Minimum Security Requirements for Issuance of Verified Mark Certificates
Version 1.0

Version 1.0
July 9, 2021

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document describes an integrated set of technologies, protocols, and identity and mark proofing requirements that are necessary for the issuance and management of Verified Mark Certificates (VMCs) - certificates that are trusted by Consuming Entities. Upon adoption, they are mandatory for Certification Authorities who issue or plan to issue Verified Mark Certificates.

VMCs assert a cryptographically verifiable and auditable binding between an identity, a logo, and a domain. The key pair of an end entity VMC is unused, and there are no requirements around the generation, storage, and protection of such key pairs. In particular, Certification Authorities MAY generate such key pairs on behalf of their customers, and VMCs need not be revoked if the unused key pair is compromised.

VMCs present Consuming Entities and Relying Parties with information about and marks asserted by the Mark Asserting Entity, some of which is gathered from legal documents and government registries (including trademark registries). When Mark Verifying Authorities verify marks presented by a Mark Asserting Entity for inclusion in a VMC, or when Mark Verifying Authorities present VMCs and the information or marks they contain to Consuming Entities, or when Consuming Entities present VMCs and the information or marks they contain to Relying Parties, they are not providing legal advice to any party.

In adopting these Verified Mark Certificate Requirements (VMCR), the Authindicators Working Group is not providing legal advice to any party. All parties (Mark Asserting Entities, Mark Verifying Authorities, Consuming Entities and Relying Parties) are advised to consult their own legal counsel on all matters.

Mark Verifying Authorities have no legal obligation to issue VMCs to any Mark Asserting Entity. Consuming Entities have no legal obligation to use or display VMCs or the information or marks they contain to any Relying Party, and may choose in their sole discretion not to use or display VMCs (or groups or categories of VMCs) or the information or marks they contain to Relying Parties or to any subset of Relying Parties they may choose.

Verified Mark Certificates may be issued with respect to marks accredited by legislation (such as Registered Marks that are in good standing with a Trademark Office) and which are owned by or licensed to the Applicant. CAs may issue Verified Mark Certificates provided that the CA satisfies the requirements in this document.

All Subscribers/Mark Asserting Entities, Consuming Entities, and Relying Parties are bound by the VMC Terms attached as Appendix D according to their terms. CAs who issue Verified Mark Certificates SHALL include the VMC Terms in their applicable Certification Practice Statement.

Relevant sections of these VMCRs have been synchronized with the following versions of the CA/Browser Forum standards:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.7.0
- Guidelines For The Issuance And Management Of Extended Validation Certificates v1.7.2

This document may be synchronized from time to time with future versions of the CA/Browser Forum documents in the sole discretion of the Authindicators Working Group. However, this document is independent of any actions of the CA/Browser Forum or of its documents.

1.2. DOCUMENT NAME AND IDENTIFICATION

This document SHALL be known as the Verified Mark Certificate Requirements (or "VMC Requirements" or simply "VMCR"). These VMC Requirements SHALL take effect upon public adoption by one or more

Certification Authorities (CAs) that offer Verified Mark Certificates to Subscribers and by one or more Consuming Entities that recognize and utilize the Verified Mark Certificates.

1.2.1. Revisions

Version	Adopted	Effective
0.97	12-19-2019	12-19-2019
0.984	06-24-2019	06-24-2019
0.985	05-26-2020	05-26-2020
0.986	02-05-2021	02-05-2021
1.0	07-09-2021	07-09-2021

1.2.2. Verified Mark Certificate OIDs

Certificates adhering to these VMC Requirements SHALL be identified by the presence of the VMC policy OID in the Certificate Policies Extension as described in section 7.1.6.

1.3. PKI PARTICIPANTS

The Authindicators Working Group is a voluntary organization that maintains these VMC Requirements. These will be published at www.bimigroup.org.

1.3.1. Certification Authorities

Certification Authority (CA), also known as Mark Verifying Authority, is defined in Section 1.6.1.

1.3.2. Registration Authorities

With the exception of section 3.2.14, the CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:
(1) Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
(2) Retain documentation in accordance with Section 5.5.2;
(3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and
(4) 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.

The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.
The CA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. The CA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace.
2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, the CA SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see Section 3.2) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

The CA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

1.3.3. Subscribers

Subscribers may also be known as Mark Asserting Entities. Both are as defined in Section 1.6.1.

1.3.4. Relying Parties

"Relying Party" and "Application Software Supplier" and "Consuming Entities" are defined in Section 1.6.1.

1.3.5. Other Participants

Other groups that have participated in the development of these Requirements include the CPA Canada WebTrust for Certification Authorities task force. Participation by CPA Canada does not imply its endorsement, recommendation, or approval of the final product.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

The primary goal of these Requirements is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates and Verified Marks. These Requirements also serve to inform users and help them to make informed decisions when relying on Certificates and Verified Marks.

1.4.2. Prohibited Certificate Uses

No Stipulation.

1.5. POLICY ADMINISTRATION

The Verified Mark Certificate Requirements present criteria established by the Authindicators Working Group for use by Certification Authorities when issuing, maintaining, and revoking Verified Mark Certificates. This document may be revised from time to time, as appropriate, in accordance with procedures adopted by the Authindicators Working Group. Because one of the primary beneficiaries of this document is the end user, the Authindicators Working Group openly invites anyone to make recommendations and suggestions by email to https://bimigroup.org/contact-us/. Authindicators Working Group members value all input, regardless of source, and will seriously consider all such input.

1.5.1. Organization Administering the Document

Authindicators Working Group https://bimigroup.org/.

1.5.2. Contact Person

Contact information for Authindicators Working Group is available here: https://bimigroup.org/contact-us/

In this section of a CA's Certification Practice Statement (CPS), the CA SHALL provide a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.

1.5.3. Person Determining CPS suitability for the policy

No stipulation.

1.5.4. CPS approval procedures

No stipulation.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

Accounting Practitioner: A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: A person, entity, or organization applying for a Verified Mark Certificate, but which has not yet been issued a Verified Mark Certificate, or a person, entity, or organization that currently has a Verified Mark Certificate or Certificates and that is applying for renewal of such Verified Mark Certificate or Certificates or for an additional Verified Mark Certificate or Certificates.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of relying-party application software that displays or uses Verified Mark Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Report: A report from a Qualified Practitioner stating the Qualified Practitioner's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CA: The Certification Authority that issues a Verified Mark Certificate. Also known as a Mark Verifying Authority.

CAA: From RFC 8659 (https://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

Certificate: A Verified Mark Certificate.

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve VMC Requests submitted by other Certificate Requesters. The Certificate Approver may also serve as the Designated Individual during the Notarization Process.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of Certificate misissuance, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of these Requirements, e.g., a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits a VMC Certificate Request on behalf of the Applicant.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates, also known as a Mark Verifying Authority. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Combined Mark: A trademark consisting of a graphic design, stylized logo, or image, with words and/or letters having a particular stylized appearance. For greater certainty, a "Combined Mark" includes trademarks made up of both word and design elements. See Appendix B for mapping of the names used by different trademarks offices to the definition of Combined Mark.

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Confirming Person: A position within an Applicant's organization that confirms the particular fact at issue.

Consuming Entity ("CE"): An entity that incorporates and uses the Mark Representation and related data contained in a Verified Mark Certificate in its products and services in accordance with the VMC Terms. Consuming Entities include mailbox providers.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements. The Contract Signer may also serve as the Designated Individual during the Notarization process.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

CRL: Certificate Revocation List as defined in RFC5280. A CRL is a list identifying which certificates are revoked meaning invalid, published periodically by CAs.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Demand Deposit Account: A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as a share draft account, a current account, or a checking account.

Design Mark: A trademark consisting of a graphic design, stylized logo, or image, without words and/or letters. For greater certainty, a "Design Mark" includes trademarks made up solely of design elements. See Appendix B for mapping of the names used by different trademarks offices to the definition of Design Mark.

Designated Individual: The person who signs the Verification Document before a Notary under the provisions of Appendix G.

DNS CAA Email Contact: The email address defined in section A.1.1.

DNS CAA Phone Contact: The phone number defined in section A.1.2.

DNS TXT Record Email Contact: The email address defined in section A.2.1.

DNS TXT Record Phone Contact: The phone number defined in section A.2.2.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Global Legal Entity Identifier Foundation (GLEIF): The organization established by the Financial Stability Board to support the implementation and use of the Legal Entity Identifier (LEI). See www.gleif.org.

Global Legal Entity Identifier Index: The GLEIF public index of LEI records for those legal entities identifiable with an LEI.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Independent Confirmation From Applicant: Confirmation of a particular fact received by the CA pursuant to the provisions of the Requirements or binding upon the Applicant.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

International Organization: An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair**.**

Key Pair: The Private Key and its associated Public Key.

Latin Notary: A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.

Legal Entity: A Private Organization, Government Entity, Business Entity, or Non-Commercial Entity.

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal Practitioner: A person who is either a lawyer or a Latin Notary as described in these Requirements and competent to render an opinion on factual claims of the Applicant.

Legal Entity Identifier ("LEI"): LEI is specified in the ISO 17442 and names legal entities in the Global Legal Entity Identifier Index.

Mark: A Combined Mark, Design Mark, or Word Mark.

Mark Asserting Entity ("MAE"): An Applicant for/Subscriber of a Verified Mark Certificate. May be the same as the Applicant and/or Subscriber.

Mark Representation: A digital representation of a Combined Mark, Design Mark, or Word Mark such as a digital or computer file, containing structured binary or textual data which can be interpreted to recreate (render) a visual representation of the mark so that it can be seen. The Mark Representation will be used as the Logotype Extension under Section 7.1.2.3.

Mark Verifying Authority ("MVA"): The authority who issues a Verified Mark Certificate. Also referred to as a Certification Authority or CA.

Maximum Validity Period: 1. The maximum time period for which the issued VMC is valid. 2. The maximum period after validation by the CA that certain Applicant information may be relied upon in issuing a VMC pursuant to these Requirements.

Notary: A notary (or legal equivalent in the applicable jurisdiction), Latin Notary, lawyer, solicitor, or other person or organization in the jurisdiction where the Contract Signer or Certificate Approver (also known as the "Designated Individual") will be verified whose commission under applicable law includes authority to authenticate the execution of a signature on a document. "Notarize" includes Remote Notarization.

Notarize: The process by which the Notary verifies the identity of the Contract Signer or Certificate Approver by means of a government-issued photo ID, observes the Contract Signer or Certificate Approver sign a Verification Document prepared by the CA, and signs and affixes the Notary's notarization seal or other equivalent method to the Verification Document to indicate the Notarization process has been completed by the Notary.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol as defined in RFC6960 that enables Relying Parties and relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

Private Key: The key of a Key Pair that corresponds to the Public Key used by the Subscriber to sign a VMC certificate request. Once the Private Key-Public Key pair has been generated, the Private Key is not used and may be discarded.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted.

Principal Individual: An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of Verified Mark Certificates.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used to generate VMC signing requests for the CA on behalf of the Subscriber.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Practitioner: A natural person or Legal Entity that meets the requirements of Section 8.2.

Qualified Government Information Source: A database maintained by a Government Entity (e.g. SEC filings) that meets the requirements of Section 3.2.13.4.

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar. A Registered Domain Name may also be called an Organizational Domain.

Registered Agent: An individual or entity that is: (i) authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and (ii) listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (i) above.

Registered Office: The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.

Registered Mark: A Mark that has been registered as a trademark with a Trademark Office, and in particular, as the Mark appears in the official database of the applicable Trademark Office.

Registered Mark Profile: Verified Mark Certificates that have been issued following the validation procedures in section 13.2.6 and designated by a Certificate General Policy Identifier OID (1.3.6.1.4.1.53087.1.1) as described under Section 7.1.2.2 and 7.1.2.3. These VMCs have a SVG in the logotype extension that contains registered mark and other distinguishing fields noted elsewhere.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA as stipulated in Section 1.3.2.

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registration Number: The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation

Registration Reference: A unique identifier assigned to a Legal Entity.

Regulated Financial Institution: A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities.

Relying Party: Any natural or legal person that relies on a VMC or the information or Marks contained in a VMC or displayed to the person by a Consuming Entity. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Remote Notarization: The process by which a Notary Notarizes a document over a live video/audio link while the Notary and the Contract Signer or Certificate Approver are physically in different locations.

Repository: An online database containing publicly-disclosed VMC governance documents (such as Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token: A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. The CA SHOULD define within its CPS (or a document clearly referenced by the CPS) the format and method of Request Tokens it accepts.

The Request Token SHALL incorporate the key used in the certificate request.

A Request Token MAY include a timestamp to indicate when it was created.

A Request Token MAY include other information to ensure its uniqueness.

A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.

A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.

A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Note: Examples of Request Tokens include, but are not limited to:
(i) a hash of the public key; or
(ii) a hash of the Subject Public Key Info [X.509]; or
(iii) a hash of a PKCS#10 CSR.

A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.

Note: This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR.

```
echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr` \| sed "s/[ -]//g"
```

The script outputs:

201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The VMC Requirements found in this document.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subscriber: A person, entity, or organization that has applied for and has been issued a Verified Mark Certificate.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company: A company that is controlled by a Parent Company.

Superior Government Entity: Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of the Applicant.

