TLS/HTTPS : Au-delà du certificat X.509 [1]

9 octobre 2019

[1] https://romain.blogreen.org/files/tls-https-au-dela-du-certificat-x-509.pdf

Particulier | Pro/Entreprise | Groupe OPT | Agences | Assistance | Actualités

Rechercher

TELECOM | POSTE | BANQUE

Téléphonie fixe

Sabonner
- ouvrir une ligne

Nos Formules
- Forfaits
- Formules libres
- Cartes prépayées

Déjà abonné ?
- Changer de formule
- Assistance

Courrier

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
- WebVoscoms

TIME

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

VAPEURS D'OPTIQUE

OFFRES D'EMPLOI

OPT.PF

J'aime cette Pag

Soyez le premier de vos amis à aimer ça.

Accès Client
- WebVoscoms
- WebCCP

Suivi des envois

numéro de suivi

OK

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 Tiurauta'a
Votre Protection Sociale, Notre Métier

Accueil | Assuré | Employeur | Professionnel de Santé | La CPS et la PSG | Espace Presse | Carrières | Aide

Recherche

Pour en savoir plus

VOUS PARTEZ À LA RETRAITE

Les nouvelles modalités de départ à la retraite

ASSURE

EMPLOYEUR

PROFESSIONNEL DE

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

>> 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 invité à "adhérer" à une prétendue nouvelle réglementation.

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

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

- Ne cliquez sur aucun lien
- Détruisez le mail

>> Lire la suite

Informations clients - WEBSOC

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

>> 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 »

Photo : Ollivier Robert

Plan

Plan

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`

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.

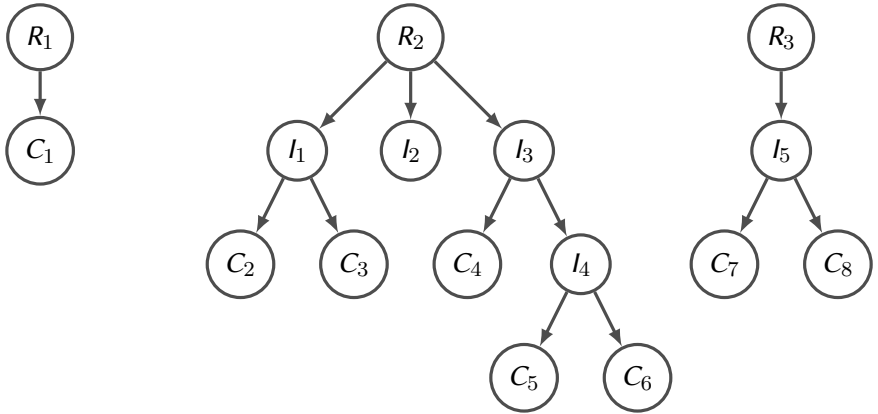
Le tout signé avec la clé privée de l'*émetteur*.

Anatomie d'un certificat X.509

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

Lorsque le *suject* 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 Stappling)
- Demander OCSP Must Stapple

Redirigier 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.

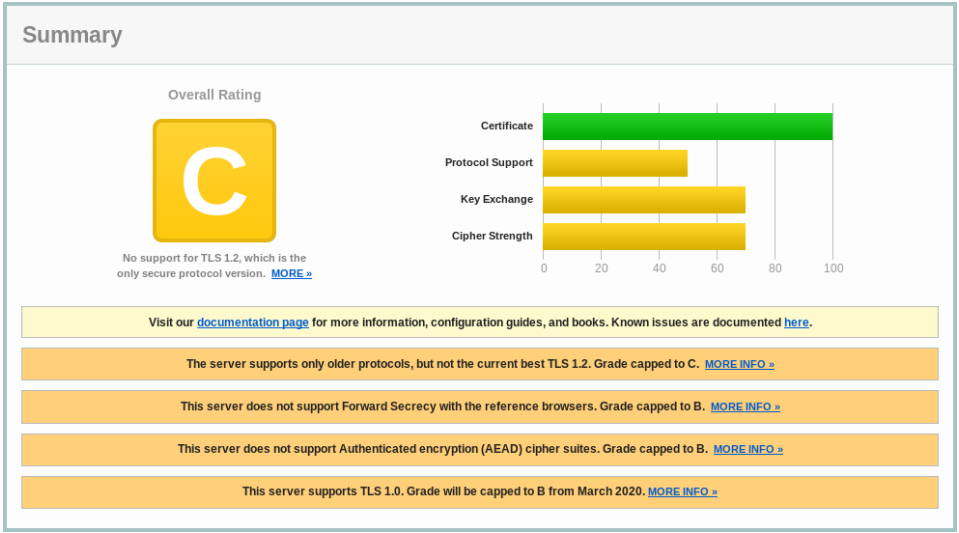
Configurer TLS 1.2 et supérieur uniquement

