# David Miller Trust Services

# Certification Practices Statement

pki.davidmiller.top

## TABLE OF CONTENTS

# 1. INTRODUCTION

## *1.1. OVERVIEW*

This document is the David Miller Trust Services ("DMTS") Certification Practices Statement (CPS) that outlines the principles and practices related to DMTS's certification and time-stamping services. This CPS applies to all entities participating in or using DMTS's certificate and time-stamping services, excluding participants in DMTS's Private PKI services, which are not cross-certified or publicly trusted. This CPS only addresses the actions of DMTS and not those of third parties operating with cross certificates issued by DMTS. Specific requirements regarding those Certificates are set forth in the individual agreements with the appropriate DMTS customer and in that third party's own CPS.

This CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

| **Name of Policy/Guideline/ Requirement Standard** | **Location of Source Document/Language** |
|---|---|
| DMTS Certificate Policy | https://cps.davidmiller.top/ |
| The Adobe Approved Trust List Technical Requirements | https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf |
| the Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") | https://cabforum.org/baseline-requirements-document/ |
| the CAB Forum Guidelines for Extended Validation Certificates ("EV Guidelines") | https://cabforum.org/extended-validation/ |
| the CAB Forum Guidelines for the Issuance and Management of Code Signing Certificates | https://cabforum.org/baseline-requirements-code-signing/ |
| the CAB Forum Network and Certificate System Security Requirements | https://cabforum.org/network-security-requirements/ |
| Microsoft Trusted Root Store (Program Requirements) | https://docs.microsoft.com/en-us/security/trusted-root/program-requirements |
| Mozilla Root Store Policy | https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/ |
| Mozilla CA/Forbidden or Problematic Practices | https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices |

| | |
|---|---|
| Apple Root Store Program | https://www.apple.com/certificateauthority/ca_program.html |
| 360 Browser CA Policy | https://caprogram.360.cn/#strategy |
| Wi-Fi Alliance Hotspot 2.0 Specification | https://www.wi-fi.org/discover-wi-fi/specifications |
| Chromium Project Root Store Certificate Policy | https://www.chromium.org/Home/chromium-security/root-ca-policy |

If any inconsistency exists between this CPS and the normative provisions of the foregoing policies, guidelines, and requirements ("Applicable Requirements"), then the Applicable Requirements take precedence over this CPS.

This CPS is only one of several documents that control DMTS's certification services. Other important documents include both private and public documents, such as the CP, DMTS's agreements with its customers, Relying Party agreements, and DMTS's privacy policy. DMTS may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine parts that cover the security controls and practices and procedures for certificate and time-stamping services within the DMTS PKI. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation."

## *1.2. DOCUMENT NAME AND IDENTIFICATION*

This document is the DMTS Certification Practices Statement and was first approved for publication on 9 August 2010 by the DMTS Policy Authority (DMPA). The OID arc for DMTS is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DMTS (114535).

OIDs found in Certificates reliant upon CAB Forum requirements and guidelines include the designated reserved policy identifiers in the Certificate Policy extension as of September 30, 2020 as specified in section 7.1.6 of the CA/B Baseline Requirements. Certificates issued before that date include other OIDs that are designated in section 7.1.6 of this document.

## *1.3. PKI PARTICIPANTS*

### 1.3.1. Certification Authorities

DMTS operates certification authorities (CAs) that issue digital certificates. As the operator of several CAs, DMTS performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking, rekeying, and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. General information about DMTS's products and services are available at www.davidmiller.top.

In limited circumstances, root CAs owned by DMTS are used to issue cross Certificates to external third parties operating their own PKIs. An external Issuer CA is an unaffiliated third party that is issued a subordinate CA Certificate by DMTS where the Private Key associated with that CA Certificate is not maintained under the physical control of DMTS.

All external subordinate CAs are prohibited, either technically or contractually, from issuing Certificates to domain names or IP addresses that a Subscriber does not legitimately own or control (i.e. issuance for purposes of "traffic management" is prohibited), and external subordinate CAs are required to implement procedures that are at least as restrictive as those found herein.

DMTS is also a time stamping authority (TSA) and provides proof-of-existence for data at an instant in time as described herein.

### 1.3.2. Registration Authorities and Other Delegated Third Parties

A Registration Authority is an entity that performs identification and authentication of certificate Applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of an Issuer CA on identity management systems (IdMs). DMTS and subordinate Issuer CAs may act as RAs for certificates they issue. Affiliates do not perform domain or IP address validation. Validation of domains for S/MIME Certificates cannot be delegated to a third party and is only validated by the RA of the Issuer CA.

Except for the authentication of domain control or IP address verification performed solely by DMTS in accordance with Section 3.2.2, DMTS may delegate the performance of certain functions to third party Registration Authorities (RA) if it meets the requirements of the DMTS CP and the relevant requirements listed in sections 1.1 and 1.6.3 of this CPS and the DMTS CP. The specific role of an RA or Delegated Third Party varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information. For IGTF Certificates, designated RAs are responsible for vetting the identity of each certificate applicant.

DMTS contractually obligates each Delegated Third Party to abide by the policies and industry standards that are applicable to that Delegated Third Party's delegated responsibilities. RA personnel involved in the issuance of publicly-trusted SSL/TLS Server Certificates must undergo the skills and training required under Section 5.3.

### 1.3.3. Subscribers

Subscribers use DMTS's services and PKI to support transactions and communications. Subscribers under this CPS include all end users (including entities) of certificates issued by an Issuer CA. A Subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an organization's employees. The *Subject* of a Certificate is the party named in the Certificate. A *Subscriber*, as used herein, may refer to the Subject of the Certificate and the entity that contracted with DMTS for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

CAs are technically also subscribers of certificates within the DMTS Public PKI, either as the primary Certificate Authority issuing a self- signed Certificate to itself, or as an Issuer CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CPS, however, apply only to end-user Subscribers.

