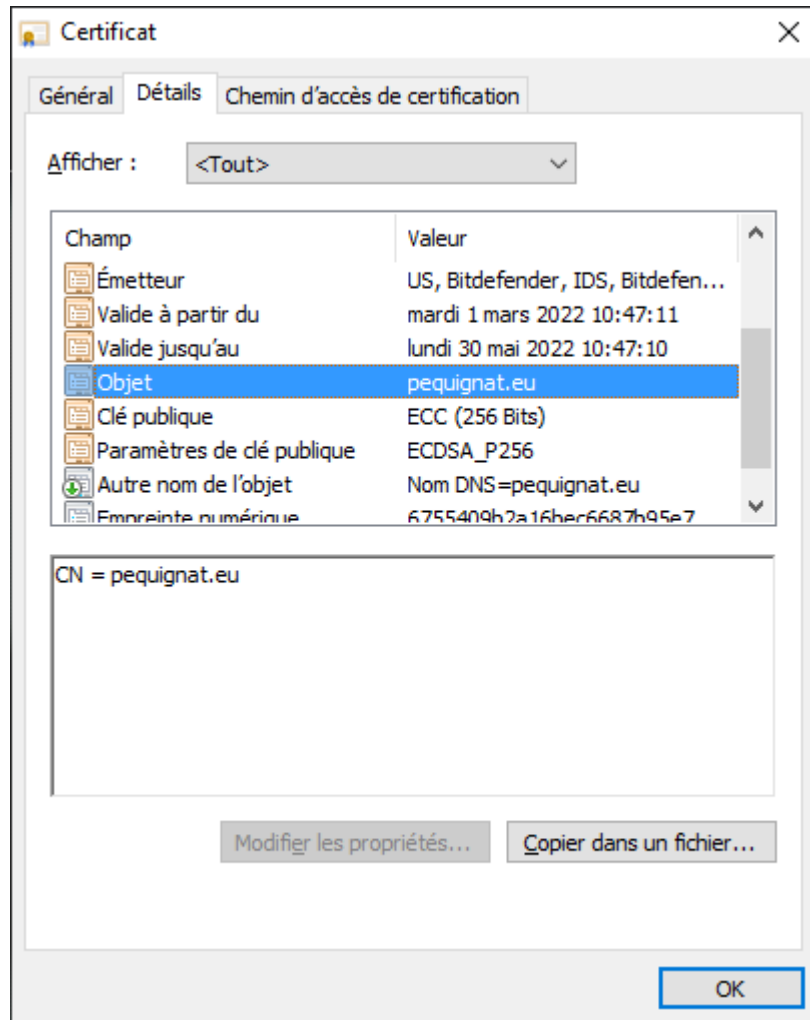
Allez dans Détails :



Cliquer sur Objet

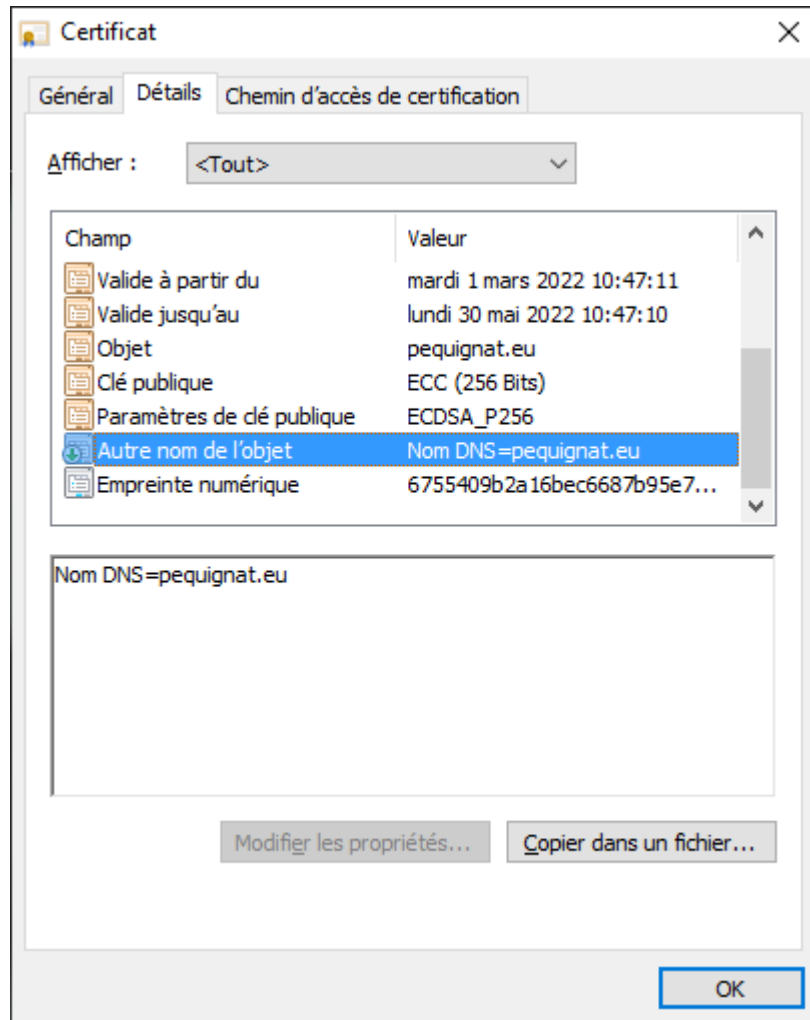
Vous trouverez le CN (Common Name) qui doit correspondre au domaine du site « pequignat.eu »



