CHARTERED PROFESSIONAL ACCOUNTANTS CANADA
COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

WebTrust® for Certification Authorities

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – CODE SIGNING BASELINE REQUIREMENTS

Release Date 31 March 2024

Effective Date For engagement periods commencing on or after 1 April 2024

Version 3.7

Based on the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates – Version 3.7

Copyright © 2024 by Chartered Professional Accountants of Canada ("CPA Canada"). All rights reserved. These Principles and Criteria may be reproduced and distributed provided that reproduced materials are not in any way directly or indirectly offered for sale or profit and attribution is given.

Document History

Version	Publication Date	Revision Summary
3.2	31 January 2023	Revised to address Version 3.2 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates. Addition of new principle 4 regarding meeting the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum that has been clarified as required by reference. All criteria references changed to reflect reference change in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (Convert Code Signing Baseline Requirements to RFC 3647 Framework). Principle 2 Criteria 4.13 Reuse of data for non-EV certificates. Principle 2 Criteria 9.3, 9.5 Update to subscriber key protection requirements. Note original effective date of November 15, 2022 changed to June 1, 2023. Principle 3, Criteria 9.3, 9.4 Update to subscriber key protection requirements. Note original effective date of November 15, 2022 changed to June 1, 2023. Introduction in Principle 3 of Column for reference to EV Requirements as needed. Other minor changes throughout.
3.7	1 April 2024	Revised to address Version 3.7 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates Updates to revocation requirements Elimination of references to SSL Baseline requirements and incorporation of relevant materials. Removal of Principle 4 related to the separate reporting for the Network and Certificate System Security Requirements.

Acknowledgements

This document has been prepared by the WebTrust/PKI Assurance Task Force (the "Task Force") for use by those practitioners enrolled by CPA Canada to perform WebTrust for Certification Authorities engagements.

Members of the Task Force are:

- Timothy Crawford, *BDO USA, PC* (co-Chair)
- Dan Adam
- Donoghue Clarke, *Ernst & Young LLP*
- Chris Czajczyc, *Deloitte LLP*
- Adam Fiock, *BDO USA, PC*
- David Lachmansingh, *Richter LLP*
- Eric Lin, *Ernst & Young LLP*
- Zain Shabbir, *KPMG LLP*
- Jinhwan Shin, *Deloitte LLP (Korea)*

CPA Canada Support

- Anna-Marie Christian, Director Emerging Issues & Strategic Partnerships
- Dave Chin, Principal, International Programs (co-Chair)
- Lilia Dubko, Manager, Assurance Programs

Table of Contents

Introduction

The primary goal of the CA/Browser Forum ("CA/B Forum" or the "Forum") *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* ("CS BRs") is to enable efficient and secure electronic communication, whilst addressing user concerns about the trustworthiness of Code Signing Certificates ("CS Certificates"). The Guidelines also serve to inform users and help them to make informed decisions when relying on Certificates.

The purpose of these WebTrust Principles and Criteria for Certification Authorities–Code Signing Baseline Requirements ("Criteria") is to set out criteria that would be used as a basis for a practitioner to conduct an engagement on the Issuance and Management of Publicly-Trusted Code Signing Certificates.

Information about Code Signing Certificates

A Code Signature created by a Subscriber may be considered valid for a period not exceeding 39 months. However, the life of a Code Signature may be extended for up to 135 months by using either:

a. Timestamp Method: In this method, the Subscriber signs the code, appends its Code Signing Certificate (whose expiration time does not exceed 39 months in the future) and submits it to a Timestamp Authority to be time-stamped. The resulting package can be considered valid up to the expiration time of the timestamp certificate (that may be up to 135 months in the future); or

b. Signing Service Method: In this method, the Subscriber submits the code, or a digest of the code, to a Signing Service for Code Signature. The resulting Code Signature is valid up to the expiration time of the Signing Service certificate (that may be up to 39 months in the future).

Adoption and effective dates

These Criteria incorporate and make reference to relevant Guidelines and Requirements from the CA/B Forum as listed in Appendix A and are effective for engagement periods commencing on or after 1 April 2024.

The CA/B Forum and/or the Forum may periodically publish updated Guidelines and Requirements. The practitioner is not required to consider these updated versions until reflected in the updated Criteria.

In certain instances, the CA/B Forum and/or the Forum updates its Guidelines and Requirements with certain criteria only effective at a date later than the publication date. The practitioner is directed to review the document history, revisions and relevant dates in the Forum documents to understand the applicability of certain Guidelines and Requirements.

For a list of Guidelines and Requirements that have effective dates later than the effective date of these Criteria, refer to Appendix D.

Extended Validation overview

The growth of Internet transactions has emphasized the importance of strong authentication of the identity of websites, domain owners, online servers and software code. Certificates that have been issued under stronger authentication controls, processes and procedures are called Extended Validation Certificates ("EV Certificates"). EV Certificates are currently differentiated by their intended use as:

- Certificates intended to ensure the identity of a remote computer ("EV SSL Certificates"); and
- Certificates intended to ensure the identity of a software publisher and the integrity of software code ("EV Code Signing Certificates").

This document also addresses EV Code Signing Certificates as Principle 3.

Browsers and software developers often provide EV Certificates with elevated status within their applications, for example, through the use of favourable user interface elements or, in some cases, prohibiting the use of non-EV Certificates.

References to SSL Baseline Requirements

In 2011, the CA/Browser Forum introduced its Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements," "SSL Baseline Requirements" or "BRs").

These Criteria previously included references to both the relevant sections of the CS BRs and the SSL Baseline Requirements for each criterion as applicable, and the practitioner was directed to consider both of these in performing their engagement.

In September 2023, the CA Browser Forum eliminated the SSL BR references in its *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*. As a result, SSL BR references have been removed in this version of the WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements.

For the CS Baseline Requirements, the practitioner is directed to consider the version as outlined in Appendix A.

Connection with the CA/Browser Forum's Network and Certificate System Security Requirements

In February 2023, it was clarified that CA/Browser Forum's *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* incorporates the CA/Browser Forum's Network and Certificate System Security Requirements by reference as if fully set forth in that document. Please note that effective for engagement periods commencing on or after 1 April 2024 this requirement is addressed in a separate reporting engagement: WebTrust Principles and Criteria for Certification Authorities -Network Security. Early adoption is allowed.

Connection with WebTrust for CA

These Criteria are designed to be used in conjunction with an assurance engagement of a CA as required by the CA/Browser Forum. Due to significant overlap between these Criteria and the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2 or later ("WebTrust for CA" or "WTCA"), this engagement should be conducted simultaneously with the WebTrust for CA engagement.

Requirements not subject to assurance

In preparing these Criteria, the Task Force reviewed the relevant documents as outlined in Appendix A, with the intent of identifying items that would not be subject to the engagement. The results of this review are set out in Appendix B.