SVG Guidelines: The draft-svg-tiny-ps-abrotman-01 version of the SVG Tiny Portable/Secure (SVG Tiny PS) Guidelines document located at this URL: https://bimigroup.org/resources/RFC_SVG_PS.txt as well as a RNC validator located at this URL: http://bimigroup.org/resources/SVG_PS-latest.rnc.txt
Both are published by the Authindicators Working Group.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Third Party Validator: A person or organization who performs the face-to-face validation of the Contract Signer or Certificate Approver under Appendix G.

Trademark Office: An intellectual property office recognized by the World Intellectual Property Organization for registration of trademarks (see: https://www.wipo.int/directory/en/urls.jsp), and that is listed in Appendix C.

Translator: An individual or Business Entity that possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

Verification Document: A document used to verify the identity and relevant information of the Contract Signer or Certificate Approver (acting as the Designated Individual) that is Notarized by a Notary. The Verification Document should:

(1) List the Contract Signer or Certificate Approver's name, title, Applicant organization name, and the address where the Contract Signer or Certificate Approver is located when the Notarization procedure occurs,
(2) Contain language that the Contract Signer or Certificate Approver confirms the information listed in (1) is correct and a place for the Contract Signer or Certificate Approver to sign the document, and
(3) Contain appropriate text for the Notary to sign and affix a seal (as appropriate in the jurisdiction) to indicate the Verification Document was Notarized by the Notary.

Verified Accountant Letter: A document meeting the requirements specified in Section 3.2.13.2 of these Requirements

Verified Legal Opinion: A document meeting the requirements specified in Section 3.2.13.1 of these Requirements.

Verified Mark Certificate: A certificate that contains subject information and extensions specified in these VMC Requirements and that has been verified and issued by a CA in accordance with these VMC Requirements.

Verified Method of Communication: The use of a telephone number, a fax number, an email address, or postal delivery address, confirmed by the CA in accordance with Section 3.2.8 of the Requirements as a reliable way of communicating with the Applicant.

Verified Professional Letter: A Verified Accountant Letter or Verified Legal Opinion.

VMC Authority: A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the VMC Certificate Request, to take the Request actions described in these Requirements.

VMC Certificate Request: A request from an Applicant to the CA requesting that the CA issue a VMC Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Certificate Approver.

VMCR: These VMC Requirements

VMC Terms: The terms of use that apply to a VMC Certificate and to the Mark Representation and related data contained in a Verified Mark Certificate, as set out in Appendix D to these VMC Requirements.

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Word Mark: A trademark consisting exclusively of text expressed without regard to the font, style, size or color that has been registered as a trademark with a Trademark Office. See Appendix B for mapping of the names used by different trademarks offices to the definition of Word Mark.

1.6.2. Acronyms

AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol
BIPM	International Bureau of Weights and Measures
BIS	(US Government) Bureau of Industry and Security
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPA	Chartered Professional Accountant
CSO	Chief Security Officer
EV	Extended Validation
gTLD	Generic Top-Level Domain
IFAC	International Federation of Accountants
IRS	Internal Revenue Service
ISP	Internet Service Provider
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
SEC	(US Government) Securities and Exchange Commission
UTC(k)	National realization of Coordinated Universal Time

1.6.3. References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

FIPS 186-4, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, July 2013.

ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework.

Network and Certificate System Security Requirements, v1.7, 4/5/2021.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

RFC3912, Request for Comments: 3912, WHOIS Protocol Specification, Daigle, September 2004.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013.

RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format, Newton, et al, March 2015.

WebTrust for Certification Authorities , SSL Baseline with Network Security, Version 2.0, available at http://www.webtrust.org/homepage-documents/item79806.pdf.

RFC8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, Hoffman-Andrews, November 2019.

X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

1.6.4. Conventions

The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements shall be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

2.1. REPOSITORIES

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy.

2.2. PUBLICATION OF INFORMATION

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8.1).

The Certificate Policy and/or Certification Practice Statement MUST be structured in accordance with RFC 3647 and MUST include all material required by RFC 3647.

Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy SHALL be consistent with these Requirements. It SHALL clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issuevmc" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.

The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA MAY fulfill this requirement by incorporating these Requirements directly into its Certificate Policy and/or Certification Practice Statements or by incorporating them by reference using a clause such as the following (which MUST include a link to the official version of these Requirements):

> [Name of CA] conforms to the current version of the Verified Mark Certificate Requirements published at https://bimigroup.org. In the event of any inconsistency between this document and those Requirements, those requirements take precedence over this document.

2.3. TIME OR FREQUENCY OF PUBLICATION

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

2.4. ACCESS CONTROLS ON REPOSITORIES

The CA SHALL make its Repository publicly available in a read-only manner.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of names

No stipulation.

3.1.2. Need for names to be meaningful

No stipulation.

3.1.3. Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of names

No stipulation.

3.1.6. Recognition, authentication, and role of trademarks

No stipulation.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method to Prove Possession of Private Key

The Public Key contained in Verified Mark Certificates is not used, so CAs are not required to prove possession of the associated Private Key.

3.2.2. Authentication of Organization and Domain Identity

The CA MAY only issue VMC Certificates to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements specified below.

3.2.2.1. Private Organization Subjects

An Applicant qualifies as a Private Organization if:

(1) The entity's legal existence is created or recognized by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation, registration number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);
(2) The entity designated with the Incorporating or Registration Agency a Registered Agent, a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration), or an equivalent facility;
(3) The entity is not designated on the records of the Incorporating or Registration Agency by labels such as "inactive," "invalid," "not current," or the equivalent;
(4) The entity has a verifiable physical existence and business presence;
(5) The entity's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
(6) The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

3.2.2.2. Government Entity Subjects

An Applicant qualifies as a Government Entity if:

(1) The entity's legal existence was established by the political subdivision in which the entity operates;
(2) The entity is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
(3) The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

3.2.2.3. Business Entity Subjects

An Applicant qualifies as a Business Entity if:

(1) The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;
(2) The entity has a verifiable physical existence and business presence;
(3) At least one Principal Individual associated with the entity is identified and validated by the CA;
(4) The identified Principal Individual attests to the representations made in the Subscriber Agreement;
(5) The entity and the identified Principal Individual associated with the entity are not located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
(6) The entity and the identified Principal Individual associated with the entity are not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

3.2.2.4. Non-Commercial Entity Subjects

An Applicant qualifies as a Non-Commercial Entity if:

(A) The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of Applicants who qualify as an International Organization for Verified Mark eligibility; and
(B) The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
(C) The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Subsidiary organizations or agencies of an entity that qualifies as a Non-Commercial Entity also qualifies for Verified Mark Certificates as a Non-Commercial Entity.

3.2.3. Verification Requirements – Overview

Before issuing an Verified Mark Certificate, the CA MUST ensure that all Subject organization information to be included in the VMC conforms to the requirements of, and is verified in accordance with, these Requirements and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

Verify Applicant's existence and identity, including;
(A) Verify the Applicant's legal existence and identity (as more fully set forth in Section 3.2 herein),
(B) Verify the Applicant's physical existence (business presence at a physical address), and
(C) Verify the Applicant's operational existence (business activity).

Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the Verified Mark Certificate;

(3) Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;

Verify the Applicant's authorization for the Verified Mark Certificate, including;
(A) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
(B) Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized individual acknowledged and agreed to the Terms of Use; and
(C) Verify that a Certificate Approver has signed or otherwise approved the Verified Mark Certificate Request.

3.2.4. Acceptable Methods of Verification – Overview

As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subsections below. The Acceptable Methods of Verification set forth in each of Sections 3.2.5 through 3.2.18 (which usually include alternatives) are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

3.2.5. Verification of Applicant's Legal Existence and Identity

3.2.5.1. Verification Requirements

To verify the Applicant's legal existence and identity, the CA MUST do the following.

(1) **Private Organization Subjects**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.

(B) **Organization Name:** Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the Verified Mark Certificate Request.

(C) **Registration Number:** Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.

(D) **Registered Agent:** Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

(2) **Government Entity Subjects**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the Verified Mark Certificate Request.

(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity.

(3) **Business Entity Subjects**

(A) **Legal Existence:** Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.

(B) **Organization Name:** Verify that the Applicant's formal legal name as recognized by the Registration Agency in the Applicant's Jurisdiction of Registration matches the Applicant's name in the Verified Mark Certificate Request.

(C) **Registration Number:** Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Registration.

(D) **Principal Individual:** Verify the identity of the identified Principal Individual.

(4) **Non-Commercial Entity Subjects (International Organizations)**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized International Organization Entity.

(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the Verified Mark Certificate Request.

(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances

where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

3.2.6. Acceptable Method of Verification

(1) **Private Organization Subjects:** All items listed in Section 3.2.5.1 (1) MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Such verification MAY be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Incorporating or Registration Agency, or from a Qualified Independent Information Source.

(2) **Government Entity Subjects:** All items listed in Section 3.2.5.1 (2) MUST either be verified directly with, or obtained directly from, one of the following: (i) a Qualified Government Information Source in the political subdivision in which such Government Entity operates; (ii) a superior governing Government Entity in the same political subdivision as the Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department)
Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

(3) **Business Entity Subjects:** Items listed in Section 3.2.5.1 (3) (A) through (C) above, MUST be verified directly with, or obtained directly from, the Registration Agency in the Applicant's Jurisdiction of Registration. Such verification MAY be performed by means of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Qualified Governmental Tax Information Source or Registration Agency, or from a Qualified Independent Information Source. In addition, the CA MUST validate a Principal Individual associated with the Business Entity pursuant to the requirements in subsection (4), below.

(4) **Principal Individual:** A Principal Individual associated with the Business Entity MUST be validated in a face-to-face setting. The CA MAY rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements of the Requirements for face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Requirements, the CA SHALL perform face-to-face validation.

(A) **Face-To-Face Validation:** The face-to-face validation MUST be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator). In all cases, the Third-Party Validator must be working on behalf of the CA. The Principal Individual(s) MUST present the following documentation (Vetting Documents) directly to the Third-Party Validator:

(i) A Personal Statement that includes the following information:

1. Full name or names by which a person is, or has been, known (including all other names used);
2. Residential Address at which he/she can be located;
3. Date of birth; and
4. An affirmation that all of the information contained in the Certificate Request is true and correct.

(ii) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

1. A passport;
2. A driver's license;
3. A personal identification card;
4. A concealed weapons permit; or

5. A military ID.

(iii) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.

1. Acceptable financial institution documents include:

a. A major credit card, provided that it contains an expiration date and it has not expired'

b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired,

c. A mortgage statement from a recognizable lender that is less than six months old,

d. A bank statement from a regulated financial institution that is less than six months old.

2. Acceptable non-financial documents include:

a. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),

b. A copy of a statement for payment of a lease, provided that the statement is dated within the past six months,

c. A certified copy of a birth certificate,

d. A local authority tax bill for the current year,

e. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

The Third-Party Validator performing the face-to-face validation MUST:

(i) Attest to the signing of the Personal Statement and the identity of the signer; and

(ii) Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

(B) **Verification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.

(C) **Cross-checking of Information:** The CA MUST obtain the signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. The CA MUST review the documentation to determine that the information is consistent, matches the information in the application, and identifies the Individual. The CA MAY rely on electronic copies of this documentation, provided that:

(i) the CA confirms their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and

(ii) electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of the CA's jurisdiction.

(5) **Non-Commercial Entity Subjects (International Organization):** Unless verified under subsection (6), all items listed in Section 3.3.1(4) MUST be verified either:

(A) With reference to the constituent document under which the International Organization was formed; or

(B) Directly with a signatory country's government in which the CA is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or

(C) Directly against any current list of qualified entities that the Authindicators/BIMI Group may maintain at https://bimigroup.org.

(D) In cases where the International Organization applying for the VMC is an organ or agency - including a non-governmental organization of a verified International Organization, then the CA may verify the International Organization Applicant directly with the verified umbrella International Organization of which the Applicant is an organ or agency.

3.2.7. Verification of Applicant's Physical Existence

3.2.7.1. Address of Applicant's Place of Business

(1) **Verification Requirements:** To verify the Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.

(2) **Acceptable Methods of Verification**

(A) **Place of Business in the Country of Incorporation or Registration**

(i) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used in Section 3.2.5 to verify legal existence:

(1) For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, the CA MUST confirm that the Applicant's address, as listed in the Verified Mark Certificate Request, is a valid business address for the Applicant or a Parent/Subsidiary Company by reference to such QGIS, QIIS, or QTIS, and MAY rely on the Applicant's representation that such address is its Place of Business;

(2) For Applicants who are not listed at the same Place of Business address in the current version of either at least one QIIS or QTIS, the CA MUST confirm that the address provided by the Applicant in the Verified Mark Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

(a) Verify that the Applicant's business is located at the exact address stated in the Verified Mark Certificate Request (e.g., via permanent signage, employee confirmation, etc.),

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant,

(d) Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.), and

(e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.

(3) For all Applicants, the CA MAY alternatively rely on a Verified Professional Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

(4) For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.

(5) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in Section 3.2.5 to verify legal existence contains a business address for the Applicant, the CA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the Verified Mark Certificate Request, and MAY rely on the Applicant's representation that such address is its Place of Business.

(B) **Place of Business not in the Country of Incorporation or Registration:** The CA MUST rely on a Verified Professional Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

3.2.8. Verified Method of Communication

3.2.8.1. Verification Requirements

To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the CA MUST verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

3.2.8.2. Acceptable Methods of Verification

To verify a Verified Method of Communication with the Applicant, the CA MUST:

(A) Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in: (i) records provided by the applicable phone company; (ii) a QGIS, QTIS, or QIIS; or (iii) a Verified Professional Letter; and

(B) Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication.

