Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

UNCLASSIFIED

Government of Canada

Recommendations for TLS Server Certificates for GC Public Facing Web Services

14 May 2021

Revision History

Document Version No.	Changes	Date
0.1	Preliminary draft prepared by TBS-CIOB, Cyber Security.	16 March 2018
0.2	Incorporated feedback resulting from peer review of the initial draft – several issues still pending resolution as indicated by comments in the margin and placeholders in main body	30 April 2018
0.3	Incorporated feedback resulting from peer review of the second draft, revised Section 3, made a number of enhancements throughout, retitled document	28 May 2018
0.4	Enhanced the browser display related material with additional industry trend information; particularly with respect to Google Chrome. Added clarification regarding recommended CAs leaving the door open for additional approaches/recommendations in the future. Made various enhancements/clarifications in response to additional feedback.	13 August 2018
1.0	Made additional clarifications and added a consolidated CA conformance requirements checklist at Appendix B.	27 August 2018
1.1	Refreshed the document to bring it up-to-date, condensed some of the more technical details, removed Appendix B.	14 May 2021

Table of Contents

Acronyms and Abbreviations

ACME	Automated Certificate Management Environment
CA	Certification Authority
CA/B	Certification Authority and Browser (Forum)
CIOB	Chief Information Officer Branch
CRL	Certificate Revocation List
CSE	Communications Security Establishment
CT	Certificate Transparency
DV	Domain Validated
EV	Extended Validation
FIPS	Federal Information Processing Standard (US)
GC	Government of Canada
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
ISRG	Internet Security Research Group
IT	Information Technology
ITSP	Information Technology Security Publication
OCSP	Online Certificate Status Protocol
OV	Organization Validated
PKI	Public Key Infrastructure
RFC	Request for Comments
SCT	Signed Certificate Timestamp
SSC	Shared Services Canada
TBS	Treasury Board Secretariat
TLS	Transport Layer Security

1. Introduction

All Government of Canada (GC) external facing websites[1] must support the Hyper Text Transfer Protocol Secure (HTTPS). HTTPS combines HTTP with the Transport Layer Security (TLS) protocol which provides data integrity and confidentiality between a web browser and a web server.

In order to enable HTTPS, GC public facing websites must obtain TLS server certificates. This document outlines various aspects related to TLS server certificates and identifies minimum requirements associated with certificate type and content, Certification Authority (CA) conformance and website responsibilities. Recommendations regarding which type of certificates should be used and where to obtain them are also provided.

[1] A GC external facing website is any GC web site that provides information and/or services to the general public.

2. TLS Server Certificate Considerations

2.1 Public Key Certificates

Essentially, a public key certificate (hereafter referred to as certificate) is a data structure that is digitally signed by the issuing Certification Authority (CA). The information contained within the certificate includes the name of the entity associated with the certificate, name of the issuing CA, validity period, purpose, and public key corresponding to the associated private key.

When used in conjunction with TLS, server certificates are used to authenticate the web server[2] and to establish a secure session between a web browser and a web server that maintains data confidentiality and integrity for the life of the session.

2.1.1 Types of Certificates

There are three types of server certificates based on the level of validation before initial issuance:

1) A Domain Validated (DV) certificate - the issuing CA verifies the requesting entity's control of the specified domain(s). In this case, certificate issuance is relatively quick and can be fully automated.
2) An Organization Validated (OV) certificate - the issuing CA verifies an organization's control of the specified domain(s) and includes the organization's name within the certificate. This requires additional vetting of the organization which requires human intervention and therefore introduces some delay in the certificate issuance process, typically up to a day or so.
3) An Extended Validation (EV) certificate – as in the case of OV certificates the issuing CA verifies an organization's control of the specified domain(s) and includes the organization's name within the certificate. EV applicants must also pass a more extensive vetting process resulting in additional delays in the certificate issuance process which can take up to several days.

Important considerations regarding these different types of certificates include the following:

- there is no difference between DV, OV and EV certificates in terms of the level of security provided by the TLS session between a web browser and a web server;
- many of the major web browsers no longer distinguish between DV, OV and EV certificates, they simply display a padlock if HTTPS is enabled or indicate that the session is not secure if HTTPS is not enabled;
- while there are additional verification steps for OV certificates and even more for EV certificates, this is not done consistently across all CAs and the additional validation steps do not necessarily translate to improved security or assurance;

[2] Essentially this means that the web server is in possession of the private key that corresponds to the associated public key certificate. It does not necessarily mean that the website is legitimate or trustworthy.

- issuance and life cycle management of DV certificates can be fully automated, issuance of OV and EV certificates requires human intervention; and
- DV certificates can be obtained at no cost (e.g., see Let's Encrypt), OV and EV certificate prices vary (but reduced pricing can be obtained via Shared Services Canada (SSC) [3]).

