CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

WebTrust® for Certification Authorities

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES – S/MIME CERTIFICATES

Release Date 31 March 2023

Effective Date For engagement periods commencing on or after 1 April 2023

Based on the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates – Version 1.0.0

Document History

Version	Publication Date	Revision Summary
1.0	TBD	Initial release

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, LLP* (co-Chair)
- Dan Adam
- Donoghue Clarke, *Ernst & Young LLP*
- Chris Czajczyc, *Deloitte LLP*
- Adam Fiock, *BDO USA, LLP*
- Eric Lin, *Ernst & Young LLP*
- Zain Shabbir, *KPMG LLP*
- Donald E. Sheehy

CPA Canada Support

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

The Task Force would like to thank retiring long-term task force members Jeffrey Ward, *BDO USA, LLP* who also chaired the Task Force since 2016, and David Roque, *Ernst & Young LLP* for their significant contributions to the advancement of the WebTrust program during their membership on the Task Force.

Table of Contents

Introduction

The primary goal of the CA/Browser Forum's ("Forum") Baseline Requirements for the Issuance and Management of S/MIME Certificates ("S/MIME") is to enable efficient and secure electronic communication, whilst addressing user concerns about the trustworthiness of Certificates. The Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

The CA/Browser Forum, that consists of many of the issuers of digital certificates and browser and other application developers, has developed guidelines that set out the expected requirements for issuing S/MIME certificates (the "S/MIME Baseline Requirements").

The Forum has also issued additional security guidelines (the "Network and Certificate System Security Requirements") that apply to all publicly trusted Certification Authorities (CAs), regardless of certificate type being issued.

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

Adoption and effective dates

These Criteria incorporate and make reference to relevant CA/Browser Forum Guidelines and Requirements as listed in Appendix A, and are effective for engagement periods commencing on or after 1 April 2023. Earlier adoption is permitted and encouraged.

The Forum may periodically publish updated Guidelines and Requirements. The practitioner is generally not required to consider these updated versions until reflected in the subsequently updated Criteria. However, in certain circumstances whereby a previous requirement or guideline is eliminated or made less restrictive, the practitioner may consider those changes as of their effective dates even if the changes are not reflected in the most current Criteria.

In certain instances, 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 Forum Guidelines and Requirements that have effective dates later than the effective date of these Criteria, as well as other nuances, refer to Appendix D.

Additionally, practitioners should be aware that Browsers may impose additional requirements, above and beyond the CA/Browser Forum Guidelines and Requirements that would be outside of the scope of an engagement performed in accordance with WebTrust Principles and Criteria – Baseline Requirements for the Issuance and Management of S/MIME Certificates. The practitioner is encouraged to make such enquiries of the CA to determine whether any additional procedures should be performed and related reporting undertaken to satisfy the relevant Browser(s). When such additional procedures are required outside of the scope of the WebTrust criteria specified herein, practitioners should also consider the appropriate reporting to be issued to the Browser(s) to satisfy their requirements.

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.x or later ("WebTrust for CA" or "WTCA"), this engagement should be conducted simultaneously with the WebTrust for CA engagement.

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

Section 6.7 of the CA/Browser Forum's ("Forum") Baseline Requirements for the Issuance and Management of S/MIME Certificates incorporate the CA/Browser Forum's Network and Certificate System Security Requirements by reference as if fully set forth in the document. This forms Principle 4 of these WebTrust Principles and Criteria for Certification Authorities – Baseline Requirements for the Issuance and Management of S/MIME Certificates. Please note that Principle 4 references to the WebTrust Principles and Criteria for Certification Authorities – Network Security.

Requirements not subject to assurance

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

Principle 1: Baseline Requirements for S/MIME Certificates Business Practices Disclosure

The Certification Authority (CA) discloses its S/MIME Certificate practices and procedures and its commitment to provide S/MIME Certificates in conformity with the applicable CA/Browser Forum Requirements.

