

# TLS/HTTPS : Au-delà du certificat X.509 <sup>1</sup>



9 octobre 2019

---

<sup>1</sup><https://romain.blogreen.org/files/tls-https-au-dela-du-certificat-x-509.pdf>

DE LONG I  
NS BPOCHE  
OMONBS



de dda qes Polue  
su zeluce de b  
sur d' lles dans les 2  
87 Bureaux de Poste



Rechercher



**VbbEz D.OEbbez**

**OEBBEz D.EWbGOI**

**OPT.PF**  
 J'aime cette Page

Soyez le premier de vos amis à aimer ça.

**LANCEZ LE F&F**  
  
**A LA LIBRE  
TESZ D.EFCIBIGITE**

**ASSURANCE SCOLAIRE**  
**KEWBOBZES**  
**AOZ IMAZ WIFON**

**Téléphonie fixe**

- Sabonner
- ouvrir une ligne
- Nos Formules
- Forfaits
- Formules libres
- Cartes prépayées
- Déjà abonné ?
- Changer de formule
- Assistance

**Courier**

Envoi de courrier

- vers la Polynésie
- vers l'international
- les services plus

Produits et services

- Ouvrir une Boîte Postale
- Prêt à poster
- Emballages
- Tracking Chronopost

**Services financiers**

Devenir client

- Ouvrir un compte

Produits et services

- Moyens de paiement
- Envoyer de l'argent

Déjà client ?

- Consultez votre compte
- Assistance

**Gérez votre consommation**

- Simulateur tarifaire
- Forfaits bloqués (OPTCOMPTE)
- OPTCARD
- Web Voscoms

**TIME**

La liberté d'une formule sans engagement Vous ne payez que ce que vous téléphonez

**Accès Client**

- Web Voscoms
- Web CCP

**Suivi des envois**

numéro de suivi

**Nos Agences**

Plus de 80 agences à votre service sur toute la Polynésie

- Trouver une agence

**Besoin d'aide ?**

- Toute l'assistance
- Top pages assistance :**
- Téléphoner à l'étranger



Caisse de Prévoyance Sociale  
Te Fare Tuarua'o  
Votre Protection Sociale,  
Notre Métier

[Accueil](#)

[Assuré](#)

[Employeur](#)

[Professionnel de Santé](#)

[La CPS et la PSG](#)

[Espace Presse](#)

[Carrières](#)

[Aide](#)



Pour en savoir plus

VOUS PARTEZ À LA RETRAITE

Les nouvelles modalités  
de départ à la retraite

ASSURÉ

EMPLOYEUR

PROFESSIONNEL DE  
SANTÉ

## ESPACE CLIENT

- Mon compte en ligne
- Mes alertes SOCMS
- Ma carte AMEX
- Mes relevés de comptes

## BANQUE PRATIQUE

- Banque à distance
- Réseau d'agences
- Faire opposition
- Sécurité
- Téléchargements
- Glossaires
- Guides de la FBF
- Charte de la Médiation - Réclamations
- Contactez-nous
- Fonds de Garantie des Dépôts et de Résolution

## DEVENEZ CLIENT

- Ouvrir un compte
- Ouvrir un compte à distance
- Rencontrer un conseiller

## CASDEN

- Présentation de la CASDEN
- L'épargne
- Les points
- Emprunter selon les conditions CASDEN

## TARIFS

- Tarifs en vigueur



## CRÉDIT ET ASSURANCE AUTO

&gt;&gt; En savoir plus

## ACTUALITÉS

## ALERTE PHISHING

## AVERTISSEMENT

Nous vous informons que le nom de la Banque SOCREDO est utilisé pour une tentative de phishing par email.

Le mail prétend que votre carte est bloquée pour des achats sur internet et vous invite à "adhérer" à une prétendue nouvelle réglementation.

Il s'agit d'une tentative de récupération de vos données sensibles.

Pour rappel, jamais une banque ne vous demandera de fournir de tels renseignements par email.

- Ne cliquez sur aucun lien
- Détruisez le mail

&gt;&gt; Lire la suite

## Informations clients - WEBSOC

Depuis hier, l'accès à Websoc subit un dysfonctionnement aléatoire et qui n'est pas encore résolu.

&gt;&gt; Lire la suite

## INFO CONSEILS : BANQUE A DISTANCE

# Romain Tartière

Infâme (Free)BSDiste (romain@)

Je casse des trucs

Expérience PKI :

- ▶ Grilles
- ▶ CPS
- ▶ HDS
- ▶ opus-codium/pakotoa
- ▶ Puppet

« C'est peut-être évident pour vous, mais ça ne l'est pas pour tout le monde »



# Plan

TLS Crash Course

Se protéger des menaces qui ciblent les internautes

Se protéger des menaces qui ciblent les fournisseurs de services

Se protéger en temps qu'internaute

Configurations pour les développeur·ses et administrateur·trices systèmes

Éviter les problèmes

# Plan

## TLS Crash Course

Qu'est-ce-que TLS ?

