



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

UNCLASSIFIED / NON CLASSIFIÉ

Canada

UNCLASSIFIED

Government of Canada

Recommendations for TLS Server Certificates for GC Public Facing Web Services

03 October 2018

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
1.0	V1.0 final post governance endorsement	03 October 2018

Table of Contents

1. Introduction 1

 1.1 Overview 1

 1.2 Purpose and Scope..... 1

 1.3 Intended Audience..... 1

 1.4 Requirements Language Conventions 2

2. Considerations and Recommendations 3

 2.1 Public Key Certificates..... 3

 2.2 Certification Authorities (CAs) 7

 2.3 GC Website Responsibilities..... 8

3. Ongoing Developments 9

4. Summary 10

5. References 11

Appendix A - Let’s Encrypt 13

Appendix B – Consolidated CA Conformance Requirements Checklist 15

Acronyms and Abbreviations

AIA	Authority Information Access
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
DLP	Data Loss Prevention
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
LSA	Lead Security Agencies
OCSP	Online Certificate Status Protocol
OV	Organization Validated
PKI	Public Key Infrastructure
RFC	Request for Comments
SCT	Signed Certificate Timestamp
SSC	Shared Services Canada
SSL	Secure Sockets Layer
TBS	Treasury Board Secretariat
TLS	Transport Layer Security

1. Introduction

1.1 Overview

The Government of Canada (GC) has recently launched an initiative that will require all GC public facing websites¹ to support the Hyper Text Transfer Protocol Secure (HTTPS). This [HTTPS Everywhere initiative](#) is consistent with industry direction as well as with other federal governments including the Australia, the United States and the United Kingdom.

Essentially, HTTPS combines HTTP with the Transport Layer Security (TLS) protocol which provides data integrity and confidentiality between the web browser and the web server. TLS replaces the Secure Sockets Layer (SSL) protocol, although it is recognized that the term SSL continues to be used within the industry. However, TLS is used throughout this paper rather than SSL since it is technically more accurate. Furthermore, the reader should be aware that there are known flaws in earlier versions of TLS so all implementations should be upgraded to TLS Version 1.2 (or its successor) in accordance with CSE guidance (see [ITSP.40.062](#)) and the overall GC HTTPS strategy.

1.2 Purpose and Scope

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.

Note that the recommendations provided within this document pertain to GC public facing websites only. This document does not address internal website requirements.

In addition, this initiative relies upon existing browser technology - no changes to the external browsers used to access GC websites are required to support the HTTPS Everywhere initiative.

1.3 Intended Audience

This guide is primarily for business owners, web developers, IT and IT security practitioners who are involved in implementing externally-facing GC web-based applications.

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

1 **1.4 Requirements Language Conventions**

2 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",
3 "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC](#)
4 [2119](#).

2. Considerations and Recommendations

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 certificate data structure includes various information including the name of the CA that issued it, its validity period, what it can be used for, the public key corresponding to the associated private key, etc.

When used in conjunction with TLS, server certificates are used to authenticate the web server² and to establish a secure session between the web browser and the web server that maintains data confidentiality and integrity for the life of the session.

2.1.1 Types of Certificates

In general, there are three types of server certificates based on the process used to validate the entity requesting a certificate for the first time³:

- 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. Note that the CA/B forum has developed guidelines that identify the minimum requirements that a CA must meet in order to issue EV certificates (see <https://cabforum.org/extended-validation/> for the latest version).

Additional distinctions between these certificate types include:

- *Browser Display Characteristics*: From a browser display perspective, there is no distinction or perceived difference between a DV and an OV certificate. Although the display will vary depending on the type and version of browser used, most browsers display the closed padlock

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.

³ Note that the vetting process applies to first time certificate issuance only and does not apply to certificate renewal.

