NON CLASSIFIÉ

Gouvernement du Canada

Recommandations liées aux certificats de serveur TLS pour les services Web du GC axés sur le public

Le 14 mai 2021

Historique des révisions

No de version du document	Modifications	Date
0,1	Ébauche provisoire préparée par le SCT-DDPI, Cybersécurité.	Le 16 mars 2018
0,2	Intégration de la rétroaction à la suite de l'examen par les pairs de la première ébauche – plusieurs questions en attente de résolution, comme l'indiquent les commentaires dans la marge et les espaces réservés dans le corps principal.	Le 30 avril 2018
0,3	Intégration de la rétroaction à la suite à l'examen par les pairs de la deuxième ébauche, révision de la section 3, on a apporté un certain nombre d'améliorations dans tout le document, changement du titre du document.	Le 28 mai 2018
0,4	Amélioration des documents liés à l'affichage du navigateur avec des renseignements supplémentaires sur les tendances de l'industrie; particulièrement en ce qui concerne Google Chrome. Des précisions ont été apportées au sujet des AC recommandées qui laissent la porte ouverte à d'autres approches ou recommandations à l'avenir. Nous avons apporté diverses améliorations et précisions en réponse à des commentaires supplémentaires.	Le 13 août 2018
1,0	On a apporté des précisions supplémentaires et ajouté une liste de vérification consolidée des exigences de conformité liées aux AC à l'annexe B.	Le 27 août 2018
1,1	Actualisation du document pour le mettre à jour, regroupement de certains des détails plus techniques, suppression de l'annexe B.	Le 14 mai 2021

Table des matières

1. Introduction 1
2. Considérations liées au certificat du serveur TLS 2
2.1 Certificats de clé publique 2
2.2 Autorités de certification (AC) 4
2.3 Responsabilités liées aux sites Web du GC 4
3. Sommaire et recommandations 6
4. Références 7
Annexe A – Chiffrons! (Let's Encrypt) 8

Acronymes et abréviations

ACME	Automated Certificate Management Environment
AC	Autorité de certification
CA/B	Certification Authority and Browser (Forum)
DDPI	Direction du dirigeant principal de l'information
LCR	Liste des certificats révoqués
CST	Centre de la sécurité des télécommunications
TC	Transparence du certificat
DV	Domaine validé
EV	Validation étendue
FIPS	Federal Information Processing Standard (É.-U.)
GC	Gouvernement du Canada
HSM	Module de sécurité du matériel
HSTS	HTTP Strict Transport Security
HTTP	Protocole de transfert hypertexte
HTTPS	Protocole de transfert hypertexte sécurisé
IETF	Internet Engineering Task Force
ISRG	Groupe de recherche sur la sécurité Internet
TI	Technologie de l'information
ITSP	Publication relative à la sécurité des technologies de l'information
OCSP	Online Certificate Status Protocol
OV	Organisation validée
ICP	Infrastructure à clé publique
DC	Demande de commentaires
SCT	Horodatage du certificat signé
SPC	Services partagés Canada
SCT	Secrétariat du Conseil du Trésor du Canada
TLS	Sécurité de la couche de transport

1. Introduction

Tous les sites Web externes du gouvernement du Canada (GC)[1] doivent prendre en charge le protocole HTTPS (Protocole de transfert hypertexte sécurisé). Le protocole HTTPS combine le protocole HTTP avec le protocole TLS (Sécurité de la couche de transport) qui assure l'intégrité et la confidentialité des données entre un navigateur Web et un serveur Web.

Afin d'activer le protocole HTTPS, les sites Web publics du GC doivent obtenir des certificats de serveur TLS. Le présent document décrit divers aspects liés aux certificats de serveur TLS et détermine les exigences minimales associées au type et au contenu de certificat, à la conformité des autorités de certification (AC) et aux responsabilités du site Web. Des recommandations concernant le type des certificats à utiliser et l'emplacement pour les obtenir sont également fournies.

