WEBTRUST® FOR CERTIFICATION AUTHORITIES

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – PUBLICLY TRUSTED CODE SIGNING CERTIFICATES

Version 1.0.1

Release Date 1 October 2017

Effective Date For audit periods commencing on or after 1 October 2017

Based on the Code Signing Working Group's Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates – Version 1.1

Document History

Version	Publication Date	Revision Summary
1.0	1 February 2017	Initial release
1.0.1	1 October 2017	Removed Principle 2, Criterion 5.11 as it was determined not to be auditable, and clarified Principle 2, Criterion 3.2 with regards to the signing of Subscriber Agreements

Acknowledgements

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

Members of the Task Force are:

- Jeffrey Ward, *BDO USA, LLP* (Chair)
- Donald E. Sheehy (Vice-Chair)
- Chris Czajczyc, *Deloitte LLP*
- Reema Anand, *KPMG LLP*
- David Roque, *Ernst & Young LLP*

Significant support has been provided by:

- Daniel J. Adam, *Deloitte & Touche LLP*
- Donoghue Clarke, *Ernst & Young LLP*
- Timothy Crawford, *BDO USA, LLP*
- Zain Shabbir, *KPMG LLP*

CPA Canada Support

- Kaylynn Pippo, (Staff Contact)
- Bryan Walker, Consultant
- Janet Treasure, Vice President, Member Development and Support
- Gord Beal, Vice President, Research, Guidance and Support

Table of Contents

Introduction

The primary goal of the Code Signing Working Group's ("CSWG") *Minimum Requirements for the Issuance and Management of Code Signing Certificates* ("MRCS Guidelines") 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 – Publicly Trusted Code Signing Certificates ("Audit Criteria") is to set out criteria that would be used as a basis for an auditor to conduct an engagement on the Issuance and Management of Publicly Trusted CS 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 Authority Method:** In this method, the Subscriber submits the code, or a digest of the code, to a Signing Authority for signature. The resulting signature is valid up to the expiration time of the Signing Authority certificate (that may be up to 39 months in the future).

Adoption and effective dates

These Audit Criteria incorporate and make reference to relevant Guidelines and Requirements from the CSWG and the CA/Browser Forum ("CA/B Forum" or the "Forum") as listed in Appendix A, and are effective for audit periods commencing on or after 1 October 2017.

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

In certain instances, the CSWG and/or the Forum updates its Guidelines and Requirements with certain criteria only effective at a date later than the publication date. The auditor 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 Audit Criteria, refer to Appendix D.

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 Audit Criteria include references to both the relevant sections of the MRCS Guidelines and the SSL Baseline Requirements for each criterion as applicable, and the auditor is directed to consider both of these in performing its audit.

For the MRCS Guidelines and the SSL Baseline Requirements, the auditor is directed to consider the version as outlined in Appendix A.

Connection with WebTrust for CA

These Audit Criteria are designed to be used in conjunction with an audit of a CA as required by the CA/Browser Forum. Due to significant overlap between these Audit Criteria and the WebTrust Principles and Criteria for Certification Authorities Version 2.x or later ("WebTrust for CA" or "WTCA"), this audit should be conducted simultaneously with the WebTrust for CA audit.

Requirements not subject to audit

In preparing these Audit 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 audit. 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 Minimum Requirements for Code Signing Certificate Guidelines.

#	Criterion	Ref[1]	BR Ref[2]
1	The CA and its Root CA discloses[3] 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 Minimum Requirements for Code Signing Certificates issued by the Code Signing Working Group	8.2.2, 8.4	N/A
2	The Certificate Authority has published guidelines for revoking CS Certificates	13	4.9
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.	13	4.9
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 24x7 basis, and the content and structure of the CP and/or CPS are in accordance with either RFC 2527 or RFC 3647.	8.2.2	N/A

[1] Reference to the applicable section(s) of the Minimum Requirements for Code Signing for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.
[2] Reference to the applicable section(s) of the SSL Baseline Requirements for this criterion. The auditor is directed to consider the referenced section(s) as part of assessing the CA's compliance with each criterion.
[3] The criteria are those that are to be tested for the purpose of expressing an opinion on these WebTrust Principles and Criteria for Certification Authorities – Minimum Requirements for Code Signing. 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 MRCS.

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.