for both DV and OV certificates (although the padlock approach may be eliminated in the near future by some browser vendors as discussed below). The only way that a user can tell the difference between a DV and OV certificate is to examine the contents of the server certificate. However, there is a difference in the visual display when using EV certificates. In addition to the closed padlock, the browser will typically display the name of the organization associated with the EV server certificate and may also display the name of the organization in green (although this too is not presented consistently across all browser implementations and there are examples where the organization name is not consistent with what the user is expecting to see). Note that there is considerable debate about the value of this enhanced display. Some would suggest that since the vetting process for EV certificates is more involved/rigorous than the vetting process associated with DV or OV certificates, the enhanced display may provide some measure of additional assurance to end users that they are connected to the organization they are expecting. On the other hand, it is unclear that the enhanced address bar display rendered by the browser is actually noticed or understood by most users (e.g., see <https://www.troyhunt.com/on-the-perceived-value-ev-certs-cas-phishing-lets-encrypt/> and <http://www.usablesecurity.org/papers/jackson.pdf>). This is complicated by the fact that the enhanced display varies with each browser (type and version). Even more importantly, there are indications that major browser vendors such as Google Chrome are going to change the way the visual display is presented to the user. With the release of Google Chrome 68, users will be warned that any website that is not HTTPS enabled is “not secure” and, in addition, Google Chrome 69 is expected to remove the green padlock from the visual display for websites that are HTTPS enabled. Google’s approach is to move from a positive indication model to a negative indication model. It remains to be seen if other browser vendors will also adopt this approach but since Google Chrome has the largest market share (almost 50% in Canada and approximately 60% world-wide) the impact will be significant regardless.

- *Vetting process:* As noted above, the vetting process associated with certificate issuance varies depending on the type of certificate. This is another area of contention. DV certificates have been criticised since they are being used to establish phishing websites and some commercial CA vendors cite this as a (self-serving) reason to purchase the more expensive OV or, more typically, EV certificates. However, this is not a weakness in the DV certificate itself but is due to the fact that the vetting requirements to obtain a DV certificate are much simpler and require only that the entity requesting the certificate has control over the domain name. The ability to obtain DV certificates with little effort at no cost⁴ makes this even more attractive to an attacker. However, it should be noted that OV and EV certificates can also be (and have been) exploited as well (e.g., see <https://www.bleepingcomputer.com/news/security/extended-validation-ev-certificates-abused-to-create-insanely-believable-phishing-sites/>). In addition, EV

⁴ Many CA vendors offer free server certificates for a trial period of 30 days or more so this exploitation is not limited to Let’s Encrypt.

certificates do nothing to enhance the security of the TLS session between the web browser and the web server as compared to either a DV or OV certificate. Finally, the vetting process for issuing EV certificates is not implemented consistently by the commercial CAs, and the underlying vetting requirements have also been subject to criticism.

- *Automation:* Another difference between the certificate types is that the initial certificate issuance process can be fully automated with DV certificates since no manual intervention is required to facilitate the certificate issuance process. In fact, the entire certificate life cycle management process can be automated with the Let's Encrypt service as discussed in Appendix A.
- *Cost:* The price of server certificates varies among commercial CAs and depends on a number of factors including the type of certificate, the validity period of the certificate and the number (or scope in the case of a wildcard certificate) of supported domains per certificate. DV server certificates can be obtained from Let's Encrypt at no cost⁵ but the retail price for DV server certificates from other CA vendors can be as high as a few hundred dollars. The price for OV and EV certificates varies and can cost up to several hundred dollars.⁶ However, note that Shared Services Canada (SSC) currently has a contract with a CA vendor to obtain OV and EV server certificates on behalf of GC departments at reduced prices.

Some of the more important points/considerations discussed above can be summarized as follows:

- 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,
- browser displays are inconsistent and vary by browser type and version,
- it is unclear that the enhanced browser display for EV certificates provides any value for most users and there are indications that at least one major browser vendor is moving from a positive display model to a negative display model and the enhanced display for EV certificates may disappear altogether,
- while there are differences associated with vetting process for each certificate type, this does not necessarily translate to improved security or assurance,
- DV certificate issuance can be automated, and
- DV certificates can be obtained at no cost; OV and EV certificate prices can vary (but reduced pricing can be obtained via SSC).

Given these considerations, DV server certificates are recommended for use by GC public facing websites. Note that this direction is consistent with industry trends and other federal government initiatives (e.g., DV server certificates have been endorsed by the US General Services Administration -

⁵ Other CA vendors also offer free server certificates but this is for a limited trial period only.

⁶ Based on the advertised retail prices at the time of this writing from Commodo, Digicert, GeoTrust and Entrust Datacard, the retail price of a one year EV server certificate ranged from as low as \$180 USD to as high as \$430 USD. However, it should be noted that these are just a few examples and other CA vendors may offer lower prices.