#	Criterion	Ref[1]
1	The CA discloses[2] on its website: • S/MIME 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); and • its commitment to conform to the latest version of the S/MIME Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.	2.2, 3.2.7
2	The CA discloses in the Certificate Policy (CP) and/or Certification Practice Statement (CPS) that it includes its limitations on liability, if the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement.	9.8
3	The Issuing CA documents in its CP or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with the S/MIME Baseline Requirements.	7.1.6
4	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 S/MIME Baseline Requirements are updated at least every 365 days.	2.0, 2.3

1 Reference to the applicable section(s) of the Baseline S/MIME Requirements for the Issuance and Management of S/MIME 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 the WebTrust Principles and Criteria for Certification Authorities – Certification Authorities – Baseline Requirements for the Issuance and Management of S/MIME Certificates engagement. 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 Baseline S/MIME Requirements.

#	Criterion	Ref[1]
5	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 and include all material required by RFC 3647.	2.2
6	The CA's CP/CPS provides a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.	1.5.2
7	The CA has controls to provide reasonable assurance that public access to its repository is read-only.	2.4

Principle 2: S/MIME Service Integrity

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

- 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 certificates it manages is established and protected throughout their life cycles.

Key generation ceremonies

#	Criterion	Ref[3]
1.1	The CA maintains controls to provide reasonable assurance that Root CA and Subordinate CA Key Pairs are created in accordance with S/MIME Baseline Requirements Section 6.1.1.1.	6.1.1.1

Certificate content and profile

#	Criterion	Ref[3]
2.1	The CA maintains controls to provide reasonable assurance that Root, Subordinate, and Subscriber certificates generated by the CA contain certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output from a CSPRNG.	7.1
2.2	The CA maintains controls to provide reasonable assurance that the version of certificates issued are of type x.509 v3.	7.1.1
2.3	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Root CA certificates generated conform to the S/MIME Baseline Requirements.	7.1.2.1, 6.1.5, 7.1.6, 7.1.6.2

3 Reference to the applicable section(s) of the SSL Baseline S/MIME 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.

#	Criterion	Ref[3]
2.4	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subordinate CA certificates conform to the S/MIME Baseline Requirements.	7.1.2.2, 6.1.5, 7.1.6, 7.1.6.3
2.5	The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated conform to the S/MIME Baseline Requirements.	7.1.2.3, 6.1.5, 7.1.6, 7.1.6.4
2.6	The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the S/MIME Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated are set in accordance with RFC 5280.	7.1.2.4
2.7	The CA maintains controls to provide reasonable assurance that the validity period of Subscriber certificates issued does not exceed the maximum as specified in the S/MIME Baseline Requirements.	6.3.2
2.8	The CA maintains controls to provide reasonable assurance that it does not issue certificates with extensions that do not apply in the context of the public Internet, unless: a. Such values fall within an OID arc for which the Applicant demonstrates ownership; or b. The Applicant can otherwise demonstrate the right to assert the data in public context.	7.1.2.4
2.9	The CA maintains controls to provide reasonable assurance that it does not issue certificates with field or extension values which have not been validated according to the processes and procedures described in the S/MIME Baseline Requirements or the CA's CP and/or CPS.	7.1.2.4

#	Criterion	Ref[3]
2.10	The CA maintains controls to provide reasonable assurance that it follows the requirements of Algorithm object identifiers in the subjectPublicKeyInfofield as set out in the S/MIME Baseline Requirements: For RSA • The CA SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters SHALL be present, and SHALL be an explicit NULL. • The CA SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID:1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key. • When encoded, the AlgorithmIdentifier for RSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500. For ECDSA • The CA SHALL indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters SHALL use the namedCurve encoding. — For P-256 keys, the namedCurve SHALL be secp256r1 (OID: 1.2.840.10045.3.1.7). — For P-384 keys, the namedCurve SHALL be secp384r1 (OID: 1.3.132.0.34). — For P-521 keys, the namedCurve SHALL be secp521r1 (OID: 1.3.132.0.35). • When encoded, the AlgorithmIdentifier for ECDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes: — For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107. — For P-384 keys, 301006072a8648ce3d0201060 52b81040022. — For P-521 keys, 301006072a8648ce3d0201060 52b81040023. For EdDSA • The CA SHALL indicate an EdDSA key using one of the following algorithm identifiers — For curve25519 keys, the algorithm SHALL be id-Ed25519 (OID: 1.3.101.112). — For curve448 keys, the algorithm SHALL be id-Ed448 (OID: 1.3.101.113). • The parameters for EdDSA keys SHALL be absent.	7.1.3, 7.1.3.1, 7.1.3.1.2, 7.1.3.1.3