Anatomie d'une clé RSA

Anatomie d'un certificat X.509

Établissement d'une connexion TLS

## Qu'est-ce-que TLS ?

**RFC 2246** The TLS Protocol Version 1.0 (1999)

<https://tools.ietf.org/html/rfc2246>

**RFC 4346** The Transport Layer Security (TLS) Protocol Version 1.1 (2006)

<https://tools.ietf.org/html/rfc4346>

**RFC 5246** The Transport Layer Security (TLS) Protocol Version 1.2 (2008)

<https://www.bortzmeyer.org/5246.html>

<https://tools.ietf.org/html/rfc5246>

**RFC 8446** The Transport Layer Security (TLS) Protocol Version 1.3 (2018)

<https://www.bortzmeyer.org/8446.html>

<https://tools.ietf.org/html/rfc8446>

*The Rocky Road to TLS 1.3 and better Internet Encryption*, Hanno Böck

[https://media.ccc.de/v/35c3-9607-the\\_rocky\\_road\\_to\\_tls\\_1\\_3\\_and\\_better\\_internet\\_encryption](https://media.ccc.de/v/35c3-9607-the_rocky_road_to_tls_1_3_and_better_internet_encryption)



# Anatomie d'une clé RSA

Deux parties :

1. Une **clé publique** ;
2. Une **clé privée**.

## Anatomie d'un certificat X.509

- ▶ Un sujet (**subject**, e.g. /CN=example.com);
- ▶ Un émetteur (**issuer**, e.g. /CN=Root CA/O=Acme Inc);
- ▶ Une date de début de validité (**not-before**);
- ▶ Une date de fin de validité (**not-after**);
- ▶ Une clé publique (celle du *sujet*);
- ▶ Des extensions ;
- ▶ etc.

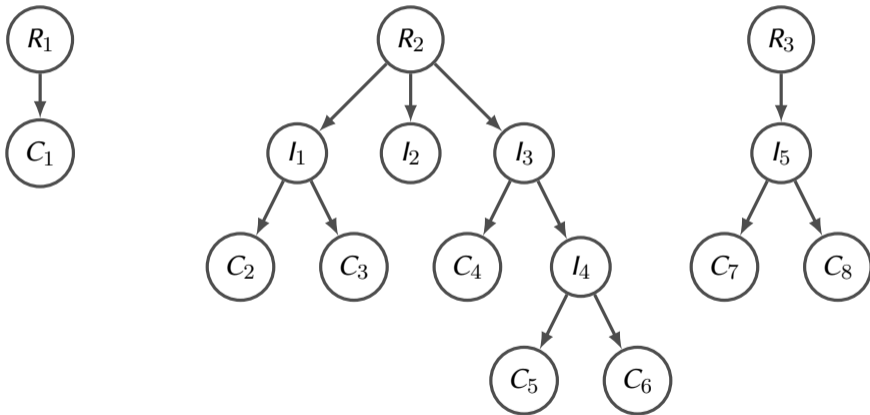
Le tout signé avec la clé privée de l'*émetteur*.

## Anatomie d'un certificat X.509

L'*émetteur* joue le rôle de **tiers de confiance**.

Lorsque le *sujet* et l'*émetteur* sont identiques, on parle de **certificat auto-signé**.

## Anatomie d'un certificat X.509



# Établissement d'une connexion TLS

1. Handshake TCP ;
2. Communication en clair et demande de chiffrement (STARTTLS) ;
3. Handshake TLS ;
  - ▶ Choix de la version de TLS utilisée ;
  - ▶ Choix des algorithmes de chiffrement ;
  - ▶ Échange des certificats ;
  - ▶ Vérification de la validité de la chaîne de certification :
    - ▶ Identité du serveur ;
    - ▶ Certificats en cours de validité ;
    - ▶ Certificats non révoqués ;
    - ▶ Possibilité de remonter du certificat jusqu'à une AC de confiance.
  - ▶ Création d'une clé de session.
4. Communication chiffrée avec la clé de session.