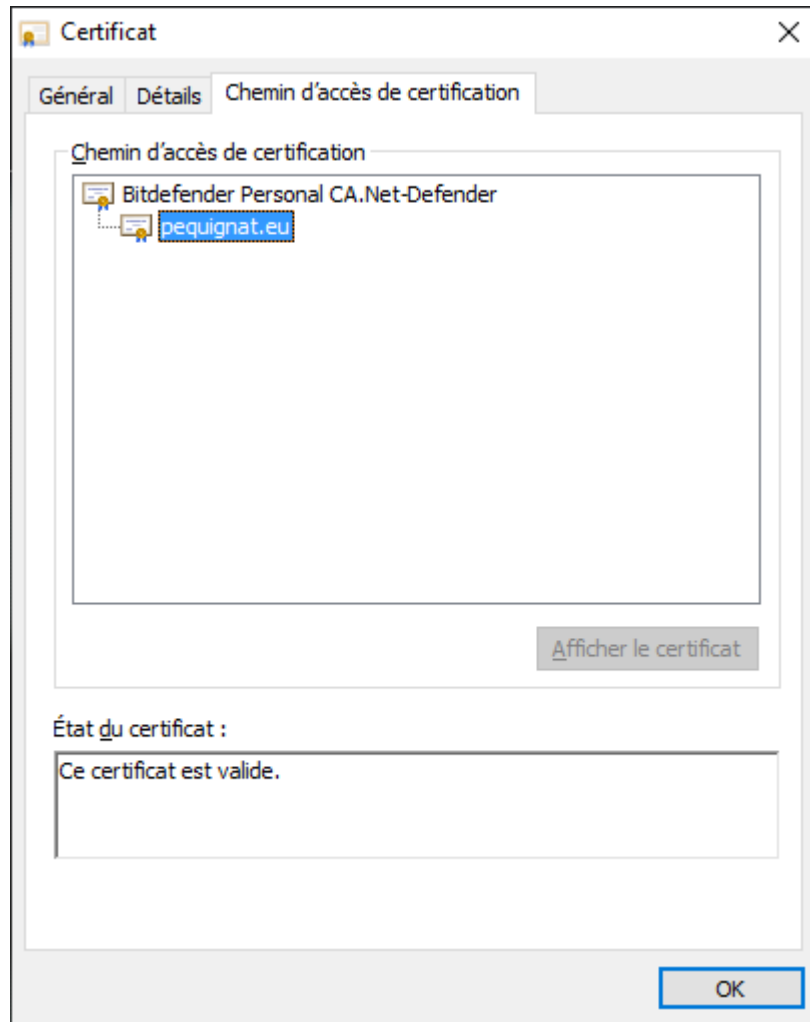


Le CN doit être celui du site pour que le navigateur accepte la clef publique, sinon il met une alerte de sécurité.

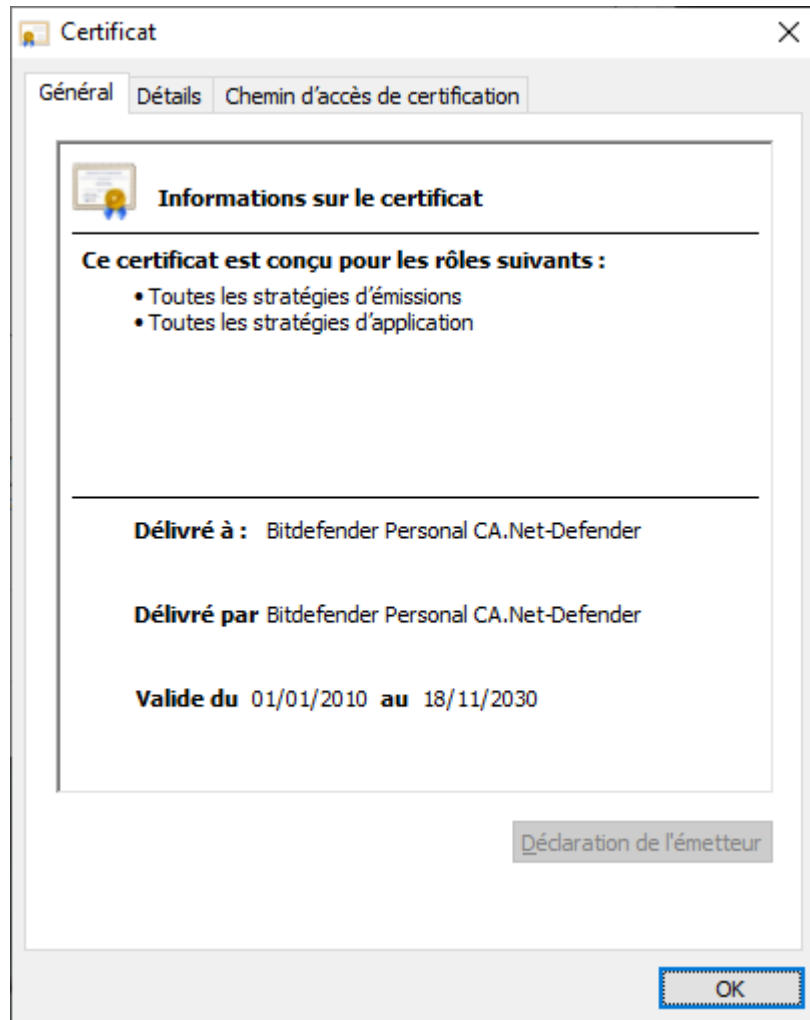
De plus il doit y avoir aussi un champ DNS qui doit aussi être sur le nom du domaine : « pequignat.eu ». Pour le voir, cliquer sur « Autre nom de l'objet ».