#	Criterion	Ref[3]
2.10	*(continued)* • When encoded, the AlgorithmIdentifier for EdDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes: — For Curve25519 keys, 300506032b6570. — For Curve448 keys, 300506032b6571.	7.1.3, 7.1.3.1, 7.1.3.1.2, 7.1.3.1.3
2.11	The CA maintains controls to provide reasonable assurance that all objects signed by a CA Private Key meet the requirements of set out in the S/MIME Baseline Requirements on the use AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures: For RSA • The CA SHALL use one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the specified hex-encoded bytes. — RSASSA-PKCS1-v1_5 with SHA-256: Encoding: 300d06092 a864886f70d01010b0500. — RSASSA-PKCS1-v1_5 with SHA-384: Encoding: 300d06092a864886f70d01010c0500. — RSASSA-PKCS1-v1_5 with SHA-512: Encoding: 300d06092 a864886f70d01010d0500. — RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes: Encoding: 304106092a864886f70d01010a3034a00f300d060960864 80165030402010500a11c301a06092a864886f70d0101083 00d0609608648016503040201 0500a203020120 — RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes: Encoding: 304106092a864886f70d01010a3034a00f300d060960864 80165030402020500a11c301a301a06092a864886f70d0101 08300d0609608648016503040202 0500a203020130 — RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes: Encoding: 304106092a864886f70d01010a3034a00f300d06096086 48016503040203030500a11c301a06092a864886f70d010108 300d0609608648016503040203 0500a203020140	7.1.3.2, 7.1.3.2.1, 7.1.3.2.2, 7.1.3.2.3

#	Criterion	Ref[3]
2.11	*(continued)* For ECDSA • The CA SHALL use the appropriate signature algorithm and encoding based upon the signing key used. — If the signing key is P-256, the signature SHALL use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040302. — If the signing key is P-384, the signature SHALL use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040303. — If the signing key is P-521, the signature SHALL use ECDSA with SHA-512. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040304. For EdDSA • The CA SHALL use the appropriate signature algorithm and encoding based upon the signing key used. — If the signing key is Curve25519, the signature algorithm SHALL be id-Ed25519 (OID: 1.3.101.112). When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300506032b6570. — If the signing key is Curve448, the signature algorithm SHALL be id-Ed448 (OID: 1.3.101.113). When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300506032b6571.	7.1.3.2, 7.1.3.2.1, 7.1.3.2.2, 7.1.3.2.3
2.12	The CA maintains controls to provide reasonable assurance that for every valid Certification Path (as defined by RFC 5280, Section 6): • For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CACertificate. • For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.	7.1.4.1

#	Criterion	Ref[3]
2.13	The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued: • The subjectAltName extension is present and contains at least one entry • Each entry MUST be either: — Rfc822Name and/or — otherName of type id-on-SmtpUTF8Mailbox, encoded in accordance with RFC 8398	7.1.4.2.1
2.14	The CA maintains controls to provide reasonable assurance that it does not include a Mailbox Address in a Mailbox Field except as verified in accordance with Section 3.2.2 of the S/MIME Baseline Requirements. • All Mailbox Addresses in the subject field or entries of type dirName of this extension SHALL be repeated as rfc822Name or otherName values of type id-on-SmtpUTF8Mailbox in this extension.	7.1.4.2, 7.1.4.2.1
2.15	The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the S/MIME Baseline Requirements, including: • commonName • organizationName • organizationalUnitName • organizationalIdentifier • givenName • Pseudonym • serialNumber • emailAddress • title • streetAddress • localityName • stateOrProvinceName • postalCode • countryName • Subject Information for Root and Subordinate CA certificates	7.1.4.2.2, 7.1.6, 7.1.4.3

#	Criterion	Ref[3]
2.16	The CA maintains controls to provide reasonable assurance that Subordinate CA certificates technically constrained using the nameConstraints extension conform to the S/MIME Baseline Requirements.	7.1.5
2.17	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 Section 6.1.5 and/or Section 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 or proven method that exposes the Applicant's Private Key to compromise; 4. The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, 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, see https://wiki.debian.org/SSLkeys).	6.1.1.3, 6.1.5, 6.1.6