# Établissement d'une connexion TLS

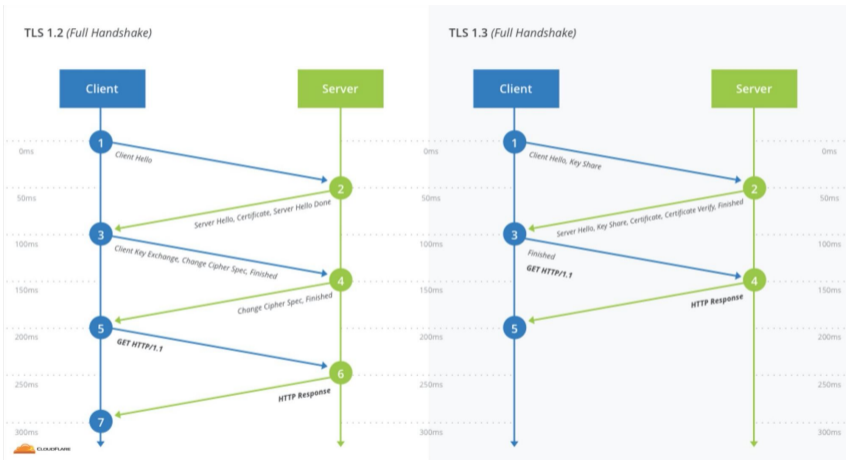


Illustration : CloudFlare

# Plan

## Se protéger des menaces qui ciblent les internautes

- Redirigier HTTP vers HTTPS

- Activer HTTP Strict Transport Security (HSTS)

- Précharger HSTS

- Configurer TLS 1.2 et supérieur uniquement

- Configurer la confidentialité persistante

- Vérifier le support d'Online Certificate Status Protocol (OCSP)

- Configurer l'agrafage OCSP (OCSP Stapling)

- Demander OCSP Must Staple

## Rediriger HTTP vers HTTPS

Un seul hôte virtuel qui écoute sur le port 80.

```
<VirtualHost *:80>  
  RewriteEngine On  
  RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301]  
</VirtualHost>
```

301 : *Moved Permanently*



## Activer HTTP Strict Transport Security (HSTS)

```
Strict-Transport-Security:
```

```
max-age=500max-age=3600max-age=63072000;includeSubDomains
```

```
https://ssl-config.mozilla.org/
```

## Précharger HSTS

```
Strict-Transport-Security: max-age=63072000;includeSubDomains;preload
```

Puis faire une demande : <https://hstspreload.org/>

## Configurer TLS 1.2 et supérieur uniquement

### *Recommandations de sécurité relatives à TLS, ANSSI*

<https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-tls/>

Extrait des recommandations (2016, donc antérieures à TLS 1.3) :

- R1** Restreindre la compatibilité en fonction du profil des clients ;
- R2** Utiliser des composants logiciels à jour ;
- R3** Utiliser uniquement TLS 1.2 ;
- R3-** Privilégier TLS 1.2 et tolérer TLS 1.1 et TLS 1.0 ;
- R3--** Privilégier TLS 1.2 et tolérer TLS 1.1, TLS 1.0 et SSLv3.

## Configurer TLS 1.2 et supérieur uniquement

En 2019 : Privilégier TLS 1.3 et tolérer TLS 1.2

```
SSLProtocol TLSv1.3 +TLSv1.2
```

<https://ssl-config.mozilla.org/>

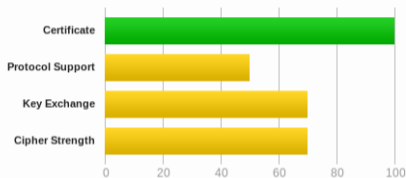
# Configurer TLS 1.2 et supérieur uniquement

## Summary

Overall Rating



No support for TLS 1.2, which is the only secure protocol version. [MORE »](#)



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. [MORE INFO »](#)

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.0. Grade will be capped to B from March 2020. [MORE INFO »](#)

# Configurer la confidentialité persistante

Forward Secrecy (FS) / Perfect Forward Secrecy (PFS)

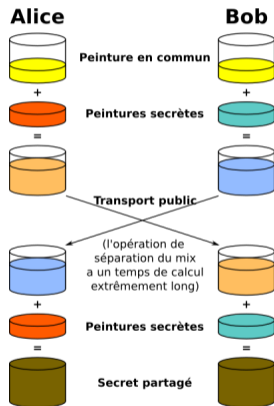
Que se passe-t-il si le serveur est compromis ?

Que se passe-t-il si la clé privée est compromise ?

Que se passe-t-il si les clés de sessions sont compromises ?

**TLS 1.3** Systématique ;

**TLS ≤ 1.2** Il faut prioriser les algorithmes de chiffrement qui le permettent.



Infographie : A.J. Han Vinck,  
Flugaal, Dereckson

# Configurer la confidentialité persistante

Forward Secrecy (FS) / Perfect Forward Secrecy (PFS)

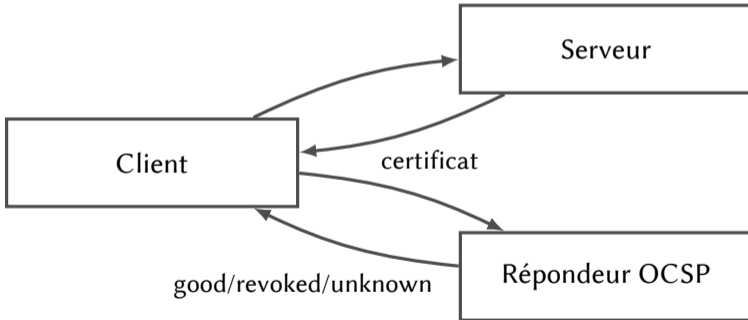
```
SSLHonorCipherOrder    off
SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:
                        :...:DES-CBC3-SHA
```