3.2.9. Verification of Applicant's Operational Existence

3.2.9.1. Verification Requirements

The CA MUST verify that the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence. The CA MAY rely on its verification of a Government Entity's legal existence under Section 3.3 as verification of a Government Entity's operational existence.

3.2.9.2. Acceptable Methods of Verification

To verify the Applicant's ability to engage in business, the CA MUST verify the operational existence of the Applicant, or its Affiliate/Parent/Subsidiary Company, by:

(1) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;

(2) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;

(3) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or

(4) Relying on a Verified Professional Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

3.2.10. Verification of Identity and Authority of Contract Signer and Certificate Approver

3.2.10.1. Verification Requirements

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.

(1) **Name, Title and Agency:** The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.

(2) **Signing Authority of Contract Signer:** The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.

(3) **VMC Authority of Certificate Approver:** The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the Verified Mark Certificate Request:

(A) Submit, and, if applicable, authorize a Certificate Requester to submit, the Verified Mark Certificate Request on behalf of the Applicant; and

(B) Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the Verified Mark Certificate; and

(C) Approve Verified Mark Certificate Requests submitted by a Certificate Requester.

(4) **Notary Validation:** The CA must conduct validation of the Contract Signer or Certificate Approver for the Applicant following the validation steps described in Appendix G. The CA must verify that the validator is a legally-qualified Notary (or legal equivalent in the Contract Signer or Certificate Approver's jurisdiction), Latin Notary, lawyer, or solicitor (collectively, "Notary") in the jurisdiction where the Contract Signer or Certificate Approver is verified.

3.2.10.2. Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.

(1) **Name and Title:** The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role**.**

(2) **Agency:** The CA MAY verify the agency of the Contract Signer and the Certificate Approver by:

(A) Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee;

(B) Obtaining an Independent Confirmation From the Applicant (as described in Section 3.2.13.4), or a Verified Professional Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant; or

(C) Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

The CA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

3.2.10.3. Acceptable Methods of Verification – Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the VMC Authority of the Certificate Approver, as applicable, include:

(1) **Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the VMC Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;

(2) **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the VMC Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Section 3.2.13.1);

(3) **Contract between CA and Applicant:** The VMC Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA and the Applicant that designates the Certificate Approver with such VMC Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(5) **Prior Equivalent Authority:** The signing authority of the Contract Signer, and/or the VMC Authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.

(A) Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the Verified Mark Certificate application. The CA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the Verified Mark application. Such details MAY include any of the following:

(i) Agreement title,

(ii) Date of Contract Signer's signature,

(iii) Contract reference number, and

(iv) Filing location.

(B) Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the VMC Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:
  (i) Under contract to the CA, has served (or is serving) as an Enterprise RA for the Applicant, or
  (ii) Has participated in the approval of one or more certificate requests, for certificates issued by the CA and which are currently and verifiably in use by the Applicant. In this case the CA MUST have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.

(6) **QIIS or QGIS**: The Signing Authority of the Contract Signer, and/or the VMC Authority of the Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as a corporate officer, sole proprietor, or other senior official of the Applicant.

(7) **Contract Signer's Representation/Warranty:** Provided that the CA verifies that the Contract Signer is an employee or agent of the Applicant, the CA MAY rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments:
  (A) That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,
  (B) That the Subscriber Agreement is a legally valid and enforceable agreement,
  (C) That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions,
  (D) That serious consequences attach to the misuse of an Verified Mark certificate, and
  (E) The contract signer has the authority to obtain the digital equivalent of a corporate seal, stamp or officer's signature to establish the authenticity of the company's Web site.

3.2.10.4. Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future Verified Mark Certificate Requests, then, after the CA:

- Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and
- Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 3.2.10.

The CA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise VMC Authority with respect to each future Verified Mark Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement MUST provide that the Applicant SHALL be obligated under the Subscriber Agreement for all Verified Mark Certificates issued at the request of, or approved by, such Certificate Approver(s) until such VMC Authority is revoked, and MUST include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when Verified Mark Certificate Requests are approved, (ii) periodic re-confirmation of the VMC Authority of the Certificate Approver, (iii) secure procedures by which the Applicant can notify the CA that the VMC Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

3.2.11. Verification of Signature on Subscriber Agreement and Verified Mark Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized Verified Mark Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The Verified Mark Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section 3.2.10.4 of these Requirements. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the Verified Mark Certificate Request. In all cases, applicable signatures MUST be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or Verified Mark Certificate Request), or a legally valid and enforceable electronic signature (for an

electronic Subscriber Agreement and/or Verified Mark Certificate Request), that binds the Applicant to the terms of each respective document.

3.2.11.1. Verification Requirements

(1) **Signature:** The CA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each Verified Mark Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

(2) **Approval Alternative:** In cases where an Verified Mark Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the Verified Mark Certificate Request by a Certificate Approver in accordance with the requirements of Section 3.2.12 can substitute for authentication of the signature of the Certificate Requester on such Verified Mark Certificate Request.

3.2.11.2. Acceptable Methods of Signature Verification

Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following:

(1) Contacting the Applicant using a Verified Method of Communication for the Applicant, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;

(2) A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with these Requirements, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response through a Verified Method of Communication from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;

(3) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate; or

(4) Notarization by a notary, provided that the CA independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer.

3.2.12. Verification of Approval of Verified Mark Certificate Request

3.2.12.1. Verification Requirements

In cases where an Verified Mark Certificate Request is submitted by a Certificate Requester, before the CA issues the requested Verified Mark Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the Verified Mark Certificate Request.

3.2.12.2. Acceptable Methods of Verification

Acceptable methods of verifying the Certificate Approver's approval of a Verified Mark Certificate Request include:

(1) Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the Verified Mark Certificate Request;

(2) Notifying the Certificate Approver that one or more new Verified Mark Certificate Requests are available for review and approval at a designated access-controlled and secure Web site, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site; or

(3) Verifying the signature of the Certificate Approver on the Verified Mark Certificate Request in accordance with Section 3.2.11 of these Requirements.

3.2.13. Verification of Certain Information Sources

3.2.13.1. Verified Legal Opinion

(1) **Verification Requirements:** Before relying on a legal opinion submitted to the CA, the CA MUST verify that such legal opinion meets the following requirements:

(A) **Status of Author:** The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:
   (i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility, or
   (ii) A Latin Notary who is currently commissioned or licensed to practice in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary);

(B) **Basis of Opinion:** The CA MUST verify that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise;

(C) **Authenticity:** The CA MUST confirm the authenticity of the Verified Legal Opinion.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:

(A) **Status of Author:** The CA MUST verify the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction;

(B) **Basis of Opinion:** The text of the legal opinion MUST make it clear that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion MAY also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous;

(C) **Authenticity:** To confirm the authenticity of the legal opinion, the CA MUST make a telephone call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner, and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Legal Practitioner in records provided by the applicable phone company, QGIS, or QIIS.
In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 3.2.13.1(2)(A), no further verification of authenticity is required.

3.2.13.2. Verified Accountant Letter

(1) **Verification Requirements:** Before relying on an accountant letter submitted to the CA, the CA MUST verify that such accountant letter meets the following requirements:

(A) **Status of Author:** The CA MUST verify that the accountant letter is authored by an Accounting Practitioner retained or employed by the Applicant and licensed within the country of the Applicant's Jurisdiction of Incorporation, Jurisdiction of Registration, or country where the Applicant maintains an office or physical facility. Verification of license MUST be through the member organization or regulatory organization in the Accounting Practitioner's country or jurisdiction that is appropriate to contact when verifying an accountant's license to practice in that country or jurisdiction. Such country or jurisdiction must have an accounting standards body that maintains full membership status with the International Federation of Accountants.

(B) **Basis of Opinion:** The CA MUST verify that the Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise;

(C) **Authenticity:** The CA MUST confirm the authenticity of the Verified Accountant Letter.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are listed here.
   (A) **Status of Author:** The CA MUST verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction.
   (B) **Basis of Opinion:** The text of the Verified Accountant Letter MUST make clear that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The Verified Accountant Letter MAY also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the Verified Accountant Letter prove to be erroneous.
   (C) **Authenticity:** To confirm the authenticity of the accountant's opinion, the CA MUST make a telephone call or send a copy of the Verified Accountant Letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Accountant in records provided by the applicable phone company, QGIS, or QIIS.
   In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 3.2.13.2(2)(A), no further verification of authenticity is required.

3.2.13.3. Face-to-Face Validation

(1) **Verification Requirements:** Before relying on face-to-face vetting documents submitted to the CA, the CA MUST verify that the Third-Party Validator meets the following requirements:
   (A) **Qualification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency;
   (B) **Document Chain of Custody:** The CA MUST verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated;
   (C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the attestation and vetting documents.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for vetting documents are:
   (A) **Qualification of Third-Party Validator:** The CA MUST verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction;
   (B) **Document Chain of Custody:** The Third-Party Validator MUST submit a statement to the CA which attests that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual;
   (C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the vetting documents received from the Third-Party Validator. The CA MUST make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. The CA MAY rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by the CA in Section 3.2.13.1 (1)(A), no further verification of authenticity is required.

3.2.13.4. Independent Confirmation From Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the VMC Authority of a Certificate Approver, etc.) that is:

(A) Received by the CA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;
(B) Received by the CA in a manner that authenticates and verifies the source of the confirmation; and
(C) Binding on the Applicant.

An Independent Confirmation from the Applicant MAY be obtained via the following procedure:

(1) **Confirmation Request:** The CA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:
   (A) **Addressee:** The Confirmation Request MUST be directed to:
      (i) A position within the Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current QGIS, QIIS, QTIS, Verified Legal Opinion, Verified Accountant Letter, or by contacting the Applicant using a Verified Method of Communication; or
      (ii) The Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or
      (iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Requirements).
   (B) **Means of Communication:** The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:
      (i) By paper mail addressed to the Confirming Person at:
         (1) The address of the Applicant's Place of Business as verified by the CA in accordance with these Requirements, or
         (2) The business address for such Confirming Person specified in a current QGIS, QTIS, QIIS, Verified Professional Letter, or
         (3) The address of the Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation, or
      (ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current QGIS, QTIS, or QIIS, Verified Legal Opinion, or Verified Accountant Letter; or
      (iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of the Applicant's Place of Business (verified in accordance with these Requirements) and asking to speak to such person, and a person taking the call identifies him- or herself as such person; or
      (iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current QGIS, QTIS, or QIIS, Verified Legal Opinion, or Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

(2) **Confirmation Response:** The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by e-mail, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(3) The CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. The CA MAY rely on this verified contact information for future correspondence with the Confirming Person if:
   (A) The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias;
   (B) The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

3.2.13.5. Qualified Independent Information Source

A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if the CA determines that:

(1) Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and
(2) The database provider updates its data on at least an annual basis.

The CA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use. The CA SHALL NOT use any data in a QIIS that the CA knows is (i) self-reported and (ii) not verified by the QIIS as accurate. Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest, do not qualify as a QIIS.

3.2.13.6. Qualified Government Information Source

A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. Nothing in these Requirements SHALL prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

3.2.13.7. Qualified Government Tax Information Source

A Qualified Government Tax Information Source is a Qualified Government Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g., the IRS in the United States).

3.2.14. Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

CAs SHALL maintain a record of which domain validation method, including relevant VMC Requirements version number, they used to validate every domain.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

3.2.14.1. Validating the Applicant as a Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.14.2. Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.
Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.3. Phone Contact with Domain Contact

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.14.4. Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by

1. sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,
2. including a Random Value in the email, and
3. receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.
The Random Value SHALL be unique in each email.
The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.
The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.
Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.5. Domain Authorization Document

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.14.6. Agreed-Upon Change to Website

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.14.7. DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.
If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Requirements).
Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.8. IP Address

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.14.9. Test Certificate

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.14.10. TLS Using a Random Number

This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.14.11. Any Other Method

This method has been retired and MUST NOT be used.

3.2.14.12. Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.13. Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659.

Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.14. Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.15. Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.
In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact.
In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.
The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.
Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.16. Phone Contact with DNS TXT Record Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.
The CA MAY NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.
In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.
The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.
Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.17. Phone Contact with DNS CAA Phone Contact

Confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659.
The CA MUST NOT be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation.
In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.
The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.
Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.18. Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and
2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

1. MUST be located on the Authorization Domain Name, and
2. MUST be located under the "/.well-known/pki-validation" directory, and

3. MUST be retrieved via either the "http" or "https" scheme, and
4. MUST be accessed over an Authorized Port.

If the CA follows redirects the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code).
2. Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
3. Redirects MUST be to resource URLs with either via the "http" or "https" scheme.
4. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. The CA MUST provide a Random Value unique to the certificate request.
2. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.19. Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, section 8.3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

If the CA follows redirects:

1. Redirects MUST be initiated at the HTTP protocol layer (e.g. using a 3xx status code).
2. Redirects MUST be the result of an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.
3. Redirects MUST be to resource URLs with either via the "http" or "https" scheme.
4. Redirects MUST be to resource URLs accessed via Authorized Ports.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

3.2.14.20. TLS Using ALPN

Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The following are additive requirements to RFC 8737.

The token (as defined in RFC 8737, section 3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for the token, in which case the CA MUST follow its CPS.

3.2.15. CAA Records for Verified Mark Certificates

(1) As part of the issuance process, the CA MUST check for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in Subsection (2). If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater. CAA checking is optional for VMCs issued before January 1, 2021, but MUST be done for VMCs issued on or after January 1, 2022.
This stipulation does not prevent the CA from checking CAA records at any other time.