### 1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by DMTS. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate. A Relying party may, or may not also be a Subscriber of the DMTS Public PKI hierarchy.

### 1.3.5. Other Participants

Other participants include Accreditation Authorities (such as Policy Management Authorities, Application Software Vendors, and applicable Community-of-Interest sponsors); Bridge CAs and CAs cross-certified with DMTS's CAs that serve as trust anchors in other PKI communities; and Time Source Entities, Time Stamp Token Requesters, and Time Stamp Verifiers involved in trusted time stamping.
Accreditation Authorities are granted an unlimited right to re-distribute DMTS's root Certificates and related information in connection with the accreditation.

## *1.4. CERTIFICATE USAGE*

A *digital Certificate* (or C*ertificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card. A *time-stamp token* (*TST*) cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by this CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non- verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. It is not the intent of this CPS to limit the types of usages for Organizational Certificates. An organizational certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by the DMTS CP, by any CPS (including this one) under which the certificate has been issued and any agreements with Subscribers.

### 1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate as specified by the requirements in section 1.1. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS.

This CPS covers several different types of end entity Certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

| Certificate | Appropriate Use |
|---|---|
| DV SSL/TLS Server Certificates | Used to secure online communication where the risks and consequences of data compromise are low, including non-monetary transactions or transactions with little risk of fraud or malicious access. |
| OV SSL/TLS Server Certificates | Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial. |
| EV SSL/TLS Server Certificates | Used to secure online communication where risks and consequences of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high. |
| Hotspot 2.0 OSU Server Certificates | Used to authenticate OSU Servers pursuant to the Wi-Fi Alliance's Hotspot 2.0 specification. |
| Code Signing Certificates, including EV Code Signing | Establishes the identity of the Subscriber named in the Certificate and that the signed code has not been modified since signing. |

| | |
|---|---|
| Rudimentary Level 1 Client Certificates – Personal | Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being signed. These Certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required. |
| Level 1 Client Certificates - Enterprise and Class 1 and 2 Certificates | Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious. |
| IGTF and Grid-only Certificates | Support identity assertions and system authentication amongst participants in the International Grid Trust Federation. IGTF Certificates include those issued as publicly-trusted client Certificates and those issued under the Grid-only arc. |
| Adobe Signing Certificates | Used to sign Adobe documents and show that the portion of the document signed by the author has not been modified since signing. |
| Time Stamp Token | Used to identify the existence of data at a set period of time. |

### 1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified in accordance with this CPS when the Certificate issued. Code signing Certificates do not indicate that the signed code is safe to install or free from malware, bugs, or vulnerabilities.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

CA Certificates subject to the Mozilla Root Store Policy will not be used for any functions except CA functions. In addition, end-user Subscriber Certificates cannot be used as CA Certificates.

Participants in the DMTS Public PKI periodically rekey Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. DMTS therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates.

DMTS strongly discourages key pinning and does not consider it a sufficient reason to delay revocation. DMTS continually researches and implements technological processes in order to detect pinned applications and other prohibited uses so we can counsel customers on the way pinning impacts the agility of the WebPKI (e.g., rotation of intermediate certificates). Customers should also take care in not mixing certificates trusted for the web with non-web PKI. Any certificates trusted by the browsers must comply with all requirements of all applicable browser root policies, including revocation periods of 24 hours and 5 days as asserted in the relevant policies, obligations, and requirements of the CP and this CPS.

## *1.5. POLICY ADMINISTRATION*

### 1.5.1. Organization Administering the Document

This CPS and the relevant documents referenced herein are maintained by the DCPA, which can be contacted at:

DMTS Policy Authority dmcert@outlook.com

### 1.5.2. Contact Person

Attn: Legal Counsel
DMTS Policy Authority
pki.davidmiller.top
dmcert@outlook.com

**Revocation Reporting Contact Person**

Attn: Support
DMTS Technical Support dmcert@outlook.com

For anyone listed in section 4.9.2 of this CPS and the CA/Browser Baseline Requirements that needs assistance with revocation or an investigative report, DMTS provides this page for reporting and submitting requests with all of the necessary information as outlined in section 4.9: https://pki.davidmiller.top/

If the problem reporting page is unavailable, there is a system outage, you have questions, or you believe our findings are incorrect please contact dmcert@outlook.com

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. DMTS or an RA will authenticate and log each revocation request according to Section 4.9 of the DMTS CP and this CPS. DMTS will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, DMTS or an RA will investigate the alleged basis for the revocation request prior to taking action in accordance with Section 4.9.1 and 4.9.3.

### 1.5.3. Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CPS based on the results and recommendations received from an independent auditor (see Section 8). The DCPA is also responsible for evaluating and acting upon the results of compliance audits.

### 1.5.4. CPS Approval Procedures

The DCPA approves the CPS and any amendments. Amendments are made after the DCPA has reviewed the amendments' consistency with the CP, by either updating the entire CPS or by publishing an addendum. The DCPA determines whether an amendment to this CPS is consistent with the CP, requires notice, or an OID change. *See also* Section 9.10 and Section 9.12 below.

## *1.6. DEFINITIONS AND ACRONYMS*

### 1.6.1. Definitions

**"Applicant"** means an entity applying for a Certificate.

**"Application Software Vendor"** means a software developer whose software displays or uses DMTS Certificates and distributes DMTS's root Certificates.

**"CAB Forum"** is defined in section 1.1.

**"Certificate"** means an electronic document that uses a digital signature to bind a Public Key and an identity.

**"Certificate Approver"** is defined in the EV Guidelines.

**"Certificate Requester"** is defined in the EV Guidelines.

**"Contract Signer"** is defined in the EV Guidelines.

**"Direct Address"** means an email address conforming to the Applicability Statement for Secure Health Transport.

**"Direct Address Certificate"** means a Certificate containing an entire Direct Address.

**"Direct Organizational Certificate"** means a Certificate containing only the domain name portion of a Direct Address.

**"Domain Name"** is as defined in the Baseline Requirements.

**"EV Guidelines"** is defined in section 1.1.

**"Key Pair"** means a Private Key and associated Public Key.

**"OCSP Responder"** means an online software application operated under the authority of DMTS and connected to its repository for processing certificate status requests.