<https://ssl-config.mozilla.org/>

## Vérifier le support d'Online Certificate Status Protocol (OCSP)

RFC 6960

<https://www.bortzmeyer.org/6960.html>

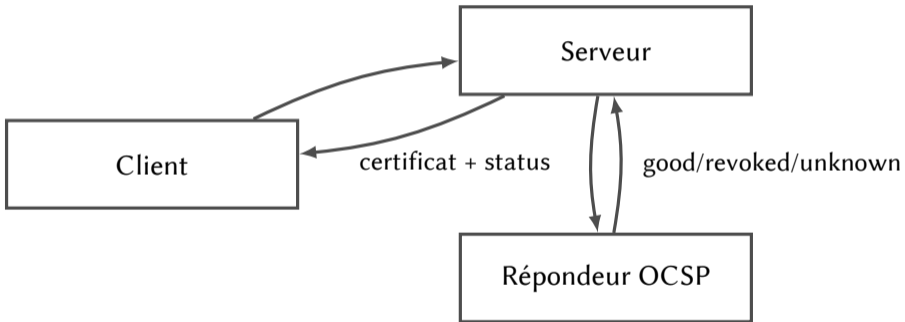




## Vérifier le support d'Online Certificate Status Protocol (OCSP)

```
% openssl x509 -noout -ocsp_uri -in cert.pem  
http://ocsp.int-x3.letsencrypt.org
```

## Configurer l'agrafage OCSP (OCSP Stapling)



## Configurer l'agrafage OCSP (OCSP Stapling)

```
SSLUseStapling On  
SSLStaplingCache "shmcb:logs/ssl_stapling(32768)"
```

<https://ssl-config.mozilla.org/>

## Demander OCSP Must Staple

Extension X.509 définie dans la RFC 6066 (Section 8) :  
`https://tools.ietf.org/html/rfc6066#section-8`

```
OCSP_MUST_STAPLE='yes'
```

# Plan

## Se protéger des menaces qui ciblent les fournisseurs de services

- Configurer DNS Certification Authority Authorization (CAA)

- Configurer DNS-based Authentication of Named Entities (DANE)

- Configurer HTTP Public Key Pinning (HPKP)

- Conserver la clé privée lors des renouvellements

- Exiger Certificate Transparency

# Configurer DNS Certification Authority Authorization (CAA)

RFC 6844

<https://www.bortzmeyer.org/6844.html>

Vérification obligatoire depuis 8 septembre 2017

```
example.com.          CAA 0 issue "letsencrypt.org"  
example.com.          CAA 0 issuewild ";"  
example.com.          CAA 0 iodef "mailto:security@example.com"
```

## Configurer DNS-based Authentication of Named Entities (DANE)

RFC 6698

<https://www.bortzmeyer.org/6698.html>

```
@           MX      10 mx
mx          A       88.161.59.228
mx          AAAA    2a01:e35:8a13:be40:6631:50ff:fed3:111d
_25._tcp.mx TLSA    3 1 1 d8aac0d602e5532136ffb9e368fbc3c9a7a4b694340800
                    b08731bcc09099a925
```

Nécessite que la zone soit signée par DNSSEC

## Configurer HTTP Public Key Pinning (HPKP)

RFC 7469

<https://www.bortzmeyer.org/7469.html>

Similaire à DANE mais dans HTTPS.

```
Public-Key-Pins: max-age=604800; pin-sha256="QWgsIGlsIGZhdXQgcXVlIGpl  
IGTDqXBsb21lIMOnYSA/"
```

Trust On First Use (TOFU)



## Conserver la clé privée lors des renouvellements

```
PRIVATE_KEY_RENEW='no'
```

# Exiger Certificate Transparency

RFC 6962

<https://www.bortzmeyer.org/6962.html>

<https://crt.sh/>

Criteria Identity = 'www.tefenua.gov.pf'