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



Configurer la confidentialité persistante

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

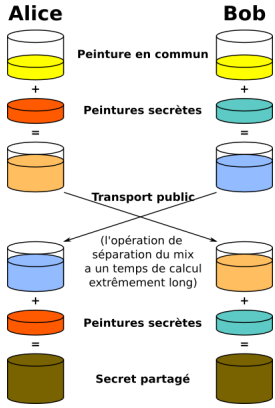
Que se passe-t-il si le serveur est compromis ?

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)

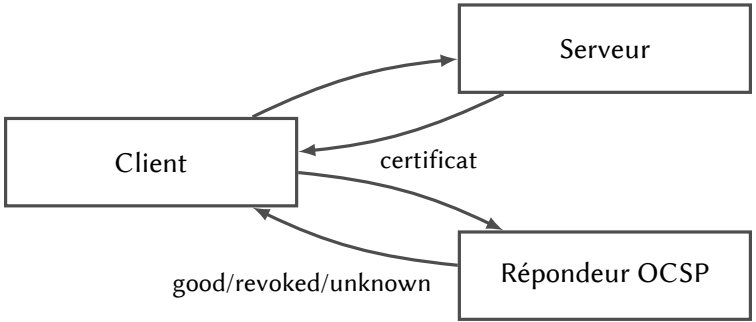
```
SSLHonorCipherOrder     off
SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES12
                        8-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:EC
                        DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA2
                        0-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RS
                        A-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

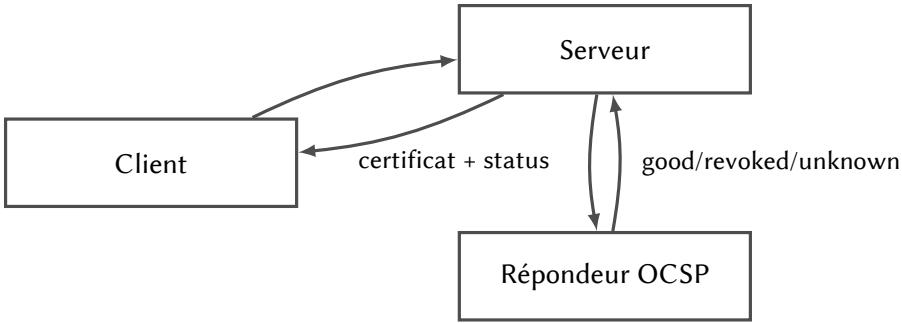
`https://www.bortzmeyer.org/6960.html`



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 Stappling)



Configurer l'agrafage OCSP (OCSP Stappling)

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

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

Demander OCSP Must Stapple

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
                 IGTDqXBsb2llIMOnYSA/"
```

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

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1817391835	2019-08-28	2019-08-15	2021-08-14	C=FR, O=DHIMYOTIS, OU=0002 48146308100036, 2.5.4.97=NTRFR-48146308100036, CN=Certigna Services CA
1772532303	2019-08-15	2019-08-15	2021-08-14	C=FR, O=DHIMYOTIS, OU=0002 48146308100036, 2.5.4.97=NTRFR-48146308100036, CN=Certigna Services CA
834601991	2018-10-08	2018-10-05	2020-10-04	C=FR, O=Certinomis, 2.5.4.97=NTRFR-433998903, CN=Certinomis - Web CA
821824312	2018-10-05	2018-10-05	2020-10-04	C=FR, O=Certinomis, 2.5.4.97=NTRFR-433998903, CN=Certinomis - Web CA
485690714	2018-05-25	2018-05-21	2018-10-06	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte RSA CA 2018
475771697	2018-05-21	2018-05-21	2018-10-06	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte RSA CA 2018
183044903	2017-08-03	2017-08-03	2018-10-06	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
9643786	2015-10-01	2015-09-24	2018-09-23	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
5340646	2014-10-22	2014-10-08	2015-10-08	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
3023361	2013-11-22	2013-10-17	2014-10-17	C=US, O="Thawte, Inc.", CN=Thawte SSL CA
493334	2013-03-26	2012-10-16	2013-11-21	C=US, O="Thawte, Inc.", CN=Thawte SSL CA

