

Version 1.0.1 Niveau requis : 5/7



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

Péquignat.eu

www.pequignat.eu

Sommaire

I.	PREA	MBULE	3
	I.I. Of	BJET	
	I.II. Pr	EREQUIS	
	1.111.	VERSIONS DU DOCUMENT	3
	I.IV.	DOCUMENTS DE REFERENCE	
п.	UN P	EU DE THEORIE	3
	II.I. Pr	INCIPE DE LA SECURISATION	3
	11.11.	GESTION DES CERTIFICATS	4
	<i>II.II.</i> 1	Principe de signature / autorité de certification	4
	11.11.2	Exemple du site https://pequignat.eu	4
	11.11.3	Magasins de certificats sous windows	
	11.111.	ECHANGES RESEAU	16
Ш	MISE	EN ŒUVRE	17
	III.I.1	Configuration de Wamp / Apache	
	111.1.2	Génération de la clef privée et clef publique	
	III.I.3	Configuration du Virtual Host en SSL	
	111.1.4	Tests	20
IV	. SOUF	RCES D'INFORMATIONS	28
v.	FIN D	DU DOCUMENT	28

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 reconnaitre 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	1.0.1	Péquignat.eu
	Wamp		

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.

ן י	Ŀ	nttps://pequignat.eu	
f	À pr	\times	
~	Ċ	La connexion est sécurisée	>
P	P	Autorisations de ce site	
e		Cookies (4 en cours d'utilisation)	>
	₽ª	Prévention de suivi activée pour ce site (Usage normal)	-
		Dispositifs de suivi (0 bloqués)	>

Cliquer sur « La connexion est sécurisée »



Cliquer ensuite sur la carte d'identité du certificat.

厦 Certific	at	×
Général	Détails Chemin d'accès de certification	
	Informations sur le certificat	
Cece	ertificat est conçu pour les rôles suiv	/ants :
	 Toutes les stratégies d'application 	
	2	
	Délivré à : pequignat.eu	
	Délivré par Bitdefender Personal CA.Ne	t-Defender
	Valide du 01/03/2022 au 30/05/2022	2
	D	éclaration de l'émetteur
		OK

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

Allez dans Détails :

💼 Certificat		×		
Général Détails Chemin d'accès	de certification			
Afficher : <tout> ~</tout>				
Champ Version Numéro de série Algorithme de signature Algorithme de hachage de l Émetteur Valide à partir du Valide jusqu'au Mobiet	Valeur V3 0096dca92677c69957f2ddd14 sha256ECDSA sha256 US, Bitdefender, IDS, Bitdefen mardi 1 mars 2022 10:47:11 lundi 30 mai 2022 10:47:10 nequiranat eu	•		
	ОК			

Cliquer sur Objet

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

💼 Certificat			\times	
Général Détails	Chemin d'accès de	ecertification		
Afficher : <tout> ~</tout>				
Champ		Valeur	^	
Émetteur	du	US, Bitdefender, IDS, Bitdefen mardi 1 mars 2022 10:47:11 Jundi 30 mai 2022 10:47:10		
Dbjet	<u>.</u>	pequignat.eu		
Clé publique Paramètres d Autre nom de Empreinte put CN = pequignat.e	e dé publique l'objet mérique	ECC (256 Bits) ECDSA_P256 Nom DNS=pequignat.eu 6755409h2a16hec6687h95e7	*	
Modifi <u>e</u> r les propriétés <u>Copier dans un fichier</u> OK				

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 ».

💽 Certificat				×
Général Détails	Chemin d'accès de	e certification		
<u>A</u> fficher : <1	Tout>	~		
Champ Valide à part Valide jusqu' Objet Clé publique Paramètres Autre nom d Empreinte nu Nom DNS=pequi	tir du 'au de clé publique le l'objet umérique gnat.eu Modifi <u>e</u> r les prop	Valeur mardi 1 mars 2022 10:47:11 lundi 30 mai 2022 10:47:10 pequignat.eu ECC (256 Bits) ECDSA_P256 Nom DNS=pequignat.eu 6755409b2a16bec6687b95e7	er	
			OK	

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

Certificat	×
Général Détails Chemin d'accès de certification	
Chemin d'accès de certification Bitdefender Personal CA.Net-Defender Pequignat.eu	
<u>A</u> fficher le certificat	
État <u>d</u> u certificat :	
Ce certificat est valide.	

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



Vous remarquerez que le certificat est auto signé.