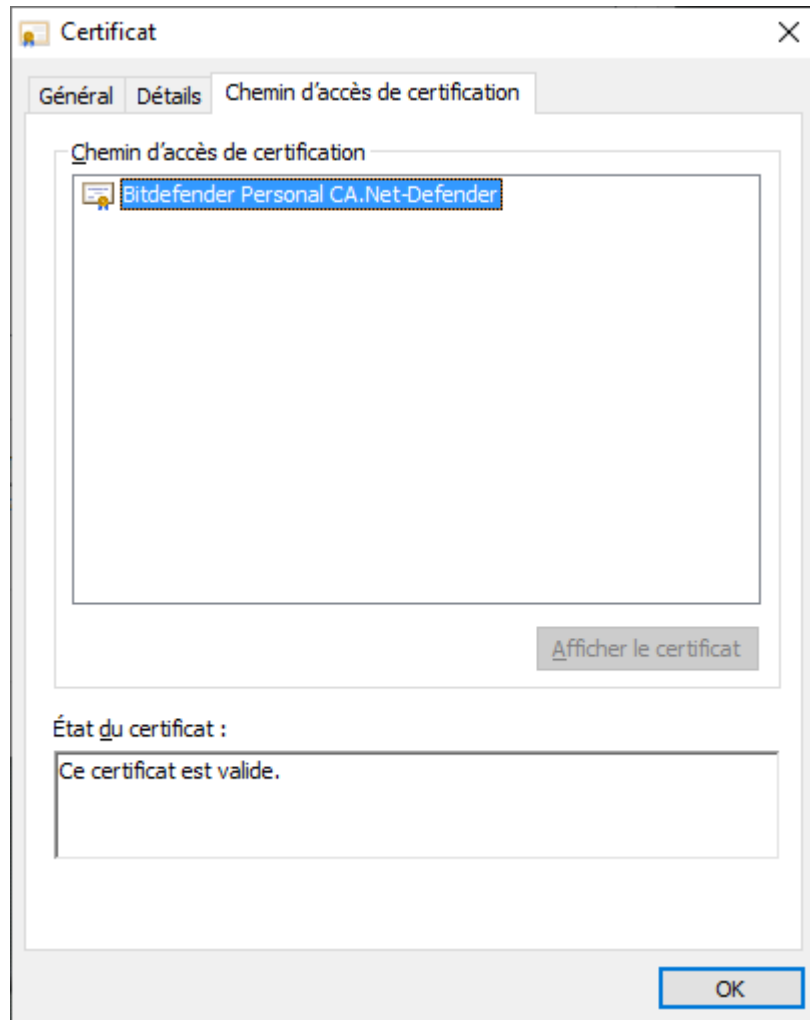
Allons donc cliquer maintenant sur l'onglet « Chemin d'accès de certification » pour y voir les informations du CA.



Cliquer sur la racine « Bitdefender Personal CA.Net-Defender » et cliquer sur Afficher le certificat.



Vous remarquerez que le certificat est auto signé.