**"Private Key**" means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

**"Public Key**" means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

**"Relying Party"** means an entity that relies upon either the information contained within a Certificate or a time-stamp token.

**"Relying Party Agreement"** means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DMTS's Repository. The Relying Party Agreement is available for reference through a DMTS online repository.

**"Subscriber"** means either the entity identified as the subject in the Certificate or the entity that is receiving DMTS's time-stamping services.

**"Subscriber Agreement"** means an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

**"WebTrust"** means the current version of CPA Canada's WebTrust Program for Certification Authorities.

**"WHOIS"** Information retrieved directly from the Domain Name Registrar or registry operator via the protocol, the Registry Data Access Protocol, or an HTTPS website.

### 1.6.2. Acronyms

| | |
|---|---|
| AATL | Adobe Approved Trust List |
| CA | Certificate Authority or Certification Authority |
| CAA | Certification Authority |
| CAB | Authorization ”CA/Browser” as in “CAB Forum” |
| CMS | Card Management System |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| CT | Certificate Transparency |
| DBA | Doing Business As (also known as "Trading As") |
| DCPA | DMTS Policy Authority |
| DNS | Domain Name Service |
| DV | Domain Validated |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| EV | Extended Validation |
| FIPS | (US Government) Federal Information Processing Standard |
| FQDN | Fully Qualified Domain Name |
| FTP | File Transfer Protocol |
| GLEIF | Global Legal Entity Identifier Foundation |
| HISP | Health Information Service Provider |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| IANA | Internet Assigned Numbers Authority |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IdM | Identity Management System |
| IDN | Internationalized Domain Name |
| ISSO | Information System Security Officer |
| IETF | Internet Engineering Task Force |
| IGTF | International Grid Trust Federation |
| ITU | International Telecommunication Union |
| IV | Individual Validated |
| LEI | Legal Entity Identifier |
| LOA | Level of Assurance |
| MICS | Member-Integrated Credential Service (IGTF) |
| NIST | National Institute of Standards and Technology |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| ONC | Office of the National Coordinator for Healthcare (U.S.) |
| OSU | Online Sign-Up (Wi-Fi Alliance Hotspot 2.0) |
| OV | Organization Validated |
| PIN | Personal Identification Number (e.g. a secret access code) |
| PKI | Public Key Infrastructure |
| PKIX | IETF Working Group on Public Key Infrastructure |
| RA | Registration Authority |
| RFC | Request for Comments (at IETF.org) |
| SAN | Subject Alternative Name |
| SHA | Secure Hashing Algorithm |
| SSL | Secure Sockets Layer |
| TLD | Top-Level Domain |
| TLS | Transport Layer Security |
| TSA | Time Stamping Authority |

| | |
|---|---|
| TST | Time-Stamp Token |
| TTL | Time To Live |
| UTC | Coordinated Universal Time |
| X.509 | The ITU-T standard for Certificates and their corresponding authentication framework |

### 1.6.3. References

If not listed in section 1.1:

Adobe Approved Trust List Technical Requirements, v.2.0

CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”)

CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (“EV Guidelines”)

CA/Browser Forum Guidelines for the Issuance and Management of Publicly-Trusted Code Signing Certificates

Wi-Fi Alliance Hotspot 2.0 Release 2 Online Signup Certificate Policy Specification (Hotspot 2.0 CP)

Mozilla Root Store Policy v.2.7

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

## *2.1. REPOSITORIES*

DMTS makes its root Certificates, revocation data for issued digital Certificates, CPs, CPSs, Relying Party Agreements, and standard Subscriber Agreements available in public repositories. DMTS develops, implements, enforces, and annually updates this CPS to meet the compliance standards of the documents listed in Sections 1.1 and 1.6.3. These updates also describe how the latest version of the Baseline Requirements are implemented. As Baseline Requirements are updated, DMTS reviews the changes to determine their impact on these practices. Each section impacted by the Baseline Requirements will be updated and provided to the DCPA for approval and implementation. If an SSL/TLS Server Certificate is intended to be trusted in Chrome, it is published by posting it in a Certificate Transparency log.

DMTS's legal repository for most services is located at https://cps.davidmiller.top/. DMTS's publicly trusted root Certificates and its CRLs and OCSP responses are regularly accessible online with systems described in Section 5 to minimize downtime.

## *2.2. PUBLICATION OF CERTIFICATION INFORMATION*

The DMTS certificate services, business practices (as required by section 8 of this CPS and the CP), and the repository are accessible through several means of communication:

1. On the web: https://pki.davidmiller.top (and via URIs included in the certificates themselves)
2. By email to admin@davidmiller.top

As specified in section 1.1, this CPS and the corresponding CP is structured in accordance with RFC 3647 and includes all material required by RFC 3647.

DMTS hosts test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate.

These separate Web pages are located at pki.davidmiller.top.

## *2.3. TIME OR FREQUENCY OF PUBLICATION*

CA Certificates are published in a repository as soon as possible after issuance. CRLs for end-user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least every 6 months and also within 24 hours if a CA Certificate is revoked. Under special circumstances, DMTS may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

For Certificates subject to the Baseline Requirements, CRLs for end-user Subscriber Certificates are issued at least once every seven days. CRLs for CAs that only issue CA Certificates subject to the Baseline Requirements are generally issued at least annually, and also whenever a CA Certificate is revoked. CRLs for Authenticated Content Signing (ACS) Root CAs are published annually and also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later issued CRLs after the Certificate's expiration.