<u>ू</u> Certifi	cat			×
Général	Détails	Chemin d'accès de certification		
<u>C</u> hem	in d'accès Bitdefend	e de certification		
			<u>A</u> fficher le certificat	
État <u>d</u> u	certificat	:		
Ce cert	tificat est	valide.	ОК	

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 :



Péquignat.eu

🚡 certmgr - [Certificats - Utilisateur actuel]

<u>Fichier Action Affichage ?</u>						
 Certificats - Utilisateur actuel Personnel Autorités de certification racines de confiance Confiance de l'entreprise Autorités de certification intermédiaires Objet utilisateur Active Directory Éditeurs approuvés Certificats non autorisés Autorités de certification racine tierce partie Personnes autorisées Émetteurs d'authentification de client MSIEHistoryJournal Demandes d'inscription de certificat Racines de confiance de carte à puce Périphériques approuvés 	Nom de magasin logique Personnel Autorités de certification racines de confiance Confiance de l'entreprise Autorités de certification intermédiaires Objet utilisateur Active Directory Éditeurs approuvés Certificats non autorisés Autorités de certification racine tierce partie Personnes autorisées Émetteurs d'authentification de client MSIEHistoryJournal Demandes d'inscription de certificat Racines de confiance de carte à puce Périphériques approuvés					

Cliquer sur la deuxième ligne : « Autorités de certification racines de confiance » puis « Certificats »

Vous retrouverez le certificat reconnu.

🚟 certmgr - [Certificats - Utilisateur actuel\Autorités de	e certification racines de confiance\Certificats]			- 0	×
<u>Fichier</u> <u>Action</u> Affic <u>h</u> age <u>?</u>					
🗢 🔿 🚈 🔜 🔏 🖦 🗙 🖼 🖬					
🗊 Certificats - Utilisateur actuel	Délivré à	Délivré par	Date d'expirati	Rôles prévus	No ^
> 🦰 Personnel	Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	<tout></tout>	<a< td=""></a<>
 Autorités de certification racines de confiance 	Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Authentification du	Dig
Certificats	Bitdefender Personal CA.Net-Defender	Bitdefender Personal CA.Net-Defe	18/11/2030	<tout></tout>	<a< td=""></a<>
Contiance de l'entreprise	🔄 Buypass Class 2 Root CA	Buypass Class 2 Root CA	26/10/2040	Authentification du	Buy
Objet utilisateur Active Directory	🔄 Certigna	Certigna	29/06/2027	Authentification du	Сег
Éditeurs approuvés	🔄 Certigna Root CA	Certigna Root CA	01/10/2033	Authentification du	Сег
Certificats non autorisés	🔄 Certinomis - Root CA	Certinomis - Root CA	21/10/2033	Authentification du	Сег
Autorités de certification racine tierce partie	🔄 Certum CA	Certum CA	11/06/2027	Authentification du	Сег
> Personnes autorisées	🔄 Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029	Authentification du	Сег
> interpretente providential de la comparación de client	🔄 Class 2 Primary CA	Class 2 Primary CA	07/07/2019	Authentification du	Cei
> 🦳 MSIEHistoryJournal	🔄 Class 3 Public Primary Certification Autho	Class 3 Public Primary Certificatio	02/08/2028	Authentification du	Ver
> Commendes d'inscription de certificat	COMODO RSA Certification Authority	COMODO RSA Certification Auth	19/01/2038	Authentification du	Sec
> 📫 Racines de confiance de carte à puce	🔄 Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Enregistrement des	Mie
> Périphériques approuvés	📮 demo.atmosylva.com	demo.atmosylva.com	27/10/2022	<tout></tout>	<a td="" 🗸<="">
	<				>
Le magasin Autorités de certification racines de confiance	e contient 90 certificats.				

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.

 \times

_

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

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

- ✓ actions_module
- ✓ alias module
- ✓ allowmethods_module
- ✓ asis_module
- ✓ auth_basic_module
 ✓ auth_digest_module auth_form_module authn_anon_module
- ✓ authn_core_module authn_dbd_module authn_dbm_module
- ✓ authn_file_module authn_socache_module authnz_fcgi_module authnz_ldap_module authz_dbd_module authz_dbm_module
- authz_groupfile_module authz_owner_module
- ✓ authz_user_module
 ✓ autoindex_module
 brotli_module
 buffer module
- ✓ cache_disk_module
 ✓ cache module
- cache_socache_module cern_meta_module

cgi_module
 charset_lite_module
 data_module
 dav_fs_module
 dav_lock_module
 dav_module
 dbd_module
 deflate_module

- ✓ dir_module dumpio_module
 ✓ env_module
- expires_module ext_filter_module
- ✓ file_cache_module filter_module headers_module heartbeat_module heartmonitor_module http2_module ident_module imagemap_module
- ✓ include_module info_module