Principle 1: Code Signing Business Practices Disclosure

The Certification Authority (CA) discloses its Code Signing Certificate practices and procedures and its commitment to provide CS Certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

#	Criterion	CS BR Ref[1]
1	The CA and its Root CA discloses[2] on its website: • CS Certificate practices, policies and procedures; • Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e., the Cross Certificate at issue); • CAs in the hierarchy whose subject name is the same as the CS issuing CA; and • its commitment to conform to the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates issued by the CA/Browser Forum.	2.2
2	The Certificate Authority has published guidelines for revoking CS Certificates.	4.9.2
3	The CA provides instructions on its website to Anti-Malware Organization, Subscribers, Relying Parties, Application Software Vendors and other third parties for reporting complaints or suspected private key compromise, CS Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks or other types of fraud, compromise, misuse, or inappropriate conduct related to CS Certificates to the CA.	4.9.2
4	The CA and its Root has controls to provide reasonable assurance that there is public access to the CP and/or CPS on a 24/7 basis, and the content and structure of the CP and/or CPS are in accordance with RFC 3647.	2.2
5	The Certificate Authority has controls to provide reasonable assurance that the CA CP and/or CPS that describes how the CA implements the latest version of the Baseline Requirements are updated annually.	2.3

1 Reference to the applicable section(s) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates for this criterion. The practitioner is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.

2 The criteria are those in scope for WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements. For an initial "readiness assessment" where there has not been a minimum of two months of operations, disclosure to the public is not required. The CA, however, must have all other aspects of the disclosure completed such that the only action remaining is to activate the disclosure so that it can be accessed by users in accordance with the CS BRs.

Principle 2: Code Signing Service Integrity

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:

- CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
- The integrity of keys and CS certificates it manages is established and protected throughout their life cycles.

Key generation ceremonies

#	Criterion	CS BR Ref
1.1	The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs used for CS Certificates are created in accordance with CS Baseline Requirements Section 6.1.1.1.	6.1.1.1

Certificate content and profile

Certificate content and profile

#	Criterion	CS BR Ref
2.1	The CA maintains controls to provide reasonable assurance that CS certificates issued meet the minimum requirements for Certificate Content and Profile based on both the applicable requirements of Non-EV and EV Code Signing Certificates, including additional technical requirements as specifically established in section 9 of the CS BRs, including the following: • Issuer Common Name Field • Issuer Domain Component Field • Issuer Organization Name Field • Issuer Country Name Field	7.1.4.1, 7.1.4.2.

#	Criterion	CS BR Ref
2.1 (cont'd)	• Subject Organization Name Field • Subject Street Address Field • Subject Locality Name Field • Subject State or Province Field • Subject Postal Code Field • Subject Alternative Name Extension • Subject Common Name Field • Subject Domain Component Field • Subject Organizational Unit Field • Other Subject Attributes	7.1.4.1, 7.1.4.2
2.2	The CA maintains controls to provide reasonable assurance that EV CS certificates issued meet the minimum requirements for Subject Distinguished Name Fields certificates, including additional technical requirements as specifically established in section 9 of the CS BRs.	7.1.4.2.4
2.3	The CA maintains controls to provide reasonable assurance that Certificates issued include the minimum requirements for the content of CS Certificates, including: • Certificate Policy Identification requirements • Subscriber Public Key • Certificate Serial Number • Minimum Cryptographic Algorithm and Key Size Requirements • Certificate Extensions as established in the CS BRs relating to: — CS Subscriber Certificates — CS Subordinate CA Certificates — CS Root CA Certificates — Timestamp Certificates — Timestamp Subordinate CA Certificates — Timestamp Root CA Certificates — Timestamp Tokens	7.1.6, 7.1

#	Criterion	CS BR Ref
2.4	The CA maintains controls to provide reasonable assurance that: • Code Signing Certificates issued to a Subscriber are valid for a period not exceeding 39 months; • Non-EV Code Signing Certificates issued to a Signing Service that fully complies with the CS BRs are valid for a period not exceeding 39 months; • Time Stamping Certificates issued to a Timestamp Authority that fully complies with the CS BRs are valid for a period not exceeding 135 months; and • Time Stamping Certificates issued to a Timestamp Authority are replaced with a new certificate and a new private key no later than every 15 months.	6.3.2

CS Certificate requests and code signing requests requirements

#	Criterion	CS BR Ref
3.1	The CA maintains controls to provide reasonable assurance that the CS Certificate Request or Signing Service Signing Request obtained is complete prior to the issuance of CS Certificates or signing of code, including the following in accordance with the CS BRs: • General requirements • Request and certification • Information requirements • Subscriber key requirements	4.1.2

Subscriber agreements and terms of use

#	Criterion	CS BR Ref
3.2	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of a CS Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the CS BRs. That agreement is: • signed by the Applicant; and • contains provisions imposing obligations and warranties on the Application relating to: — the accuracy of information — protection of Private Key — use of the CS certificate — compliance with industry standards — prevention of misuse — acceptance of the CS certificate — reporting and revocation — sharing of information — termination of use of the CS certificate — acknowledgement and acceptance.	9.6.3
3.3	The CA maintains controls to provide reasonable assurance that Subscriber and/or Terms Agreements between itself and its customers (if operating as a Signing Service) and/or between its Signing Services and their customers: • are signed by an authorized Contract Signer; • names the applicant and the individual Contract Signer; • provide notification to the CA when it becomes aware that it has signed code containing malicious code or a serious vulnerability; • provide notification to the CA and request revocation when it suspects it private key or private key activation data has been compromised or believed to be compromised; and • contain provisions imposing obligations and warranties to their clients relating to: — use of the signing service; — not knowingly submitting suspect code for signing; and — reporting signed code contained malware or a serious vulnerability.	9.6.5

Subscriber and subordinate CA private keys

#	Criterion	CS BR Ref
3.4	The CA maintains controls to provide reasonable assurance that it does not archive the Subscriber or Subordinate CA Private Keys. Additionally, if the CA or any of its designated Ras generated the Private Key on behalf of the Subscriber or Subordinate CA, then the entity generating the Private Key must either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption. The CA only archives a Subscriber or Subordinate CA Private Key if it receives authorization from the Subscriber or Subordinate CA.	6.1.2
3.5	The CA maintains controls to provide reasonable assurance that it rejects a certificate request if one or more of the following conditions are met: 1. The Key Pair does not meet the requirements set forth in Sections 6.1.5 or 6.1.6; 2. There is clear evidence that the specific method used to generate the Private Key was flawed; 3. The CA is aware of a demonstrated proven method that exposes the Applicant's Private Key to compromise; 4. The CA Key Compromise has previously been made aware that the Applicant's Private Key has suffered such as through the provisions of Section 4.9.1.1; The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a **Debian weak key**.	6.1.1.3

Information verification requirements

Verification of organizational applicants

#	Criterion	CS BR Ref
4.1	The CA maintains controls to provide reasonable assurance that prior to issuing a CS Certificate, it verifies the identity of Organizational Applicants in accordance with the CS BRs, including the following: • Legal identity (including any DBA names to be included in the CS Certificate) in accordance with SSL BR Sections 3.2.2.1 and 3.2.2.2. The CA MUST also obtain, whenever available, a specific Registration Identifier assigned to the Applicant by a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition. • Address in accordance with SSL BR Section 3.2.2.1 • Certificate Requester's authority to obtain a CS Certificate • Certificate Requester's Identity • Registration Identifier • Authenticity of Certificate Request	3.2.2.1, 3.2.2.2, 3.2.5