Certificates	<a href="#">crt.sh ID</a>	<a href="#">Logged At</a> ↑	<a href="#">Not Before</a>	<a href="#">Not After</a>	<a href="#">Issuer Name</a>
	<a href="#">1817391835</a>	2019-08-28	2019-08-15	2021-08-14	<a href="#">C=FR, O=DHIMYOTIS, OU=0002.48146308100036, 2.5.4.97=NTRFR-48146308100036, CN=Certigna Services CA</a>
	<a href="#">1772532303</a>	2019-08-15	2019-08-15	2021-08-14	<a href="#">C=FR, O=DHIMYOTIS, OU=0002.48146308100036, 2.5.4.97=NTRFR-48146308100036, CN=Certigna Services CA</a>
	<a href="#">834601991</a>	2018-10-08	2018-10-05	2020-10-04	<a href="#">C=FR, O=Certinomis, 2.5.4.97=NTRFR-433998903, CN=Certinomis - Web CA</a>
	<a href="#">821824312</a>	2018-10-05	2018-10-05	2020-10-04	<a href="#">C=FR, O=Certinomis, 2.5.4.97=NTRFR-433998903, CN=Certinomis - Web CA</a>
	<a href="#">485690714</a>	2018-05-25	2018-05-21	2018-10-06	<a href="#">C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte RSA CA 2018</a>
	<a href="#">475771697</a>	2018-05-21	2018-05-21	2018-10-06	<a href="#">C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte RSA CA 2018</a>
	<a href="#">183044903</a>	2017-08-03	2017-08-03	2018-10-06	<a href="#">C=US, O="thawte, Inc.", CN=thawte SSL CA - G2</a>
	<a href="#">9643786</a>	2015-10-01	2015-09-24	2018-09-23	<a href="#">C=US, O="thawte, Inc.", CN=thawte SSL CA - G2</a>
	<a href="#">5340646</a>	2014-10-22	2014-10-08	2015-10-08	<a href="#">C=US, O="thawte, Inc.", CN=thawte SSL CA - G2</a>
	<a href="#">3023361</a>	2013-11-22	2013-10-17	2014-10-17	<a href="#">C=US, O="Thawte, Inc.", CN=Thawte SSL CA</a>
	<a href="#">493334</a>	2013-03-26	2012-10-16	2013-11-21	<a href="#">C=US, O="Thawte, Inc.", CN=Thawte SSL CA</a>

# Plan

## Se protéger en temps qu'internaute

Accéder aux paramètres avancés de Firefox

Autoriser TLS 1.2 et supérieur uniquement

Désactiver les mécanisme des restauration de sessions

Indiquer explicitement les sites non sécurisés

Désactiver les noms de domaines internationalisés

Tester son navigateur

## Accéder aux paramètres avancés de Firefox

Dans **Firefox**, ouvrir l'URI :

`about:config`

Source : <https://github.com/opus-codium/puppet-firefox/wiki>

## Autoriser TLS 1.2 et supérieur uniquement

```
security.tls.version.min=3
```

Valeurs supportées :

- 1 TLS 1.0 (valeur par défaut)
- 2 TLS 1.1
- 3 TLS 1.2
- 4 TLS 1.3

TLS 1.0 et 1.1 déjà dépréciés dans Firefox Nightly. Suppression en Mars 2020 :

<https://hacks.mozilla.org/2019/05/tls-1-0-and-1-1-removal-update/>

## Désactiver les mécanisme des restauration de sessions

```
security.tls.enable_Ortt_data=false  
security.ssl.enable_false_start=false
```

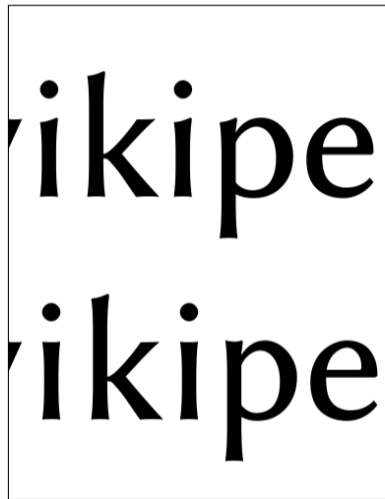
## Indiquer explicitement les sites non sécurisés

```
security.insecure_connection_icon.enabled=true  
security.insecure_connection_icon.pbmode.enabled=true  
security.insecure_connection_text.enabled=true  
security.insecure_connection_text.pbmode.enabled=true
```

## Désactiver les noms de domaines internationalisés

IDN	Punycode
wikipedia.org	wikipedia.org
wikipedia.org	xn-wkd-8cdx9d7hbd.org

```
network.IDN_show_punycode=true
```





# Tester son navigateur

Qualys SSL Labs — Projects / SSL Client Test

<https://www.ssllabs.com/ssltest/viewMyClient.html>

The screenshot shows the Qualys SSL Labs website interface. At the top, there is a navigation bar with the logo and links for Home, Projects, Qualys Free Trial, and Contact. Below the navigation bar, the page title is "SSL/TLS Capabilities of Your Browser" with a link for "Other User Agents". The user agent string is displayed as "Mozilla/5.0 (X11; Linux i686; rv:8.0) Gecko/20100101 Firefox/8.0". The main content area contains several sections:

- Protocol Support:** "Your user agent has good protocol support. Your user agent supports TLS 1.2, which is recommended protocol version at the moment. Experimental: Your user agent supports TLS 1.3."
- Logjam Vulnerability:** "Your user agent is not vulnerable. For more information about the Logjam attack, please go to [weakdh.org](#). To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site."
- FREAK Vulnerability:** "Your user agent is not vulnerable. For more information about the FREAK attack, please go to [www.freakattack.com](#). To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site."
- POODLE Vulnerability:** "Your user agent is not vulnerable. For more information about the POODLE attack, please read [this blog post](#)."
- Protocol Features:** (partially visible)

# Plan

## Configurations pour les développeur·ses et administrateur·trices systèmes

- Configurer son navigateur

- Tester ses services

- Générer des configurations

## Configurer son navigateur

```
security.mixed_content.block_display_content=true
```

# Tester ses services

SSL Server Test (Powered by Qualys SSL Labs)

<https://www.ssllabs.com/ssltest/>

The screenshot shows a Qualys SSL Labs report for the domain <https://www.ssllabs.com/ssltest/>. The report is for the domain [remain.blogreen.org](https://www.ssllabs.com/ssltest/) (IP: 88.161.59.228). The overall rating is **A+**. The report includes a summary section with a bar chart showing scores for Certificate, Protocol Support, Key Exchange, and Cipher Strength, all of which are at 100%. Below the summary, there are several informational bars: 'Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).', 'Experimental: This server supports TLS 1.3 (RFC 8446).', 'HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [SSL INFO](#)', and 'DNS Certification Authority Authorization (CAA) Policy found for this domain. [SSL INFO](#)'. The certificate details section shows 'Certificate #1: RSA 4096 bits (SHA256withRSA)'. A table below provides details for the 'Server Key and Certificate #1', including the Subject (Blogreen.org), Common names (multiple domains), and Alternative names (multiple domains).

Subject	Blogreen.org
Common names	blogreen.org blogreen.org/calendar.blogreen.org/conference.blogreen.org/info.blogreen.org/gf.blogreen.org haxe.blogreen.org/fo.blogreen.org/marvin.blogreen.org/mayville.blogreen.org/packages.blogreen.org phonebook.blogreen.org/projects.blogreen.org/pubsub.blogreen.org/puppetboard.blogreen.org puppetexplorer.blogreen.org/remain.blogreen.org/sign.blogreen.org/status.blogreen.org/vcs.blogreen.org
Alternative names	www.blogreen.org

# Tester ses services

Hardenize

<https://www.hardenize.com/>

The screenshot shows the Hardenize interface for a security report on **blogreen.org**. The report is dated 20 Sep 2019 03:04 UTC. The main section is titled "WEB SECURITY OVERVIEW" and lists several security checks with their status and effort levels:

- HTTPS**: Status: ✔. Description: Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted. Effort: For all sites (Very Important, Medium Effort).
- HTTPS Redirection**: Status: ✔. Description: To deploy HTTPS properly, web sites must redirect all unsafe (plaintext) traffic to the encrypted variant. This approach ensures that no sensitive data is exposed and that further security technologies can be activated. Effort: For all sites (Very Important, Low Effort).
- HTTP Strict Transport Security**: Status: ✔. Description: HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and enforce strict security requirements. Without HSTS, active network attacks are easy to carry out. Effort: For important sites (Very Important, Medium Effort).
- HSTS Preloaded**: Status: ✔. Description: HSTS Preloading is informing browsers in advance about a site's use of HSTS, which means that strict security can be enforced even on the first visit. This approach provides best HTTPS security available today. Effort: For important sites (Very Important, Medium Effort).
- Content Security Policy**: Status: ✔. Description: Content Security Policy (CSP) is an additional security layer that enables web sites to control browser behavior, creating a safety net that can counter attacks such as cross-site scripting. Effort: For important sites (Important, High Effort).

On the left sidebar, various security categories are listed with their status:

- Domain**: Name servers, DNSSEC, CAA (all checked).
- Email**: Mail servers (checked); SECURE TRANSPORT (SMTP): TLS, Certificates, MTA-STS, TLS-RPT, DANE (all checked); AUTHENTICATION AND POLICY: SPF, DMARC (checked).
- WWW**: PROTOCOLS: HTTP (80), HTTPS (443) (both checked).
- SECURE TRANSPORT**: (Section header)

# Tester ses services

ImmuniWeb

`https://www.immuniweb.com/ssl/`

Platform Solutions Compliance Free Security Tests Company Partners More Tests LOGIN

### Summary of blogreen.org:443 (HTTPS) SSL Security Test

blogreen.org was tested 7 times during the last 12 months.