1 see <https://https.cio.gov/certificates/> and the Australian government Digital Transformation Agency has
2 not only endorsed DV certificates but has also endorsed Let's Encrypt – see
3 <https://www.dta.gov.au/blog/buckle-up-browser-changes-ahead>). While the use of OV certificates is
4 not precluded, the additional cost and lack of automated issuance renders OV certificates a much less
5 attractive option compared to DV certificates. EV certificates are also permitted; however, as discussed
6 above there are trade-offs between cost and lack of automated certificate issuance compared to the
7 perceived value that EV certificates actually provide. In any case, GC departments that wish to obtain
8 OV or EV server certificates should contact SSC rather than purchase their own at the more expensive
9 retail rates (contact SSC at ssc.ssltls.spc@canada.ca for additional information).

10 **2.1.2 Certificate Validity Period**

11 In accordance with the [CA/B Forum Baseline Requirements](#), the maximum lifetime for DV and OV
12 certificates issued after 1 March 2018 is 825 days (~27 months). As specified in the [CA/B forum EV](#)
13 [certificate guidelines](#), the maximum lifetime for EV certificates is also 825 days but 12 months is
14 recommended.

15 Most CA vendors offer a choice of a 1 or 2 year validity period for server certificates.⁷ Certificates issued
16 by Let's Encrypt (as discussed under Appendix A) have a set validity period of 90 days (there are no
17 exceptions) with a recommended certificate renewal period of 60 days.

18 **2.1.3 Number of Domains**

19 Certificates can be issued for a single domain, multiple domains or to cover all sub-domains within a
20 parent domain. A single domain certificate is used for a single website, a multi-domain certificate is
21 used for multiple websites⁸, and a wildcard certificate is used for any website that is a sub-domain under
22 the identified wildcard domain (e.g., *.canada.ca.). Any one of these may be appropriate depending on
23 the intended use of the certificate. However, care must be exercised when using multi-domain and
24 wildcard certificates to ensure collateral damage is minimized in the event of private key compromise.
25 Copying the same private key to multiple web servers is strongly discouraged unless appropriate risk
26 mitigation measures are in place such as using CSE approved Hardware Security Modules to protect the
27 private key.

28 **2.1.4 Certificate Content**

29 Server certificates obtained and used by the GC MUST be X.509 Version 3 certificates that align with RFC
30 5280 and the CA/B Forum baseline requirements subject to the following clarifications:

⁷ CAs that still offer 3 year validity periods will likely eliminate this option in order to comply with the CA/B forum guidelines.

⁸ A multi-domain certificate may also include wildcards.

- 1 • The signature algorithm, signature hash algorithm and public key size MUST be in conformance
- 2 with CSE guidelines as stipulated in [ITSP.40.111](#).⁹
- 3 • The validity period MUST not exceed CA/B forum guidelines as discussed in Section 2.1.2 above.
- 4 • The Key Usage certificate extension MUST include Digital Signature and either Key Encipherment
- 5 or Key Agreement (choice is algorithm dependent), no other values are permitted.
- 6 • The Extended Key Usage certificate extension MUST include Server Authentication and MAY also
- 7 include Client Authentication, no other values are permitted.
- 8 • The Certificate Policies certificate extension MUST include a recognized OID that identifies the
- 9 type of certificate. Values established by the CA/B forum SHOULD be used (i.e., DV =
- 10 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
- 11 MUST be registered with the CA/B forum (see <https://cabforum.org/object-registry/>).
- 12 • The Subject Alternative Name certificate extension is subject to the guidance identified under
- 13 Section 2.1.3. Note that wildcards are not permitted within EV certificates in accordance with
- 14 the [CA/B forum EV certificate guidelines](#).
- 15 • The Signed Certificate Timestamp (SCT) List certificate extension SHOULD be populated with at
- 16 least two entries in accordance with Google's Certificate Transparency policy (see
- 17 https://github.com/chromium/ct-policy/blob/master/ct_policy.md#qualifying-certificate)^{10,11,12}.

18 2.2 Certification Authorities (CAs)

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

- 21 • The CA MUST conform to the [CA/B Forum Baseline Requirements](#). Note that this includes
- 22 requirements associated with Certification Authority Authorization (CAA) as described in [RFC](#)
- 23 [6844](#).
- 24 • For EV certificates only, the CA MUST conform to the [CA/B Forum EV certificate guidelines](#).

⁹ The CSE guidelines and CA/B Forum Baseline Requirements are in alignment with respect to subscriber certificates.

¹⁰ Note that Google mandates that at least one of the logs must be a Google log and at least one must be a non-Google log. So far the CT Policies published by other browser vendors (e.g., see <https://support.apple.com/en-us/HT205280>) are less restrictive with respect to the logs used and are in alignment (i.e., do not conflict) with Google's policy. This will be revisited as participating browser vendors publish their respective certificate transparency policies.