Verification of individual applicants

#	Criterion	CS BR Ref
4.2	The CA maintains controls to provide reasonable assurance that prior to issuing a CS Certificate, it verifies the identity of Individual Applicants in accordance with section 3.2.3 of the CS BRs, including the following: • Individual identity • Authenticity of identity	3.2.3

High risk applicants

#	Criterion	CS BR Ref
4.7	The CA maintains controls to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates (including those relating to Code Signatures on Suspect Code) and previously rejected certificate requests to identify subsequent suspicious certificate requests.	4.2.1
4.8	The CA maintains controls to provide reasonable assurance that the CA identifies high risk certificate requests, and conducts additional verification activities, including: • activities in accordance with Section 4.2.2 of the Requirements • determining whether the entity is identified as requesting a Code Signing Certificate from a High-Risk Region of Concern	4.2.2
4.9	The CA maintains controls to provide reasonable assurance that it processes High-Risk Applications in accordance with Section 4.2.2 of the CS BRs.	4.2.2

Certificate issuance by a Root CA

#	Criterion	CS BR Ref
4.10	The CA maintains controls to provide reasonable assurance that certificate issuance by the Root CA shall require an individual authorized by the CA (i.e., the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.	4.3.1
4.11	The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign certificates or create other Signatures, except in the following cases: • Self-signed certificates to represent the Root CA itself; • Certificates for Subordinate CAs and Cross certificates; • Certificates for the infrastructure purposes (administrative role certificate, internal CA operational devices certificates); • Certificates for OCSP Response verification; and • Signature for OCSP Responses.	6.1.7

Other matters

#	Criterion	CS BR Ref
4.12	The CA maintains controls to provide reasonable assurance that: • the set of information gathered to support a certificate request is reviewed for completeness and accuracy by an individual who did not gather such information; and • any identified discrepancies are documented and resolved before certificate issuance. (Note requirements reference Section 11.13 of the EV guidelines "Final Cross-Correlation and Due Diligence")	4.2.1
4.13	The CA maintains controls to provide reasonable assurance that, prior to using a data source, the CA evaluates the data source's accuracy and reliability in accordance with the requirements set forth in Section 3.2.7. For Non-EV Code Signing Certificates, if the CA uses the documents and data provided in Section 3.2 to verify certificate information, or reuses previous validations themselves, the CA obtains the data or document from a source specified under Section 3.2 or completes the validation itself no more than 825 days prior to issuing the Certificate.	3.2.7, 4.2.1

Certificate revocation and status checking

#	Criterion	CS BR Ref	SSL BR Ref
5.1	The CA maintains controls to provide reasonable assurance that a process is available 24/7 that the CA is able to accept and respond to revocation requests and related inquiries, and that the CA provides a process for Subscribers to request revocation of their own certificates.	4.9.3	

#	Criterion	CS BR Ref	SSL BR Ref
5.2	The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24/7 basis; • identifies high-priority Certificate Problem Reports; • begins investigation of Certificate Problem Reports within 24 hours; • decides whether revocation or other appropriate action is warranted; and • where appropriate, forwards such complaints to law enforcement.	4.9.3, 4.9.5	
5.3	The CA maintains controls to provide reasonable assurance that prior to 2024-04-15, the CA treats revocation of Certificates in accordance with the requirements specified in Section 4.9 of the current version of the CS BRs, or Section 4.9 specified in version 3.2.0 of the CS BRs. Effective 2024-04-15, the CA treats revocation of Certificates in accordance with Section 4.9 specified in the current version of the CS BRs. The CA maintains controls to provide reasonable assurance that when revocation of a Subscriber Certificate is done due to a Key Compromise or use in Suspect Code the CA determines an appropriate value for the revocation Date based on its own investigation. The CA sets a Historic date as revocation Date if deemed appropriate.	4.9, 4.9.1	4.9
5.4	The CA maintains controls to provide reasonable assurance that a Certificate is revoked within 24 hours if one or more of the following occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; 4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;	4.9.1.1	

#	Criterion	CS BR Ref	SSL BR Ref
5.4	5. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed; 6. The CA has reasonable assurance that a Certificate was used to sign Suspect Code; The CA maintains controls to provide reasonable assurance that a Certificate is revoked within five days if one or more of the following occurs: 7. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6; 8. The CA obtains evidence that the Certificate was misused. 9. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use. 10. The CA is made aware of a material change in the information contained in the Certificate. 11. The CA is made aware that the Certificate was not issued in accordance with these [CA Browser] Requirements or the CA's Certificate Policy or Certification Practice Statement. 12. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate. 13. The CA's Right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository. 14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement. The CA MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.	4.9.1.1	

#	Criterion	CS BR Ref	SSL BR Ref
5.5	The CA maintains controls to provide reasonable assurance that Subordinate CA Certificates are revoked within seven days if any of the following events occurs: 1. The Subordinate CA requests revocation in writing; 2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and Section 6.1.6; 4. The Issuing CA obtains evidence that the Certificate was misused; 5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these Requirements or the applicable Certificate Policy or Certification Practice Statement; 6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or 9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.	4.9.1.2	

#	Criterion	CS BR Ref	SSL BR Ref
5.6	The CA maintains controls to provide reasonable assurance that an online 24/7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • For the status of Subordinate CA Certificates: — The Issuing CA SHALL publish a CRL, then update and reissue a CRL at least once every 12 months and within 24 hours after revoking a Subordinate CA Certificate. The nextUpdate field MUST NOT be more than 12 months beyond the value of the thisUpdate field; and — If the Issuing CA provides OCSP responses, the Issuing CA SHALL update information provided via an OCSP response at least every 12 months and within 24 hours after revoking a Subordinate CA Certificate; • For the status of Code Signing Certificates: The Subordinate CA SHALL publish a CRL, then update and reissue a CRL at least once every seven days, and the value of the nextUpdate field MUST NOT be more than 10 days beyond the value of the thisUpdate field; and • If the Subordinate CA provides OCSP responses, the Subordinate CA SHALL update information provided via an OCSP response at least every four days. OCSP responses from this service MUST have a maximum expiration time of 10 days. • For the status of Timestamp Certificates — The Subordinate CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Timestamp Certificate, and the value of the nextUpdate field must not be more than 12 months beyond the value of the thisUpdate field; and — The Subordinate CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Timestamp Certificate. • If the Issuing CA provides OCSP responses, the Issuing CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the CS BRs.	4.9.7, 4.9.10	
5.7	The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.	4.10.2	

#	Criterion	CS BR Ref	SSL BR Ref
5.8	The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP responses for revoked Subscriber Code Signing Certificates and revoked Timestamp Certificates for at least 10 years following the expiry date of the certificate, unless the certificate contained the Lifetime Signing OID. Revocation entries on an OCSP response remain for the same amount of time as for the CRL entries, as described in Section 7.2.	4.9.10, 4.10.1, 7.2	
5.9	The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either: • by the CA that issued the Certificates whose revocation status is being checked; or • by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960).	4.9.9	
5.10	The CA maintains controls to provide reasonable assurance that if the OCSP responder receives a request for the status of a certificate serial number that is not “assigned,” as defined in Section 4.9.10, then the responder DOES NOT respond with a “good” status.	4.9.10	
5.11	The CA maintains controls to provide reasonable assurance that its Repository does not include entries that indicate that a Certificate is suspended, effective 2023-09-15.	4.9.13	5.11

Employees and third parties

#	Criterion	CS BR Ref	SSL BR Ref
6.1	The CA maintains controls to provide reasonable assurance that prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA: 1. Verifies the identity of such person: Verification of identity is performed through: a. The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and b. The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses); 2. Verifies the trustworthiness of such person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent: a. Confirmation of previous employment, b. Check of professional references; c. Confirmation of the highest or most-relevant educational qualification obtained; d. Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed; and In the case of employees already in the employ of the CA at the time of adoption of these Guidelines whose identity and background has not previously been verified as set forth above, conducts such verification within three months of the date of adoption of these Guidelines.		