DMTS develops, implements, enforces, and annually updates this CPS to describe in detail how DMTS complies with the CA/Browser Baseline Requirements and other documents as listed in section 1.1 and 1.6.3 of this CPS. Those updates indicate conformance by incrementing the version number and adding a dated changelog entry even if no other changes are made to the document as specified in section 1.2 of this CPS.

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

## *2.4. ACCESS CONTROLS ON REPOSITORIES*

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

# 3. IDENTIFICATION AND AUTHENTICATION

## *3.1. NAMING*

### 3.1.1. Types of Names

For TLS and s/MIME Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards except that DMTS may issue a Level 1 Certificate with a null subject DN if it includes at least one alternative name form that is marked critical. When DNs are used, common names must respect namespace uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates, except where stated otherwise under Section 3.1.3.

DMTS issues EV SSL/TLS Certificates to .onion domains in accordance with Appendix F of the EV Guidelines or Appendix C of the Baseline Requirements when the FQDN contains "onion" as the rightmost label.

DMTS issues OSU Server Certificates with subject alternative names that contain: (1) OSU Server FQDN(s) and (2) Friendly Name(s) that identify the wifi service provider, in accordance with section 3.4 of the Hotspot 2.0 CP.

### 3.1.2. Need for Names to be Meaningful

DMTS uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. DMTS only allows directory information trees that accurately reflect organization structures.

### 3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, DMTS does not issue anonymous or pseudonymous Certificates; however, for IDNs, DMTS may include the Punycode version of the IDN as a subject name. DMTS may also issue other pseudonymous end-entity Certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

### 3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

### 3.1.5. Uniqueness of Names

The uniqueness of each subject name in a Certificate is enforced as follows:

| | |
|---|---|
| SSL/TLS Server Certificates | Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). |
| Client Certificates | Requiring a unique email address or a unique organization name combined/associated with a unique serial integer. |
| Document Signing Certificates | Requiring a unique email address or a unique organization name combined/associated with a unique serial integer. |
| IGTF and Grid-only Device Certificates | For device Certificates, an FQDN is included in the appropriate fields. For other Certificates, DMTS may append a unique ID to a name listed in the Certificate. |
| Code Signing Certificates (including CDS Certificates) | Requiring a unique organization name and address or a unique organization name combined/associated with a unique serial integer. |
| Time Stamping | Requiring a unique hash and time or unique serial integer assigned to the time stamp |

The names of Subscribers shall be unique within a subordinate Issuer CA's and Customer's Sub-domain for a specific type of Certificate. Name uniqueness is not violated when multiple certificates are issued to the same entity.

### 3.1.6. Recognition, Authentication, and Role of Trademarks

For OSU Server Certificates, DMTS conducts a trademark search of logos and Friendly Names in relevant mark registration databases, such as the U.S. Patent and Trademark Office or WIPO, to confirm an applicant's right to use a particular trademark. Based on the results of such search(es), DMTS issues an OSU Server Certificate with one or more logotype extensions containing the hash algorithm and hash value of logos associated with the service provider. If an applicant does not have a friendly name or logo available, DMTS may include a logo and friendly name specified by the Wi-Fi Alliance.

For publicly-trusted TLS/SSL Certificates, DMTS implements a process that prevents Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless DMTS has verified this information in accordance with the EV Guidelines, Baseline Requirements, and section 3.2 of the CP and this CPS.

For all other Certificates, unless otherwise specifically stated in this CPS, DMTS does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. DMTS may reject any application or require revocation of any Certificate that is part of a trademark dispute.

## *3.2. INITIAL IDENTITY VALIDATION*

DMTS may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. DMTS may refuse to issue a Certificate in its sole discretion.

### 3.2.1. Method to Prove Possession of Private Key

No stipulation.

### 3.2.2. Authentication of Organization and Domain/Email Control

| | |
|---|---|
| DV SSL/TLS Server Certificates | DMTS validates the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures from section 3.2.2.4 of the Baseline Requirements:<br>1. This method (BR Section 3.2.2.4.1) is no longer used because it is deprecated as of 1-August-2018;<br>2. Email, Fax, SMS, or Postal Mail to the Domain Contact by sending a unique Random Value (valid for no more than 30 days from its creation) through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with BR Section 3.2.2.4.2;<br>3. (BR Section 3.2.2.4.3) is no longer used because it is deprecated as of 31-May-2019;<br>4. Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an email created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4; |

| | |
|---|---|
| | 5. (BR Section 3.2.2.4.5) is no longer used because it is deprecated as of 1-August-2018;<br>6. (BR Section 3.2.2.4.6) is no longer used because it is deprecated as of 24-April-2020 and not allowed after June 2020[1];<br>7. Domain Name Service (DNS) Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7;<br>8. IP Address - by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and3.2.2.4.8;<br>9. (BR Section 3.2.2.4.9) is no longer used because it was deprecated upon publication of v.4.16 of thisCPS;<br>10. (BR Section 3.2.2.4.10) is no longer used because it was deprecated upon publication of v.4.16 of thisCPS;<br>11. (BR Section 3.2.2.4.11) is no longer used because it is deprecated as of 5-February-2018;<br>12. Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12;<br>13. 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 will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 performed in accordance with BR Section3.2.2.4.13;<br>14. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.14;<br>15. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section 3.2.2.4.15; |

[1] DMTS may continue to re-use information and validations for domains validated under this method per the applicable certificate data reuse periods in section 4.2.1.