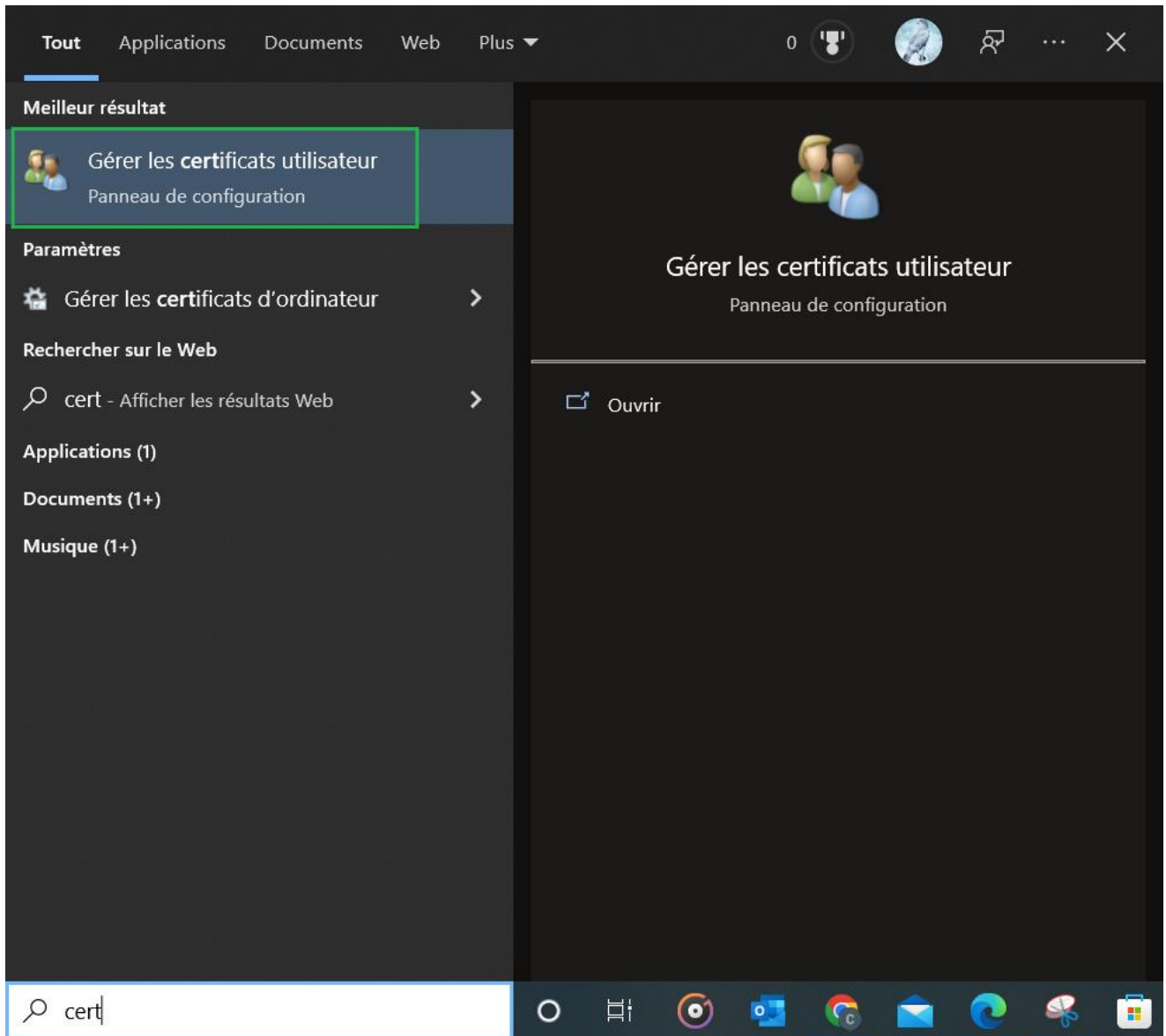


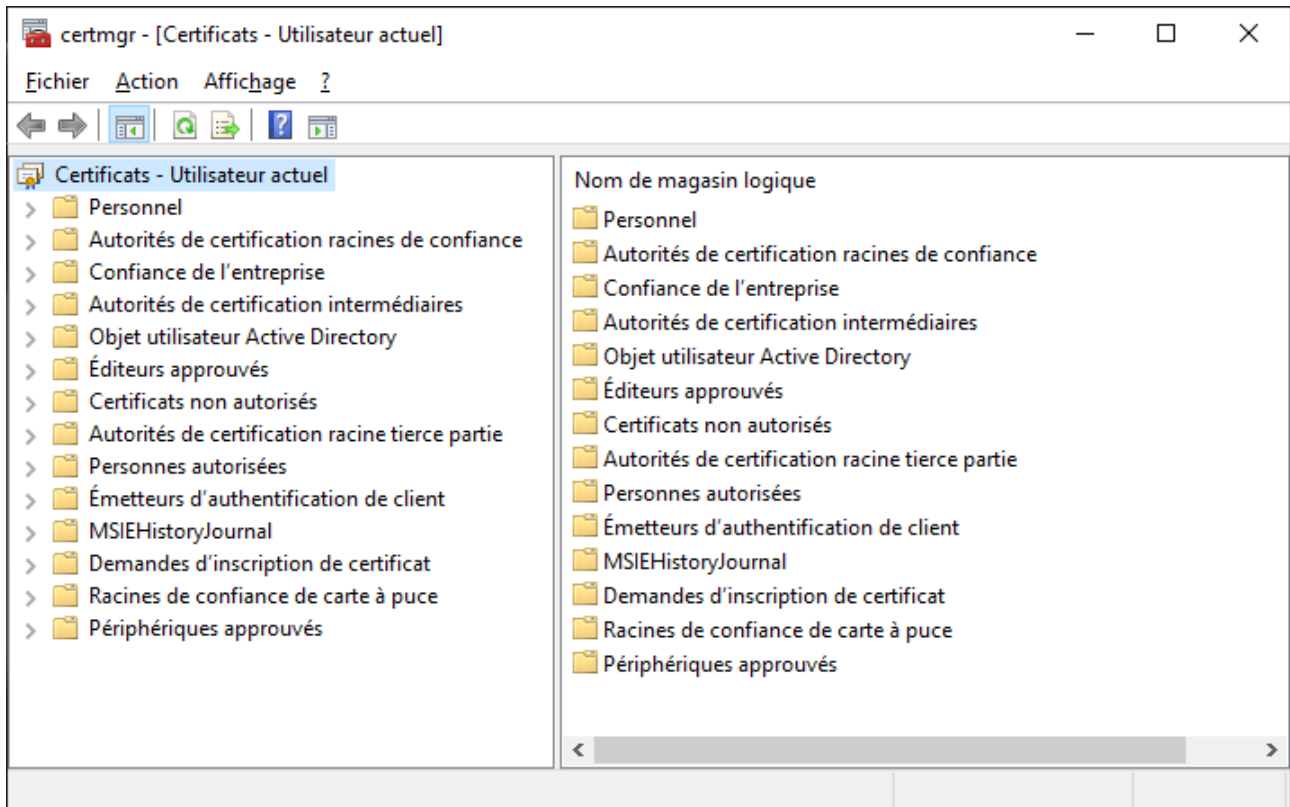
S'il est reconnu, c'est parce qu'il est inscrit dans Windows et que le navigateur le reconnaît donc par ce biais.

### II.II.3 Magasins de certificats sous windows

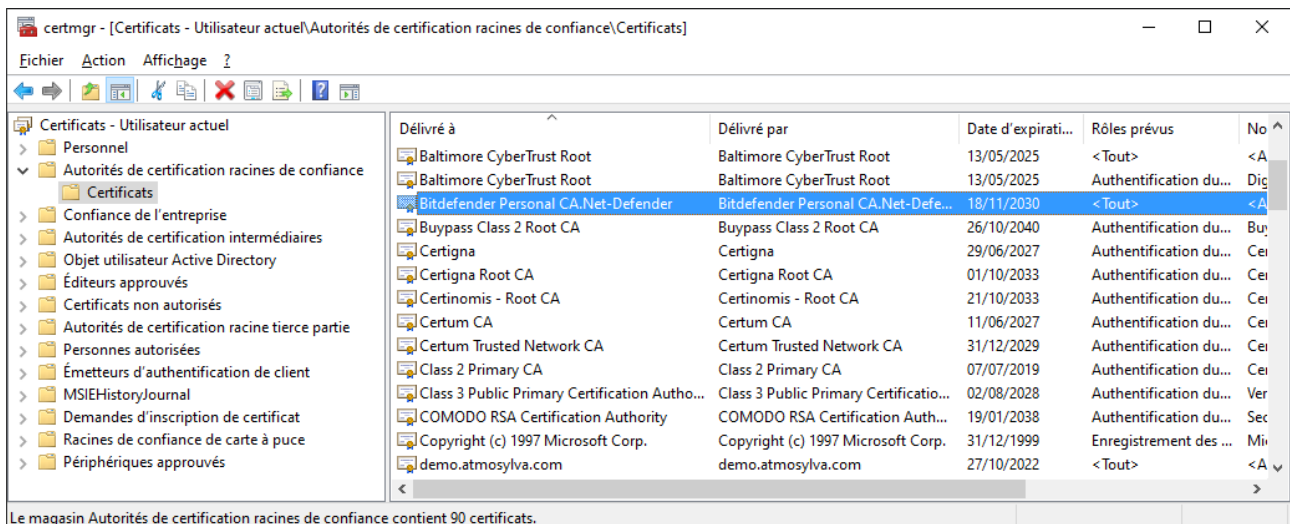
Pour voir les magasins de l'utilisateur courant :

Entrez « cert » dans la loupe :





Cliquer sur la deuxième ligne : « Autorités de certification racines de confiance » puis « Certificats »  
 Vous retrouverez le certificat reconnu.



**ATTENTION : Surtout, ne supprimez aucun certificat d'ici.**

Par la suite nous allons rajouter dans ce magasin le certificat auto signé « HelloWorld » afin de permettre qu'il soit reconnu par le navigateur.