Certificate request requirements

#	Criterion	Ref[3]
3.1	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of a Certificate obtains the following documentation from the Applicant: 1. A certificate request, 2. An executed Subscriber or Terms of Use Agreement, and 3. Any additional documentation the CA determines necessary to meet the S/MIME Baseline Requirements.	4.1.2

#	Criterion	Ref[3]
3.2	The CA maintains controls to provide reasonable assurance that the Certificate Request is: • obtained and complete prior to the issuance of Certificates; • signed by the appropriate Applicant Representative on behalf of the applicant; • properly certified as to being correct by the applicant; and • contains the information specified in Section 4.2.1 of the S/MIME Baseline Requirements.	4.1.2, 4.2.1

Subscriber and subordinate CA Private Keys

#	Criterion	Ref[3]
3.3	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.	6.1.2, 6.2.5, 6.2.6

Subscriber agreements and terms of use

#	Criterion	Ref[3]
3.4	The CA maintains controls to provide reasonable assurance that the CA, prior to the issuance of a Certificate, obtains a Subscriber and/or Terms of Use agreement in accordance with the S/MIME Baseline Requirements Section 9.6.3. That agreement contains provisions imposing obligations and warranties on the Application relating to: • the accuracy of information • protection of Private Key • acceptance of certificate • use of certificate • reporting and revocation • termination of use of certificate • responsiveness • acknowledgement and acceptance.	9.6.3

Validation practices

Validation of mailbox authorization or control

#	Criterion	Ref[3]
4.1	The CA maintains controls to provide reasonable assurance that prior to issuing a Certificate: • The CA verifies that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the account holder's behalf. • The CA does not delegate the verification of mailbox authorization or control. • The CA's CP and/or CPS specifies the procedures that the CA employs to perform this verification. • The CA maintains a record of which validation method, including the relevant version number from the TLS Baseline Requirements or S/MIME Baseline Requirements, was used to validate every domain or email address in issued Certificates. In all cases, the validation has been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.	3.2.2, 4.2.1

#	Criterion	Ref[3]
4.2	The CA maintains controls to provide reasonable assurance to validate authority over mailbox via domain: • If the CA confirms the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate, the CA uses only the approved methods in Section 3.2.2.4 of the TLS Baseline Requirements to perform this verification.	3.2.2.1
4.3	The CA maintains controls to provide reasonable assurance to validate control over mailbox via domain: • Where applicable, the CA confirms the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receives a confirming response utilizing the Random Value. • Control over each Mailbox Address is confirmed using a unique Random Value. • The Random Value — is sent only to the email address being validated and is not shared in any other way. — is unique in each email. — is valid for use in a confirming response for no more than 24 hours from its creation. — is reset upon each instance of the email sent by the CA to a Mailbox Address, however all relevant Random Values sent to that Mailbox Address can remain valid for use in a confirming response within the validity period described in this Section. — is reset upon first use by the user if intended for additional use as an authentication factor following the Mailbox Address verification.	3.2.2.2
4.4	The CA maintains controls to provide reasonable assurance to validate an applicant as operator of associated mail server(s) • If the CA confirms the Applicant's control over each Mailbox Field to be included in the Certificate by confirming control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed. • In this case, the SMTP FQDN is identified using the address resolution algorithm defined in RFC 5321 Section 5.1 that determines which SMTP FQDNs are authoritative for a given Mailbox Address.	3.2.2.3

#	Criterion	Ref[3]
4.4	*(continued)* • If more than one SMTP FQDN has been discovered, the CA verifies control of an SMTP FQDN following the selection process at RFC 5321 Section 5.1. Aliases in MX record RDATA SHALL NOT be used for this validation method. • To confirm the Applicant's control of the SMTP FQDN, the CA uses only the currently-approved methods in Section 3.2.2.4 of the TLS Baseline Requirements.	3.2.2.3

Validation of organization identity

#	Criterion	Ref[3]
4.5	For authentication of organization identity, the CA maintains controls to provide reasonable assurance that the following information is collected and retained as evidence for the Organization: • Formal name of the Legal Entity; • A registered Assumed Name for the Legal Entity (if included in the Subject); • An organizational unit of the Legal Entity (if included in the Subject); • An address of the Legal Entity (if included in the Subject); • Jurisdiction of Incorporation or Registration of the Legal Entity; and • Unique identifier and type of identifier for the Legal Entity. The unique identifier SHALL be included in the Certificate subject:organizationIdentifier as specified in S/MIME Baseline Requirements Section 7.1.4.2.2 and Appendix A; • Verification of name, address, and unique identifier.	3.2.3.1
4.6	The CA maintains controls to provide reasonable assurance that for Verification of name, address, and unique identifier and assumed name, it follows the relevant S/MIME Baseline requirements.	3.2.3.2.1, 3.2.3.2.2