#	Criterion	CS BR Ref	SSL BR Ref
6.2	The CA maintains controls to provide reasonable assurance that the CA shall meet the requirements of EV Guidelines Section 14.1 for Non-EV and EV Code Signing Certificates: • The CA and its Signing Services provide all personnel performing information verification duties (Validation Specialists) with skills – training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. • The CA and its Signing Services maintain records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. • The CA and its Signing Services document each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. • The CA and its Signing Services require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. • All personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.	1.3.2, 5.3.3, 5.3.4	
6.3	The CA maintains controls to provide reasonable assurance that its employees and its Signing Services' Delegated Third Parties meet the qualification requirements of Section 14.1 of EV Guidelines for non-EV and EV Code Signing Certificates.	5.3	N/A
6.4	The CA maintains controls to provide reasonable assurance that the CA and its Signing Services verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of the CS BRs Section 5.3, and the document retention and event logging requirements of the CS BRs Section 5.4.	5.3, 5.4.1	5.3.3, 5.4.1

#	Criterion	CS BR Ref	SSL BR Ref
6.5	For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA and its Signing Services verify that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests.	4.2.1, 4.2.2	N/A
6.6	The CA maintains controls to provide reasonable assurance that the Subject of a specified valid EV Code Signing Certificate is not permitted to perform the RA function and authorize the CA to issue additional EV Code Signing Certificates.		

Data records

#	Criterion	CS BR Ref	SSL BR Ref
7.1	The CA maintains controls to provide reasonable assurance that the CA and its Signing Services record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.	5.4.1.1	

#	Criterion	CS BR Ref	SSL BR Ref
7.2	The CA maintains controls to provide reasonable assurance that at least the following events are recorded by itself and its Signing Services: • CA certificate and key lifecycle management events, including: — key generation, backup, storage, recovery, archival, and destruction — Certificate requests, renewal, and re-key requests, and revocation — Approval and rejection of certificate requests — Cryptographic device lifecycle management events — Generation of Certificate Revocation Lists and OCSP entries — Introduction of new Certificate Profiles and retirement of existing Certificate Profiles • CA and Subscriber lifecycle management events, including: — Certificate Requests, renewals, re-key requests, and revocation — all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement — acceptance and rejection of certificate requests — issuance of Certificates — generation of Certificate Revocation Lists and OCSP entries; — signing of OCSP Responses • security events, including: — successful and unsuccessful PKI system access attempts — PKI and security system actions performed — security profile changes — system crashes, hardware failures, and other anomalies — firewall and router activities — entries to and exits from CA facility. • Log entries must include the following elements: — Date and time of entry — Identity of the person making the journal entry — Description of entry	5.4.1.1	

#	Criterion	CS BR Ref	SSL BR Ref
7.3	The CA maintains controls to provide reasonable assurance that the CA, and Delegated Third Parties, retain, for at least two years: 1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1.1) after the later occurrence of: a. the destruction of the CA Private Key; or b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key; 2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1.2) after the revocation or expiration of the Subscriber Certificate; 3. Timestamp Authority data records (as set forth in Section 5.4.1.2) after the revocation or renewal of the Timestamp Certificate private key (as set forth in Section 6.3.2); and 4. Any security event records as set forth in Section 5.4.1.1 (3) and for Timestamp Authority security event records set forth in Section 5.4.1.2 (3) after the event occurred.	5.4.3	5.4.3
7.4	The CA maintains controls to provide reasonable assurance that the following events for its Timestamp Authority are recorded: 1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server; 2. History of the timestamp server configuration; 3. Any attempt to delete or modify timestamp logs; 4. Security events, including: a. Successful and unsuccessful Timestamp Authority access attempts; b. Timestamp Authority server actions performed; c. Security profile changes; d. System crashes, and other anomalies; e. Firewall and router activities; and f. Entries to and exits from the CA facility; 5. Revocation of a timestamp certificate; 6. Major changes to the timestamp server's time; and 7. System startup and shutdown.	5.4.1	

Vulnerability assessments

#	Criterion	CS BR Ref
7.5	The CA maintains controls to provide reasonable assurance that its security program includes an annual risk assessment that: 1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; 2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and 3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.	5.4.8

Audit and legal

#	Criterion	CS BR Ref
8.1	The CA maintains controls to provide reasonable assurance that: • Independent audits of any function performed by a Delegated Third Party are performed; • The audit period of the Delegated Third Party does not exceed one year; and • If the Delegated Third Party is found to be non-compliant with the CS BRs, the CA does not allow the Delegated Third Party to continue performing its functions.	8.1
8.2	The CA maintains controls to provide reasonable assurance that: • Applicable requirements of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates are included (directly or by reference) in contracts with Subordinate CAs, RAs, Signing Services and subcontractors that involve or relate to the issuance or maintenance of Certificates, and that they are contractually obligated to comply with the applicable requirements in the CS BRs and to perform them as required of the CA itself; and • The CA monitors and enforces compliance with the terms of the contracts.	8., 8.1, 1.3.2

#	Criterion	CS BR Ref
8.3	The CA maintains controls to provide reasonable assurance that it complies with: • laws applicable to its business and the certificates it issues in each jurisdiction where it operates; and • licensing requirements in each jurisdiction where it issues EV CS certificates.	8.

Timestamp authority, signing services and private key protection

#	Criterion	CS BR Ref
9.1	The CA maintains controls to provide reasonable assurance that: • It operates an RFC-3161-compliant Timestamp Authority that is available for use by customers of its Code Signing Certificates • It recommends to Subscribers that they use the CA's Timestamping Authority to time-stamp signed code.	6.8
9.2	The CA maintains controls to provide reasonable assurance that: • It protects its Timestamp Authority signing key using a process that is at least to FIPS 140-2 Level 3, Common Criteria EAL 4+ (ALC_FLR.2), or higher. • Any changes to its Timestamp signing process are an auditable event. • The Timestamp Authority ensures that clock synchronization is maintained when a leap second occurs. • The Timestamp Authority synchronizes its timestamp server at least every 24 hours with a UTC(k) time source • The timestamp server is configured to automatically detect and report on clock drifts or jumps out of synchronization with UTC. • Clock adjustments of one second or greater are auditable events.	6.2.7.2, 6.8