RFC 8659 requires that CAs "MUST NOT issue a certificate unless either (1) the certificate request is consistent with the applicable CAA Resource Record set or (2) an exception specified in the relevant Certificate Policy or Certification Practices Statement applies." For issuances conforming to these

Baseline Requirements, CAs MUST NOT rely on any exceptions specified in their CP or CPS unless they are one of the following:

- CAA checking is optional for certificates for which a Certificate Transparency pre-certificate was created and logged in at least one public log listed in Appendix F, and for which CAA was checked.
- CAA checking is optional if the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

CAs are permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure; and
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

CAs MUST document potential issuances that were prevented by a CAA record and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), If present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

(2) Prior to the issuance of Verified Mark Certificates, the CA MUST check for the publication of a Relevant RRSet for each FQDN to be included in a dNSName within the Verified Mark Certificate's subjectAlternativeName extension. The Relevant RRSet for each FQDN must be determined using the algorithm defined in section 3 of RFC 8659.

For each FQDN, if a Relevant RRSet exists, the CA MUST NOT issue the Certificate unless the CA determines that the certificate request is consistent with the Relevant RRSet. If the Relevant RRSet for an FQDN does not contain any Property Tags that restrict issuance of a Verified Mark Certificate and does not contain any unrecognized Property Tags that are marked critical, then the Relevant RRSet does not restrict issuance of a Verified Mark Certificate containing the given FQDN. In particular, CAA records with "issue" and "issuewild" Property Tags do not restrict the issuance of Verified Mark Certificates.

If a CAA record with the "issuevmc" Property Tag is present in the Relevant RRset for an FQDN, it is a request that the CA:

1. Perform CAA issue restriction processing for the FQDN, and
2. Grant authorization to issue Verified Mark Certificates containing that FQDN to the holder of the issuer-domain-name or a party acting under the explicit authority of the holder of the issuer-domain-name.

The sub-syntax of the "issuevmc" Property Tag value is the same as the "issue" Property Tag as defined in section 4.2 of RFC 8659. The semantics of the "issuevmc" Property Tag are similar to the "issue" Property Tag, with the only difference being that the "issuevmc" Property Tag restricts issuance of Verified Mark Certificates as opposed to TLS Server Authentication Certificates.

3.2.16. Registered Mark Verification

VMCs may be issued for Combined Marks, Design Marks, and Word Marks under the Registered Mark Profile designated by a Certificate General Policy Identifier OID (1.3.6.1.4.1.53087.1.1) as described under Section 7.1.2.2 and 7.1.2.3 . In addition to the identity and domain verification required by Section 3.1, CAs issuing Verified Mark Certificates SHALL perform verification of the submitted Registered Mark as follows:

3.2.16.1. Verification of Mark with Trademark Office

The Subscriber will provide the CA with (a) the Registered Mark's trademark registration number and name of the Trademark Office that granted the trademark registration, and (b) the Mark Representation in SVG

format that the Applicant wishes to include in the Verified Mark Certificate. Registered Marks must be in good standing, and MUST be verified through consultation with the official database of the applicable Trademark Office, to be eligible for inclusion within a Verified Mark Certificate. In addition, only Registered Marks are eligible for inclusion within the logotype (as defined in RFC3709). For clarity and without limitation, unregistered marks are not eligible as a logotype in the registered mark profile.

In the alternative, the CA may verify the Registered Mark through the WIPO Global Brand Database at https://www3.wipo.int/branddb/en/

The CA SHALL confirm that the Mark Representation submitted by the Subject organization matches the Registered Mark as it appears in the official database of the applicable Trademark Office or the WIPO Global Brand Database. In determining whether the Mark Representation matches the Registered Mark, the CA SHALL maintain a record of its decisions and reasons therefor. The CA may, but is not required to, follow the guidelines in Appendix E for comparison of the Registered Trademark with the Mark Representation.

The CA SHALL also retain a screenshot or other record of the Mark Representation provided by the Applicant and all information about the Registered Mark obtained from the applicable Trademark Office as well as all other supporting data that the CA relies upon in issuing the Verified Mark Certificate.

3.2.16.2. Verification of Registered Mark Ownership or License

The CA SHALL confirm that the owner of the Registered Mark identified in the official database of the applicable Trademark Office or the WIPO Global Brand Database is the same Subject organization verified by the Verified Mark vetting process under Section 3.2 (or to a Parent, Subsidiary, or Affiliate of the organization as confirmed in accordance with the Verified Mark Requirements), or if the owner of the Registered Mark is not the same organization, that the Subject organization has obtained the right to use the Registered Mark through a mutually agreed-upon license from the entity who is the owner of record of the Registered Mark (or a Parent, Subsidiary, or Affiliate of the owner). If the owner of a Registered Mark is not the Applicant, the Applicant may only use the Registered Mark if the CA obtains an authorization letter from the owner of record of the Registered Mark.

In determining whether the Applicant is the owner or a licensee of the Registered Mark corresponding to the Mark Representation, the CA SHALL maintain a record of its decisions and reasons therefor in the CA's records required in section 3.2.1.

3.2.16.3. Color Restrictions

Mark Representations in Verified Mark Certificates for Combined Marks and Design Marks SHALL only be in colors as permitted for the Registered Mark by the applicable Trademark Office. The CA SHALL examine the Registered Mark to determine what rights, if any, the Subject organization has to use of the Registered Mark in the colors of the Mark Representation submitted by the Subscriber.

In determining whether the colors in the Mark Representation submitted by the Subscriber match the colors permitted by the Registered Mark registration, the CA SHALL maintain a record of its decision and reasons therefor in the CA's records required in section 3.2.1.

3.2.17. Other Verification Requirements

3.2.17.1. Denied Lists and Other Legal Block Lists

(1) **Verification Requirements:** The CA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:
   (A) Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or

(B) Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

The CA MUST NOT issue any Verified Mark Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

(2) **Acceptable Methods of Verification:** The CA MUST take reasonable steps to verify with the following lists and regulations:

(A) If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with the following US Government denied lists and regulations:

(i) BIS Denied Persons List - http://www.bis.doc.gov/dpl/thedeniallist.asp

(ii) BIS Denied Entities List - http://www.bis.doc.gov/Entities/Default.htm

(iii) US Treasury Department List of Specially Designated Nationals and Blocked Persons - http://www.treas.gov/ofac/t11sdn.pdf

(iv) US Government export regulations

(B) If the CA has operations in any other country, the CA MUST take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

3.2.17.2. Parent/Subsidiary/Affiliate Relationship

A CA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under section 3.2.7.1, 3.2.8.2, 3.2.9.1, or 3.2.14, MUST verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate include the following:

(1) QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;

(2) Independent Confirmation from the Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Section 3.2.13.2);

(3) Contract between CA and Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA and the Parent, Subsidiary, or Affiliate that designates the Certificate Approver with such VMC Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(4) Corporate Resolution: A CA MAY verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated corporate resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

3.2.18. Final Cross-Correlation and Due Diligence

(1) The results of the verification processes and procedures outlined in these Requirements are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, the CA MUST have a second Validation Specialist who is not responsible for the collection of information review all of the information and documentation assembled in support of the Verified Mark Certificate application and look for discrepancies or other details requiring further explanation.

(2) The CA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.

(3) The CA MUST refrain from issuing an Verified Mark Certificate until the entire corpus of information and documentation assembled in support of the Verified Mark Certificate Request is such that issuance of the Verified Mark Certificate will not communicate factual information that the CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate,. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the Verified Mark Certificate Request and SHOULD notify the Applicant accordingly.

(4) In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or its Affiliate MUST perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 5.3 of these Requirements. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator.

3.2.19. Criteria for Interoperation or Certification

The CA SHALL disclose 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).

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

No stipulation.

3.3.2. Identification and Authentication for Re-key After Revocation

No stipulation.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

In accordance with Section 5.5.2, the CA SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA SHALL use this information to identify subsequent suspicious certificate requests.

The CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

4.1.2. Enrollment Process and Responsibilities

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 4.2.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name to be included in the Certificate's SubjectAltName extension.

Section 6.3.2 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 398 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

As an exception to the validation reuse period of 398 days defined above, face-to-face validation is not required more than once for any Subscriber Organization (or Parent, Subsidiary, or Affiliate) so long as the CA has maintained continuous contact with one or more Subscriber representatives and maintains a system for authorization by the Subscriber of new Subscriber representatives (or representatives of a Parent, Subsidiary, or Affiliate). "Continuous contact" means the CA has one or more direct contacts with a Subscriber representative during the validity period of any VMC issued to the Subscriber or within 90 days of the expiration of the last of the Subscriber's VMC to expire.

After the change to any validation method specified in the Verified Mark Requirements, a CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this section unless otherwise specifically provided in these Requirements.

4.2.2. Approval or Rejection of Certificate Applications

CAs SHALL NOT issue certificates containing Internal Names (see section 7.1.4.2.1).

4.2.3. Time to Process Certificate Applications

No stipulation.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

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.

Before issuance of a Verified Mark Certificate, the CA SHALL log the Verified Mark Certificate pre-certificate (including all the data included in the Subject field of the certificate plus the Mark Representation) to one or more public CT logs. The list of CT logs that are acceptable for the fulfillment of this requirement is found in Appendix F.

4.3.2. Notification of Certificate Issuance

No stipulation.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct constituting certificate acceptance

No stipulation.

4.4.2. Publication of the certificate by the CA

No stipulation.

4.4.3. Notification of certificate issuance by the CA to other entities

No stipulation.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber private key and certificate usage

The Subscriber private key does not need to be protected, and may be discarded.

4.5.2. Relying party public key and certificate usage

No stipulation.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for certificate renewal

No stipulation.

4.6.2. Who may request renewal

No stipulation.

4.6.3. Processing certificate renewal requests

No stipulation.

4.6.4. Notification of new certificate issuance to subscriber

No stipulation.

4.6.5. Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6. Publication of the renewal certificate by the CA

No stipulation.

4.6.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for certificate re-key

No stipulation.

4.7.2. Who may request certification of a new public key

No stipulation.

4.7.3. Processing certificate re-keying requests

No stipulation.

4.7.4. Notification of new certificate issuance to subscriber

No stipulation.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6. Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstance for certificate modification

No stipulation.

4.8.2. Who may request certificate modification

No stipulation.

4.8.3. Processing certificate modification requests

The CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:

(1) The expiration date of the replacement certificate is the same as the expiration date of the VMC that is being replaced, and
(2) The Subject Information of the Certificate is the same as the Subject in the VMC that is being replaced.

4.8.4. Notification of new certificate issuance to subscriber

No stipulation.

4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6. Publication of the modified certificate by the CA

No stipulation.

4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; or
3. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name in the Certificate should not be relied upon.

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following 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 a Fully-Qualified Domain in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the 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 Certificate Policy or Certification Practice Statement;
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 Certificate Policy and/or Certification Practice Statement.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 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 this document 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.

4.9.2. Who Can Request Revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3. Procedure for Revocation Request

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS.

4.9.4. Revocation Request Grace Period

No stipulation.

4.9.5. Time within which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

4.9.6. Revocation Checking Requirement for Relying Parties

No stipulation.

Note: Following certificate issuance, a certificate may be revoked for reasons stated in Section 4.9.1. Therefore, relying parties should check the revocation status of all certificates that contain a CDP or OCSP pointer.

4.9.7. CRL Issuance Frequency

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 days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates:

The CA SHALL update and reissue CRLs at least (i) once every twelve 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.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. On-line Revocation/Status Checking Availability

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. On-line Revocation Checking Requirements

OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

For the status of Subscriber Certificates:

- The CA SHALL update information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days. .

For the status of Subordinate CA Certificates:

- The CA SHALL update information provided via an Online Certificate Status Protocol (i) at least every twelve months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder MUST NOT respond with a "good" status.

The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

See Section 4.9.1.

4.9.13. Circumstances for Suspension

The Repository MUST NOT include entries that indicate that a Certificate is suspended.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.

4.10.2. Service Availability

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3. Optional Features

No stipulation.

4.11. END OF SUBSCRIPTION

No stipulation.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policy and practices

Not applicable.

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable.

5. MANAGEMENT, OPERTIONAL, AND PHYSICAL CONTROLS

The CA/Browser Forum's Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein.

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process MUST include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to 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 MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL 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.

5.1. PHYSICAL SECURITY CONTROLS

5.1.1. Site location and construction

No stipulation.

5.1.2. Physical access

No stipulation.

5.1.3. Power and air conditioning

No stipulation.

5.1.4. Water exposures

No stipulation.

5.1.5. Fire prevention and protection

No stipulation.

5.1.6. Media storage

No stipulation.

5.1.7. Waste disposal

No stipulation.

5.1.8. Off-site backup

No stipulation.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

No stipulation.

5.2.2. Number of Individuals Required per Task

The CA Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3. Identification and Authentication for Trusted Roles

No stipulation.

5.2.4. Roles Requiring Separation of Duties

No stipulation.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

5.3.2. Background Check Procedures

No stipulation.

5.3.3. Training Requirements and Procedures

The CA SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure 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 SHALL maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

The CA SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

5.3.4. Retraining Frequency and Requirements

All personnel in Trusted Roles SHALL maintain skill levels consistent with the CA's training and performance programs.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

No stipulation.

5.3.7. Independent Contractor Controls

The CA SHALL verify 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.

5.3.8. Documentation Supplied to Personnel

No stipulation.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

The CA and each Delegated Third Party SHALL 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. The CA SHALL make these records available to its Qualified Practitioner as proof of the CA's compliance with these Requirements.