#	Criterion	Ref[3]
4.7	The CA maintains controls to provide reasonable assurance that it verifies the unique identifier used in the Certificate from a register that is maintained or authorized by the relevant government agency. The CA does not use third-party vendors to obtain regularly-updated and current information from the government register provided that the third party obtains the information directly from the government. The CA maintains controls to provide reasonable assurance that it discloses its authorized sources used to verify the Applicant's creation, existence, or recognition. • This disclosure is made through an appropriate and readily accessible online means. • The CA SHALL document where to obtain this information within Section 3.2 of the CA's CP and/or CPS.	3.2.3.3
4.8	The CA maintains controls to provide reasonable assurance that, in all cases, the validation has been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.	4.2.1

Validation of individual identity

#	Criterion	Ref[3]
4.9	The CA maintains controls to provide reasonable assurance that it collects and retains evidence supporting the following identity attributes for the Individual Applicant: • Given name(s) and surname(s), which are current names; • Pseudonym (if used); • Title (if used); • Address (if displayed in Subject); and • Further information as needed to uniquely identify the Applicant. And to comply with applicable data protection legislation in the gathering and retention of evidence relating to Individual identity supporting this Requirement in accordance with S/MIME Baseline Requirements Section 9.4.	3.2.4

#	Criterion	Ref[3]
4.10	The CA maintains controls to provide reasonable assurance that it documents and publishes the methods it uses to collect Individual identity attributes and follows the requirements as set out in S/MIME Baseline Requirements Section 3.2.4.1 for using such as evidence obtained: • From a physical identity document • From a digital identity document • Using electronic identification (EID) • From a certificate supporting a digital signature applied by the Applicant • From Enterprise RA records • From an affiliation from company attestation • From a general attestation	3.2.4.1
4.11	The CA maintains controls to provide reasonable assurance that it validates all identity attributes of the Individual to be included in the Certificate and follows the requirements as set out in S/MIME Baseline Requirements Section 3.2.4.2 for • Validation of a physical identity document • Validation of a digital identity document • Validation of EID • Validation of digital signature with certificate • Validation of an Attestation If the evidence has an explicit validity period, the CA maintains controls to provide reasonable assurance that it verifies that the time of the identity validation is within this validity period. The CA maintains controls to provide reasonable assurance that it can reuse existing evidence to validate Individual identity subject to the age restrictions in S/MIME Baseline Requirements Section 4.2.1.	3.2.4.2, 4.2.1

Non-verified subscriber information

#	Criterion	Ref[3]
4.12	The CA maintains controls to provide reasonable assurance that Subscriber information that has not been verified in accordance with S/MIME Baseline Requirements is not included in Publicly-Trusted S/MIME Certificates.	3.2.5

Validation of authority

#	Criterion	Ref[3]
4.13	The CA maintains controls to provide reasonable assurance that before commencing to issue Organization-validated and Sponsor-validated Certificates for an Applicant, it uses a Reliable Method of Communication to verify the authority and approval of an Applicant Representative to perform one or more of the following: • to act as an Enterprise RA; • to request issuance or revocation of Certificates; or • to assign responsibilities to others to act in these roles. The CA maintains controls to provide reasonable assurance it provides an Applicant with a list of its authorized Applicant Representatives upon the Applicant's verified written request.	3.2.6, 3.2.3.2.1
4.14	In all cases, the validation has been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.	4.2.1

Criteria for interoperation

#	Criterion	Ref[3]
4.15	The CA maintains controls to provide reasonable assurance that it discloses all 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).	3.2.7

Reliability of verification source

#	Criterion	Ref[3]
4.16	The CA maintains controls to provide reasonable assurance that before relying on a source of verification data to validate Certificate Requests, • It verifies its suitability as a Reliable Data Source. • When relying upon a letter attesting that Subject Information or other fact is correct, it verifies that the letter was written by an accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction customarily relied upon for such information.	3.2.8