2.1.2 Certificate Content

TLS server certificates used by the GC must be X.509 Version 3 certificates that conform to RFC 5280 and the CA/B Forum Baseline Requirements subject to the following clarifications:

- The signature algorithm, signature hash algorithm and public key size must be in conformance with CSE guidelines as stipulated in Cryptographic Algorithms for Unclassified, Protected A and Protected B Information (ITSP.40.111).
- The validity period must not exceed CA/B forum guidelines.
- The Key Usage certificate extension must include Digital Signature and either Key Encipherment or Key Agreement (choice is algorithm dependent), no other values are permitted.
- The Extended Key Usage certificate extension must include Server Authentication and may also include Client Authentication, no other values are permitted.
- The Certificate Policies certificate extension must include a recognized OID that identifies the type of certificate. Values established by the CA/B forum should be used (i.e., DV = 2.23.140.1.2.1, OV = 2.23.140.1.2.2 and EV = 2.23.140.1.1). If CA specific OIDs are used, they should be registered with the CA/B forum (see https://cabforum.org/object-registry/).
- The Signed Certificate Timestamp (SCT) List certificate extension should be populated with the appropriate number of entries. [4,5]

2.2 Certification Authorities (CAs)

Any commercial or public CA service used to issue server certificates to the GC must, at a minimum, meet the following requirements:

- The CA must conform to the CA/B Forum Baseline Requirements. Note that this includes requirements associated with Certification Authority Authorization (CAA) as described in RFC 6844.

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

[4] The required number of entries depends on the certificate lifetime (e.g., see https://github.com/chromium/ct-policy/blob/master/ct_policy.md#qualifying-certificate). Since the CA/B forum baseline requirements limit TLS server certificate lifetimes to 27 months or less, the minimum number of SCT entries required will be either 2 (less than 15 months) or 3 (greater than or equal to 15 months and less than or equal to 27 months).

[5] RFC 6962 describes three methods that the web server can use to convey the SCT List to the browser, one of which is to embed the SCT List in the certificate as stipulated here. The other two methods are OCSP stapling and TLS extension. Use of the embedded SCT List is recommended since it does not require changes to existing web servers. Note that if the issuing CA does not embed the SCT List in the certificate, OCSP stapling or the TLS extension method must be used and may require software/configuration changes to the web server.

- For EV certificates only, the CA must conform to the CA/B Forum EV certificate guidelines.
- The CA must participate in the Certificate Transparency (CT) initiative.
- The CA must adhere to CSE guidelines for key lengths and algorithms associated with acceptable key establishment schemes, digital signature algorithms and secure hash functions as stipulated in Cryptographic Algorithms for Unclassified, Protected A and Protected B Information (ITSP.40.111).[6]
- The issuing CA must support certificate revocation as stipulated by the CA/B Forum Baseline Requirements.
- The CA must populate the server certificate as discussed under Section 2.1.2.
- The issuing CA must be "trusted" by all major browsers including, but not limited to, Google Chrome, Mozilla Firefox, Microsoft IE/Edge, Apple Safari, etc.

2.3 GC Website Responsibilities

In general, GC websites owners are responsible for determining the type and source[7] of the server certificate and ensuring the appropriate life cycle management of the public key certificate and associated private key over time. This includes submission of a revocation request in the event of suspected or known private key compromise. Use of automation to support the life cycle management process is recommended where possible.

GC website owners must ensure appropriate risk mitigation measures are in place to minimize the risk of private key compromise. Use of FIPS 140-2 or FIPS 140-3 Level 2 or higher Hardware Security Modules (HSMs) is recommended where warranted by risk assessment or cost/benefit trade-off analysis. In the absence of HSMs, risk mitigation measures should include effective monitoring and auditing of the system so that private key compromise can be detected as early as possible followed immediately with revocation of the associated server certificate. Note that care must be exercised when using multi-domain and wildcard certificates to ensure collateral damage is minimized in the event of private key compromise. Copying the same private key to multiple web servers is strongly discouraged unless appropriate risk mitigation measures are in place such as using CSE approved HSMs to protect the private key.

[6] It is recognized that the CA/B Forum baseline requirements allow for legacy root CA certificates that do not meet CSE's minimum requirements with respect to RSA key length and secure hash algorithms. However, it should be noted that all certificates in the certification path must meet CSE's minimum requirements.

[7] Recommended sources for obtaining certificates are provided within this document.

3. Summary and Recommendations

This document has been developed in support of enabling HTTPS for all GC public facing websites and identifies the minimum requirements for certificate type and content, CA conformance and website responsibilities.