¹¹ The required number of entries depends on the certificate lifetime. Since the CA/B forum baseline requirements limit TLS server certificate lifetimes to 27 months or less, the 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).

¹² 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.

- 1 • The CA MUST participate in the [Certificate Transparency \(CT\) initiative¹³](#) and MUST publish the
2 certificates it issues to multiple CT logs in accordance with Google's Certificate Transparency
3 policy (see [https://github.com/chromium/ct-policy/blob/master/ct_policy.md#qualifying-](https://github.com/chromium/ct-policy/blob/master/ct_policy.md#qualifying-certificate)
4 [certificate](#)).
- 5 • The CA MUST adhere to CSE guidelines for key lengths and algorithms associated with
6 acceptable key establishment schemes, digital signature algorithms and secure hash functions
7 as stipulated in [ITSP.40.111](#).¹⁴
- 8 • The issuing CA MUST support certificate revocation as stipulated by the [CA/B Forum Baseline](#)
9 [Requirements](#).¹⁵
- 10 • The CA MUST populate the server certificate as discussed under Section 2.1.4.
- 11 • The issuing CA MUST be "trusted" by all major browsers including, but not limited to, Google
12 Chrome, Mozilla Firefox, Microsoft IE/Edge, Apple Safari, etc.

13 2.3 GC Website Responsibilities

14 In general, GC websites owners are responsible for determining the type and source¹⁶ of the server
15 certificate and ensuring the appropriate life cycle management of the public/private key pair and
16 associated public key certificate over time. This includes submission of a revocation request in the event
17 of suspected or known private key compromise. Use of automation to support the life cycle
18 management process is RECOMMENDED where possible.

19 GC website owners MUST ensure appropriate risk mitigation measures are in place to minimize the risk
20 of private key compromise. Use of FIPS 140-2 Level 2 or higher Hardware Security Modules (HSMs) is
21 RECOMMENDED where warranted by risk assessment or cost/benefit trade-off analysis. In the absence
22 of HSMs, risk mitigation measures should include effective monitoring and auditing of the system so
23 that private key compromise can be detected as early as possible followed immediately with revocation
24 of the associated server certificate.

¹³ The Certificate Transparency initiative is replacing HTTP Public Key Pinning with a more secure and robust solution.

¹⁴ 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.

¹⁵ Note that how the web browsers handle revocation information is outside the GC's control and therefore outside the scope of this document.

¹⁶ Recommended sources for obtaining certificates are provided within this document.

3. Ongoing Developments

There are several areas that require additional investigation or will evolve naturally over time, including:

- *Certificate Management Agents for Let's Encrypt*: Numerous open source certificate management agents that support the automated certificate life cycle management process in conjunction with Let's Encrypt are available on-line. Let's Encrypt recommends Certbot from the Electronic Frontier Foundation (see <https://certbot.eff.org/>) but this is only for Linux based systems. Several certificate management agents for Windows-based systems are also available (refer to <https://letsencrypt.org/docs/client-options/>). Note that these certificate management agents may evolve over time (e.g., to support bug fixes, comply with new versions of the ACME protocol, etc.) so web site administrators should be prepared to update the software as required (assuming the update process is not automated).
- *Recommended CAs*: This document essentially recommends two CAs - Let's Encrypt for obtaining DV certificates and the commercial CA vendor under contract with SSC (which may be subject to change over time) for obtaining OV or EV certificates. It is recognized that there may be circumstances where certificates could be obtained from other sources (e.g., from a cloud service provider in conjunction with GC web sites hosted in the cloud). Furthermore, it is also recognized that circumstances change with time and other approaches and/or CAs may be recommended in the future. Regardless of the source, it should be noted that the issuing CA MUST conform to the minimum conformance requirements identified within this paper. A consolidated CA conformance requirements checklist is provided in Appendix B to assist in the evaluation of candidate CAs.
- *Certificate Transparency (CT)*: As discussed under Section 2, CAs MUST participate in the CT initiative. Requirements associated with this initiative may change with time and this document will be updated to reflect any changes as required. Responsibility within the GC for monitoring CT logs is to be determined.
- *Certification Authority Authorization (CAA)*: As noted previously, requirements for CAA are identified in the CA/B Forum baseline requirements. In addition, the GC may leverage Domain Name System (DNS) CAA records in the future to help reduce the chance that an unapproved CA issues a certificate to a GC website.
- *Evolving GC Security Architecture*: It is recognized that the GC is constantly evolving from a security perspective and that changes in the GC security architecture may have an impact on the content of this document over time. Any changes will be reflected within this document as required.