Idap_module

✓ isapi_module
 Ibmethod_bybusyness_module
 Ibmethod_byrequests_module
 Ibmethod_bytraffic_module
 Ibmethod_heartbeat_module

 ✓ log_config_module log_debug_module log_forensic_module logio_module lua_module macro_module md_module mime_magic_module
 ✓ mime_module

✓ negotiation_module proxy_ajp_module proxy_balancer_module proxy_connect_module proxy_express_module proxy_fcgi_module proxy_ftp_module proxy hcheck module proxy_html_module proxy_http2_module proxy_http_module proxy_module proxy_scgi_module proxy_uwsgi_module proxy_wstunnel_module ratelimit_module reflector module remoteip_module reqtimeout_module request_module

- ✓ rewrite_module sed_module session cookie module session_crypto_module session_dbd_module session_module ✓ setenvif module slotmem plain module slotmem_shm_module socache_dbm_module socache_memcache_module socache redis module socache_shmcb_module spelina module ssl_module status module substitute module unique_id_module ✓ userdir_module usertrack_module version_module
- ✓ vhost_alias_module watchdog_module xml2enc_module
 Module irréversible
 i) authz_core_module
 ii) authz_host_module
 - php7_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
0 = 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 une 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.



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>
```

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.



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.

Póm	iian	at ou
requ	uyn	ui.eu

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 ».

GR Certificat	Х
Général Détails Chemin d'accès de certification	
Informations sur le certificat	
Vous ne pouvez pas faire confiance à ce certificat racine de l'autorité de certification. Pour activer la confiance, installez ce certificat dans le magasin d'autorités de certification de la racine de confiance.	
	_
Délivré à : helloworld	
Délivré par helloworld	
Valide du 09/04/2022 au 09/03/2024	
Installer un <u>c</u> ertificat <u>D</u> éclaration de l'émetteu	r
OK	

Cliquer sur « Installer un certificat ...»

X

← 🚂	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
<u> </u>
O Ordinateur local

Cliquez sur Suivant pour continuer.

<u>S</u> uivant Annuler

Laissez « Utilisateur actuel », Suivant

 \times

← *§* 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.

 \bigcirc Sélectionner a<u>u</u>tomatiquement le magasin de certificats en fonction du type de certificat

Placer tous les certificats dans le magasin suivant



Parcourir...

<u>S</u> uivant	Annuler

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

Sélectionner un magasin de certificats	\times
<u>S</u> électionnez le magasin de certificats que vou voulez utiliser.	S
Personnel	~
	onf
Confiance de l'entreprise	
	es
Éditeurs approuvés	
Certificats non autorisés	× .
<	>
Afficher les magasins physiques	
OK Ann	uler

Mettre dans « Autorité de certification racines de confiance ».

Х

← *§* 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.

 \bigcirc Sélectionner a<u>u</u>tomatiquement 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...

<u>S</u> uivant	Annuler

Cliquez sur « Suivant »

Péar	iian	iat.ei	I
1			-

 \times

← 🔄 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 Contenu	Autorités de certification racines de co Certificat
<	>

Terminer Annuler	
<u>i</u> enniner Annuer	iner Annuler

Terminer.

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

Avertissement de sécurité				
	Vous allez installer un certificat d'une autorité de certification qui dit représenter : helloworld Windows ne peut pas vérifier que le certificat provient vraiment de « helloworld ». Nous vous recommandons d'en vérifier l'origine en contactant « helloworld ». Le numéro suivant vous aidera dans cette opération :			
	Empreinte numérique (sha1) : 6FB35D64 79DD3C78 BB4F8484 6C873760 5A5DC5E7			
	Avertissement : Si vous installez ce certificat racine, Windows fait automatiquement confiance à tous les certificats émis par cette autorité de certification. L'installation d'un certificat dont l'empreinte numérique n'est pas vérifiée constitue un risquSi vous cliquez sur « Oui », vous acceptez ce risque. Voulez-vous installer ce certificat ?			
	<u>O</u> ui <u>N</u> on			

Oui



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

L'alerte n'est plus présente.

Péquignat.eu	Let's build our future!	ur future!		Version 1.0 Le 08/10/2022		
🔲 🕒 https://hello	world × +					×
$\leftarrow \rightarrow$ C	https://helloworld	A»	í e	∱ @	?	
Hello World						

IV.Sources d'Informations

#	Source	Lien
[S1]	TLS Wikipedia.org	https://fr.wikipedia.org/wiki/Transport_Layer_Security

V. Fin du document