The CA SHALL record at least the following events:

1. CA certificate and key lifecycle events, including:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate requests, renewal, and re-key requests, and revocation;
    3. Approval and rejection of certificate requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists and OCSP entries;
    6. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. Subscriber Certificate lifecycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    3. Approval and rejection of certificate requests;
    4. Issuance of Certificates; and
    5. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Security profile changes;
    4. Installation, update and removal of software on a Certificate System;
    5. System crashes, hardware failures, and other anomalies;
    6. Firewall and router activities; and
    7. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

5.4.2. Frequency for Processing and Archiving Audit Logs

No stipulation.

5.4.3. Retention Period for Audit Logs

The CA SHALL retain, for at least two years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
    a. the destruction of the CA Private Key; or
    b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the revocation or expiration of the Subscriber Certificate.
3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

5.4.4. Protection of Audit Log

No stipulation.

5.4.5. Audit Log Backup Procedures

No stipulation.

5.4.6. Audit Log Accumulation System (internal vs. external)

No stipulation.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

Additionally, the CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5. RECORDS ARCHIVAL

5.5.1. Types of Records Archived

No stipulation.

5.5.2. Retention Period for Archive

The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least two years after any Certificate based on that documentation ceases to be valid

5.5.3. Protection of Archive

No stipulation.

5.5.4. Archive Backup Procedures

No stipulation.

5.5.5. Requirements for Time-stamping of Records

No stipulation.

5.5.6. Archive Collection System (internal or external)

No stipulation.

5.5.7. Procedures to Obtain and Verify Archive Information

No stipulation.

5.6. KEY CHANGEOVER

No stipulation.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

CA organizations SHALL have an Incident Response Plan and a Disaster Recovery Plan.

The CA SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity

plans but SHALL make its business continuity plan and security plans available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan MUST include:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. 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
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. 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.

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

No stipulation.

5.7.3. Recovery Procedures After Key Compromise

No stipulation.

5.7.4. Business Continuity Capabilities after a Disaster

No stipulation.

5.8. CA OR RA TERMINATION

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

For Root CA Key Pairs that are either (i) used as Root CA Key Pairs or (ii) Key Pairs generated for a subordinate CA that is not the operator of the Root CA or an Affiliate of the Root CA, the CA SHALL:

1. prepare and follow a Key Generation Script,

2. have a Qualified Practitioner witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. have a Qualified Practitioner issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:

1. prepare and follow a Key Generation Script and
2. have a Qualified Practitioner witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.

In all cases, the CA SHALL:

1. generate the keys in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement;
2. generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. log its CA key generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

6.1.1.2. RA Key Pair Generation

No stipulation.

6.1.1.3. Subscriber Key Pair Generation

No stipulation.

6.1.2. Private Key Delivery to Subscriber

No stipulation.

6.1.3. Public Key Delivery to Certificate Issuer

No stipulation.

6.1.4. CA Public Key Delivery to Relying Parties

No stipulation.

6.1.5. Algorithm type and key sizes

Certificates MUST meet the following requirements for algorithm type and key size.

6.1.5.1. Root CA Certificates

- **Digest algorithm:** SHA-256, SHA-384 or SHA-512
- **Minimum RSA modulus size (bits):** 2048
- **ECC curve:** NIST P-256, P-384, or P-521

6.1.5.2. Subordinate CA Certificates

- **Digest algorithm:** SHA-256, SHA-384 or SHA-512
- **Minimum RSA modulus size (bits):** 2048
- **ECC curve:** NIST P-256, P-384, or P-521

6.1.5.3. Subscriber Certificates

- **Digest algorithm:** SHA-256, SHA-384 or SHA-512
- **Minimum RSA modulus size (bits):** 2048
- **ECC curve:** NIST P-256, P-384, or P-521

6.1.6. Public Key Parameters Generation and Quality Checking

RSA: The CA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].

ECC: The CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 56A: Revision 2].

6.1.7. Key Usage Purposes

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates which contain id-kp-BrandIndicatorforMessageIdentification (OID: 1.3.6.1.5.5.7.3.31) as the sole KeyPurposeId in the extendedKeyUsage extension;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

Private Keys corresponding to Subordinate CA or Cross Certificates MUST NOT sign Certificates unless the Certificate to be signed contains one of the following OIDs as the sole KeyPurposeId in the extendedKeyUsage extension:
a. id-kp-BrandIndicatorforMessageIdentification (OID: 1.3.6.1.5.5.7.3.31),; or
b. id-kp-OCSPSigning (OID: 1.3.6.1.5.5.7.3.9)

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1. Cryptographic Module Standards and Controls

No stipulation.

6.2.2. Private Key (n out of m) Multi-person Control

No stipulation.

6.2.3. Private Key Escrow

No stipulation.

6.2.4. Private Key Backup

See Section 5.2.2.

6.2.5. Private Key Archival

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

6.2.6. Private Key Transfer into or from a Cryptographic Module

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7. Private Key Storage on Cryptographic Module

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 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.

6.2.8. Activating Private Keys

No stipulation.

6.2.9. Deactivating Private Keys

No stipulation.

6.2.10. Destroying Private Keys

No stipulation.

6.2.11. Cryptographic Module Capabilities

No stipulation.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period MUST NOT exceed 398 days. If an Applicant is a licensee of a Registered Mark or Word Mark rather than the Registrant, the expiration date of the certificate SHALL have an expiration date that is no later than the final expiration date of the license held by the Applicant to use the Registered Mark or Word Mark, which SHALL be confirmed by the CA during the verification process.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

No stipulation.

6.4.2. Activation data protection

No stipulation.

6.4.3. Other aspects of activation data

No stipulation.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System development controls

No stipulation.

6.6.2. Security management controls

No stipulation.

6.6.3. Life cycle security controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

No stipulation.

6.8. TIME-STAMPING

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

Verified Mark Certificates SHALL comply with the Verified Mark Certificate profile requirements set out in this section.

CAs SHALL only issue Verified Mark Certificates from a dedicated sub-CA that contains the EKU specified in section 7.1.2.2 (g).

The CA SHALL also meet the technical requirements set forth in Section 2.2 – Publication of Information, Section 6.1.5– Key Sizes, and Section 6.1.6 – Public Key Parameters Generation and Quality Checking.
CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1. Version Number(s)

Certificates MUST be of type X.509 v3.

7.1.2. Certificate Content and Extensions; Application of RFC 5280

This section specifies the additional requirements for Certificate content and extensions for Certificates.

7.1.2.1. Root CA Certificate

a. basicConstraints
This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

b. keyUsage
This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

c. certificatePolicies
This extension SHOULD NOT be present.

d. extendedKeyUsage
This extension MUST NOT be present.

7.1.2.2. Subordinate CA Certificate

a. certificatePolicies
This extension MUST be present and SHOULD NOT be marked critical.

The CA MUST include Certificate Policy OIDs in Subordinate CA Certificates, as specified from one of the following two options:

1) Both of the following OIDs, as specified:
    a. The first certificate policies value contains an identifier that names the CA's Certification Practice Statement (CPS) applicable to the Verified Mark Certificate, together with a URL for the web page where the Certification Practice Statement can be publicly reviewed. The CA CPS identifier is the Policy Identifier of the certificate policies extension. The CA CPS URL is appended as a CPS pointer qualifier.
    b. The second certificate policies value contains a Verified Mark Certificate General Policy Identifier (1.3.6.1.4.1.53087.1.1) which indicates adherence to and compliance with these VMC Requirements and the VMC Terms. This identifier is assigned to the Policy Identifier of the certificate policies extension.

2) anyPolicy (2.5.29.32.0). The anyPolicy Policy OID MUST NOT be included if the Subordinate CA is not controlled by the Root CA.

b. cRLDistributionPoints
This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.

c. authorityInformationAccess
This extension SHOULD be present and MUST NOT be marked critical. It SHOULD contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). It MAY contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

d. basicConstraints

This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.

e. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

f. extkeyUsage

The Extended Key Usage extension [RFC5280] MUST be present and MUST contain id-kp-BrandIndicatorforMessageIdentification (OID: 1.3.6.1.5.5.7.3.31) as specified in Section 7 of the IETF Internet-Draft at https://tools.ietf.org/html/draft-chuang-bimi-certificate-00. This indicates the application of the Verified Mark Certificate Profile. Other KeyPurposeIds MUST NOT be included. This extension SHOULD be marked non-critical.

7.1.2.3. Subscriber Certificate

a. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

Each Verified Mark Certificate issued by the CA to a Subscriber SHALL be identified by the presence of the following Verified Mark Certificate OIDs in the certificate's certificatePolicies extension that:

(i) indicate which CA policy statement relates to that Certificate,

(ii) assert the CA's adherence to and compliance with these VMC Requirements and assert the requirement of adherence to and compliance with the VMC Terms as a condition of issuance of the Verified Mark Certificate.

The first certificate policies value contains an identifier that names the CA's Certification Practice Statement (CPS) applicable to the Verified Mark Certificate, together with a URL for the web page where the Certification Practice Statement can be publicly reviewed. The CA CPS identifier is the Policy Identifier of the certificate policies extension. The CA CPS URL is appended as a CPS pointer qualifier.

The second certificate policies value contains a Verified Mark Certificate General Policy Identifier (1.3.6.1.4.1.53087.1.1) which indicates adherence to and compliance with these VMC Requirements and the VMC Terms. This identifier is assigned to the Policy Identifier of the certificate policies extension.

b. cRLDistributionPoints

This extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.

c. authorityInformationAccess

This extension SHOULD be present. It MUST NOT be marked critical, and it SHOULD contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).. It MAY contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

d. basicConstraints (optional)

The cA field MUST NOT be true.

e. keyUsage (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

f. extKeyUsage (required)
The Extended Key Usage extension [RFC5280] MUST contain id-kp-BrandIndicatorforMessageIdentification (OID: 1.3.6.1.5.5.7.3.31) as specified in Section 7 of the IETF Internet-Draft at https://tools.ietf.org/html/draft-chuang-bimi-certificate-00. This indicates the application of the Verified Mark Certificate Profile. Other KeyPurposeIds MUST NOT be included. This is REQUIRED, and the extension SHOULD be marked non-critical.

g. signedCertificateTimestampList (OID: 1.3.6.1.4.1.11129.2.4.2)
Verified Mark Certificates pre-certificates MUST be logged to at least one of well-known Certificate Transparency (CT) logs [RFC6962] which then provide Signed Certificate Timestamps (SCT). The SCT must be added to the Certificate Transparency extension as a SignedCertificateTimestampList encoded as an octet string [RFC6962 section 3.3]. The Authindicators Working Group maintains a list of acceptable CT logs, and the current list is attached as Appendix F. This is REQUIRED, and SHOULD NOT be marked critical.

h. logotype extension (OID: 1.3.6.1.5.5.7.1.12)
The extension MUST:

- contain subjectLogo with a LogotypeData element [RFC3709] containing the Mark Representation asserted by the Subject of the Verified Mark Certificate and verified by the CA.
- embed the image element in "data:" URL as defined in RFC6170 section 4.
- The Mark Representation MUST:
- embedded secured SVG image [RFC6170]
- use the SVG Tiny PS profile to secure the SVG
- be compressed
- follow other requirements set forth in [RFC6170 section 5.2]

The Mark Representation MUST NOT contain <script> tags. Additionally the Authindicators Working Group has published a SVG Tiny PS Guidelines document as well as a RNC tool to help validate the SVG. The VMC SVG is also required to follow those specifications. The logotype extension is REQUIRED, and SHOULD be marked non-critical. The CA SHALL verify that the Applicant provided Mark Representation meets this secure profile.

7.1.2.4. All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in section 7.1.2.1, 7.1.2.2, or 7.1.2.3 unless the CA is aware of a reason for including the data in the Certificate.

CAs SHALL NOT issue a Certificate with:

a. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
   i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
   ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

b. semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5. Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, SHALL not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under these Requirements.

7.1.3. Algorithm Object Identifiers

CAs MUST issue Certificates using only those algorithm identifiers listed in Section 6.1.5.

7.1.4. Name Forms

7.1.4.1. Issuer Information

The content of the Certificate Issuer Distinguished Name field MUST match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.4.2. Subject Information – Subscriber Certificates

By issuing the Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. CAs SHALL NOT include a Domain Name in a Subject attribute except as specified in Section 3.2.2.4 or Section 3.2.2.5.
Subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1. Subject Alternative Name Extension

Required

Contents: This extension MUST contain at least one entry. Each entry MUST be a dNSName containing the Fully-Qualified Domain Name. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or has been granted the right to use it by the Domain Name Registrant, as appropriate.

CAs SHALL NOT issue certificates with a subjectAlternativeName extension containing an Internal Name.

Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").

7.1.4.2.2. Subject Distinguished Name Fields

a. **Certificate Field**: subject:commonName (OID 2.5.4.3)

Required/Optional: Deprecated (Discouraged, but not prohibited)

Contents:

The contents MUST either be the same as the Subject Organization Name defined in section 7.1.4.4.2 (b), or the Word Mark field defined in section 7.1.4.4.2 (p).

b. **Certificate Field:** subject:organizationName (OID 2.5.4.10)

Required

Contents:

This field MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein. A CA MAY abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated" the CA MAY include "Company Name, Inc."