## II.III. Echanges réseau

Voici comme se fait les échanges réseaux en TLS v1.2

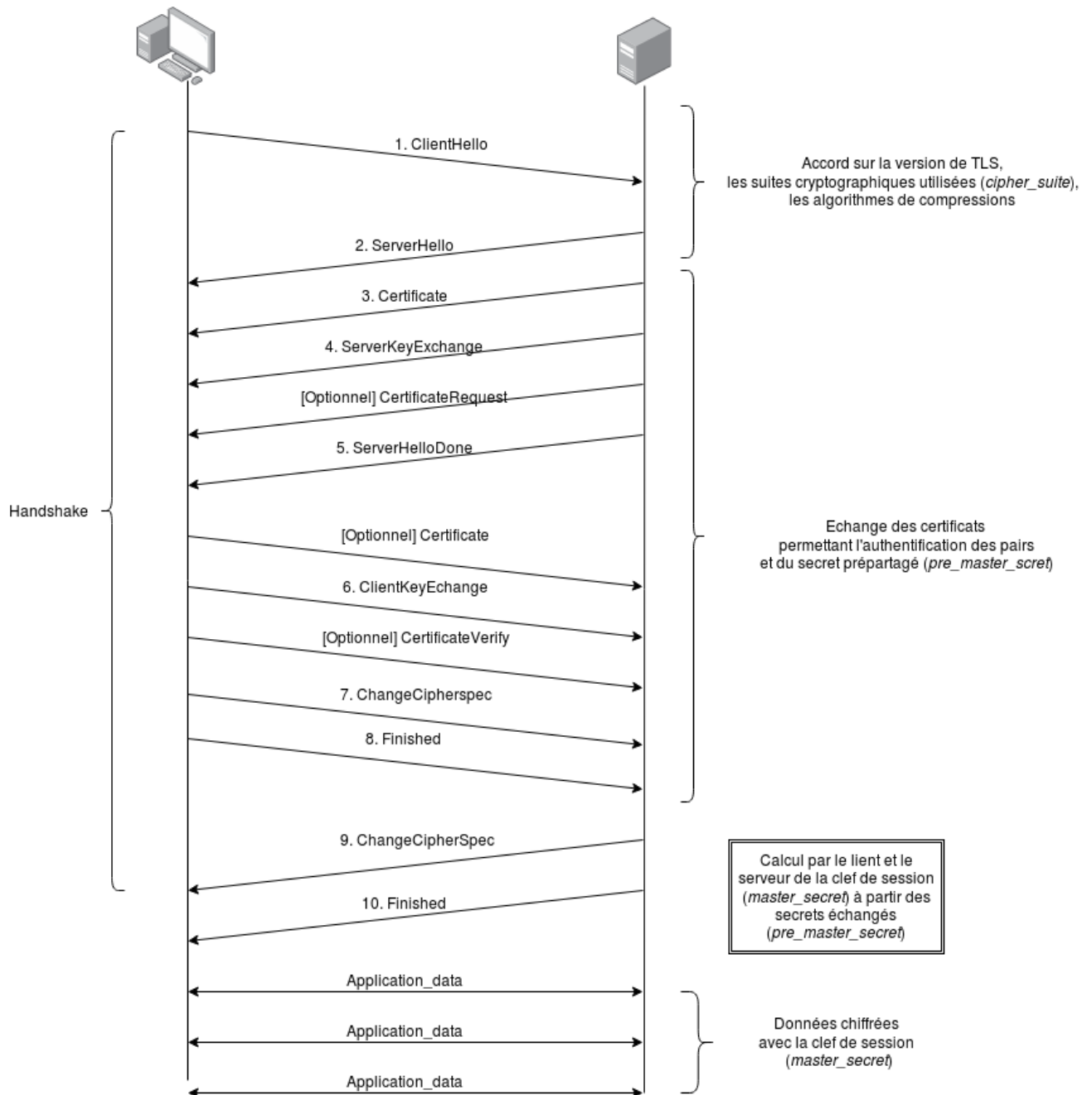


Figure 2 - [https://commons.wikimedia.org/wiki/File:Handshake\\_TLS.png?uselang=fr](https://commons.wikimedia.org/wiki/File:Handshake_TLS.png?uselang=fr)



### III. Mise en œuvre

#### III.I.1 Configuration de Wamp / Apache

Lancez Wamp, le logo doit être vert.

Allez dans Apache, puis modules afin de vérifier que le module « ssl\_module » est bien actif.

Modules Apache			
✓ access_compat_module	✓ cgi_module	✓ log_config_module	✓ rewrite_module
✓ actions_module	charset_lite_module	log_debug_module	sed_module
✓ alias_module	data_module	log_forensic_module	session_cookie_module
✓ allowmethods_module	dav_fs_module	logio_module	session_crypto_module
✓ asis_module	dav_lock_module	lua_module	session_dbd_module
✓ auth_basic_module	dav_module	macro_module	session_module
✓ auth_digest_module	dbd_module	md_module	✓ setenvif_module
auth_form_module	deflate_module	mime_magic_module	slotmem_plain_module
authn_anon_module	✓ dir_module	✓ mime_module	slotmem_shm_module
✓ authn_core_module	dumpio_module	✓ negotiation_module	socache_dbm_module
authn_dbd_module	✓ env_module	proxy_ajp_module	socache_memcache_module
authn_dbm_module	expires_module	proxy_balancer_module	socache_redis_module
✓ authn_file_module	ext_filter_module	proxy_connect_module	socache_shmcb_module
authn_socache_module	✓ file_cache_module	proxy_express_module	spelling_module
authnz_fcgi_module	filter_module	proxy_fcgi_module	✓ ssl_module
authnz_ldap_module	headers_module	proxy_ftp_module	status_module
authz_dbd_module	heartbeat_module	proxy_hcheck_module	substitute_module
authz_dbm_module	heartbeat_monitor_module	proxy_html_module	unique_id_module
authz_dbm_module	http2_module	proxy_http2_module	✓ userdir_module
✓ authz_groupfile_module	ident_module	proxy_http_module	usertrack_module
authz_owner_module	imagemap_module	proxy_module	version_module
✓ authz_user_module	✓ include_module	proxy_scgi_module	✓ vhost_alias_module
✓ autoindex_module	info_module	proxy_uwsgi_module	watchdog_module
brotli_module	✓ isapi_module	proxy_wstunnel_module	xml2enc_module
buffer_module	lbmethod_bybusyness_module	ratelimit_module	<b>Module irréversible</b>
✓ cache_disk_module	lbmethod_byrequests_module	reflector_module	ⓘ authz_core_module
✓ cache_module	lbmethod_bytraffic_module	remoteip_module	ⓘ authz_host_module
cache_socache_module	lbmethod_heartbeat_module	reqtimeout_module	ⓘ php7_module
cern_meta_module	ldap_module	request_module	

## III.I.2 Génération de la clef privée et clef publique

### III.I.2.a Préparation du fichier de description des informations du site

Créez un répertoire « ssl » dans « C:\wamp64\ssl »