Your final score

Date/Time: September 28th 2019, 23:50  
Source IP: 88.161.59.228:443  
Type: HTTPS

**A+**

Refresh test Download report

<b>PCI-DSS</b> COMPLIANT	<b>WORLD COMPLIANT</b> NO MAJOR ISSUES FOUND	<b>NIST</b> NO MAJOR ISSUES FOUND	<b>Industry Best-Practices Analysis</b> NO ISSUES FOUND	<b>Third-Party Content Analysis</b> NOT FOUND
-----------------------------	---	--------------------------------------	--	--

The server configuration supports only TLSv1.2 and TLSv1.3 protocols, precluding users with older browsers from accessing your website. Information

The server supports the most recent and secure TLS protocol version of TLS 1.3. Good configuration

Quick Start

## Web Security in a Swiss Army Knife

from \$99 per month



# Tester ses services

testssl.sh

<https://github.com/drwetter/testssl.sh>

```

romain@zappy ~ % testsssl.sh blogreen.org
romain@zappy ~ % testsssl.sh blogreen.org
#####
testssl.sh 3.0rc1 from https://testssl.sh/dev/
(©2017 by 2019-09-24 12:55:37)

This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o any WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/

#####

Using "openssl_1.0.2-chaos [1.0.2-0w]" [103 ciphers]
on zappy:/usr/local/openssl-unsafe/bin/openssl
(built: "reproducible build, data unspecified", platform: "BSD-x86_64")

Start 2019-09-24 12:55:37 --> 88.161.59.228:443 (blogreen.org) <-
Further IP addresses: 2a01:c05:b11:b640:6631:59ff:fedc:111d
rDNS (88.161.59.228): blogreen.org.
Service detected: HTTP

Testing protocols via sockets except NNTP/ALPN.
SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    offered (OK): Final
NPN/SPDY   not offered
ALPN/HTTP2 1, http/1.1 (offered)

Testing cipher categories.
NULL ciphers (no encryption)      not offered (OK)
Anonymous NULL ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADR=HLL)       not offered (OK)
LOW: 0# 0#1 + 0#5, RC2,4) (w/o export) not offered (OK)
Triple DES ciphers / IDEA         not offered (OK)
Average! SEED + 128-256 bit CBC ciphers      not offered
Strong encryption (AEAD ciphers)    offered (OK)

Testing robust (perfect) forward secrecy (PFS) --- omitting null authentication/encryption/DHES/DHE
PFS is offered (OK)
    TLS_AES_256_GCM_SHA384
    TLS_CHACHA20_POLY1305_SHA256
    ECDHE-RSA-AES256-GCM-SHA384
    ECDHE-RSA-CHACHA20-POLY1305
    TLS_AES_128_GCM_SHA256
    ECDHE-RSA-AES128-GCM-SHA256
Elliptic curves offered:
    @Proton: 28820041, 30c912171 925519 8440
  
```

# Générer des configurations

<https://ssl-config.mozilla.org/>

## moz://a SSL Configuration Generator

### Server Software

- Apache
- AWS ALB
- AWS ELB
- Caddy
- Dovecot
- HAProxy
- lighttpd
- MySQL
- nginx
- Oracle HTTP
- Postfix
- PostgreSQL
- Traefik (beta)

### Mozilla Configuration

- Modern  
Servers with clients that support TLS 1.3 and don't need backward compatibility
- Intermediate  
General purpose servers with a variety of clients, recommended for almost all systems
- Old  
Compatible with a number of very old clients, and should be used only as a last resort

### Environment

Server Version

OpenSSL Version

### Miscellaneous

HTTP Strict Transport Security  
This also redirects to HTTPS, if possible

OCSP Stapling

## nginx 1.17.0, intermediate config, OpenSSL 1.1.1c

Supports Firefox 27, Android 4.4.2, Chrome 31, Edge, IE 11 on Windows 7, Java 8u31, OpenSSL 1.0.1, Opera 30, and Safari 9

```
# generated 2018-09-24, https://ssl-config.mozilla.org/#server=nginx&server-version=1.17.0&config=intermediate
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    # redirect all HTTP requests to HTTPS with a 301 Moved Permanently response.
    return 301 https://$host$request_uri;
}

server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;

    # certs sent to the client in SERVER_HELLO are concatenated in ssl_certificate
    ssl_certificate /path/to/signed_cert_plus_intermediates;
    ssl_certificate_key /path/to/private_key;
    ssl_session_timeout 1d;
    ssl_session_cache shared:SSL:10m # about 4000 sessions
    ssl_session_tickets off;

    # curl https://ssl-config.mozilla.org/#server=nginx&server-version=1.17.0&config=intermediate
    ssl_dhparam /path/to/dhparam.pem;

    # intermediate configuration
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-GCM-SHA256:ECDHE-ECDSA-GCM-SHA256:ECDHE-RSA-GCM-SHA256:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-GCM-SHA256:ECDHE-ECDSA-GCM-SHA256:ECDHE-RSA-GCM-SHA256
```