#	Criterion	Ref	BR Ref
	KEY GENERATION CEREMONIES		
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 SSL Baseline Requirements Section 6.1.1.1.	17.7	6.1.1.1
	CERTIFICATE CONTENT AND PROFILE		
	Certificate Content and Profile		
2.1	The CA maintains controls to provide reasonable assurance that CS certificates issued meet the minimum requirements for Certificate Content and Profile, including additional technical requirements as specifically established in section 9 of the MRCS Guidelines, including the following: • Issuer Common Name Field • Issuer Domain Component Field • Issuer Organization Name Field • Issuer Country Name Field • 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	9, 9.1, 9.2	7.1.4.1, 3.2
2.2	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	9.3.3, 9.3.4, 9.5, 9.6, App. A, App. B	7.1

	• Certificate Extensions as established in the MRCS Guidelines 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		
2.3	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 Authority that fully complies with the MRCS Guidelines are valid for a period not exceeding 39 months[4]; • Time Stamping Certificates issued to a Timestamp Authority that fully complies with the MRCS Guidelines are valid for a period not exceeding 135 months. • Time Stamping Certificate issued to a Timestamp Authority are replaced with a new certificate and a new private key no later than every 15 months.	9.4	N/A
	CS CERTIFICATE REQUEST and CODE OBJECT SIGNING REQUEST REQUIREMENTS		
3.1	The CA maintains controls to provide reasonable assurance that the CS Certificate Request or Signing Authority Signing Request obtained is complete prior to the issuance of CS Certificates or signing of code objects, including the following in accordance with the MRCS Guidelines: • General requirements • Request and certification • Information requirements • Subscriber key requirements	10, 10.2	N/A
	Subscriber Agreements and Terms of Use		
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 MRCS Guidelines. That agreement is:	10.3	9.6.3

[4] EV Code Signing certificates issued to a Signing Authority may be valid for up to 135 months. EV Code Signing certificates are specifically addressed in a WebTrust for CA – Extended Validation Code Signing engagement.

	• signed by the Applicant; and • contains provisions imposing obligations and warranties on the Application relating to: o the accuracy of information o protection of Private Key o use of the CS certificate o compliance with industry standards o prevention of misuse o acceptance of the CS certificate o reporting and revocation o sharing of information o termination of use of the CS certificate o acknowledgement and acceptance.		
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 Authority) and/or between its Signing Authorities 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 it 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: o use of the signing service o not knowingly submitting suspect code for signing; and o reporting signed code contained malware or a serious vulnerability	10.3.3	N/A
	Subscriber and Subordinate CA Private Keys		
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 CA shall encrypt the Private Key for transport to the Subscriber or Subordinate CA. • If the CA or any of its designated RAs become aware that a Subscriber's or Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber or Subordinate CA, then the CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key. The CA only archives a Subscriber or Subordinate CA Private Key if it receives authorisation from the Subscriber or Subordinate CA.	16	6.1.2, 6.2.5, 6.2.6

INFORMATION VERIFICATION REQUIREMENTS			
Verification of Organisational Applicants			
4.1	The CA maintains controls to provide reasonable assurance that that prior to issuing a CS Certificate, it verifies the identity of Organisational Applicants in accordance with the MRCS Guidelines, including the following: • Legal identity (including any DBA names to be included in the CS Certificate) • Address • Certificate Requester's authority to obtain a CS Certificate • Certificate Requester's Identity • Registration Identifier	11, 11.1, 11.1.1	3.2.2.1, 3.2.2.2, 3.2.2.5
Verification of Individual Applicants			
4.2	The CA maintains controls to provide reasonable assurance that that prior to issuing a CS Certificate, it verifies the identity of Individual Applicants in accordance with the MRCS Guidelines, including the following: • Individual identity • Authenticity of identity	11.2, 11.2.1, 11.2.2	N/A
High Risk Applications			
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 signatures on Suspect Code) and previously rejected certificate requests to identify subsequent suspicious certificate requests.	11.4, 11.5	4.1.1
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 4.2.1 of the SSL Baseline Requirements • Determining whether the entity is identified as requesting a Code Signing Certificate from a High Risk Region of Concern	11.5	4.2.1
4.9	The CA maintains controls to provide reasonable assurance that it processes High Risk Applications in accordance with Section 11.7 of the MRCS Guidelines.	11.7	N/A
Certificate Issuance by a Root CA			
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	12	4.3.1

	administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.		
4.11	The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign CS certificates or create CS Signatures.	12	N/A
	Other Matters		
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	11.18	N/A
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 3.2.2.7 of the SSL Baseline Requirements.	11.6	3.2.2.7
	CERTIFICATE REVOCATION AND STATUS CHECKING		
5.1	The CA maintains controls to provide reasonable assurance that a process is available 24x7 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.	13.1	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 24x7 basis; • identifies high priority Certificate Problem Reports; • begin 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.	13.1.3, 13.1.4	4.9.3, 4.9.5, 4.10.2
5.3	The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked if any of the following events occurs: 1. An Application Software Supplier requests the revocation: a. Within 2 business days of receiving this request, the CA either revokes the certificate or informs the Application Software Supplier that it is conducting an investigation; b. If the CA chooses to conduct an investigation, it informs the Application Software Supplier whether or not it will revoke the certificate within 2 business days; and c. If the CA determines that revocation will have an unreasonable impact on its customer, it proposes an alternative course of action to the Application Software Supplier, based on its investigation.	13.1.5	N/A