4. Summary

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.

It has been noted that DV server certificates are recommended for use by GC public facing websites. Where appropriate, the use of the Let's Encrypt service is encouraged for obtaining DV certificates combined with the use of a suitable certificate management agent. Use of OV certificates is not precluded, but DV certificates are preferred due to their lower cost and the ability to support automated certificate issuance. EV certificates may also be used but it has been noted that their value is subject to question. 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. Other approaches may be appropriate as circumstances warrant. If certificates are obtained from another source, the issuing CA MUST conform to the minimum requirements identified within this document.

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

5. 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 public 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) to help enable HTTPS everywhere in the Internet. The IRSG is a non-profit organization and funding for the Let's Encrypt service comes from a number of sponsors including Google Chrome and the Mozilla Foundation.

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.
- Certificates are issued 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>.
- Only OCSP is supported for server certificates (i.e., CRLs for end-entity certificates are not supported).
- Is highly scalable - in 2017, Let's Encrypt served 46 million active certs and this number is expected to double in 2018. Let's Encrypt also generates 20 million OCSP responses per day and serves those responses 2 billion times per day.
- Capable of issuing single domain, multi-domain and wildcard¹⁷ server certificates.
- Automated certificate life cycle management is supported and there are numerous certificate management agents available to ease/simplify integration with web servers (e.g., certbot).

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 recently 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>).












¹⁷ Support for wildcard certificates is relatively new (as of March 2018) and requires an Automated Certificate Management Environment (ACME) Version 2 compatible client.

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

5

1 Appendix B – Consolidated CA Conformance Requirements Checklist



2

Issuing CA Conformance Requirements	Let's Encrypt	Entrust ¹⁸	Other
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 .)			
For EV certificates only, the CA MUST conform to the CA/B Forum EV certificate guidelines .	n/a		
The CA MUST participate in the Certificate Transparency (CT) initiative and MUST publish the certificates it issues to multiple CT logs in accordance with Google's Certificate Transparency policy (see https://github.com/chromium/ct-policy/blob/master/ct_policy.md#qualifying-certificate).			
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 ITSP.40.111 . ¹⁹			
The CA MUST support certificate revocation in accordance with the CA/B Forum Baseline Requirements .			
Server certificates obtained and used by the GC MUST be X.509 Version 3 certificates that align with RFC 5280 and the CA/B Forum baseline requirements subject to the following clarifications: <ul style="list-style-type: none"> The signature algorithm, signature hash algorithm and public key size MUST be in conformance with CSE guidelines as stipulated in ITSP.40.111.²⁰ The validity period MUST not exceed CA/B forum guidelines as discussed in Section 2.1.2. 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. 			

¹⁸ Entrust is the commercial CA vendor currently under contract to SSC to provide certificates to the GC. Note that this should not be confused with the Internal Credential Management PKI.

¹⁹ 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.

²⁰ The CSE guidelines and CA/B Forum Baseline Requirements are in alignment with respect to subscriber certificates.

<ul style="list-style-type: none"> • 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 MUST be registered with the CA/B forum (see https://cabforum.org/object-registry/). • The Subject Alternative Name certificate extension is subject to the guidance identified under Section 2.1.3. Note that wildcards are not permitted within EV certificates in accordance with the CA/B forum EV certificate guidelines. • The Signed Certificate Timestamp (SCT) List certificate extension SHOULD be populated with at least two entries in accordance with Google's Certificate Transparency policy (see https://github.com/chromium/ct-policy/blob/master/ct_policy.md#qualifying-certificate)^{21,22,23}. 			
The CA MUST be "trusted" by all major browsers including, but not limited to, Google Chrome, Mozilla Firefox, Microsoft IE/Edge, Apple Safari, etc.			

1
2
3
4

²¹ Note that Google mandates that at least one of the logs must be a Google log and at least one must be a non-Google log. So far the CT Policies published by other browser vendors (e.g., see <https://support.apple.com/en-us/HT205280>) are less restrictive with respect to the logs used and are in alignment (i.e., do not conflict) with Google's policy. This will be revisited as participating browser vendors publish their respective certificate transparency policies.

²² The required number of entries depends on the certificate lifetime. Since the CA/B forum baseline requirements limit TLS server certificate lifetimes to 27 months or less, the 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).

²³ 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.