[1] Un site Web externe du GC est un site Web du GC qui fournit des renseignements ou des services au grand public.

2. Considérations liées au certificat du serveur TLS

2.1 Certificats de clé publique

Essentiellement, un certificat de clé publique (ci-après dénommé certificat) est une structure de données qui est signée par voie numérique par l'autorité de certification (AC) émettrice. Les renseignements contenus dans le certificat comprennent le nom de l'entité associée au certificat, le nom de l'AC émettrice, la période de validité, l'objet et la clé publique correspondant à la clé privée associée.

Utilisés conjointement avec le protocole TLS, les certificats de serveur permettent d'authentifier le serveur Web[2] et d'établir une session sécurisée entre un navigateur Web et un serveur Web qui assure la confidentialité et l'intégrité des données pendant toute la durée de la séance.

2.1.1 Types de certificats

Il existe trois types de certificats de serveur en fonction du niveau de validation avant l'émission initiale :

1) Un certificat de domaine validé (DV) – L'AC émettrice vérifie le contrôle par l'entité de demande des domaines précisés. Dans ce cas, l'émission des certificats est relativement rapide et peut être entièrement automatisée.
2) Un certificat d'organisation validée (OV) – L'AC émettrice vérifie le contrôle d'un organisation sur les domaines indiqués et inclut le nom de l'organisation dans le certificat. Cela exige un examen plus approfondi de l'organisation qui exige une intervention humaine et qui, par conséquent, retarde le processus d'émission des certificats, généralement jusqu'à un jour ou plus.
3) Un certificat de validation étendue (EV) – Comme dans le cas des certificats d'OV, l'AC émettrice vérifie le contrôle d'une organisation sur les domaines indiqués et inclut le nom de l'organisation dans le certificat. Les candidats d'EV doivent également passer un processus de vérification plus étendu, ce qui entraîne des retards supplémentaires dans le processus de délivrance des certificats, qui peuvent prendre jusqu'à plusieurs jours.

Voici quelques considérations importantes concernant ces différents types de certificats :

- il n'y a aucune différence entre les certificats DV, OV et EV en matière de niveau de sécurité fourni par la séance TLS entre un navigateur Web et un serveur Web;
- un grand nombre des principaux navigateurs Web ne font plus la distinction entre les certificats DV, OV et EV, ils affichent simplement un cadenas si le protocole HTTPS est activé ou indiquent que la session n'est pas sécurisée si le protocole HTTPS n'est pas activé;

[2] Cela signifie essentiellement que le serveur Web est en possession de la clé privée qui correspond au certificat de clé publique associé. Cela ne signifie pas forcément que le site Web est légitime ou fiable.

- même s'il y a des étapes de vérification supplémentaires pour les certificats OV et encore plus pour les certificats EV, cela n'est pas fait de façon uniforme dans toutes les AC et les étapes de validation supplémentaires ne se traduisent pas nécessairement par une sécurité ou une assurance améliorée;
- l'émission et la gestion du cycle de vie des certificats DV peuvent être entièrement automatisées, l'émission de certificats OV et EV exige une intervention humaine;
- on peut obtenir des certificats DV sans frais (p. ex., voir Let's Encrypt); les prix des certificats OV et EV varient (mais on peut obtenir des prix réduits par l'entremise de Services partagés Canada (SPC)[3]).

2.1.2 Contenu du certificat

Les certificats de serveur TLS utilisés par le GC doivent être des certificats X.509 version 3 conformes à la DC 5280 et aux exigences de base du forum CA/B, sous réserve des précisions suivantes :