When abbreviating a Subject's full legal name as allowed by this subsection, the CA MUST use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration.
If the combination of names or the organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that the CA checks this field in accordance with section 3.2 and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the CA MUST NOT issue the Verified Mark Certificate.

c. **Certificate Field:** Number and street: subject:streetAddress (OID: 2.5.4.9)
Optional
Contents: The subject:streetAddress field MUST contain the Subject's street address information as verified under Section 3.2.

d. **Certificate Field:** subject:localityName (OID: 2.5.4.7)
Required if the subject:stateOrProvinceName field is absent.
Optional if the subject:stateOrProvinceName field is present.
Contents: If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 3.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 3.2.2.1.

e. **Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8)
Required if the subject:localityName field is absent.
Optional if the subject:localityName field is present.
Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 3.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 3.2.2.1.

f. **Certificate Field:** subject:postalCode (OID: 2.5.4.17)
Required, unless prohibited by applicable law or not applicable in the jurisdiction
Contents: The subject:postalCode field MUST contain the Subject's zip or postal information as verified under Section 3.2.2.1.

g. **Certificate Field:** subject:countryName (OID: 2.5.4.6))
Required
Contents: The subject:countryName MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1.. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

h. **Certificate Field:** subject:organizationalUnitName (OID: 2.5.4.11)
Optional
The Organizational Unit Name field specifies an organizational unit. It identifies an organizational unit with which the certificate is affiliated. The designated organizational unit is understood to be part of an organization designated by an organizationName field. The value for Organizational Unit Name is a string chosen by the organization of which it is part (e.g., OU = "Technology Division"). See ISO/IEC 9594-6:2014 (E) Rec. ITU-T X.520 (10/2012).

i. **Certificate Field**: subject:businessCategory (OID: 2.5.4.15)
Required

Contents: This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of Section 3.2.1 1, 2, 3, or 4 of these Requirements, respectively.

j. Certificate fields:

Locality (if required):
subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)

State or province (if required):
subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)

Country:
subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)

Required
Contents: These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

k. **Certificate field**: *Subject:serialNumber* (OID: 2.5.4.5)
Required
Contents: For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.
For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.

l. **Certificate Field:** *Subject:legalEntityIdentifier* **(**OID: 1.3.6.1.4.1.53087.1.5)
Optional:
Contents: Contains a 20-character alphanumeric LEI string from a valid registration. The validation process is as follows:
1) This information SHALL be validated by matching the organization name and registration number found in the Global LEI Index against the Subject Organization Name Field (see Verified Mark Requirements Section 7.1.4.4.2 (b)) and Subject Serial Number Field (see Verified Mark Requirements Section 71.4.4.2 (k)) within the context of the subject's jurisdiction as specified in Verified Mark Requirements Section 7.1.4.4.2 (j)) The address information from Verified Mark validation SHALL be compared to the Headquarters Address information in the LEI record in order to

detect potential matching errors or errors in the registration information. If the addresses do not match, the CA will attempt to validate the address found in the LEI record as a confirmed office location for the Subscriber, if possible.
3) The CA SHALL verify that the ValidationSources field of the associated LEI record contains the designation FULLY_CORROBORATED before including an LEI in a VMC.

m. **Certificate field:** *Subject:trademarkCountryOrRegionName* (OID: 1.3.6.1.4.1.53087.1.3)
Required
Contents: This string value identifies the country or region of the Trademark Office that registered the Registered Mark as an WIPO ST.3 two letter country and intergovernmental/regional agency code (see list at http://www.wipo.int/export/sites/www/standards/en/pdf/03-03-01.pdf). See Appendix C for a list of countries and regions currently authorized for Verified Mark Certificates and string value format.

n. **Certificate field:** *Subject:trademarkOfficeName* (OID: 1.3.6.1.4.1.53087.1.2)
Required if the applicable country/region has more than one national/regional intellectual property agency where trademarks can be registered; **optional** otherwise
Contents: This string value identifies the Trademark Office by inserting the URL listed in the "Web site" column in the WIPO directory of country and regional intellectual property agencies at https://www.wipo.int/directory/en/urls.jsp for the Trademark Office that registered the Registered Mark included in the Verified Mark Certificate. See Appendix C for a list of Trademark Offices currently authorized for Verified Mark Certificates and string value format.

o. **Certificate field:** *Subject:trademarkRegistration* (OID: 1.3.6.1.4.1.53087.1.4)
Required
Contents: This string value contains the registration number given by the Trademark Office to identify the Registered Mark. This field is REQUIRED.

p. **Certificate field:** *Subject:wordMark* (OID: 1.3.6.1.4.1.53087.1.6)
Optional
Contents: Contains a Word Mark or the word(s) included in a Combined Mark.

q. **Certificate field:** *Subject:organizationIdentifier* (OID: 2.5.4.97)
Optional
Contents: If present, this field MUST contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme.
The organizationIdentifier MUST be encoded as a PrintableString or UTF8String.
The Registration Scheme MUST be identified using the using the following structure in the presented order:

- 3 character Registration Scheme identifier;
- 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated, or if the scheme is operated globally ISO 3166 code "XG" SHALL be used;
- For the NTR Registration Scheme identifier, if required under Section 9.2.4, a 2 character ISO 3166-2 identifier for the subdivision (state or province) of the nation in which the Registration Scheme is operated, preceded by plus "+" (0x2B (ASCII), U+002B (UTF-8));
- a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
- Registration Reference allocated in accordance with the identified Registration Scheme

Note: Registration References MAY contain hyphens, but Registration Schemes, ISO 3166 country codes, and ISO 3166-2 identifiers do not. Therefore if more than one hyphen appears in the structure, the leftmost hyphen is a separator, and the remaining hyphens are part of the Registration Reference.
As in section 7.1.4.4.2 (j), the specified location information MUST match the scope of the registration being referenced.
Examples:

- NTRGB-12345678 (NTR scheme, Great Britain, Unique Identifier at Country level is 12345678)

- NTRUS+CA-12345678 (NTR Scheme, United States - California, Unique identifier at State level is 12345678)
- VATDE-123456789 (VAT Scheme, Germany, Unique Identifier at Country Level is 12345678)
- PSDBE-NBB-1234.567.890 (PSD Scheme, Belgium, NCA's identifier is NBB, Subject Unique Identifier assigned by the NCA is 1234.567.890)

Registration Schemes listed in Appendix J are currently recognized as valid under these guidelines.
The CA SHALL:

1. confirm that the organization represented by the Registration Reference is the same as the organization named in the organizationName field as specified in Section 7.1.4.4.2 (b) within the context of the subject's jurisdiction as specified in Section 7.1.4.4.2 (j);
2. further verify the Registration Reference matches other information verified in accordance with section 3.2;
3. take appropriate measures to disambiguate between different organizations as described in Appendix J for each Registration Scheme;
4. Apply the validation rules relevant to the Registration Scheme as specified in Appendix J.

r. Other Subject Attributes

Other attributes MAY be present within the subject field. If present, other attributes MUST contain information that has been verified by the CA.

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1. Subject Distinguished Name Fields

a. **Certificate Field:** subject:commonName (OID 2.5.4.3)

Required

Contents: This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

b. **Certificate Field:** subject:organizationName (OID 2.5.4.10)

Required

Contents: This field MUST be present and the contents MUST contain either the Subject CA's name as verified under Section 3.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".

c. **Certificate Field:** subject:countryName (OID: 2.5.4.6)

Required

Contents: This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

7.1.5. Name Constraints

CAs MUST NOT include the nameConstraints extension in Certificates.

7.1.6. Certificate Policy Object Identifier

7.1.6.1. Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.2. Subordinate CA Certificates

As specified in 7.1.2.2 (a).

7.1.6.3. Subscriber Certificates

As specified in 7.1.2.3 (a).

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

7.2.1. Version number(s)

No stipulation.

7.2.2. CRL and CRL entry extensions

No stipulation.

7.3. OCSP PROFILE

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The CA's audit SHALL be performed by a Qualified Practitioner. A Qualified Practitioner means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. Qualified Practitioner enrolled in the WebTrust program;
5. Bound by law, government regulation, or professional code of ethics; and
6. Maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

No stipulation.

8.4. TOPICS COVERED BY ASSESSMENT

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. "WebTrust for CAs v 2.0 or newer" AND "WebTrust Principles and Criteria for Certification Authorities – Verified Mark Certificates"

The audit scheme MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Practitioner, as specified in Section 8.2.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

No stipulation.

8.6. COMMUNICATION OF RESULTS

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert the VMC policy identifier OID (1.3.6.1.4.1.53087.1.1). The CA SHALL make the Audit Report publicly available. The CA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. The CA SHOULD make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA SHALL provide an explanatory letter signed by the Qualified Practitioner.

8.7. SELF-AUDITS

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate issuance or renewal fees

No stipulation.

9.1.2. Certificate access fees

No stipulation.

9.1.3. Revocation or status information access fees

No stipulation.

9.1.4. Fees for other services

No stipulation.

9.1.5. Refund policy

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance coverage

No stipulation.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of confidential information

No stipulation.

9.3.2. Information not within the scope of confidential information

No stipulation.

9.3.3. Responsibility to protect confidential information

No stipulation.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy plan

No stipulation.

9.4.2. Information treated as private

No stipulation.

9.4.3. Information not deemed private

No stipulation.

9.4.4. Responsibility to protect private information

No stipulation.

9.4.5. Notice and consent to use private information

No stipulation.

9.4.6. Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7. Other information disclosure circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

No stipulation.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
2. **Authorization for Certificate:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
3. **Accuracy of Information:** That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (ii) followed the procedure

when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;

4. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
5. **Subscriber Agreement:** That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. **Status:** That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
7. **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

9.6.2. RA Representations and Warranties

No stipulation.

9.6.3. Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.
Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's acknowledgement of the Terms of Use.

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
3. **Use of Certificate:** An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
4. **Reporting and Revocation:** An obligation and warranty to promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

5. **Responsiveness:** An obligation to respond to the CA's instructions concerning Certificate misuse within a specified time period.
6. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4. Relying Party Representations and Warranties

No stipulation.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

No stipulation.

9.8. LIMITATIONS OF LIABILITY

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY limit liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and/or Certification Practice Statement, pursuant to the minimum liability requirement below. If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires. 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, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement, pursuant to the minimum liability requirement below.

The CA MAY NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per Verified Mark Certificate.

9.9. INDEMNITIES

9.9.1. Indemnification by CAs

No stipulation.

9.9.2. Indemnification by Subscribers

No stipulation.

9.9.3. Indemnification by Relying Parties

No stipulation.

9.10. TERM AND TERMINATION

9.10.1. Term

No stipulation.

9.10.2. Termination

No stipulation.

9.10.3. Effect of termination and survival

No stipulation.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12. AMENDMENTS

9.12.1. Procedure for amendment

No stipulation.

9.12.2. Notification mechanism and period

No stipulation.

9.12.3. Circumstances under which OID must be changed

No stipulation.

9.13. DISPUTE RESOLUTION PROVISIONS

No stipulation.

9.14. GOVERNING LAW

No stipulation.

9.15. COMPLIANCE WITH APPLICABLE LAW

No stipulation.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section

9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the Authindicators Working Group of the relevant information newly added to its CPS by sending a message to the Authindicators Working Group and receiving confirmation that it has been received, so that the Authindicators Working Group may consider possible revisions to these Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the Authindicators Working Group, as outlined above, MUST be made within 90 days.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5. Force Majeure

No stipulation.

9.17. OTHER PROVISIONS

No stipulation.

APPENDIX A – DNS CONTACT PROPERTIES

These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.

A.1. CAA Methods

A.1.1. CAA contactemail Property

SYNTAX: contactemail <utf8emailaddress>

The CAA contactemail property takes an email address as its parameter. The entire parameter value MUST be a valid email address as defined in section 3.4 of RFC 5322 and extended by section 3.2 of RFC 6532, with no additional padding or structure, or it cannot be used.

The following is an example where the holder of the domain specified the contact property using an email address.

$ORIGIN example.com.

CAA 0 contactemail "domainowner@example.com"

The contactemail property MAY be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

A.1.2. CAA contactphone Property

SYNTAX: contactphone <rfc3966 Global Number>

The CAA contactphone property takes a phone number as its parameter. The entire parameter value MUST be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used. Global Numbers MUST have a preceding + and a country code and MAY contain visual separators.

The following is an example where the holder of the domain specified the contact property using a phone number.

$ORIGIN example.com.

CAA 0 contactphone "+1 (555) 123-4567"

The contactphone property MAY be critical if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

A.2. DNS TXT Methods

A.2.1. DNS TXT Record Email Contact

The DNS TXT record MUST be placed on the _validation-contactemail subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid email address as defined in section 3.4 of RFC 5322 and extended by section 3.2 of RFC 6532, with no additional padding or structure, or it cannot be used.

A.2.2. DNS TXT Record Phone Contact

The DNS TXT record MUST be placed on the _validation-contactphone subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid Global Number as defined in RFC 3966 section 5.1.4, or it cannot be used.