	2. The Subscriber requests revocation: a. Within 1 business day of receiving the revocation request from the Subscriber, the CA revokes the certificate; or b. Within 1 business day of being notified by the subscriber that the original certificate request was not authorised and does not grant retroactive authorisation, the CA revokes the certificate. 3. A third party provides information that leads the CA to believe that the certificate is compromised or is being used for Suspect Code; or 4. The CA otherwise decides that the certificate should be revoked.		
5.4	The CA maintains controls to provide reasonable assurance that for incidents involving malware: • Within 1 business day of being made aware of the incident, the CA contacts the software publisher and requests a response within 72 hours. • Within 72 hours of being made aware of the incident, the CA determines the volume of relying parties impacted. • If a response is received from the publisher, the CA and publisher determine a 'reasonable date' for revocation • If no response is received from the publisher, the CA notifies the publisher that the CA will revoke the certificate in 7 days unless it has documented evidence that this will cause significant impact to the general public.	13.1.5.3	N/A
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 SSL Baseline Requirements Sections 6.1.5 and 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 Baseline 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;	13.1.6	4.9.1.2, 6.1.5, 6.1.6

	9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or 10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties		
5.6	The CA maintains controls to provide reasonable assurance that an online 24x7 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 Subscriber Code Signing Certificates: o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field; and o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days. • for the status of Timestamp Certificates o The 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 o The 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. • The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the MRCS Guidelines.	13.2.2	N/A
5.7	The CA maintains controls to provide reasonable assurance that OCSP responses for revoked Subscriber Code Signing Certificates and revoked Timestamp Certificates are available for at least 10 years following the expiry date of the certificate, unless the certificate contained the Lifetime Signing OID.	13.2.1	N/A
5.8	The CA maintains controls to provide reasonable assurance that if the CA issues CRLs, the serial numbers of revoked certificates remain in the CRL for at least 10 years following the expiry date of the certificate.	13.2.1	N/A
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	13.2.1	4.9.9

	• 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).		
5.10	The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	13.2.1	4.9.10
	EMPLOYEES AND THIRD PARTIES		
6.1	The CA maintains controls to provide reasonable assurance that: • the CA and its Signing Authorities 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 Authorities 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 Authorities 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 Authorities 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.	14.1	5.3.3, 5.3.4
6.2	The CA maintains controls to provide reasonable assurance that its' and its Signing Authorities' Delegated Third Parties meet the qualification requirements of Section 14 of the MCRS Guidelines.	14	N/A
6.3	The CA maintains controls to provide reasonable assurance that the CA and its Signing Authorities verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of MRCS Guidelines Section 14 and SSL Baseline Requirements Section 5.3.3, and the document retention and event logging requirements of MRCS Guidelines Section 15 and SSL Baseline Requirements Section 5.4.1.	14.2.1, 15	5.3.3, 5.4.1
6.4	For High Risk Certificate Requests, the CA maintains controls to provide reasonable assurance that the CA and its Signing Authorities verify that the Delegated Third Party's processes to identify and further verify High	14.2.1	N/A

	Risk Certificate Requests meets the requirements of the CA's own processes for High Risk Certificate Requests.		
	DATA RECORDS		
7.1	The CA maintains controls to provide reasonable assurance that the CA and its Signing Authorities 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.	15	5.4.1

7.2	The CA maintains controls to provide reasonable assurance that the following events are recorded by itself and its Signing Authorities:
	
	• CA key lifecycle management events, including:
	  o key generation, backup, storage, recovery, archival, and destruction
	  o cryptographic device lifecycle management events.
	• CA and Subscriber Certificate lifecycle management events, including:
	  o Certificate Requests, renewal and re-key requests, and revocation
	  o all verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement
	  o date, time, phone number used, persons spoken to, and end results of verification telephone calls
	  o acceptance and rejection of certificate requests
	  o issuance of Certificates
	  o generation of Certificate Revocation Lists (CRLs) and OCSP entries.
	• security events, including:
	  o successful and unsuccessful PKI system access attempts
	  o PKI and security system actions performed
	  o security profile changes
	  o system crashes, hardware failures, and other anomalies
	  o firewall and router activities
	  o entries to and exits from CA facility.
	• Log entries must include the following elements:
	  o Date and time of entry
	  o Identity of the person making the journal entry
	  o Description of entry
		15	5.4.1

7.3	The CA maintains controls to provide reasonable assurance that audit logs are retained by itself and its Signing Authorities for at least seven years, except as described in Criteria 7.5.	15	5.4.3
7.4	The CA maintains controls to provide reasonable assurance that the following events for its Timestamp Authority are recorded: 1. All data related to the creation of a timestamp, including all requests for a time-stamp, the connecting IP, and results of the timestamp,	15	N/A