#	Criterion	Ref[3]
4.16	*(continued)* • Where an attestation is obtained, it includes a copy of documentation supporting the fact to be attested. • It uses a Reliable Method of Communication to contact the sender and to confirm the Attestation is authentic.	3.2.8

Certificate issuance by a Root CA

#	Criterion	Ref[3]
4.17	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
4.18	The CA maintains controls to provide reasonable assurance that Root CA Private Keys are not used to sign certificates, except in following cases: • Self-signed Certificates to represent the Root CA itself; • Certificates for Subordinate CAs and Cross Certificates; • Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and • Certificates for OCSP Response verification.	6.1.7

Certificate revocation and status checking

#	Criterion	Ref[3]
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 Certificate Problem Requests, and that the CA provides a process for Subscribers to request revocation of their own certificates.	4.9.3

#	Criterion	Ref[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; • begins investigation of Certificate Problem Reports within 24 hours and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report; • decides whether revocation or other appropriate action is warranted; if revocation is deemed the appropriate action, the elapsedtime from receipt of the Certificate Problem Report or revocation request and revocation status information does not exceed the timelines in S/MIME Baseline Requirements 4.9.1.1; and • selects revocation date based on: — The nature of the alleged problem (scope, context, severity, magnitude, risk of harm); — The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties); — The number of Certificate Problem Reports received about a particular Certificate or Subscriber; — The entity making the complaint (for example, a complaint from a law enforcement official should be addressed with higher priority); and — Relevant legislation.	4.9.3, 4.9.5, 4.9.7, 4.10.2
5.3	The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events 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; or 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 (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);	4.9.1.1, 6.1.5, 6.1.6

#	Criterion	Ref[3]
5.3	*(continued)* 5. The CA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon. And, Subscriber Certificates are revoked within 5 days if any of the following events occurs: 1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6; 2. The CA obtains evidence that the Certificate was misused; 3. 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; 4. The CA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name); 5. The CA is made aware of a material change in the information contained in the Certificate; 6. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP and/or CPS; 7. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate; 8. 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; 9. Revocation is required by the CA's CP and/or CPS; or 10. 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.	4.9.1.1, 6.1.5, 6.1.6

#	Criterion	Ref[3]
5.4	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 S/MIME 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 S/MIME 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; or 9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.	4.9.1.2, 6.1.5, 6.1.6
5.5	The CA maintains controls to provide reasonable assurance that the CA makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the S/MIME Baseline Requirements Section 7.1.2.	7.1.2, 4.9.11

#	Criterion	Ref[3]
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 Certificates: — 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 — the OCSP responses shall: • have a validity interval greater than or equal to eight hours; • have a validity less than or equal to ten days; • with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an OCSP prior to one-half of the validity period before the nextUpdate; and • with validity intervals greater than or equal to sixteen hours, the CA SHALL update the information provided via an OCSP at least eight (8) hours prior to the nextUpdate, and no later than four days after the thisUpdate. • for the status of subordinate CA Certificates — The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and — 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 Subordinate CA Certificate. • The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the S/MIME Baseline Requirements.	4.10.2, 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
5.8	The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP Response until after the Expiry Date of the revoked Certificate.	4.10.1

#	Criterion	Ref[3]
5.9	The CA maintains controls to provide reasonable assurance that, when provided, 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 OCSP responses by CA's which have not been technically constrained in accordance with S/MIME Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	4.9.10

Employees and third parties

#	Criterion	Ref[3]
6.1	The CA maintains controls to verify the identity and trustworthiness of an employee, agent, or independent contractor prior to engagement of such persons in the Certificate Management Process.	5.3.1

#	Criterion	Ref[3]
6.2	The CA maintains controls to provide reasonable assurance that: • the CA provides 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 maintains 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 documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. • the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the S/MIME Baseline Requirements. • all personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.	5.3.3, 5.3.4
6.3	The CA maintains controls to provide reasonable assurance that before the CA authorizes a Delegated Third Party to perform a delegated function, the CA contractually require the Delegated party to: • meet the qualification requirements of the S/MIME Baseline Requirements Section 5.3.1, when applicable to the delegated function; • retain documentation in accordance with the S/MIME Baseline Requirements Section 5.5.2; • abide by the other provisions of the S/MIME Baseline Requirements that are applicable to the delegated function; and • comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.	1.3.2, 5.3.1, 5.5.2
6.4	The CA maintains controls to provide reasonable assurance that the CA verifies that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.	5.3.7, 5.3.3, 5.4.1