#	Criterion	CS BR Ref
9.3	The CA maintains controls to provide reasonable assurance that, for Non-EV Code Signing Certificates issued prior to June 1 2023, it obtains a representation from its Subscribers that they will protect their Code Signing Private Keys using one of the following methods: 1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber's Private Key protection through a TPM key attestation. 2. A suitable Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent. 3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun. And, the CA communicates to the subscriber that Method 1 and 2 above needs to be followed over Method 3 above. The CA maintains controls to provide reasonable assurance that, effective June 1, 2023, it obtains a representation from its Subscribers that they will use one of the following methods to generate and protect their Code Signing Certificate Private Key in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+: • Subscriber uses a Hardware Crypto Module meeting the specified requirement; • Subscriber uses a cloud-base key generation and protection solution with the following requirements: — Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements; — Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key; and — Subscriber uses a Signing Service which meets the requirement of Section 6.2.7.3 of the CS BRs.	6.2.7.4.1
9.4	The CA maintains controls to provide reasonable assurance that Signing Services Subscriber uses a Signing Service that meets the requirements of section 6.2.7.	6.2.7.3

#	Criterion	CS BR Ref
9.5	The CA maintains controls to provide reasonable assurance that effective June 1 2023, the Subscriber's Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets or exceeds the requirements specified in Section 6.2.7.4.1 using one of the following methods: • The CA ships a suitable Hardware Crypto Module, with one or more pre-generated Key Pairs that the CA has generated using the Hardware Crypto Module; • The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Mode; • The Subscriber uses a CA prescribed crypto library and a suitable Hardware Crypto Module combination for the Key Pair generation and storage; • The Subscriber provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates; • The Subscriber provides a suitable report from the cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware Crypto Module; • The CA relies on a report provided by the Applicant that is signed by an auditor who is approved by the CA and who has IT and security training or has a CISA certification witnesses the Key Pair creation in a suitable Hardware Crypto Module solution, including a cloud-based key generation and protection solution; • The Subscriber provides an agreement that they use a Signing Service meeting the requirements of section 6.2.7.3.	6.2.7.4.2, 5.2.2, 6.2

Principle 3: Extended Validation Code Signing Service Integrity

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:

- EV CS subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
- The integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles.

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
1.1	The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs used for EV CS Certificates are created in accordance with SSL CS Baseline Requirements Section 6.1.1.1.	6.1.1.1	17.7
1.2	The CA maintains controls to provide reasonable assurance that Root CA Key Pairs used for EV CS certificates created on or after 1 June 2021: • have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process, and • have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.	6.1.1.1	17.7

3 Reference to the applicable section(s) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates for this criterion. The practitioner is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.

4 Reference to the applicable section(s) of the EV SSL Guidelines for this criterion. The practitioner is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
2.1.1	The CA maintains controls to provide reasonable assurance that it issues EV CS Certificates to Private Organizations as defined within the EV Guidelines that meet the following requirements: • The organization is a legally recognized entity whose existence was created or recognized by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation registration number, etc.) or created or recognized by a Government Agency (e.g., under a charter, treaty, convention, or equivalent recognition instrument); • The entity designated with the Incorporating or Registration Agency a Registered Agent, or a Registered Office (as required under the laws of the jurisdiction of Incorporation or Registration), or an equivalent facility; • The entity is not designated as inactive, invalid, non-current or equivalent in records of the Incorporating Agency or Registration Agency; • The entity has a verifiable physical existence and business presence; • The entity's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • The entity is not listed on a published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.	3.2.2.2	8.5.2
2.1.2	The CA maintains controls to provide reasonable assurance that it issues EV CS Certificates to Government Entities as defined within the EV Guidelines that meet the following requirements: • The entity's legal existence was established by the political subdivision in which the entity operates; • The entity is not in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • The entity is not listed on a government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.	3.2.2.2	8.5.3

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
2.1.3	The CA maintains controls to provide reasonable assurance that it issues EV CS Certificates to Business Entities as defined within the EV Guidelines that meet the following requirements: • The entity is a legally recognized entity that filed certain forms with a Registration Agency in its Jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency; • The entity has a verifiable physical existence and business presence; • At least one Principal Individual associated with the entity (owners, partners, managing members, directors or officers) is identified and validated by the CA; • The identified Principal Individual (owners, partners, managing members, directors or officers) attests to the representations made in the Subscriber agreement; • The CA verifies the entity's use of any assumed name, used to represent the entity pursuant to the requirements of Section 11.3 of EV Guidelines; • The entity and the identified Principal Individual (owners, partners, managing members, directors or officers) associated with the entity are not located in a country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • The entity and the identified Principal Individual (owners, partners, managing members, directors or officers) associated with the entity are not listed on any published government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.	3.2.2.2	8.5.4

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
2.1.4	The CA maintains controls to provide reasonable assurance that it issues EV CS Certificates to Non-Commercial Entities as defined within the EV Guidelines that meet the following requirements: • The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government and; • The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and • The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.	3.2.2.2	8.5.5
2.2.1	The CA maintains controls to provide reasonable assurance that EV CS certificates issued meet the minimum requirements for Certificate Content and Profile, including additional technical requirements as specifically established in section 9 of the EV Guidelines, including the following: • Issuer Common Name Field • Issuer Domain Component Field • Issuer Organization Name Field • Issuer Country Name Field • Full legal organization name • Subject Alternative Name Extension • Subject Common Name Field • Subject Business Category Field • Subject Jurisdiction of Incorporation or Registration Field • Subject Registration Number Field • Subject Physical Address of Place of Business Field • Other Subject Attributes	7.1.4.1	9

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
2.2.2	The CA maintains controls to provide reasonable assurance that EV CS Certificates issued include the minimum requirements for the content of EV CS Certificates, including: • Certificate Policy Identification requirements • Subscriber Public Key • Certificate Serial Number • Additional Technical Requirements for EV Code Signing • Certificates as established in the EV Guidelines relating to: — EV CS Subscriber Certificates — EV Subordinate CA Certificates.	7.1.4.2.4	9
2.2.3	The CA maintains controls to provide reasonable assurance that: • EV Code Signing Certificates issued to a Subscriber are valid for a period not exceeding 39 months; • EV Code Signing Certificates issued to a Signing Service that fully complies with the EV Code Signing Guidelines are valid for a period not exceeding 135 months; and • EV Time Stamping Certificates issued to a Timestamp Authority that fully complies with the EV Code Signing Guidelines are valid for a period not exceeding 135 months.	6.3.2	N/A
2.2.4	The CA maintains controls to provide reasonable assurance that the data that supports the EV CS Certificates is revalidated within the timeframes established in the EV Guidelines Section 11.14.	4.2.1	11.14.3

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
3.1	The CA maintains controls to provide reasonable assurance that the EV CS Certificate Request is: • obtained and complete prior to the issuance of EV CS Certificates; • signed by an authorized individual (Certificate Requester); • approved by an authorized individual (Certificate Approver) • properly certified as to being correct by the applicant; and • contains the information specified in Section 10 of the EV Guidelines.	4.1.2	10
3.2	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of an EV CS Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the EV Guidelines. That agreement is: • signed by an authorized contract signer; • names the applicant and individual contract signer; and • contains provisions imposing obligations and warranties on the Application relating to: — the accuracy of information — protection of Private Key — acceptance of the EV CS certificate — use of the EV CS certificate — reporting and revocation upon compromise — termination of use of the EV CS certificate — responsiveness — acknowledgement and acceptance.	9.6.3	10.3