| | |
|---|---|
| | 16. Confirming the Applicant’s control over the FQDN by calling the DNS TXT Record Phone Contact’s phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name, performed in accordance with BR Section3.2.2.4.16;<br>17. Confirming 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 can 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, performed in accordance with BR Section 3.2.2.4.17;<br>18. 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 (such as a Request Token, Random Value that does not appear in the request used to retrieve the file and receipt of a successful HTTP 2xx status code response from the request) performed in accordance with BR section 3.2.2.4.18; and<br>19. 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, performed in accordance with BR section 3.2.2.4.19 and section 8.3 of RFC 8555 as prescribed.<br>20. 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 performed in accordance with BR section 3.2.2.4.20 as defined in RFC 8737.<br>Wildcard Certificate Domain Name validation is completed using the above list as permitted by the CA/B Forum Baseline Requirements along with current best practice of consulting a public suffix list. |
| IV and OV SSL/TLS Server, OSU Server, Object Signing, and Device Certificates<br>(excluding device Certificates issued under the Grid-only arc) | DMTS validates the Applicant’s right to use or control the Domain Name(s) and the country code that will be listed in the Certificate using the DV SSL/TLS Server Certificate validation procedures above.<br>DMTS also verifies the identity and address of the Applicant using the procedures found in section 3.2.2.1 or section 3.2.3 of the Baseline Requirements.<br>DMTS verifies any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification in accordance with section 3.2.2 of the Baseline Requirements. |

| | |
|---|---|
| Device Certificates issued under the Grid-only arc | An RA or Trusted Agent validates the applicant's information in accordance with an RPS (or similar document) applicable to the community of interest. |
| EV SSL/TLS Server and EV Code Signing Certificates | Information concerning organization identity related to the issuance of EV SSL/TLS Server Certificates is validated in accordance with the EV Guidelines. |
| S/MIME Certificates issued as Level 1-4 Client Certificates [2] | DMTS verifies an individual's or organization's right to use and/or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following:<br>1. By verifying domain control over the email domain using one of the procedures listed above in this table under the heading "DV SSL/TLS Server Certificates"; or<br>2. By sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response through use of the Random Value to indicate that the Applicant and/or Organization owns or controls that same email address. |

DMTS maintains and utilizes a scoring system to flag certificate requests that potentially present a higher risk of fraud. Those certificate requests that are flagged "high risk" receive additional scrutiny or verification prior to issuance, which may include obtaining additional documentation from or additional communication with the Applicant.

Before issuing an SSL/TLS Server Certificate with a domain name that has not been previously verified as within the scope of an RA's or other Delegated Third Party's allowed domain names, DMTS establishes that the RA or Delegated Third Party has the right to use the Domain Name by independently verifying the authorization with the domain owner, as described and allowed by the above.

DMTS uses a documented internal process to check the accuracy of information sources and databases to ensure the data is acceptable, including reviewing the database provider's terms of use.

For Legal Entity Identifier (LEI) numbers listed in Certificates, DMTS may include the value after verification, through the appropriate mechanism, such as mechanisms provided by Global Legal Entity Identifier Foundation (GLEIF), that the LEI is associated with entity information provided. LEI lookups are treated as information from a source described above, but not currently relied upon as a primary source of information for verification. Instead, this information is treated as additional correlation of identity information found in the certificate and provided in the certificate for the convenience and use of data researchers and the legal entities operating the certificates.

For EV SSL, the approved sources from this process are published publicly on a readily accessible GitHub repository available here in a file link on the page: https://github.com/dmcert.

### *3.2.2.1 Verification of IP Address*

For each IP Address listed in a publicly-trusted TLS Certificate, DMTS confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

1. Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory on the IP Address, performed in accordance with BR

[2] DMTS and its subordinate Issuer CAs do not delegate validation of the domain portion of an e-mail address in S/MIME certificates. DMTS and the subordinate Issuer CAs may rely upon validation the root CA has performed for an Authorized Domain Name as being valid domain names. If DMTS is verifying the domain portion, then DMTS will use a process the CAB forum authorized to meet this requirement as listed in this section.

Section 3.2.2.5.1;
2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section3.2.2.5.3;
4. After July 31, 2019, DMTS will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;
5. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;
6. Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension,"available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or
7. Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

### *3.2.2.2 Wildcard Domain Validation*

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, DMTS follows a documented procedure that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled /1 or public suffix, DMTS refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

### *3.2.2.3 Verification of Country*

For publicly-trusted TLS, if the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then DMTS or the RA verifies the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3 in the CABF Baseline Requirements and meets the requirements of this section.

If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then DMTS verifies the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of Section 3.2.2.1 in the CABF Baseline Requirements and this section. DMTS carefully inspects any document relied upon for alteration or falsification.

When the subject:countryName field is present, then DMTS or the RA verifies the country associated with the Subject using one of the following:

1. the IP Address range assignment by country for either
   a. the web site's IP address, as indicated by the DNS record for the web site or
   b. the Applicant's IP address;
2. the ccTLD of the requested Domain Name;
3. information provided by the Domain Name Registrar; or
4. a method identified in Section 3.2.2.1.

DMTS may implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

### 3.2.3. Authentication of Individual Identity

If a Certificate will contain the identity of an individual, then DMTS or an RA validates the identity of the individual using the following procedures:

| Certificate | Validation |
|---|---|
| IV (Individual Validated)<br>SSL/TLS Server Certificates and Object Signing Certificates (issued to an individual) | 1. a. DMTS or the RA obtains and reviews a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). DMTS or the RA inspects the copy for any indication of alteration or falsification.<br>b. For Object Signing Certificates, a validation specialist also engages in a videoconference call with the Applicant, who must present their photo ID and sign a Declaration of Identity, witnessed by the validation specialist, which is recorded as evidence.<br>2. DMTS may additionally cross-check the Applicant's name and address for consistency with available third-party data sources.<br>3. If further assurance is required, then the Applicant must provide an additional form of identification, such as recent utility bills, financial account statements, credit card, an additional ID credential, or equivalent document type.<br>4. DMTS or the RA confirms that the Applicant is able to receive communication by telephone, postal mail/courier, or fax.<br>If DMTS cannot verify the Applicant's identity using the procedures described above, then the Applicant must submit a Declaration of Identity that is witnessed and signed by a Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities. |
| Device Certificate Sponsors | See section 3.2.3.3 |
| OSU Server Certificates | DMTS verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization. |
| EV Certificates issued to a business entity | As specified in section 11.2.1(3) of the EV Guidelines |
| Grid-only Certificates | Either the RA responsible for the grid community or a Trusted Agent obtains an identity document during a face-to-face meeting with the Applicant, or a Trusted Agent attests that the Applicant is personally known to the Trusted Agent. The RA must retain sufficient information about the applicant's identity to prove upon DMTS's request that the applicant was properly identified. |
| Adobe Document Signing Certificates for Individuals | In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent per section ICA5(a) of the AATL 2.0 requirements. This can be performed either physically or digitally per the stated standards.<br>RAs must retain sufficient information about the applicant's identity to prove upon DMTS's request that the Applicant was properly identified. |