APPENDIX B – MAPPING OF COMBINED, DESIGN, AND WORD MARK TERMINOLOGY TO TERMINOLOGY OF AUTHORIZED TRADEMARK OFFICES

Country/ Region	Combined Mark	Design Mark	Word Mark
United States (US)[1]	Marks comprising words plus a design are coded as **Mark Drawing Code 3 - Design Plus Words, Letters, and/or Numbers** Marks comprising stylized letters and/or numerals with no design feature are coded as **Mark Drawing Code 5**	Special Form Drawings. Marks comprising only a design are coded as **Mark Drawing Code 2 - Design Only**	Standard Character Drawings - Marks comprising words, letters, numbers, or any combination thereof without claim to any particular font style, size, or color are coded as **Mark Drawing Code 4 - Standard Character Mark**. [Prior to November 2, 2003, typed drawings (*see* TMEP §807.03(i)) these were coded as **Mark Drawing Code 1**]
Canada (CA)[2]	**Composite Mark**	**Design Mark**	**Standard Character Trademark**
European Union (EM)[3]	Type: **Figurative mark containing word elements** - A figurative mark consisting of a combination of verbal and figurative elements	Type: **Figurative mark** - It is a trade mark where non-standard characters, stylisation or layout, or a graphic feature or a colour are used, including marks that consist exclusively of figurative elements	Type: **Word mark** - A word mark consists exclusively of words or letters, numerals, other standard typographic characters or a combination thereof that can be typed
United Kingdom (GB)[4]	**Logo Mark**[5] (Image)	**Logo Mark** (Image)	**Word Mark**[6]
Germany (DE)[7]	Combined word and figurative mark (Wort-	Figurative Mark (Bildmarke) - are pictures,	Word Mark (Wortmarke) - are trade marks that

[1] https://tmep.uspto.gov/RDMS/TMEP/current#/current/TMEP-800d1e2068.html
http://www.lo101.com/mdc.html
[2] https://trademark.witmart.com/canada/registration
[3] https://euipo.europa.eu/ohimportal/en/trade-mark-definition
[4] https://www.trademarkdirect.co.uk/blog/word-marks-logo-marks
[5] See https://trademarks.ipo.gov.uk/ipo-tmcase/page/Results/1/UK00002192618 for Burger King combined mark registration in the UK. The search drop down field on the site uses the term "design". The registration does not appear to call out the words in the combined mark, so MVAs must extract the words to insert in the VMC Sec. 4.5.2.4.4 Word Mark field.
[6] See https://trademarks.ipo.gov.uk/ipo-tmcase/page/Results/1/UK00001351798 for word mark registration for Burger King. The search drop down field on the site uses the term "word". The registration does not appear to call out the words in the combined mark, so MVAs must extract the words to insert in the VMC Sec. 4.5.2.4.4 Word Mark field. Note that UK trademark registration for word marks allows "series" of the same word mark to be listed in a single registration (where words are arranged in different configurations – linear, stacked – but always read the same way to a consumer).
[7] English definition from glossary in:
https://www.dpma.de/docs/dpma/veroeffentlichungen/broschueren/200129_bromarken_engl_nichtbarr.ar

	Bildmarke) - Combined word/figurative marks consist of a combination of word elements and graphical elements, or of words in lettering styles.	graphical elements or images (without words or word elements).	consist of words, letters, numbers or other characters that are part of the standard set of characters used by the Deutsches Patent und Markenamt (DPMA).
Japan (JP)[8]	Combined (結合商標)	Symbol (**記号商標**) Figurative / Graphic Trademark (**図形商標**) Combined (結合商標)	Word Only (**文字商標**)
Australia (AU)	**Figurative Mark**[9]	**Figurative Mark**[10]	**Word Mark**[11]
Spain (ES)[12]	Device Mark	Device Mark	Word Mark

m.pdf English/German mapping is by looking at the "550 Markenform" (German version) of : https://register.dpma.de/register/htdocs/prod/en/hilfe/recherchefelder/marken/index.html and using the language translator tool to map to English. See also section "What is the difference between a word mark and a combined word/figurative mark or figurative mark?" in https://www.dpma.de/english/trade_marks/faq/index.html

[8] https://www.globalipdb.inpit.go.jp/jpowp/wp-content/uploads/2018/11/170c54c04df539b80e52f33800a1e643.pdf and https://www.jetro.go.jp/ext_images/world/asia/sg/ip/pdf/search_ip_communique2016.pdf Also https://elaws.e-gov.go.jp/document?lawid=334AC0000000127

[9] See https://search.ipaustralia.gov.au/trademarks/search/view/381026?s=9f1d9c31-769b-4472-a055-e8c636007f26 Note that registration shows "AMERICAN STANDARD IDEAL STANDARD" for "Words" field.

[10] See https://search.ipaustralia.gov.au/trademarks/search/view/373483?s=9f1d9c31-769b-4472-a055-e8c636007f26 for Delta triangle figurative mark registration. Note that registration shows "A" for "Words" field (unclear – a placeholder?).

[11] See https://search.ipaustralia.gov.au/trademarks/search/view/723899?s=6f75163b-7cac-44f6-9784-7cf7496ceec0. Note that registration shows "BURGER KING" for "Words" field

[12] https://companiesinn.com/articles/different-types-trademark

APPENDIX C – AUTHORIZED TRADEMARK OFFICES FOR VMCS

Trademark Offices Authorized for Verified Mark Certificates	String Value for Trademark Country or Region Name Under Sec. 7.1.4.4.2 (m)	String Value for Trademark Office Name Under Sec. 7.1.4.4.2 (n)
United States - United States Patent and Trademark Office	US	https://www.uspto.gov/
Canada - Canadian Intellectual Property Office	CA	http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr00002.html
European Union - European Union Intellectual Property Office	EM	https://euipo.europa.eu/ohimportal/en
United Kingdom - UK Intellectual Property Office	GB	https://www.gov.uk/search-for-trademark
Germany - Deutsches Patent- und Markenamt	DE	https://www.dpma.de/
Japan Trademark Office	JP	https://www.jpo.go.jp/
Australia - IP Australia	AU	https://www.ipaustralia.gov.au/
Spain – Oficina Española de Patentes y Marcas	ES	https://www.oepm.es/es/index.html

APPENDIX D - VMC TERMS OF USE ("VMC TERMS")

All Mark Asserting Entities (MAEs) are required, as a condition of being issued a Verified Mark Certificate, to agree to these VMC Terms. Any and all use, display, or reliance on any Verified Mark Certificate (and any Mark Representation and any other data or information therein) by Consuming Entities, Relying Parties, and any other person, is subject to and conditional upon acceptance of these VMC Terms. The OID 1.3.6.1.4.1.53087.1.1 in the Verified Mark Certificate incorporates by reference these VMC Terms. If any person does not agree to these VMC Terms, such person may not obtain, use, publish, or rely upon any Verified Mark Certificate or on any Mark Representation or any other data or information in a Verified Mark Certificate.

1. Definitions. In addition to the other definitions included in the Baseline Requirements, Verified Mark Requirements, and VMC Requirements, the following capitalized words will have the meanings set out below.
   1.1. Mark Asserting Entity (MAE): An Applicant for/Subscriber of a Verified Mark Certificate.
   1.2. VMC Marks: the Mark Representation and Word Mark, if any, contained in a MAE's Verified Mark Certificate application.

2. Limited Right to Reproduce and Display. The MAE hereby grants, subject to the terms, conditions and restrictions in the VMC Requirements and these VMC Terms:
   2.1. to the Issuing CA, a limited, non-exclusive, worldwide license to issue a Verified Mark Certificate that contains the VMC Marks and to log said certificate in a limited number of Certificate Transparency Logs as required by the VMC Requirements; and
   2.2. to Consuming Entities, a limited, non-exclusive, worldwide license to use the VMC Marks in conjunction with internal logo recognition systems, and to host, store, reproduce, display, process, and modify as permitted by section 3.1 the VMC Marks only in direct visual association with communications, correspondence, or services authored or provided by the MAE from or through one of the same domains included within the Verified Mark Certificate's Subject Alternative Name field; and
   2.3. to certificate transparency log operators if different from the Issuing CA, a limited, non-exclusive, worldwide license to retain a copy of and to reproduce the Verified Mark Certificate to support a durable public record of those issued certificates, and for the purpose of permitting members of the public to audit the verification of Verified Mark Certificates.

   No other license is granted to any other party, or for any other use.

3. License Restrictions and Conditions. Any Consuming Entity that incorporates or intends to incorporate the VMC Marks obtained through an issued and published Verified Mark Certificate into its products and services, agrees that its license to do so is subject to and conditional on the following:
   3.1. Quality Control, Same Treatment. The Consuming Entity may not distort at display time any Mark Representation obtained from a published Verified Mark Certificate, change its colors or background, modify its transparency, or alter it in any way other than to adjust its size or scale, or to crop it in a manner consistent with cropping performed on other Mark Representations displayed in the same context. If a Consuming Entity displays a Word Mark obtained from a published Verified Mark Certificate, it must do so in a neutral manner applied consistently to all Word Marks from all Verified Mark Certificates that are shown in the same visual context. The Consuming Entity may display a Mark included in a Verified Mark Certificate without also displaying a Word Mark included in the same Verified Mark Certificate, but the Consuming Entity may not display a Word Mark included in a Verified Mark Certificate without also displaying the Mark included in the same Verified Mark Certificate.
   3.2. No Partnership or Relationships implied. Subject to an express agreement to the contrary between the Consuming Entity and the MAE, neither the VMC Marks nor any other content of the Verified Mark Certificate may be used or displayed in any way that reasonably implies any relationship between the Consuming Entity and the MAE, beyond the bare licensor-licensee relationship created by these VMC Terms.

3.3. CRL or OCSP Checks. Consuming Entities must check the Certificate Revocation Lists maintained by the CA or perform an on-line revocation status check using OCSP to determine whether a Verified Mark Certificate has been revoked no less frequently than every 7 days.
3.4. Lawful Use. Consuming Entities may only use the Mark Representation in a Verified Mark Certificate in accordance with applicable law.

4. Sufficient Ownership or License. The MAE warrants that the VMC Marks published via a Verified Mark Certificate represent a Registered Mark (and Word Mark, if any) that the MAE owns or for which the MAE has obtained sufficient license to be able to grant the limited license in these VMC Terms, and that it will immediately revoke the Verified Mark Certificate if it no longer owns or has a sufficient license to the applicable Registered Mark (or Word Mark, if any). The MAE will defend and will be liable for any intellectual property or other claims against any Consuming Entity, Relying Party or CA that arise from the content of the MAE's application for a Verified Mark Certificate.

5. No obligation to display. The MAE acknowledges that Consuming Entities are under no obligation to display the VMC Marks in connection with content the MAE publishes that is associated with the domains the MAE owns or controls as a Domain Registrant, even if a communication or message is confirmed to be from the MAE and a suitable VMC Mark can be obtained and safely displayed from the applicable Verified Mark Certificate. Instead, Consuming Entities may choose to display the VMC Marks in accordance with these VMC Terms, or not display them, at their option.

6. Termination. Immediately upon revocation or expiration of the Verified Mark Certificate, the MAE will cease publishing or using the Verified Mark Certificate, and the license granted to Consuming Entities in Section 2.2 above SHALL terminate. The license to a Consuming Entity in Section 2.2 above also terminates automatically and immediately upon breach of any provision of these VMC Terms by the Consuming Entity. Consuming Entities must immediately cease any and all use of the VMC Marks upon termination of the applicable license.

7. Updates to VMC Requirements and VMC Terms. The VMC Requirements and VMC Terms may be updated from time to time. All parties agree that the version of the VMC Requirements and VMC Terms in effect at the time of issuance of a Verified Mark Certificate SHALL apply through the date of expiration or revocation of the Verified Mark Certificate (and, for those provisions that by their nature extend beyond the date of expiration or revocation, until the provisions no longer would apply by their terms). It is the responsibility of each entity who obtains, uses, publishes or relies upon a Verified Mark Certificate to review and familiarize itself from time to time with any updated versions of the VMC Requirements and VMC Terms.

APPENDIX E - OPTIONAL RULES FOR MATCHING MARK REPRESENTATION SUBMITTED BY SUBSCRIBER WITH REGISTERED MARK VERIFIED BY CA

These are optional rules approved by the Authindicators which CAs MAY use when matching the Mark Representation submitted by the Subscriber with the Registered Mark verified by the CA.

Trademarks registered in the United States

[This Appendix is still being drafted.]

APPENDIX F - CT LOGS APPROVED BY AUTHINDICATORS WORKING GROUP

Log URL	Name
https://gorgon.ct.digicert.com/log	Gorgon

APPENDIX G – ADDITIONAL F2F VERIFICATION REQUIREMENTS

Section 1 – Notarization of Document Signed by Contract Signer or Certificate Approver

The Contract Signer or Certificate Approver for the Verified Mark Certificate must perform Notarization procedure for the Applicant as defined below. If the Contract Signer and Certificate Approver roles are fulfilled by different natural persons, then only one of Contract Signer or Certificate Approver must perform the procedure below. In all cases, the natural person performing the Notarization is referred to as the "Designated Individual" in the procedure defined below.

1. Receive information from the Designated Individual. The CA will ask the Designated Individual to submit the following information: name, title, organization (Applicant) name, email address, and telephone number for use in the Notarization process and the web-based F2F process described in Sections 2 and 3 below.

2. Conduct Notarization Process. The CA will arrange for a Notary to meet with the Designated Individual. The Notary MUST NOT be an employee of the Subscriber or a member of any law firm used by the Subscriber. The Notarization process MAY be performed by Remote Notarization, provided that it is conducted in accordance with applicable law in the Notary's jurisdiction. The Designated Individual MUST be located in a jurisdiction in which the Notary is permitted to Notarize according to applicable law.

   The CA will provide the Notary in advance with a Verification Document for the Designated Individual to sign before the Notary and be Notarized. The notary should be instructed to confirm the Designated Individual's face conforms to the photo on the Designated Individual's photo ID, and that the name of the Designated Individual listed on the photo ID conforms to the Designated Individual name on the Verification Document. The Notary must observe the Designated Individual as he or she signs the Verification Document, then Notarize the Verification Document, The Notary should record any required details of the Notarization process in the Notary's notary journal (or equivalent) as normally required in the jurisdiction for a Notarization. Digital signatures may be used if accepted in the jurisdiction.