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_0rtt_data=false
security.ssl.enable_false_start=false
```

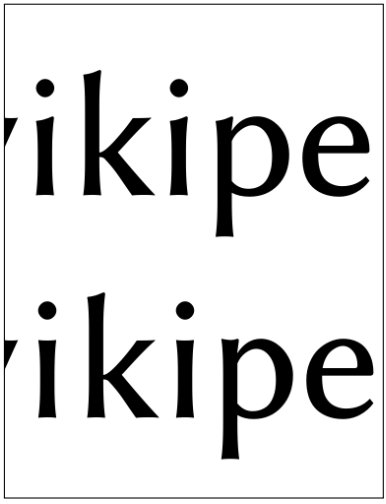
Indiquer explicitement les sites non sécurisés

```
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

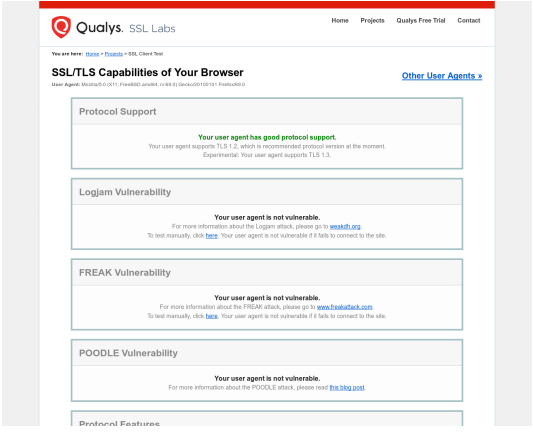
```
network.IDN_show_punycode=true
```



Tester son navigateur

Qualys SSL Labs — Projects / SSL Client Test

`https://www.ssllabs.com/ssltest/viewMyClient.html`



Plan

Configurations pour les développeur·ses et administrateur·trices systèmes

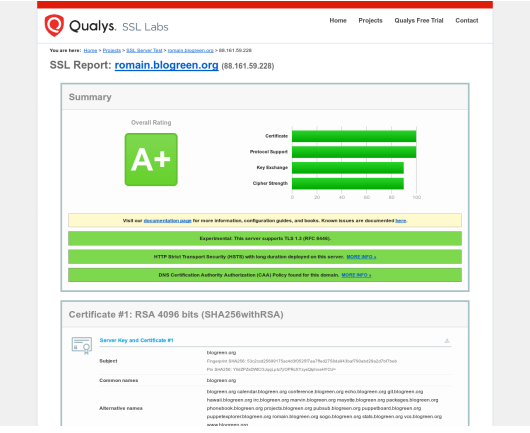
- Configurer son navigateur
- Tester ses services
- Générer des configurations

Configurer son navigateur

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

Tester ses services

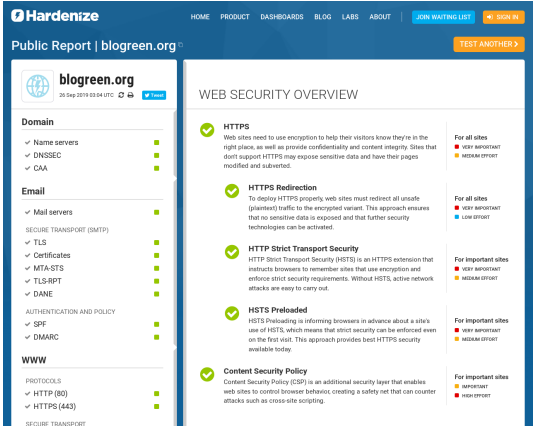
SSL Server Test (Powered by Qualys SSL Labs)
`https://www.ssllabs.com/ssltest/`