Créez un fichier vide (Document Texte) « HelloWorld.cnf » dans ce répertoire contenant :

```
[ req ]
prompt = no
distinguished_name = dn
req_extensions = req_ext

[ dn ]
CN = helloworld
emailAddress = contact@pequignat.eu
O = Pequignat.eu
OU = Hauts-de-Seine
L = Boulogne-Billancourt
ST = France
C = FR

[ req_ext ]
subjectAltName = DNS: helloworld, IP: 127.0.0.1

[SAN]
subjectAltName = DNS: helloworld, IP: 127.0.0.1
```

### III.I.2.b Créez la commande qui va générer les clefs (privée et publique)

Créez un fichier vide « HelloWorld.bat » contenant :

```
set OPENSSL_CONF=C:\wamp64\bin\apache\apache2.4.46\conf\openssl.cnf

C:\wamp64\bin\apache\apache2.4.46\bin\openssl req -x509 -nodes -days 700 -newkey
rsa:2048 -nodes -keyout C:\wamp64\ssl\HelloWorld.key -new -out
C:\wamp64\ssl\HelloWorld.crt -config HelloWorld.cnf -reqexts SAN -extensions SAN
```

Double cliquez sur ce fichier HelloWorld.bat pour l'exécuter.

Cela pour effet de générer deux fichiers :

- Clef privée : HelloWorld.key
- Clef publique auto signée : HelloWorld.crt

Nous n'allons volontairement pas enregistrer la clef publique dans le magasin des CA Windows afin de vérifier la non-reconnaissance du site.

### III.I.3 Configuration du Virtual Host en SSL

Allez dans le fichier de configuration de Virtual Host (cf [R1]).

Vous devez déjà avoir :

```
<VirtualHost *:80>
    ServerName HelloWorld
    DocumentRoot "c:/wamp64/www/helloworld"
    <Directory "c:/wamp64/www/helloworld/">
        Options +Indexes +Includes +FollowSymLinks +MultiViews
        AllowOverride All
        Require local
    </Directory>
</VirtualHost>
```

Rajoutez :

```
<VirtualHost *:443>
    ServerName HelloWorld
    DocumentRoot "c:/wamp64/www/helloworld"
    <Directory "c:/wamp64/www/helloworld/">
        Options +Indexes +Includes +FollowSymLinks +MultiViews
        AllowOverride All
        Require local
    </Directory>
    SSLEngine on
    SSLCertificateFile "C:/wamp64/ssl/HelloWorld.crt"
    SSLCertificateKeyFile "C:/wamp64/ssl/HelloWorld.key"
</VirtualHost>
```

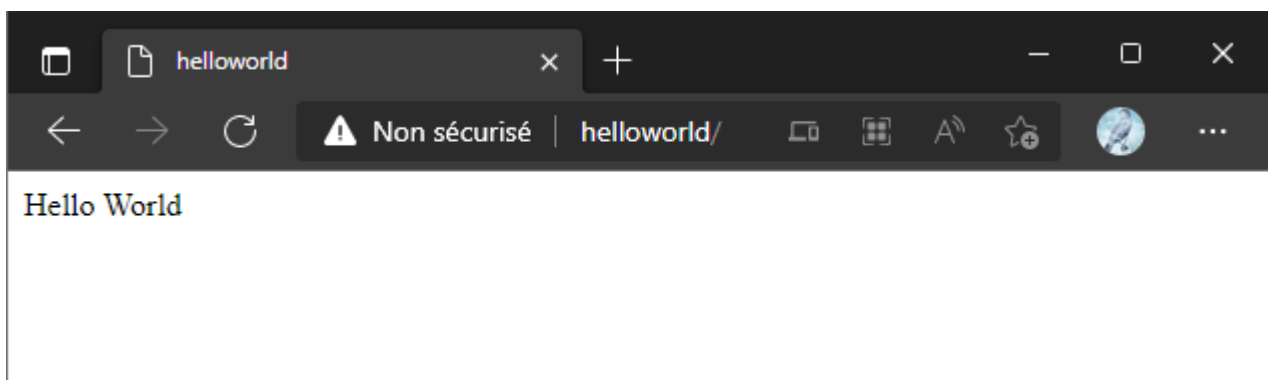
Redémarrer Wamp.

Wamp revient au vert.

### III.I.4 Tests

#### III.I.4.a Test http simple

Entrez dans votre navigateur le lien : <http://helloworld/>



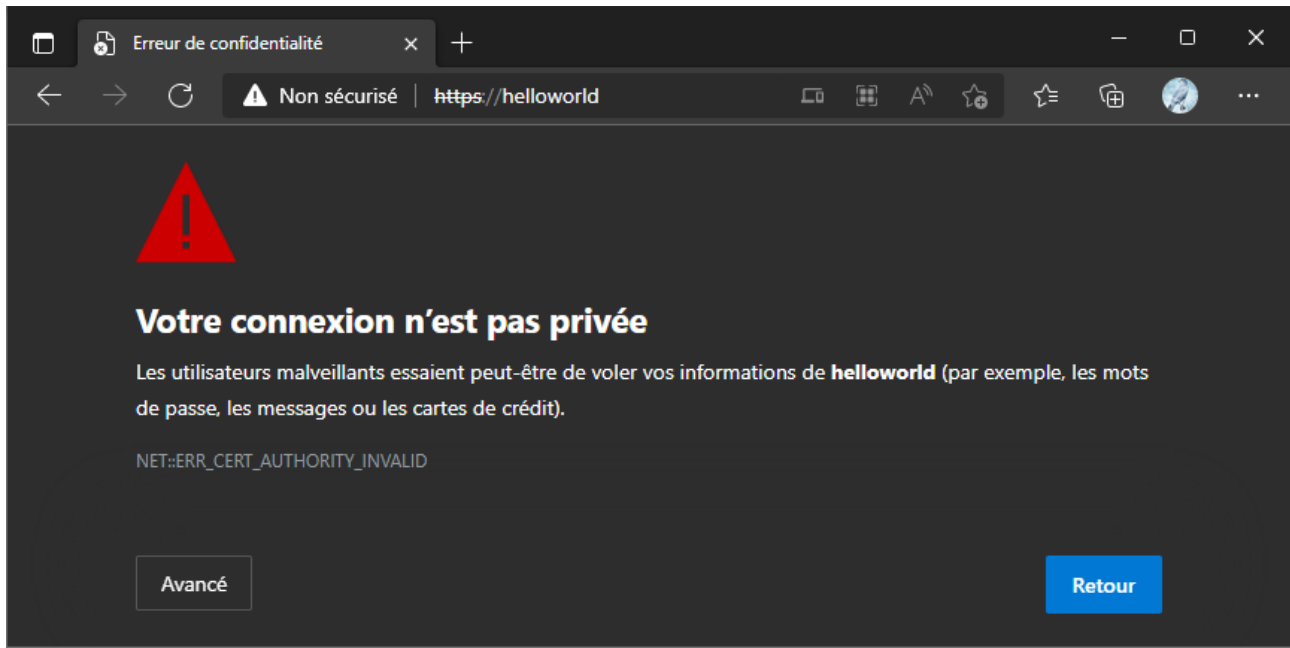
Vous remarquerez qu'il est marqué « Non sécurisé » car non application du l'HTTPS.