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
3.3	The CA maintains controls to provide reasonable assurance that Subscriber and/or Terms Agreements between itself and its customers (if operating as a Signing Service) and/or between its Signing Services and their customers: • are signed by an authorized Contract Signer; • names the applicant and the individual Contract Signer; • notification to the CA when it becomes aware that it has signed code containing malicious code or a serious vulnerability; • notification to the CA and request revocation when it suspects its private key or private key activation data has been compromised or believed to be compromised; and • contains provisions imposing obligations and warranties to their clients relating to: — use of the EV Signature; — not knowingly submitting suspect code for signing; and — reporting signed code contained malware or a serious vulnerability.	9.6.5	10.3

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
4.1	The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the EV Guidelines: For Private Organization Subjects: • legal existence and identity • legal existence and identity – assumed name • organization name • registration number • registered agent • relationship to the parent, subsidiary or affiliate (if applicable) For Government Entities: • legal existence • entity name • registration number For Business Entities: • legal existence • organization name • registration number • principal individual • relationship to the parent, subsidiary, or affiliate (if applicable) For Non-Commercial Entities: • International Organization Entities — legal entities — entity name — registration number	3.2.2.2	11.2
4.2	The CA maintains controls to provide reasonable assurance that it verifies the physical address provided by Applicant is an address where Applicant or a Parent/ Subsidiary company conducts business operations (e.g., not a mail drop or P.O. box, or "care of" C/O address, such as an address of an agent of the Organization), and is the address of Applicant's Place of Business using a method of verification established by the EV Guidelines.	3.2.2.2	11.2

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
4.3	The CA maintains controls to provide reasonable assurance that it verifies a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant by performing the steps set out in the EV Guidelines.	3.2.2.2	11.2
4.4	The CA maintains controls to provide reasonable assurance that it verifies the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence by: • verifying that the Applicant, Affiliate, Parent Company or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency; • verifying that the Applicant, Affiliate, Parent Company or Subsidiary Company is listed in either a current QIIS or QTIS; • verifying that the Applicant, Affiliate, Parent Company or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or • relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.	3.2.2.2	11.1.1
4.5	The CA maintains controls to provide reasonable assurance that EV CS Certificates do not contain a domain name.	3.2.2.2	
4.6	Reference reserved for future use.	N/A	
4.7	The CA maintains controls to provide reasonable assurance that the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests.	4.1.1	11.5, 11.12.2

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
4.8	The CA maintains controls to provide reasonable assurance that it identifies "High-Risk Applicants" and undertakes additional precautions as are reasonably necessary to ensure that such Applicants are properly verified using a verification method below: • The CA identifies high risk requests by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and by automatically flagging certificate requests that match these lists for further scrutiny before issuance; and • The CA shall use information identified by the CA's high-risk criteria to flag suspicious certificate requests. The CA shall follow a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk.	4.2.1	11.5
4.9	The CA maintains controls to provide reasonable assurance that no EV CS Certificate is issued if the Applicant, the Contract Signer, the Certificate Approver or the Applicant's Jurisdiction of Incorporation, Registration or place of Business is: • on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or • has its Jurisdiction of Incorporation, or Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.	4.2.1	11.5
4.10	The CA maintains controls to provide reasonable assurance that it verifies, using a method of verification established by the EV Guidelines: • the name and title of the Contract Signer and the Certificate Approver, as applicable and verifying that the Contract Signer and the Certificate Approver are agents representing the Applicant; • through a source other than the Contract Signer, that the Contract Signer is expressly authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant ("Signing Service");	3.2.2.2	11.2

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
4.10 (cont'd)	• through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV CS Certificate Request ("EV Authority") to: — submit, and if applicable authorize a Certificate Requester to submit, the EV CS Certificate Request on behalf of the Applicant; and — provide, and if applicable authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV CS Certificate; and — approve EV CS Certificate Requests submitted by a Certificate Requester.	3.2.2.2	11.2
4.11	The CA maintains controls to provide reasonable assurance, using a method of verification established in the EV Guidelines that: • subscriber Agreements are signed by an authorized Contract signer; • the EV CS Certificate Request is signed by the Certificate Requester submitting the document; • if the Certificate requester is not also an authorized Certificate Approver, an authorized Certificate Approver independently approves the EV CS Certificate Request unless pre-authorized; and • Code Signatures have been properly authenticated.	3.2.2.2	11.2
4.12	The CA maintains controls to provide reasonable assurance that in cases where an EV CS Certificate Request is submitted by a Certificate Requester, before it issues the requested EV CS Certificate, it verifies that an authorized Certificate Approver reviewed and approved the EV CS Certificate Request.	3.2.2.2	11.2

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
4.13	The CA maintains controls to provide reasonable assurance that it verifies information sources prior to placing reliance on them using a verification procedure set out in the EV Guidelines. The verification includes: • with respect to legal opinions: — the independent status of the author — the basis of the opinion — authenticity • with respect to accountants' letters: — the status of the author — the basis of the opinion — authenticity • with respect to face-to-face vetting documents: — qualification of third-party validator — document chain of custody — verification of attestation • with respect to independent confirmation from applicant: — the request is initiated by the CA requesting verification of particular facts — the request is directed to a Confirming Person at the Applicant or at the Applicant's Registered Agent or Registered Office using one of the acceptable methods stated by the CA/Browser Forum — the Confirming Person confirms the fact or issue • with respect to Qualified Independent Information Sources (QIIS): — the database used is a QIIS as defined by the EV SSL Guidelines 11.11.5). • with respect to Qualified Government Information Sources (QGIS): — the database used is a QGIS as defined by the EV SSL Guidelines 11.11.6 • with respect to Qualified Government Tax Information Source (QGTIS): — a Qualified Governmental information source is used that specifically contains tax information relating to Private Organizations, Business Entities or Individuals as defined by the EV SSL Guidelines 11.11.7.	3.2.2.2	11.11

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
4.14	The CA maintains controls to provide reasonable assurance that in conjunction with an EV CS Certificate Request placed by an Applicant who is already a customer of the CA, the CA performs all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV CS Certificate will still be accurate and valid, subject to any exceptions as outlined in EV SSL Guidelines Section 11.14.1 and re-issuance requests in EV SSL Guidelines Section 11.14.2.	4.2.1	11.14
4.15	The CA maintains controls to provide reasonable assurance that the system used to process and approve EV CS Certificate Requests requires actions by at least two trusted persons before the EV CS Certificate is created.	11.8	
4.16	The CA maintains controls to provide reasonable assurance that there is a separation of duties such that no one person can both validate and authorize the issuance of an EV CS Certificate at both the CA and Signing Services.	11.8	
4.19	The CA maintains controls to provide reasonable assurance that due diligence is performed as specified in Section 11.13 of the EV Guidelines. • The set of information gathered to support a certificate request is reviewed for completeness and accuracy by an individual who did not gather such information; • Further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation; • In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the Final Cross-Correlation and Due Diligence is performed by employees under its control having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 14.1.	4.2.1	11.13