#	Criterion	Ref[3]
6.5	The CA maintains controls to provide reasonable assurance that the CA has process in place to document the obligations of delegated parties and monitor and ensure each Delegated Third Party's compliance with the S/MIME Baseline Requirements and the relevant CP and/or CPS on at least an annual basis.	8.8
6.6	The CA maintains controls to provide reasonable assurance that the CA does not accept certificate requests authorized by an Enterprise RA unless the requirements in S/MIME Baseline Requirements Section 1.3.2 are met, and the CA imposes these requirements on the Enterprise RA, and monitors compliance by the Enterprise RA.	1.3.2

Data records

#	Criterion	Ref[3]
7.1	The CA maintains controls to provide reasonable assurance that the CA records 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: • CA Certificate and key lifecycle 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; — Signing of OCSP Responses (as described in Section 4.9 and Section 4.10 of the S/MIME Baseline Requirements); and — Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.	5.4.1

#	Criterion	Ref[3]
7.2	*(continued)* • Subscriber Certificate lifecycle management events, including: — Certificate requests, renewal, and re-key requests, and revocation; — All verification activities stipulated in these Requirements and the CA's Certification Practice Statement; — Approval and rejection of Certificate Requests; — Issuance of Certificates; — Generation of Certificate Revocation Lists; and — Signing of OCSP Responses (as described in Section 4.9 and Section 4.10 of the S/MIME Baseline Requirements). • Security events, including: — Successful and unsuccessful PKI system access attempts; — PKI and security system actions performed; — Security profile changes; — Installation, update and removal of software on a Certificate System; — System crashes, hardware failures, and other anomalies; — Firewall and router activities; and — Entries to and exits from the CA facility.	5.4.1
7.3	The CA maintains controls to provide reasonable assurance that the following events are recorded: • Date and time of event; • Identity of the person making the journal record; and • Description of the event.	5.4.1

#	Criterion	Ref[3]
7.4	The CA maintains controls to provide reasonable assurance that the CA and each Delegated Third Party's audit logs generated are retained 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. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.	5.4.3
7.5	The CA maintains controls to provide reasonable assurance that: • Archived audit logs (as set forth in Section 5.5.1) are retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer. • The CA and each delegated party SHALL retain, for at least two (2) years: — All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and — All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of: • such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or • the expiration of the Subscriber Certificates relying upon such records and documentation.	5.5.1, 5.5.2, 5.4.3

#	Criterion	Ref[3]
7.6	The CA maintains controls to provide reasonable assurance that all archived audit logs (as set forth in Section 5.5.1 is to be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer. The CA maintains controls to provide reasonable assurance that the CA and each Delegated Third Party's archives all audit logs (as set forth in Section 5.4.1) and also archives: • Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and • Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.	5.5.1, 5.4.1

Audit

#	Criterion	Ref[3]
8.1	The CA maintains controls to provide reasonable assurance that for Subordinate CAs whose certificates are considered technically constrained in accordance with S/MIME Baseline Requirements Section 7.1.5, the CA: • monitors the Subordinate CA's adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practices Statement; and • performs quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates issued by Delegated Third Party in the period beginning immediately after the last sample was taken to ensure all applicable S/MIME Baseline Requirements are met.	8.1, 8.7, 7.1.5
8.2	The CA maintains controls to provide reasonable assurance that for Subordinate CAs whose certificates are not considered technically constrained in accordance with S/MIME Baseline Requirements Section 7.1.5, the CA verifies that Subordinate CAs that are not technically constrained are audited in accordance with S/MIME Baseline Requirements 8.4.	8.1, 8.4, 7.1.5

#	Criterion	Ref[3]
8.3	The CA maintains controls to provide reasonable assurance that: • It performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment sample was taken; • Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in the S/MIME Baseline Requirements, the CA performs ongoing quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken; • The CA reviews each Delegated Third Party's practices and procedures to assess that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.	8.7
8.4	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 S/MIME certificates.	8.0

Principle 3: CA Environmental Security

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

- Logical and physical access to CA systems and data is restricted to authorized individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