# Plan

## Éviter les problèmes

- Fournir une chaîne de certification complète

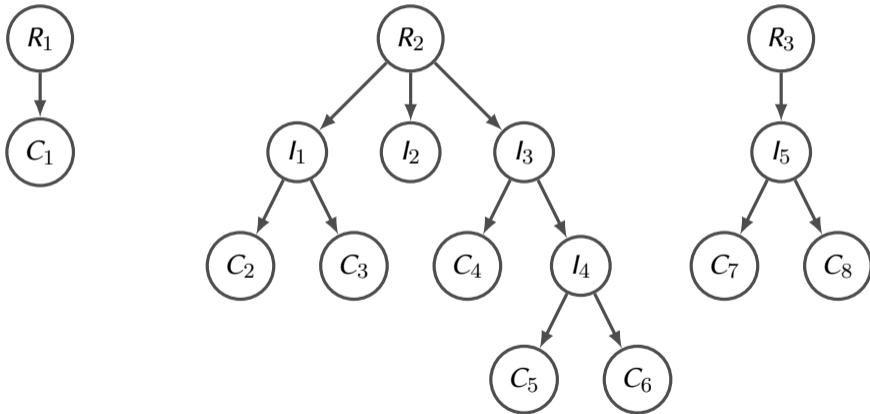
- Monitorer les certificats

- Ne patchez pas Apache

- Ne patchez pas OpenSSL

- Cloudflare ?

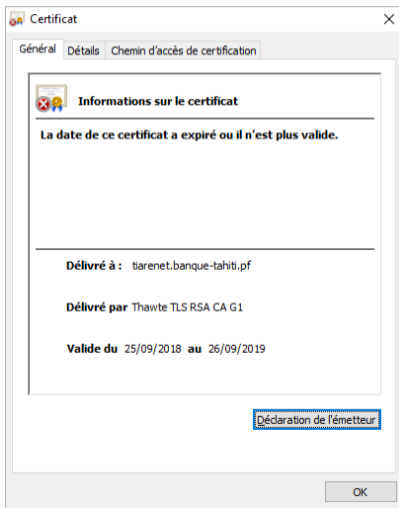
## Fournir une chaîne de certification complète



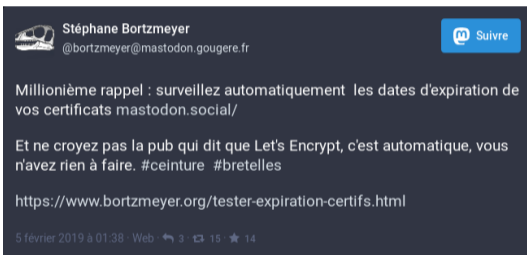
## Fournir une chaîne de certification complète

```
SSLCertificateChainFile "/usr/local/etc/dehydrated/certs/example.org/  
chain.pem"
```


# Monitorer les certificats



## Monitorer les certificats



A screenshot of a Mastodon post by Stéphane Bortzmeyer (@bortzmeyer@mastodon.gougere.fr). The post is in French and discusses monitoring certificates. It includes a link to a website for testing certificate expiration and shows engagement statistics (3 replies, 15 retweets, 14 likes).

 Stéphane Bortzmeyer  
@bortzmeyer@mastodon.gougere.fr [Suivre](#)

Millionième rappel : surveillez automatiquement les dates d'expiration de vos certificats mastodon.social/

Et ne croyez pas la pub qui dit que Let's Encrypt, c'est automatique, vous n'avez rien à faire. #ceinture #bretelles

<https://www.bortzmeyer.org/tester-expiration-certifs.html>

5 février 2019 à 01:38 · Web · 3 · 15 · 14

`https://mastodon.gougere.fr/@bortzmeyer/101539298162775223`

## Monitorer les certificats

Les certificats expirent (*not-after*).

Lorsqu'un certificat est renouvelé, les services qui l'utilisent doivent le recharger.

Le problème existe aussi pour les certificats intermédiaires.

`https://www.bortzmeyer.org/tester-expiration-certifs.html`

TLS Crash Course  
○○○○○○○

Protéger ses visiteurs  
○○○○○○○○○○○○○○

Protéger son infrastructure  
○○○○○

Se protéger  
○○○○○

Pour the IT crowd  
○○○○○

Éviter les problèmes  
○○○○●○○

# Ne patchez pas Apache

TLS Crash Course  
○○○○○○○

Protéger ses visiteurs  
○○○○○○○○○○○○○○

Protéger son infrastructure  
○○○○○

Se protéger  
○○○○○

Pour the IT crowd  
○○○○○

Éviter les problèmes  
○○○○○●○

# Ne patchez pas OpenSSL



TLS Crash Course  
○○○○○○○

Protéger ses visiteurs  
○○○○○○○○○○○○○○

Protéger son infrastructure  
○○○○○

Se protéger  
○○○○○

Pour the IT crowd  
○○○○○

Éviter les problèmes  
○○○○○○●

# Cloudflare ?

Prochain rendez-vous :

Distribution de la confiance dans les infrastructures à clés publiques

*Gaëtan Bisson, Romain Tartière*



<https://www.clusir-tahiti.org/>