#	Criterion	CS BR Ref[3]	EV SSL Ref[4]
4.19 (cont'd)	— When employees do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA shall rely on the translations by a Translator; or — If an RA is used, the CA must review the work completed by the RA and determine that all requirements have been met; or — The CA shall rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with its requirements and is subjected to the Audit Requirements of Sections 17.5 and 17.6 as specified in the EV SSL Guidelines.	4.2.1	11.13

Certificate revocation and status checking

#	Criterion	CS BR Ref[3]
5.1	The CA maintains controls to provide reasonable assurance that a process is available 24/7 that the CA is able to accept and respond to revocation requests and related inquiries, and that the CA provides a process for Subscribers to request revocation of their own certificates.	4.9.3
5.2	The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24/7 basis; • identifies high priority Certificate Problem Reports; • begins investigation of Certificate Problem Reports within 24 hours; • decides whether revocation or other appropriate action is warranted; and • where appropriate, forwards such complaints to law enforcement.	4.9.3

#	Criterion	CS BR Ref[3]
5.3	The CA maintains controls to provide reasonable assurance that prior to 2024-04-15, the CA treats revocation of Certificates in accordance with the requirements specified in Section 4.9 of the current version of the CS BRs, or Section 4.9 specified in version 3.2.0 of the CS BRs. Effective 2024-04-15, the CA treats revocation of Certificates in accordance with Section 4.9 specified in the current version of the CS BRs. The CA maintains controls to provide reasonable assurance that when revocation of a Subscriber Certificate is done due to a Key Compromise or use in Suspect Code, the CA determines an appropriate value for the revocation Date based on its own investigation. The CA sets a Historic date as revocation Date if deemed appropriate.	4.9.1
5.4	The CA maintains controls to provide reasonable assurance that a Certificate is revoked within 24 hours if one or more of the following occurs: 1. The Subscriber requests in writing that the CA revoke the Certificate; 2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; 4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate; 5. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed; or 6. The CA has reasonable assurance that a Certificate was used to sign Suspect Code. The CA maintains controls to provide reasonable assurance that a Certificate is revoked within five days if one or more of the following occurs: 7. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6; 8. The CA obtains evidence that the Certificate was misused. 9. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use. 10. The CA is made aware of a material change in the information contained in the Certificate.	4.9.1.1

#	Criterion	CS BR Ref[3]
5.4 (cont'd)	11. The CA is made aware that the Certificate was not issued in accordance with these [CA Browser] Requirements or the CA's Certificate Policy or Certification Practice Statement. 12. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate. 13. The CA's Right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository. 14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement. The CA MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.	4.9.1.1
5.5	The CA maintains controls to provide reasonable assurance that Subordinate CA Certificates are revoked within 7 days if any of the following events occurs: 1. The Subordinate CA requests revocation in writing; 2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization; 3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6; 4. The Issuing CA obtains evidence that the Certificate was misused; 5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the CS BRs or the applicable Certificate Policy or Certification Practice Statement; 6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading; 7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or 9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.	4.9.1

#	Criterion	CS BR Ref[3]
5.6	The CA maintains controls to provide reasonable assurance that an online 24/7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subordinate CA Certificates: — The Issuing CA SHALL publish a CRL, then update and reissue a CRL at least once every 12 months and within 24 hours after revoking a Subordinate CA Certificate. The nextUpdate field MUST NOT be more than 12 months beyond the value of the thisUpdate field; and • If the Issuing CA provides OCSP responses, the Issuing CA SHALL update information provided via an OCSP response at least every 12. • for the status of Timestamp Certificates — The Subordinate CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Timestamp Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and — The Subordinate CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Timestamp Certificate. If the Issuing CA provides OCSP responses, the Issuing CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the CS BRs.	4.9.9, 4.9.7, 4.9.10
5.7	The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.	4.10.2

#	Criterion	CS BR Ref[3]
5.8	The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP responses for revoked Subscriber Code Signing Certificates and revoked Timestamp Certificates for at least 10 years following the expiry date of the certificate, unless the certificate contained the Lifetime Signing OID. Revocation entries on an OCSP response remain for the same amount of time as for the CRL entries, as described in Section 7.2.	4.9.10, 4.10.1, 7.2
5.9	The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either: • by the CA that issued the Certificates whose revocation status is being checked; or • by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960).	4.9.9
5.10	The CA maintains controls to provide reasonable assurance that if the OCSP responder receives a request for the status of a certificate serial number that is not “assigned,”, as defined in Section 4.9.10, then the responder MUST NOT respond with a “good” status.	4.9.10
5.11	Effective 2023-09-15, The CA maintains controls to provide reasonable assurance that its Repository does not include entries that indicate that a Certificate is suspended.	4.9.13

Employees and third parties

#	Criterion	CS BR Ref[3]
6.1	The CA maintains controls to provide reasonable assurance that prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA: 1. Verifies the identity of such person: Verification of identity is performed through: a. The personal (physical) presence of such person before trusted persons who perform human resource or security functions;, and b. The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licences); 2. Verifies the trustworthiness of such person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent: a. Confirmation of previous employment, b. Check of professional references; c. Confirmation of the highest or most-relevant educational qualification obtained; d. Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed; and 3. In the case of employees already in the employ of the CA at the time of adoption of these Guidelines whose identity and background has not previously been verified as set forth above conducts such verification within three months of the date of adoption of these Guidelines.	5.3.2

#	Criterion	CS BR Ref[3]
6.2	The CA maintains controls to provide reasonable assurance that: • The CA and its Signing Services provide all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements; • The CA and its Signing Services maintain records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily; • The CA and its Signing Services document each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task; • The CA and its Signing Services require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements; and • All personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.	1.3.2, 5.3.3, 5.3.4
6.3	The CA maintains controls to provide reasonable assurance that its and its Signing Services' Delegated Third Parties meet the qualification requirements of Section 14.1 of the EV Guidelines.	1.3.2
6.4	The CA maintains controls to provide reasonable assurance that the CA and its Signing Services verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of the CS BRs Section 5.3 and the document retention and event logging requirements of the CS BRs Section 5.4.	1.3.2, 5.3.7, 5.3.3, 5.4.1
6.5	For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA and its Signing Services verify that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests.	4.2.1
6.6	The CA maintains controls to provide reasonable assurance that the Subject of a specified valid EV Code Signing Certificate is not permitted to perform the RA function and authorize the CA to issue additional EV Code Signing Certificates.	N/A

Data records

#	Criterion	CS BR Ref[3]
7.1	The CA maintains controls to provide reasonable assurance that the CA and its Signing Services record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.	5.4.1
7.2	The CA maintains controls to provide reasonable assurance that the following events are recorded by itself and its Signing Services: • CA certificate and key lifecycle management events, including: — key generation, backup, storage, recovery, archival and destruction — Certificate requests, renewal and re-key requests, and revocation — approval and rejection of certificate requests — cryptographic device lifecycle management events. — generation of Certificate Revocation Lists and OCSP entries — introduction of new Certificate Profiles and retirement of existing Certificate Profiles. • CA and Subscriber lifecycle management events, including: — Certificate Requests, renewals and re-key requests, and revocation — all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement — acceptance and rejection of certificate requests — issuance of Certificates — generation of Certificate Revocation Lists (CRLs) and OCSP entries. — signing of OCSP Responses. • security events, including: — successful and unsuccessful PKI system access attempts — PKI and security system actions performed — security profile changes — system crashes, hardware failures, and other anomalies — firewall and router activities — entries to and exits from CA facility. • Log entries must include the following elements: — date and time of entry — identity of the person making the journal entry — description of entry	5.4.1