#	Criterion	Ref[4]
1	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a comprehensive security program designed to: • protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes; • protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes; • protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes; • protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and • comply with all other security requirements applicable to the CA by law.	5.0
2	The CA maintains controls to provide reasonable assurance that it performs a risk assessment at least annually which: • 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; • Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and • Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.	5.0, 5.4.8

4 Reference to the applicable section(s) of the Baseline S/MIME 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.

#	Criterion	Ref[4]
3	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan: • includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes; • takes into account then-available technology and the cost of implementing the specific measures; and • is designed to implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.	5.0
4	The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Business Continuity Plan that includes at a minimum: • the conditions for activating the plan; • emergency procedures; • fall-back procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); • regular testing of contingency plans; • the CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes; • a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • what constitutes an acceptable system outage and recovery time; • how frequently backup copies of essential business information and software are taken; • the distance of recovery facilities to the CA's main site; and	5.7.1

#	Criterion	Ref[4]
4	*(continued)* • procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site. The Business Continuity Plan is tested at least annually, reviewed, and updated.[5]	5.7.1
5	The CA maintains controls to provide reasonable assurance that its Certificate Management Process includes: • physical security and environmental controls (see WTCA 2.2.2 Section 3.4); • system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/ prevention (see WTCA 2.2.2 Section 3.7); • network security and firewall management, including port restrictions and IP address filtering (see WTCA 2.22 Section 3.6); • user management, separate trusted-role assignments, education, awareness, and training (see WTCA 2.2.2 Section 3.3); and • logical access controls, activity logging, and inactivity time-outs to provide individual accountability (see WTCA 2.2.2 Section 3.6).	5.0
6	The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.	5.0 (WTCA v2.2.2 Sec 3.4)

5 For organizations that are undergoing a WebTrust for CA engagement (examination), all of the above are required and already tested with the exception of the disclosure of the distance of recovery facilities to the CA's main site.

#	Criterion	Ref[4]
7	The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	5.0 (WTCA v2.2.2 Sec 3.7)
8	The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: • operating system and database access is limited to authorized individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorized individuals, applications and services; and • CA application use is limited to authorized individuals. Such controls must include, but are not limited to: • network security and firewall management, including port restrictions and IP address filtering; • logical access controls, activity logging (WTCA 2.2.2. Section 3.10), and inactivity time-outs to provide individual accountability.	5.0 (WTCA v2.2.2 Sec 3.6)
9	The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	5.0 (WTCA v2.2.2 Sec 3.3)
10	The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	5.0 (WTCA v2.2.2 Sec 3.10)
11	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;	5.2.2, 6.2, 6.2.7

#	Criterion	Ref[4]
11	*(continued)* • 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.	5.2.2, 6.2, 6.2.7
12	The CA maintains controls to provide reasonable assurance that it enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.	6.5.1

Principle 4: Network and Certificate System Security Requirements

The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

For Criteria needed to satisfy this Principle, refer to WebTrust Principles and Criteria for Certification Authorities – Network Security.

Appendix A: CA/Browser Forum Documents

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

Document Name	Version	Effective Date
Network and Certificate System Security Requirements	1.7	5 April 2021
Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates	1.0	1 January 2023

Appendix B: Sections of S/MIME Baseline Requirements not subject to assurance

Sections of the S/MIME Baseline Requirements which contain no content or the phrase "No Stipulation" were not considered. Additionally, the following items are not subject to assurance:

Ref	Topic	Reasons for exclusion
1.1	Overview	Information only
1.2	Document Name and Identification	Information only
1.3 (except 1.3.2)	PKI Participants	Information only
1.4	Certificate Usage	Information only
1.5 (except 1.5.2)	Policy Administration	Information only
1.6	Definitions and Acronyms	The practitioner is directed to consider these definitions when interpreting the S/MIME Baseline Requirements and these criteria.
4.9.2	Who Can Request Revocation	Information only
8.2	Identity/Qualifications of Assessor	Information only
8.6	Communication of Results	Information only
9.6.1	CA Representations and Warranties	Legal item
9.9.1	Indemnification by CAs	Legal item
9.16.3	Severability	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: CA/Browser Forum effective date differences

S/MIME Baseline Requirements

The following S/MIME Baseline Requirements have effective dates later than the effective date of these Criteria. Refer to details and instructions below for guidance on how to address these as part of an engagement:

No differences in this version.