| | |
|---|---|
| Adobe Document Signing Certificates for Organizations | In-person appearance (either physically or digitally) before a person performing identity proofing for a Registration Authority or a Trusted Agent; and<br>Evidence of association with, and proofs of entitlement to represent, that organization per methods described for Applicants for a Level 2, 3, or 4 Client Certificate.<br>RAs must retain sufficient information about the applicant's identity to prove upon DMTS's request that the Applicant was properly identified. |
| Level 1 Client Certificates – Personal (email Certificates) | As specified in Section 3.2.2 (no identity verification other than control of the email address listed in the Certificate). |
| Level 1 Client Certificates – Enterprise (email certificates) | 1. For a certificate capable of being used for digitally signing or encrypting email messages, DMTS takes reasonable measures to verify that the Applicant submitting the request controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf.<br>2. DMTS may rely on validation performed for an Authorization Domain Name (as specified in the Baseline Requirements and section 3.2.2 of this CPS) as being valid for subdomains of that Authorization Domain Name. |

| | |
|---|---|
| Level 2 Client Certificates (email certificate) and IGTF Classic/MICS Certificates | The CA or an RA confirms that the following are consistent with the application and sufficient to identify a unique individual:<br>(a) the name on the government-issued photo-ID referenced below;<br>(b) date of birth; and<br>(c) current address or personal telephone number.<br>1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by a state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID.<br>2. The Applicant must possess a valid, current, government-issued, photo ID. The Registration Authority or Trusted Agent performing identity proofing must obtain and review, which may be through remote verification, the following information about the Applicant: (i) name, date of birth, and current address or telephone number; (ii) serial number assigned to the primary, government-issued photo ID; and (iii) one additional form of ID such as another government-issued ID, an employee or student ID card number, telephone number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. Identity proofing through remote verification may rely on database record checks with an agent/institution or through credit bureaus or similar databases. DMTS or an RA may confirm an address by issuing credentials in a manner that confirms the address of record or by verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records available to DMTS or the RA.<br>3. Where DMTS or an RA has a current and ongoing relationship with the Applicant, identity may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret.<br>4. Any of the methods used to verify the identity of an applicant for a DMTS Level 3 or 4 Client Certificate. |

| | |
|---|---|
| Level 3 Client Certificates | In-person proofing[4] before an RA, Trusted Agent, or an entity certifiedby a state, federal, or national entity that is authorized to confirm identities[5]. The information must be collected and stored in a secure manner. Required identification consists of one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9.<br>The person performing identity proofing examines the credentials and determines whether they are authentic and unexpired and checks the provided information (name, date of birth, and current address) to ensure legitimacy.<br>DMTS also employs the in-person antecedent process to meet this in-person identity proofing requirement. Under this definition, historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity.<br>In one use case, the Applicant (e.g. an employee) has been identified previously by an employer using USCIS Form I-9 and is bound to the asserted identity remotely through the use of known attributes or shared secrets.<br>In another use case, DMTS uses a third party Identity Verification Provider that constructs a real-time, five-question process, based on multiple historic antecedent databases.<br>The identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance. |

| | |
|---|---|
| Level 4 Client Certificates (Biometric ID Certificates) | In-person proofing before an RA, Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities. A certified entity must forward the collected information directly to an RA in a secure manner. The Applicant must supply one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D.. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9. The entity collecting the credentials must also obtain at least one form of biometric data (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate the application.<br>The person performing identity verification for DMTS or the RA examines the credentials for authenticity and validity. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. DMTS or the RA reviews and keeps a record of the Declaration of Identity.<br>Use of an in-person antecedent is not allowed. The identity of the Applicant must be established by in-person proofing no earlier than 30 days prior to initial certificate issuance. Level 4 Client Certificates are issued in a manner that confirms the Applicant's address. |

If in-person identity verification is required and the Applicant cannot participate in face-to-face registration alone (e.g. because Applicant is a network device, minor, or person not legally competent), then the Applicant may be accompanied by a person already certified by the PKI or who has the required identity credentials for a Certificate of the same type applied for by the Applicant. The person accompanying the Applicant (i.e. the "Sponsor") will present information sufficient for registration at the level of the Certificate being requested, for himself or herself, and for the Applicant.

For in-person identity proofing at Levels 3 and 4, DMTS may rely on an entity certified by a state, federal, or national entity as authorized to confirm identities may perform the authentication on behalf of the RA. The certified entity should forward the information collected from the applicant directly to the RA in a secure manner.

#### *3.2.3.1. Authentication for Role-based Client Certificates*

DMTS may issue Certificates that identify a specific role that the Subscriber holds, if the role identifies a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). These role-based Certificates are used when non-repudiation is desired. DMTS only issues role-based Certificates to Subscribers who first obtain an individual Subscriber Certificate that is at the same or higher assurance level as the requested role-based Certificate. DMTS may issue Certificates with the same role to multiple Subscribers. However, DMTS requires that each Certificate have a unique Key Pair. Individuals may not share their issued role-based Certificates and are required to protect the role-based Certificate in the same manner as individual Certificates.