- L'algorithme de signature, l'algorithme de hachage de signature et la taille de clé publique doivent être conformes aux lignes directrices du CST telles qu'elles sont stipulées dans les Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111).
- La période de validité ne doit pas dépasser les lignes directrices du forum CA/B.
- L'extension de certificat d'utilisation de clé doit inclure la signature numérique, et le chiffrage de clés ou l'accord de clés (le choix dépend de l'algorithme); aucune autre valeur n'est autorisée.
- L'extension de certificat d'utilisation de clé étendue doit inclure l'authentification du serveur et peut également inclure l'authentification client; aucune autre valeur n'est autorisée.
- L'extension de certificat Stratégies de certificat doit inclure un OID reconnu qui identifie le type de certificat. Les valeurs établies par le forum CA/B doivent être utilisées (c'est-à-dire, DV = 2.23.140.1.2.1, OV = 2.23.140.1.2.2 et EV = 2.23.140.1.1). Si des OID propres à l'AC sont utilisés, ils doivent être enregistrés auprès du forum CA/B (voir https://cabforum.org/object-registry/).
- L'extension de certificat Liste d'horodatage de certificat signé (SCT) doit contenir le nombre approprié d'entrées[4,5].

[3] SSC has a contract with a CA vendor to obtain TLS server certificates on behalf of GC departments at reduced prices.

[4] Le nombre exigé d'entrées dépend de la durée de vie du certificat (p. ex., voir https://github.com/chromium/ct-policy/blob/master/ct_policy.md#qualifying-certificate). Les exigences de base du forum CA/B limitent la durée de vie des certificats de serveur TLS à 27 mois ou moins; le nombre minimum d'entrées SCT exigé sera de 2 (moins de 15 mois) ou 3 (entre 15 ou 27 mois).

[5] La DC 6962 décrit trois méthodes que le serveur Web peut utiliser pour transmettre la Liste SCT au navigateur, dont l'une consiste à intégrer la Liste SCT dans le certificat comme indiqué ici. Les deux autres méthodes sont l'agrafage OCSP et l'extension du protocole TLS. L'utilisation de la Liste SCT intégrée est recommandée, car elle ne nécessite pas de modification des serveurs Web existants. Veuillez prendre note que si l'autorité de certification émettrice n'intègre pas la liste SCT dans le certificat, la méthode de l'agrafage OCSP ou d'extension du protocole TLS doit être utilisée et peut nécessiter des modifications logicielles ou de configuration sur le serveur Web.

2.2 Autorités de certification (AC)

Tout service commercial ou public d'AC utilisé pour émettre des certificats de serveur au GC doit, au minimum, satisfaire aux exigences suivantes :

- Les AC doivent se conformer aux exigences de base du forum CA/B. Veuillez prendre note que cela comprend les exigences associées à l'Autorisation des autorités de certification (AAC), comme décrit dans la DC 6844.
- Pour les certificats EV uniquement, les AC doivent se conformer aux lignes directrices du certificat EV du forum CA/B (en anglais).
- Les AC doivent participer à l'initiative Certificate Transparency (CT).
- Les AC doivent se conformer aux lignes directrices du CST concernant les longueurs et les algorithmes de clé associés à des schémas d'établissement de clé acceptables, des algorithmes de signature numérique et des fonctions de hachage sécurisées, comme stipulé dans les Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)[6].
- Les AC émettrices doivent appuyer la révocation de certificat conformément aux exigences de base du forum CA/B.
- Les AC doivent remplir le certificat de serveur comme indiqué à la section 2.1.2.
- Les AC émettrices doivent être « approuvées » par tous les principaux navigateurs, y compris, sans toutefois s'y limiter, Google Chrome, Mozilla Firefox, Microsoft IE/Edge, Apple Safari, etc.

2.3 Responsabilités liées aux sites Web du GC

En général, les responsables de sites Web du GC sont chargés de déterminer le type et la source[7] du certificat de serveur et d'assurer la gestion appropriée du cycle de vie du certificat de clé publique et de la clé privée associée au fil du temps. Cela comprend la présentation d'une demande de révocation en cas de compromission soupçonnée ou connue de la clé privée. L'utilisation de l'automatisation pour appuyer le processus de gestion du cycle de vie est recommandée dans la mesure du possible.