Given the considerations associated with cost, automation and security, DV server certificates are recommended for use by GC public facing websites. This recommendation is consistent with industry trends as well as other federal governments such as the United States (see https://https.cio.gov/certificates/) and Australia (see https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-https-and-opportunistic-tls). Furthermore, use of reputable services such as Let's Encrypt that offer free, automated life cycle management of DV certificates using the Automated Certificate Management Environment (ACME) protocol is encouraged where appropriate.[8] A brief summary of Let's Encrypt features and considerations is provided in Appendix A.

While the use of OV and EV certificates is not precluded, DV certificates are preferred due to their lower cost and the ability to support automated certificate issuance. If used, OV and EV certificates should be obtained from SSC (contact ssc.ssltls.spc@canada.ca) in order to take advantage of the reduced pricing from an approved CA vendor.

Questions or comments regarding this document should be directed to ZZTBSCYBERS@tbs-sct.gc.ca.

[8] While use of Let's Encrypt is encouraged wherever possible, it is recognized that there are circumstances where this service may not be suitable, particularly where operational requirements/constraints impede its use or certificates from other sources may be more appropriate (e.g., from a cloud service provider when hosting GC web services in the cloud).

4. References

[1] GC HTTPS Everywhere Initiative on GCPedia, [Online]. Available: http://www.gcpedia.gc.ca/wiki/HTTPS_Initiative.

[2] Communications Security Establishment, "[ITSP.40.062] Guidance on Securely Configuring Network Protocols," August 2016, [Online]. Available: https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.062-eng.pdf.

[3] Internet Engineering Task Force (IETF),"[RFC 2119] Key words for use in RFCs to Indicate Requirement Levels", March 1997. [Online]. Available: https://www.ietf.org/rfc/rfc2119.

[4] CA/B Forum, "Guidelines for the Issuance and Management of Extended Validation Certificates", [Online]. Available: https://cabforum.org/extended-validation/.

[5] United States Government, "The HTTPS-Only Standard", [Online]. Available: https://https.cio.gov/certificates/.

[6] Communications Security Establishment, "[ITSP.40.111] Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information," August 2016, [Online]. Available: https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.111-eng.pdf.

[7] CA/B Forum, "Object Registry", [Online]. Available: https://cabforum.org/object-registry/.

[8] CA/B Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", [Online]. Available: https://cabforum.org/baseline-requirements-documents/.

[9] Internet Engineering Task Force (IETF), "[RFC 6844] DNS Certification Authority Authorization (CAA) Resource Record", [Online]. Available: https://tools.ietf.org/html/rfc6844.

[10] Google LLC, "Google's Certificate Transparency Project", [Online]. Available: https://www.certificate-transparency.org/.

[11] Internet Security Research Group (ISRG) Let's Encrypt, "Let's Encrypt Website", [Online]. Available: https://letsencrypt.org/.

[12] Internet Security Research Group (ISRG), "Why ninety-day lifetimes for certificates", [Online]. Available: https://letsencrypt.org/2015/11/09/why-90-days.html.

Appendix A - Let's Encrypt

Let's Encrypt is a global CA service that provides automated DV certificate issuance and renewal free of charge. Let's Encrypt was established by the Internet Security Research Group (ISRG)[9] to help enable HTTPS everywhere in the Internet.

Some of the important features and considerations associated with Let's Encrypt include:

- Only issues DV certificates.
- Conforms to the CA/B Forum Baseline Requirements.
- Participates in the Certificate Transparency (CT) initiative and populates the SCT List certificate extension.
- Issues certificates with a 90 day validity period with a recommended rollover period of 60 days. (Rationale for the 90 day validity period is available here https://letsencrypt.org/2015/11/09/why-90-days.html.)
- Supports the On-line Certificate Status Protocol (OCSP). (CRLs for end-entity certificates are not supported.)
- Is highly scalable.
- Capable of issuing single domain, multi-domain and wildcard[10] server certificates.
- Automated certificate life cycle management using the Automated Certificate Management Environment (ACME) protocol.

In addition, CSE performed a supply chain integrity assessment which concludes that the use of the Let's Encrypt service poses low risk to the GC. Furthermore, there are already examples where this service is being used in practice by other governments. For example, the US National Aeronautics and Space Administration (NASA) has implemented HTTPS on approximately 3,000 public facing websites using DV server certificates issued from Let's Encrypt (see https://18f.gsa.gov/2017/05/25/from-launch-to-landing-how-nasa-took-control-of-its-https-mission/). The Australian government Digital Transformation Agency has also endorsed Let's Encrypt (see https://www.dta.gov.au/blog/buckle-up-browser-changes-ahead).

[9] The IRSG is a non-profit organization. Funding for Let's Encrypt is provided by a number of sponsors including Google Chrome, Mozilla, Cisco, Amazon Web Services and many others.

[10] Support for wildcard certificates requires an ACME Version 2 compatible client.