DMTS verifies the identity of the individual requesting a role-based Certificate (the sponsor) in accordance with Section 3.2.3 before issuing a role-based Certificate. The sponsor must hold a DMTS-issued client individual Certificate at the same or higher assurance level as the role-based Certificate.

Regarding the issuance of role-based Certificates, this CPS requires compliance with all provisions of DMTS's CP regarding key generation, private key protection, and Subscriber obligations.

IGTF Certificates are not issued as role-based Certificates.

#### *3.2.3.2. Authentication of Devices with Human Sponsors*

DMTS issues Level 1, 2, 3 or 4 Client Certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNSname);
2. Equipment Public Keys;
3. Equipment authorizations and attributes (if any are to be included in the Certificate); and
4. Contact information.

If the Certificate's sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive Certificates. Each sponsor is required to provide proof that the device is still under the sponsor's control or responsibility on request. Sponsors are contractually obligated to notify DMTS if the equipment is no longer in use, no longer under their control or responsibility, or no longer requires a Certificate. All registration is verified commensurate with the requested certificate type.

### 3.2.4. Non-verified Subscriber Information

The common name of a Level 1 - Personal Client Certificates is not verified as the legal name of the Subscriber. DV SSL/TLS Server Certificates do not include a verified organizational identity. A trusted agent may be used to verify identity information where allowed. Unverified information is never included in a Level 2, Level, 3, Level 4, or Object Signing Certificate. TLS OU information is verified in accordance with 7.1.4 of the CAB baseline requirements. Other Certificate OU input is generally not verified except where verification is required by industry standards.

### 3.2.5. Validation of Authority

The authorization of a certificate request is verified as follows:

| Certificate | Verification |
|---|---|
| DV SSL/TLS Server Certificate | The authority of the requester is verified by using one or more of the procedures listed in section 3.2.2.4. of the Baseline Requirements. |
| OV SSL/TLS Server Certificates | The request is verified using a Reliable Method of Communication, in accordance with section 3.2.5 of the Baseline Requirements. |
| OSU Server Certificates | DMTS verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization. |
| EV Certificates | The request is verified in accordance with section 11.8.3 of the EV Guidelines. |
| Object Signing Certificates | If the Certificate names an organization, the requester's contact information is verified with an authoritative source within the applicant's organization using a Reliable Method of Communication. The contact information is then used to confirm the authenticity of the certificate request. |
| Adobe Signing Certificates | If the Certificate names an organization, the requester's contact information is verified with an authoritative source within the applicant's organization using a Reliable Method of Communication. The contact information is then used to confirm the authenticity ofthe certificate request. |
| Level 1 Client Certificates Personal (email Certificates) and Enterprise (email Certificates) | The authority of the request is verified through the email address listed in the Certificate or with a person who has technical or administrative control over the domain or the email address to be listed in the Certificate. |

| | |
|---|---|
| Client Certificates Levels 2, 3 and 4 Certificates | The organization named in the Certificate confirms to DMTS or an RA that the individual is authorized to obtain the Certificate.<br>The organization is required to request revocation of the Certificate when that affiliation ends. |
| IGTF Certificates | An authorized individual approves the certificate request. For device Certificates, the RA retains contact information for each device's registered owner. The device owner is required to notify the RA and request revocation if the device sponsor is no longer authorized to use the device or the FQDN in the Certificate. |

An organization may limit who is authorized to request Certificates by sending a request to DMTS. A request to limit authorized individuals is not effective until approved by DMTS will respond to an organization's verified request for DMTS's list of its authorized requesters.

### 3.2.6. Criteria for Interoperation

Interoperation with DMTS PKI is permitted pursuant to the CP.

## *3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS*

### 3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, DMTS creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, DMTS may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

| Certificate | Routine Re-Key Authentication | Re-Verification Required |
|---|---|---|
| DV and OV SSL/TLS Server and Device Certificates | Username and password | According to the Baseline Requirements |
| EV SSL/TLS Certificates | Username and password | According to the EV Guidelines |
| Subscriber Code Signing Certificates (Minimum Requirements and EV) | Username and password | According to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates |
| Signing Authority EV Code Signing Certificates | Username and password | According to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates |
| Timestamp EV Code Signing Certificates | Username and password | According to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates |
| Object Signing Certificates | Username and password | At least every six years |
| Adobe Signing Certificates | Username and password | At least every six years |
| Level 1 Client Certificates | Username and password or a challenge phrase | At least every nine years |

| | | |
|---|---|---|
| Level 2 Client Certificates | Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3 or a challenge phrase | At least every nine years |
| Level 3 and 4 Client Certificates | Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3 | At least every nine years |
| IGTF Certificates | Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated Private Key | At least every 13 months. However, Certificates associated with a Private Key restricted solely to a hardware token may be rekeyed or renewed for a period of up to 5 years |

### 3.3.2. Identification and Authentication for Re-key After Revocation

DMTS does not re-key after revocation. The Subscriber must undergo initial validation as specified in section 3.2.

## *3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST*

DMTS or an RA authenticates all revocation requests. DMTS may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

# 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## *4.1. CERTIFICATE APPLICATION*

### 4.1.1. Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to DMTS.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

DMTS does not issue Certificates to entities on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business.

In accordance with Section 5.5.2, DMTS maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. DMTS uses this information to identify subsequent suspicious certificate requests in accordance with section 3.2 of this CPS and the CP.

### 4.1.2. Enrollment Process and Responsibilities

In no particular order, the enrollment process includes:

- Submitting a certificate application;
- Generating a Key Pair;
- Delivering the Public Key of the Key Pair to DMTS;
- Agreeing to the applicable Subscriber Agreement; and
- Paying any applicable fees.