Les responsables de sites Web du GC doivent veiller à ce que des mesures appropriées d'atténuation des risques soient en place afin de réduire au minimum le risque de compromission des clés privées. Il est recommandé d'utiliser les modules de sécurité du matériel (HSM) FIPS 140-2 ou FIPS 140-3 de niveau 2 ou supérieur lorsque cela est justifié par l'évaluation des risques ou l'analyse de compromis coûts-avantages. En l'absence de HSM, les mesures d'atténuation des risques doivent inclure une surveillance et un audit efficaces du système afin que la compromission des clés privées puisse être détectée le plus

[6] Il est reconnu que les exigences de base du Forum CA/B permettent d'obtenir d'anciens certificats d'AC racine qui ne répondent pas aux exigences minimales du CST en ce qui concerne la longueur des clés RSA et les algorithmes de hachage sécurisés. Toutefois, il faut prendre note que tous les certificats dans le chemin d'accès de certification doivent satisfaire aux exigences minimales du CST.

[7] Les sources recommandées pour l'obtention des certificats sont fournies dans le présent document.

tôt possible, suivi immédiatement de la révocation du certificat de serveur associé. Veuillez prendre note que l'utilisation de certificats multidomaines et génériques doit faire l'objet d'une attention particulière afin de réduire au minimum les dommages collatéraux en cas de compromission de clés privées. Il est fortement déconseillé de copier la même clé privée sur plusieurs serveurs Web à moins que des mesures d'atténuation des risques appropriées ne soient en place, comme l'utilisation de HSM approuvés par le CST pour protéger la clé privée.

3. Sommaire et recommandations

Le présent document a été élaboré pour appuyer l'activation du protocole HTTPS pour tous les sites Web du GC axés sur le public, et détermine les exigences minimales pour le type de certificat et le contenu, la conformité des AC et les responsabilités liées aux sites Web.

Compte tenu des considérations liées aux coûts, à l'automatisation et à la sécurité, les certificats de serveur DV sont recommandés pour utilisation par les sites Web publics du GC. Cette recommandation est conforme aux tendances de l'industrie ainsi qu'à d'autres gouvernements fédéraux comme les États-Unis (voir https://https.cio.gov/certificates/) et l'Australie (voir https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-https-and-opportunistic-tls). De plus, on encourage l'utilisation de services fiables comme Let's Encrypt qui offrent une gestion gratuite et automatisée du cycle de vie des certificats DV à l'aide du protocole ACME (Automated Certificate Management Environment)[8]. Un sommaire des fonctions et des considérations de Let's Encrypt se trouve à l'annexe A.

Même si l'utilisation de certificats OV et EV n'est pas interdite, on privilégie l'utilisation des certificats DV en raison de leur coût moindre et de leur capacité à soutenir l'émission automatique des certificats. En cas d'utilisation, on doit obtenir des certificats OV et EV auprès de SPC (envoyer un courriel à ssc.ssltls.spc@canada.ca) afin de tirer parti de la réduction des prix d'un fournisseur agréé d'AC.

Les questions ou commentaires au sujet du présent document doivent être adressés à ZZTBSCYBERS@tbs-sct.gc.ca.

[8] Même si l'utilisation du service Let's Encrypt est encouragée dans la mesure du possible, on reconnaît qu'il peut y avoir des circonstances où ce service ne convient pas, particulièrement lorsque les exigences et contraintes opérationnelles empêchent son utilisation, ou que des certificats provenant d'autres sources peuvent être plus appropriés (p. ex., d'un fournisseur de services infonuagiques lorsqu'il héberge des services Web GC dans le nuage).

4. Références

[1] UK Government, «Web Check — helping you to secure your public sector websites,» 17 July 2017. [En ligne]. Available: https://www.ncsc.gov.uk/blog-post/web-check-helping-you-secure-your-public-sector-websites#whoicanuseit.

[2] Communications Security Establishment, «[ITSP.40.111] Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information,» August 2016.