	2. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server, 3. History of the timestamp server configuration, 4. Any attempt to delete or modify timestamp logs, 5. Security events, including: a. Successful and unsuccessful PKI system access attempts; b. PKI and security system actions performed; c. Security profile changes; d. System crashes, hardware failures, and other anomalies; e. Firewall and router activities; and f. Entries to and exits from the CA facility 6. Revocation of a timestamp certificate, 7. Major changes to the timestamp server's time, 8. System startup and shutdown, and 9. Equipment failures or malfunctions.		
7.5	The CA maintains controls to provide reasonable assurance that all data related to the creation of a timestamp, including all requests for a time-stamp, the connecting IP, and results of the timestamp are retained for at least 5 days.	15	N/A
	AUDIT AND LEGAL		
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 • If the Delegated Third Party is found to be non-compliant with the MRCS Guidelines, the CA does not allow the Delegated Third Party to continue performing its functions.	17.5	N/A
8.2	The CA maintains controls to provide reasonable assurance that: • applicable requirements of the Minimum Requirements for Code Signing Certificates Guidelines 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 MRCS 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 MRCS	8.3, 14.2.2	N/A
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	8.1	8.0

	• licensing requirements in each jurisdiction where it issues EV CS certificates.		
TIMESTAMP AUTHORITY, SIGNING SERVICES, AND PRIVATE KEY PROTECTION			
9.1	The CA maintains controls to provide reasonable assurance that: • It operates a 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.	16.1	N/A
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 synchronisation is maintained when a leap second occurs. • The Timestamp Authority synchronises 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 synchronisation with UTC. • Clock adjustments of one second or greater are auditable events.	16.1	N/A
9.3	The CA maintains controls to provide reasonable assurance that 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 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 encourages Method 1 and 2 above and discourages Method 3 above.	16.3	N/A
9.4	The CA maintains controls to provide reasonable assurance that Signing Services:	16.2	N/A

	• ensure that a Subscriber's private key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. • enforce multi-factor authentication to access and authorize Code Signing and obtain a representation from the Subscriber that they will securely store the tokens required for multi-factor access. • A system used to host a Signing Service is not used for web browsing. • The Signing Service runs a regularly updated antivirus solution to scan the service for possible virus infection. • The Signing Service complies with the Network Security Guidelines as a "Delegated Third Party".		
9.5	The CA maintains controls to provide reasonable assurance that: • CA private keys are protected in a system or device that has been validated as meeting at least FIPS 140[-2] level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats; • CA private keys outside the validated system or device specified above are protected with physical security, encryption, or a combination of both in a manner that prevents disclosure of the private keys; • CA private keys are encrypted with an algorithm and key-length that meets current strength requirements (2048 bit minimum); • CA private keys are backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment; and • physical and logical safeguards to prevent unauthorized certificate issuance.	16	5.2.2, 6.2, 6.2.7

Appendix A: CSWG and CA/Browser Forum Documents

These Audit Criteria are based on the following CSWG Documents:

Document Name	Version	Effective Date
Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates https://casecurity.org/wp-content/uploads/2016/09/Minimum-requirements-for-the-Issuance-and-Management-of-code-signing.pdf	1.1	22 September 2016

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

Document Name	Version	Effective Date
Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates	1.4	5 July 2016
Guidelines for the Issuance and Management of Extended Validation SSL Certificates	1.6.2	17 March 2017
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	1.4.9	11 July 2017

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

https://cabforum.org/documents

Appendix B: Sections of the MRCS Guidelines not subject to audit

Sections of the MRCS Guidelines which contain no content or the phrase 'No Stipulation' were not considered for audit. Additionally, the following items are not subject to audit:

Ref	Topic	Reasons for exclusion
1	Scope	Information only, no auditable items
2	Purpose	Information only, no auditable items
3	References	Information only, no auditable items
4	Definitions	No auditable items, however the auditor is directed to consider these definitions when interpreting the EV CS Guidelines and these audit criteria.
5	Abbreviations and Acronyms	Information only, no auditable items
6	Conventions	Information only, no auditable items
7	Certificate Warranties and Representations	Legal item
16	Data Security	References to the CA/Brower Forum's Network Security Requirements are addressed in *WebTrust Principles and Criteria – SSL Baseline with Network Security,* Principle 4, and are not subject to audit in these audit criteria.
17 (except 17.5, 17.7)	Audit	Information only, no auditable items
18	Liability and Indemnification	Legal item

Appendix C: Unused

This section is currently unused.

Appendix D: Effective date differences

MRCS Guidelines

No differences

SSL Baseline Requirements

No differences