Tester ses services

Hardenize

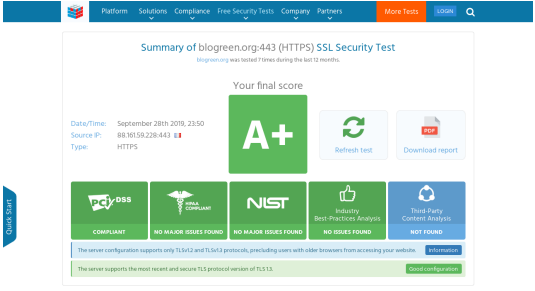
`https://www.hardenize.com/`



Tester ses services

ImmuniWeb

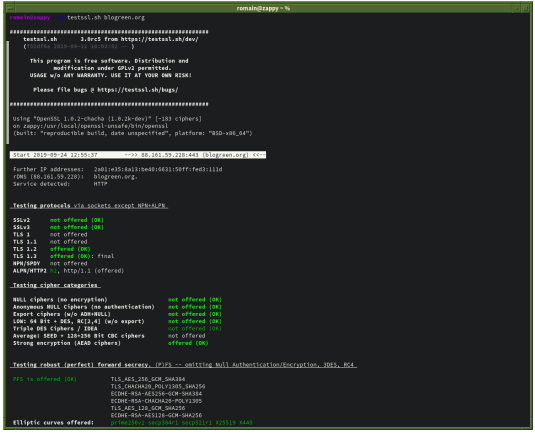
`https://www.immuniweb.com/ssl/`



Tester ses services

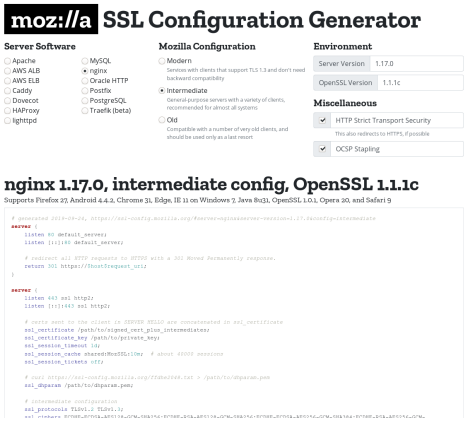
testssl.sh

`https://github.com/drwetter/testssl.sh`



Générer des configurations

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

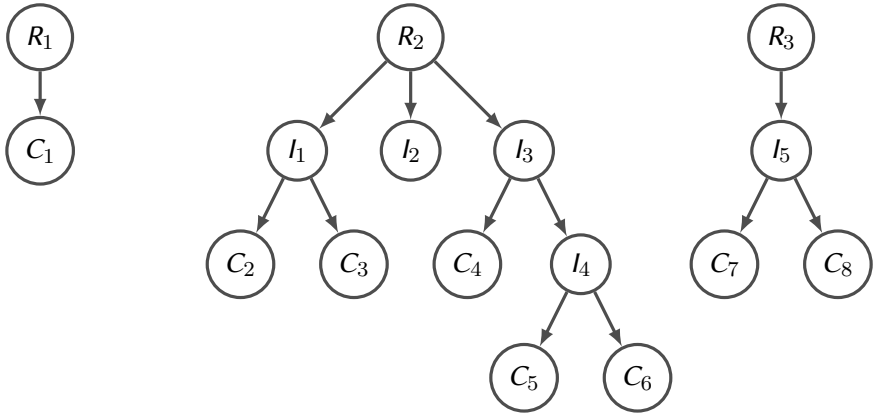


Plan

Éviter les problèmes

- Fournir une chaîne de certification complète
- Monitorer les certificats
- Ne patchez pas Apache
- Ne patchez pas OpenSSL
- Cloudflare ?

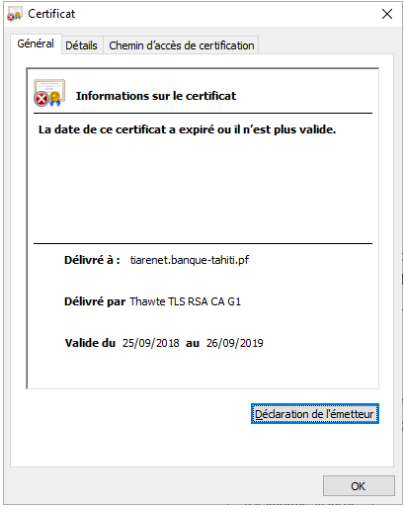
Fournir une chaîne de certification complète



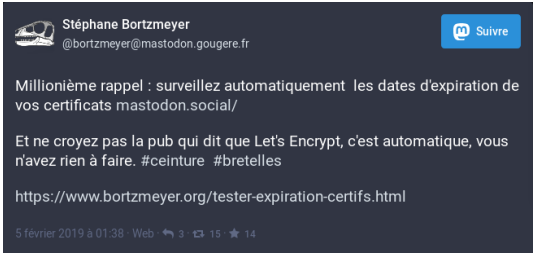
Fournir une chaîne de certification complète

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

Monitorer les certificats



Monitorer les certificats



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`

Ne patchez pas Apache

Ne patchez pas OpenSSL

Cloudflare ?

Prochain rendez-vous :

Distribution de la confiance dans les infrastructures à clés publiques
Gaëtan Bisson, Romain Tartière

`https://www.clusir-tahiti.org/`