[3] Communications Security Establishment, «[ITSP.40.062] Guidance on Securely Configuring Network Protocols,» August 2016.

[4] Government of Canada, «Departmental Guide to Adoption of Secure Channel Mandatory Services,» Government of Canada, 22 October 2007. [En ligne]. Available: http://publiservice.tbs-sct.gc.ca/cio-dpi/docs/secure-protegee/secure-protegeepr-eng.asp.

[5] United States Government, «Pulse.CIO.Gov,» 18F and the General Services Administration, 8 June 2015. [En ligne]. Available: https://pulse.cio.gov/.

[6] Hardenize Inc., «Hardenize,» Hardenize, 2017. [En ligne]. Available: https://www.hardenize.com/.

[7] Google, Inc., «Google's Certificate Transparency Project,» [En ligne]. Available: https://www.certificate-transparency.org/.

[8] US-CERT, «Alert TA17-05A: HTTPS Interception Weakens TLS Security,» 16 March 2017. [En ligne]. Available: https://www.us-cert.gov/ncas/alerts/TA17-075A.

[9] Treasury Board of Canada Secretariat, «GC IT Strategic Plan 2017-2021,» November 2017.

[10] Internet Security Research Group (ISRG), «Let's Encrypt,» [En ligne]. Available: https://letsencrypt.org/about/.

[11] Internet Engineering Task Force (IETF), « The Transport Layer Security (TLS) Protocol Version 1.3 (DRAFT), » [En ligne]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/. [Accès le 29 Déc. 2017].

Annexe A – Chiffrons! (Let's Encrypt)

Let's Encrypt est un service d'AC mondial qui offre gratuitement l'émission et le renouvellement automatisés des certificats DV. Let's Encrypt a été créé par l'Internet Security Research Group (ISRG)[9] pour aider à activer le protocole HTTPS partout sur Internet.

Voici quelques-unes des principales fonctions et considérations liées à Let's Encrypt :

- Il n'émet que des certificats DV.
- Il est conforme aux exigences de base du forum CA/B.
- Il participe à l'initiative Certificate Transparency (CT) et remplit l'extension de certificat de la Liste SCT.
- Il émet des certificats avec une période de validité de 90 jours avec une période de roulement recommandée de 60 jours. (Voici la justification de la période de validité de 90 jours https://letsencrypt.org/2015/11/09/why-90-days.html (en anglais).)
- Il prend en charge le protocole OCSP (On-line Certificate Status Protocol). (Les LCR pour les certificats d'entité finale ne sont pas prises en charge.)
- Il est très évolutif.
- Il est capable d'émettre des certificats de serveur à domaine unique, multidomaines et génériques[10].
- Il offre une gestion gratuite et automatisée du cycle de vie des certificats à l'aide du protocole ACME.

En outre, le CST a effectué une évaluation de l'intégrité de la chaîne d'approvisionnement et a conclu que l'utilisation du service Let's Encrypt présente un faible risque pour le GC. En outre, il existe déjà des exemples où ce service est utilisé dans la pratique par d'autres gouvernements. Par exemple, la National Aeronautics and Space Administration (NASA) des États-Unis a mis en œuvre le protocole HTTPS sur environ 3 000 sites Web publics à l'aide de certificats de serveur DV émis à partir de Let's Encrypt (voir https://18f.gsa.gov/2017/05/25/from-launch-to-landing-how-nasa-took-control-of-its-https-mission/). La Digital Transformation Agency du gouvernement australien a également approuvé Let's Encrypt (voir https://www.dta.gov.au/blog/buckle-up-browser-changes-ahead).

[9] L'IRSG est un organisme à but non lucratif. Le financement de Let's Encrypt est fourni par un certain nombre de commanditaires dont Google Chrome, Mozilla, Cisco, Amazon Web Services et bien d'autres.

[10] La prise en charge des certificats génériques exige un client compatible à la version 2 d'ACME.