Note : le port par défaut en http simple est le port 80.

### III.I.4.b Tests en HTTPS non fiable

Entrez maintenant l'URL : <https://helloworld/>

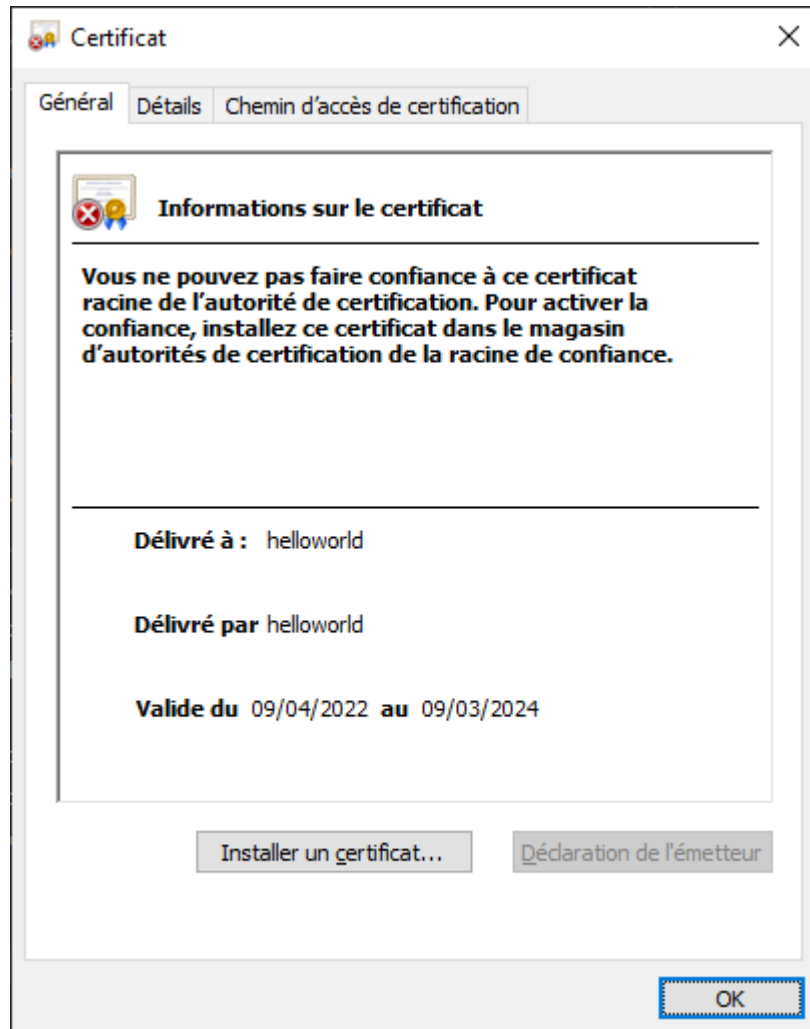
Le site est reconnu comme non sécurisé. C'est qui est attendu dans l'état actuel.



Il n'est pas recommandé d'accès aux sites qui ont cette alerte. Vous pouvez à vos risques tout de même forcer le passage dans « Avancé ».


### III.I.4.c Test fiable après rajout de la clef publique dans les CA

Maintenant, vous allez rajouter dans les Autorités Racines de confiance la clef publique. Pour cela, double cliquer sur le fichier « C:\wamp64\ssl\HelloWorld.crt ».



Cliquer sur « Installer un certificat ... »



←  Assistant Importation du certificat

## Bienvenue dans l'Assistant Importation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.

Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

Emplacement de stockage

Utilisateur actuel

Ordinateur local


Cliquez sur Suivant pour continuer.

Suivant

Annuler

Laissez « Utilisateur actuel », Suivant



←  Assistant Importation du certificat

### Magasin de certificats

Les magasins de certificats sont des zones système où les certificats sont conservés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

Sélectionner automatiquement le magasin de certificats en fonction du type de certificat

Placer tous les certificats dans le magasin suivant :

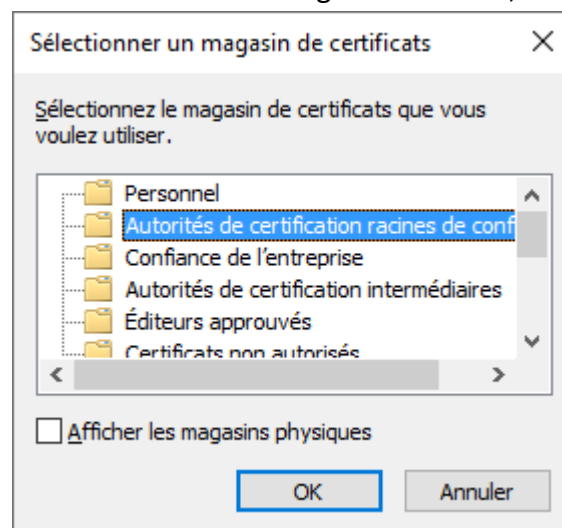
Magasin de certificats :

Parcourir...

Suivant

Annuler


Sélectionnez « Placer tous les certificats dans le magasin suivant », Parcourir



Mettre dans « Autorité de certification racines de confiance ».





←  Assistant Importation du certificat

#### Magasin de certificats

Les magasins de certificats sont des zones système où les certificats sont conservés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

- Sélectionner automatiquement le magasin de certificats en fonction du type de certificat
- Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Autorités de certification racines de confiance


Parcourir...