#	Criterion	CS BR Ref[3]
7.3	The CA maintains controls to provide reasonable assurance that the CA, and Delegated Third Parties, retain, for at least two years: 1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1.1) after the later occurrence of: a. the destruction of the CA Private Key; or b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key; 2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1.2) after the revocation or expiration of the Subscriber Certificate; 3. Timestamp Authority data records (as set forth in Section 5.4.1.2) after the revocation or renewal of the Timestamp Certificate private key (as set forth in Section 6.3.2); and 4. Any security event records (as set forth in Section 5.4.1.1 (3) and for Timestamp Authority security event records set forth in Section 5.4.1.2 (3) after the event occurred.	5.4.3
7.4	The CA maintains controls to provide reasonable assurance that the following events for its Timestamp Authority are recorded: 1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server; 2. History of the timestamp server configuration; 3. Any attempt to delete or modify timestamp logs; 4. Security events, including: a. Successful and unsuccessful Timestamp Authority access attempts; b. Timestamp Authority server actions performed; c. Security profile changes; d. System crashes, and other anomalies; e. Firewall and router activities; and f. Entries to and exits from the CA facility; 5. Revocation of a timestamp certificate; 6. Major changes to the timestamp server's time; and 7. System startup and shutdown.	5.4.1

Audit and legal

#	Criterion	CS BR Ref[3]
8.1	The CA maintains controls to provide reasonable assurance that: • it performs ongoing self-audits on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the EV CS Certificates issued during the period commencing immediately after the previous self-assessment samples were taken. For all EV CS certificates where the final cross-correlation and due diligence requirements of Section 8 are performed by a Delegated Third Party, the sample size is increased to at least six percent (6%).	8.7
8.2	The CA maintains controls to provide reasonable assurance that: • Applicable requirements of the CA/Browser Forum Guidelines for Extended Validation Certificates are included (directly or by reference) in contracts with subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV CS Certificates, and that they are contractually obligated to comply with the applicable requirements in the EV Guidelines and to perform them as required of the CA itself; • The CA monitors and enforces compliance with the terms of the contracts; and • The CA annually internally audits compliance with the EV Guidelines.	8.3
8.3	The CA maintains controls to provide reasonable assurance that it complies with: • laws applicable to its business and the certificates it issues in each jurisdiction where it operates, and • licensing requirements in each jurisdiction where it issues EV CS certificates.	8.
8.4	The CA maintains controls and procedures to provide reasonable assurance that: • The CA and Root CA maintain the minimum levels of Commercial General Liability Insurance (occurrence form) and Professional Liability/ Errors & Omissions insurance as established by the EV Guidelines; and • The providers of the Insurance coverage meet the ratings qualifications established under the EV Guidelines; or • If the CA and/or its root CA self-insures for liabilities, the CA and/ or its root CA maintains the minimum liquid asset size requirement established in the EV Guidelines.	9.2.1

Timestamp authority, signing services and private key protection

#	Criterion	CS BR Ref[3]
9.1	The CA, if operating an EV Timestamp Authority, maintains controls to provide reasonable assurance that: • The private key is protected in a cryptographic module validated to FIPS 140-2 Level 2 or greater; and • The time is synchronized with a UTC time source recognized by the International Bureau of Weights and Measures.	6.8, 6.2.7.2
9.2	The CA maintains controls to provide reasonable assurance that: • The EV Timestamp Authority's private key is protected in a cryptographic module validated to at FIPS 140-2 Level 2 or greater; • The EV Timestamp Authority's time is synchronized with a UTC time source recognized by the International Bureau of Weights and Measures; • The Signing Service's private key is protected in a cryptographic module validated to FIPS 140-2 Level 2 or greater; and • The Subscriber's private key is generated, stored and used in a cryptographic module that meets or exceeds the requirements of FIPS 140-2 level 2.	6.8
9.3	The CA maintains controls to provide reasonable assurance that: For EV Code Signing Certificates issued prior to June 1 2023, CAs SHALL ensure that the Subscriber's Private Key is generated, stored and used in a Hardware Crypto Module that meets or exceeds the requirements of FIPS 140-2 level 2 or Common Criteria EAL 4+ using acceptable methods that include (but are not limited to) the following: • The CA ships a suitable Hardware Crypto Module, with a preinstalled Private Key, in the form of a smartcard or USB device or similar; • The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the Private Key is managed in a suitable Hardware Crypto Module; and • The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.	6.2.7.4

#	Criterion	CS BR Ref[3]
9.3 (cont'd)	The CA maintains controls to provide reasonable assurance that, effective June 1, 2023, it obtains a representation from its Subscribers that they will use one of the following methods to generate and protect their Code Signing Certificate Private Key in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+: • Subscriber uses a Hardware Crypto Module meeting the specified requirement; • Subscriber uses a cloud-based key generation and protection solution with the following requirements: — Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements; — Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key. — Subscriber uses a Signing Service which meets the requirement of Section 6.2.7.3 of the CS BRs	6.2.7.4
9.4	The CA maintains controls to provide reasonable assurance that, effective June 1 2023, it obtains a representation from its Subscribers that they will protect their Code Signing Private in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+: • Subscriber uses a Hardware Crypto Module meeting the specified requirement; • Subscriber uses a cloud-based key generation and protection solution with the following requirements: — Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements; — Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.	6.2.7.4

Appendix A: CA/Browser Forum Documents

These Criteria are also based on the following CA/Browser Forum Documents:

Document Name	Version	Effective Date
Guidelines for the Issuance and Management of Extended Validation SSL Certificates	1.8	30 November 2022
Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates	3.7	28 February 2024

Copies of these documents are available on the CA/Browser Forum's website.

Appendix B: Sections of the CS BRs Not Subject to Assurance

Sections of the CS BRs which contain no content or the phrase "No Stipulation" were not considered for audit. Additionally, the following items are not subject to assurance:

Ref	Topic	Reasons for exclusion
1	Scope	Information only
1.1	Purpose	Information only
1.6.3	References	Information only
1.6.1	Definitions	The practitioner is directed to consider these definitions when interpreting the EV Guidelines and these audit criteria.
1.6.2	Abbreviations and Acronyms	Information only
1.6.4	Conventions	Information only
1.6.1	Certificate Warranties and Representations – definitions – Certificate Beneficiaries	Legal item
9.6.1	Certificate Warranties and Representations – Certificate Warranties	Legal item
9.6.3	Certificate Warranties and Representations – Applicant Warranty	Legal item
6	Technical Security Controls	References to the CA/Browser Forum's Network Security Requirements are addressed in WebTrust Principles and Criteria – Network Security, Principle 1, and are not subject to assurance.
8 (except 8.1, 8.6, 8.4)	Audit	Information only
9 (except 9.2.1, 9.6.3, 9.6.5)	Liability and Indemnification	Legal item

Appendix C: Sections of Network and Certificate System Security Requirements not subject to assurance

Not applicable at this time as incorporated by reference.

Appendix D: Effective Date Differences

CS BRs

No differences

Network Security

No differences