   The Notary must then either: (1) Send a photo or PDF copy of the Notarized Verification Document to the CA according to the CA's instructions and give the original document to the Designated Individual for his or her files or destruction, or (2) send the original signed Verification Document to the CA. The Notary should not retain a copy of the Verification Document or the Designated Individual's photo ID in the Notary's own files unless required to do so by applicable law or regulation in the jurisdiction, in which case the Notary should treat the document and photo ID as PII to be archived and disposed of in a secure manner and in accordance with any applicable law or regulation.

3. Conduct web-based F2F session with Designated Individual. The CA or its third party agent will also perform a web-based recorded or photographed session with the Designated Individual. This form of validation must include the following basic steps:

   (a) The CA or agent initiates a live, recorded video conference with Designated Individual. The recording can either be saved by the CA, or appropriate screen shots of the conference can be saved by the CA instead.
   (b) The Designated Individual recites on the video conference his or her basic information, including name, address, organization, title, telephone number, ID type (passport national ID, driver's license, etc.), and ID number that will be used during the validation session.
   (c) The CA or agent asks the Designated Individual to present his or her ID document to the camera, close enough to provide a clear picture of the front, back, and any other pages as may be necessary to read and examine the document and capture it on the video and/or screen shots. The CA or agent is not expected to determine whether or not the ID document is genuine, only to record what was

presented. CA agent may reject the ID document in its discretion if appropriate (e.g., expired, name mis-match, photo mis-match).

(d) The CA or agent asks the Designated Individual to hold ID in front of his or her face, to turn the document around in that position, and to wave his or her other hand in the space between the ID and the Designated Individual's face. The CA must make reasonable accommodations if necessary in case the Designated Individual has a relevant physical disability. The CA or agent may ask additional questions at his or her discretion.

(e) The video conference is completed. The CA or agent then approves or fails the ID verification request based on the procedure and securely archives the recording.

The CA may use a competent third party service provider trusted by the CA to perform this recorded or photographed web-based session with Designated Individual so long as the CA obtains and retains the recorded session and/or screen shots in the validation file.

Other provisions.

If the CA is unable to perform any of these F2F validation steps, the CA will notify the AuthIndicators group but will not issue the VMC until the CA and AuthIndicators either agree to waive the step or agree on additional or alternate F2F validation steps as a substitute.

Section 2 – PII and Privacy Requirements

VMC Designated Individual PII & Privacy Processes

The issuance of a VMC requires the issuing CA to validate the following information:

- The applying organization's ownership of their business domain
- The applying organization's ownership of the logo to be used
- The Designated Individual's connection to the organization
- The Designated Individual's identity

Due to the novel nature of validating the identity of the Designated Individual in-person, which is performed through a meeting with a notary or equivalent, additional information that is not typically collected for certificate issuance is required. As such, measures to protect Designated Individual personally identifiable information must be exercised.

Initial Designated Individual Guidance

1. **Before** an applicant begins the VMC application process, each CA should:
    - Set expectations and prepare the Designated Individual by providing a shortlist of items needed for the VMC application and a brief explanation of the Notarization process and required personal documents and information:
        - Description of the Notarization process that will be followed and PII details to be collected, including types of government-issued ID that will be accepted.

      (Not related to PII:)
        - The requirements that the Subscriber have a registered trademark, and which trademark jurisdictions are authorized.
        - The requirement of DMARC at enforcement on the organizational domain.
        - Specifications for the SVG Tiny PS logo that must be submitted by the Subscriber.
    - Provide links to the CA's official privacy policies

2. **During** the application process, each CA must ensure:

- Designated Individual PII is collected via **secure portal or safe file share site**. This will also include typical account set-up. PII such as name, title, phone, and email address for Designated Individuals information.

CA PII Retention Transparency Guidance

- Where PII is collected, the CA must include links to or information about the following:
    - Summary of the collection, use, storage, and destruction of information as it applies to the application and process; point to relevant standards
        - Explanation and reasoning for collection of required information by the CA (and, if applicable, by the notary)
            - Context as to the relative normalcy of this (e.g. for standard notarization process, SSL certs or home loans etc.)
            - Include CA's official privacy policies

3. **Guidance on PII sent to Notary**
    - For the in-person meeting the Designated Individual should provide only the below fields to the CA. The collection of additional, personally identifiable information is not required or recommended.
        - Name
        - Title
        - Organization
        - Email address
        - Meeting location, date, time
        - Cell phone number *(for the purposes of coordinating the meeting between the Designated Individual and notary)*

4. **Guidance on Designated Individual PII Treatment by Notary**
    - The Notary must maintain limited Designated Individual PII, as noted in the required fields of Item 3, including data entries in a Notary Journal that the Notary must retain by law or practice (or similar record that a Latin Notary, lawyer, or solicitor must retain).
    - The CA should provide the Designated Individual with information about the in-person meeting and document(s) that will be presented for signature(s).
        - The CA should provide the Designated Individual the lifecycle details of the signed documents or PII retained by the Notary.

APPENDIX H - COUNTRY-SPECIFIC INTERPRETATIVE GUIDELINES (NORMATIVE)

NOTE: This appendix provides alternative interpretations of the VMC Requirements for countries that have a language, cultural, technical, or legal reason for deviating from a strict interpretation of these Requirements. More specific information for particular countries may be added to this appendix in the future.

1. Organization Names

(1) Non-Latin Organization Name

Where an Verified Mark Applicant's organization name is not registered with a QGIS in *Latin* characters and the Applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Requirements, a CA MAY include a Latin character organization name in the Verified Mark Certificate. In such a case, the CA MUST follow the procedures laid down in this section.

(2) Romanized Names

In order to include a transliteration/Romanization of the registered name, the Romanization MUST be verified by the CA using a system officially recognized by the Government in the Applicant's Jurisdiction of Incorporation.

If the CA can not rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's Jurisdiction of Incorporation, then it MUST rely on one of the options below, in order of preference:

(A) A system recognized by the International Organization for Standardization (ISO);
(B) A system recognized by the United Nations; or
(C) A Lawyer's Opinion or Accountant's Letter confirming the proper Romanization of the registered name.

(3) Translated Name

In order to include a Latin character name in the Verified Mark certificate that is not a direct Romanization of the registered name (e.g. an English Name) the CA MUST verify that the Latin character name is:

(A) Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration; or
(B) Recognized by a QTIS in the Applicant's Jurisdiction of Incorporation as the Applicant's recognized name for tax filings; or
(C) Confirmed with a QIIS to be the name associated with the registered organization; or
(D) Confirmed by a Verified Legal Opinion or Accountant's Letter to be a translated trading name associated with the registered organization.

<u>Country-Specific Procedures</u>

D-1. Japan

As interpretation of the procedures set out above:

1. Organization Names

(A) The Revised Hepburn method of Romanization, as well as Kunrei-shiki and Nihon-shiki methods described in ISO 3602, are acceptable for Japanese Romanizations.
(B) The CA MAY verify the Romanized transliteration, language translation (e.g. English name), or other recognized Roman-letter substitute of the Applicant's formal legal name with either a QIIS, Verified Legal Opinion, or Verified Accountant Letter.
(C) The CA MAY use the Financial Services Agency to verify a Romanized, translated, or other recognized Roman-letter substitute name. When used, the CA MUST verify that the translated English is recorded in the audited Financial Statements.
(D) When relying on Articles of Incorporation to verify a Romanized, translated, or other recognized Roman-letter substitute name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a Verified Legal Opinion or a Verified Accountant Letter. The CA MUST verify the authenticity of the Corporate Stamp.
(E) A Romanized, translated, or other recognized Roman-lettered substitute name confirmed in accordance with this Appendix H-1 stored in the ROBINS database operated by JIPDEC MAY be relied

upon by a CA for determining the allowed organization name during any issuance or renewal process of an Verified Mark Certificate without the need to re-perform the above procedures.

2. Accounting Practitioner

In Japan:

(A) Accounting Practitioner includes either a certified public accountant (公認会計士 - Konin-kaikei-shi) or a licensed tax accountant (税理士 – Zei-ri-shi).

(B) The CA MUST verify the professional status of the Accounting Practitioner through direct contact with the relevant local member association that is affiliated with either the Japanese Institute of Certified Public Accountants (http://www.hp.jicpa.or.jp), the Japan Federation of Certified Tax Accountant's Associations (http://www.nichizeiren.or.jp), or any other authoritative source recognized by the Japanese Ministry of Finance (http://www.mof.go.jp) as providing the current registration status of such professionals.

3. Legal Practitioner

In Japan:

(A) Legal Practitioner includes any of the following:
a licensed lawyer (弁護士 - Ben-go-shi),
a judicial scrivener (司法書士 - Shiho-sho-shi lawyer), an administrative solicitor (行政書士 - Gyosei-sho-shi Lawyer), or a notary public (公証人 - Ko-sho-nin).
For purposes of these Requirements, a Japanese Notary Public is considered equivalent to a Latin Notary.

(B) The CA MUST verify the professional status of the Legal Practitioner by direct contact through the relevant local member association that is affiliated with one of the following national associations:
the Japan Federation of Bar Associations (http://www.nichibenren.or.jp),
the Japan Federation of Shiho-Shoshi Lawyer's Associations (http://www.shiho-shoshi.or.jp),
the Japan Federation of Administrative Solicitors (http://www.gyosei.or.jp),
the Japan National Notaries Association (http://www.koshonin.gr.jp), or
any other authoritative source recognized by the Japanese Ministry of Justice (http://www.moj.go.jp) as providing the current registration status of such professionals.

APPENDIX I – ABSTRACT SYNTAX NOTATION ONE MODULE FOR EV CERTIFICATES

The definition of these attributes is identical to those included in EV Certificates and are included in Verified Mark Certificates.

```
CABFSelectedAttributeTypes {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
module(4) cabfSelectedAttributeTypes(1) 1}
DEFINITIONS ::=
BEGIN
-- EXPORTS All
IMPORTS
  -- from Rec. ITU-T X.501 | ISO/IEC 9594-2
  selectedAttributeTypes, ID, ldap-enterprise
    FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 7}

  -- from the X.500 series
  ub-locality-name, ub-state-name
    FROM UpperBounds {joint-iso-itu-t ds(5) module(1) upperBounds(10) 7}

  -- from Rec. ITU-T X.520 | ISO/IEC 9594-6
  DirectoryString{}, CountryName
    FROM SelectedAttributeTypes selectedAttributeTypes;

id-evat-jurisdiction ID ::= {ldap-enterprise 311 ev(60) 2 1}
id-evat-jurisdiction-localityName ID ::= {id-evat-jurisdiction 1}
id-evat-jurisdiction-stateOrProvinceName ID ::= {id-evat-jurisdiction 2}
id-evat-jurisdiction-countryName ID ::= {id-evat-jurisdiction 3}

jurisdictionLocalityName ATTRIBUTE ::= {
  SUBTYPE OF            name
  WITH SYNTAX           DirectoryString{ub-locality-name}
  LDAP-SYNTAX           directoryString.&id
  LDAP-NAME             {"jurisdictionL"}
  ID                    id-evat-jurisdiction-localityName }

jurisdictionStateOrProvinceName ATTRIBUTE ::= {
  SUBTYPE OF            name
  WITH SYNTAX           DirectoryString{ub-state-name}
  LDAP-SYNTAX           directoryString.&id
  LDAP-NAME             {"jurisdictionST"}
  ID                    id-evat-jurisdiction-stateOrProvinceName }
jurisdictionCountryName ATTRIBUTE ::= {
  SUBTYPE OF            name
  WITH SYNTAX           CountryName
  SINGLE VALUE          TRUE
  LDAP-SYNTAX           countryString.&id
  LDAP-NAME             {"jurisdictionC"}
  ID                    id-evat-jurisdiction-countryName }

END
```

APPENDIX J – REGISTRATION SCHEMES

The following Registration Schemes are currently recognized as valid under these Requirements:
NTR: The information carried in this field SHALL be the same as held in Subject Serial Number Field as specified in 7.1.4.4.2 (k) and the country code used in the Registration Scheme identifier SHALL match that of the subject's jurisdiction as specified in Section 7.1.4.4.2 (j).
Where the Subject Jurisdiction of Incorporation or Registration Field in 7.1.4.4.2 (j)includes more than the country code, the additional locality information SHALL be included as specified in section in 7.1.4.4.2 (j).
VAT: Reference allocated by the national tax authorities to a Legal Entity. This information SHALL be validated using information provided by the national tax authority against the organization as identified by the Subject Organization Name Field (see 7.1.4.4.2 (b)) and Subject Serial Number Field (see 7.1.4.4.2 (k)) within the context of the subject's jurisdiction as specified in Section 7.1.4.4.2 (j).
PSD: Authorization number as specified in ETSI TS 119 495 clause 4.4 allocated to a payment service provider and containing the information as specified in ETSI TS 119 495 clause 5.2.1. This information SHALL be obtained directly from the national competent authority register for payment services or from an information source approved by a government agency, regulatory body, or legislation for this purpose. This information SHALL be validated by being matched directly or indirectly (for example, by matching a globally unique registration number) against the organization as identified by the Subject Organization Name Field (see 7.1.4.4.2 (b)) and Subject Serial Number Field (see 7.1.4.4.2 (k)) within the context of the subject's jurisdiction as specified in Section 7.1.4.4.2 (j). The stated address of the organization combined with the organization name SHALL NOT be the only information used to disambiguate the organization.