Suivant

Annuler

Cliquez sur « Suivant »



←  Assistant Importation du certificat

## Fin de l'Assistant Importation du certificat

Le certificat sera importé après avoir cliqué sur Terminer.

Vous avez spécifié les paramètres suivants :

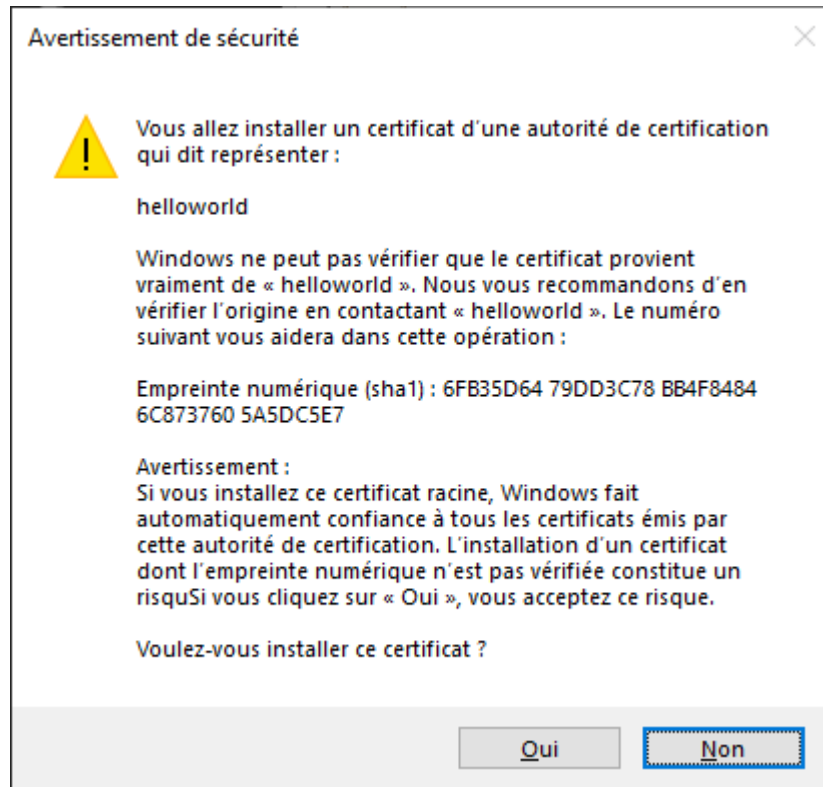
Magasin de certificats sélectionné par l'utilisateur	Autorités de certification racines de cc
Contenu	Certificat

Terminer

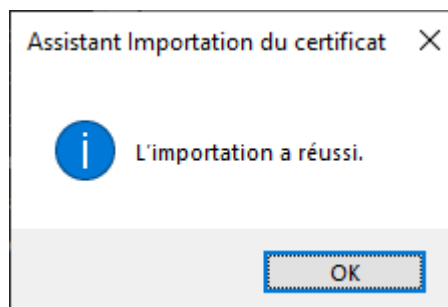
Annuler

Terminer.

A le popup de vérification, confirmez. En, cliquant sur Oui.

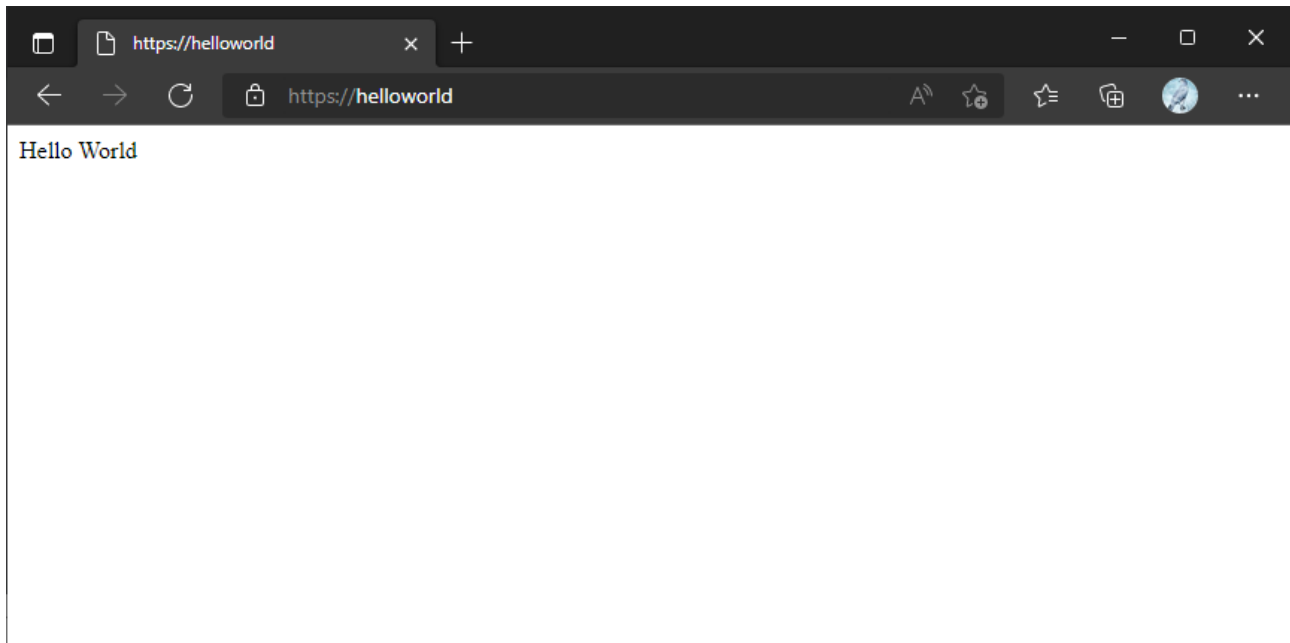


Oui



Fermez le navigateur et relancer le lien : <https://helloworld/>

L'alerte n'est plus présente.



## IV. Sources d'Informations

#	Source	Lien
[S1]	TLS Wikipedia.org	<a href="https://fr.wikipedia.org/wiki/Transport_Layer_Security">https://fr.wikipedia.org/wiki/Transport_Layer_Security</a>

## V. Fin du document