DMTS obtain any additional documentation determined necessary to meet the CP, this CPS, and items listed in section 1.2.

A CSR is not required for the application process.

Prior to the issuance of a Publicly Trusted Certificate, DMTS obtains from the Applicant a certificate request from the Applicant and that complies with the CP and this CPS. For publicly-trusted TLS, the certificate request may be used for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 4.2.1 of the Baseline Requirements, 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 contains 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

After receiving a certificate application, DMTS or an RA verifies the application information and other information in accordance with Section 3.2. In cases where the certificate request does not contain all the necessary information about the Applicant, DMTS or the RAs obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. DMTS and its RAs follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Prior to issuing a publicly-trusted SSL/TLS Server Certificate, DMTS checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 8659, and in accordance with section 3.2.2.8 of the Baseline Requirements (for publicly issued TLS Certificates).

If the Certificate is issued, it will be issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater.

DMTS logs actions taken based on CAA records, and documents issuance prevented by CAA for feedback to the CAB Forum. DMTS processes the “issue” and “issuewild” property tags and may not dispatch reports of issuance requests to the contact(s) listed in an “iodef” property tag. CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5 and section 3.2.2.5 in this CPS.

If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to DMTS.

For EV SSL Certificates, after verification is complete, DMTS evaluates the corpus of information and decides whether or not to issue the Certificate. If some or all of the documentation used to support an application is in a language other than English, a DMTS employee, RA, or agent skilled in the language performs the final cross-correlation and due diligence.

DMTS develops, maintains, and implements documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate’s approval, as reasonably necessary to ensure that such requests are properly verified under the CABF Baseline Requirements. DMTS considers a source’s availability, purpose, and reputation when determining whether a third-party source is reasonably reliable. For TLS DMTS does not consider a database, source, or form of identification reasonably reliable if DMTS is the sole source of the information.

### 4.2.2. Approval or Rejection of Certificate Applications

DMTS rejects any certificate application that DMTS or an RA cannot verify. DMTS does not issue Certificates containing a new gTLD under consideration by ICANN until the gTLD has been approved. DMTS may also reject a certificate application if DMTS believes that issuing the Certificate could damage or diminish DMTS’s reputation or business. DMTS does not issue certificates containing internal names.

Except for Enterprise EV Certificates, EV Certificate issuance approval requires two separate DMTS validation specialists. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV Certificate. The second validation specialist reviews the collected information and documents any discrepancies or details that require further explanation. The second validation specialist may require additional explanations and documents prior to authorizing the Certificate’s issuance. Enterprise RAs may perform the final cross-correlation and due diligence described herein using a single person representing the Enterprise RA. If satisfactory explanations and/or additional documents are not received within a reasonable time, DMTS will reject the EV Certificate request and notify the Applicant accordingly.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, DMTS will approve the certificate application and issue the Certificate. DMTS is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate’s contents for accuracy prior to using the certificate.

### 4.2.3. Time to Process Certificate Applications

Under normal circumstances, DMTS verifies an Applicant’s information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. For non-EV SSL/TLS Server Certificates, DMTS will usually complete the validation process and issue or reject a certificate application within two working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of DMTS can delay the issuance process.

## *4.3. CERTIFICATE ISSUANCE*

### 4.3.1. CA Actions during Certificate Issuance

DMTS confirms the source of a certificate request before issuance. For TLS certificates, DMTS does not issue end entity Certificates directly from its root Certificates. DMTS logs those SSL/TLS Server Certificates intended to be trusted in Chrome in two or more Certificate Transparency databases. See RFC 6962. Certificate issuance by the Root CA requires an individual authorized by DMTS (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. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

### 4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

DMTS may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, DMTS delivers Certificates via email to the email address designated by the Subscriber during the application process.

## *4.4. CERTIFICATE ACCEPTANCE*

### 4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

### 4.4.2. Publication of the Certificate by the CA

DMTS publishes all CA Certificates in its repository or according to the requirements in section 1.1. DMTS publishes end-entity Certificates by delivering them to the Subscriber.

### 4.4.3. Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's issuance if the RA was involved in the issuance process.

## *4.5. KEY PAIR AND CERTIFICATE USAGE*

### 4.5.1. Subscriber Private Key and Certificate Usage

The certificate shall be usedlawfully in accordance with DMTS's Subscriber Agreementthe terms of this CP and the relevant CPS.

Subscribers are obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

### 4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. DMTS does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by DMTS are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the DMTS repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. the digital signature or SSL/TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate

prior to the Certificate's use by referring to the relevant CRLs or OCSP responses and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

Before relying on a time-stamp token, a Relying Party must:

1. verify that the time-stamp token has been correctly signed and that the Private Key used to sign the time-stamp token has not been compromised prior to the time of the verification,
2. take into account any limitations on the usage of the time-stamp token indicated by the time-stamp policy, and
3. take into account any other precautions prescribed in this CPS or elsewhere.

## *4.6. CERTIFICATE RENEWAL*

### 4.6.1. Circumstance for Certificate Renewal

DMTS may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the Subscriber and attributes are consistent, and
3. the associated Private Key remains uncompromised.

DMTS may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. DMTS may notify Subscribers prior to a Certificate's expiration date. Certificate renewal requires payment of additional fees. DMTS may renew a certificate after expiration if the relevant industry permits such practices.

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew the expiring certificate to maintain continuity of Certificate usage.

### 4.6.2. Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates. DMTS may renew a Certificate without a corresponding request if the signing Certificate is re-keyed.

### 4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. DMTS will refresh any information that is older than the periods specified in the Baseline Requirements or EV Guidelines. DMTS may refuse to renew a Certificate if it cannot verify any rechecked information. If an individual is renewing a client Certificate and the relevant information has not changed, then DMTS does not require any additional identity vetting. Some device platforms, e.g. Apache, allow renewed use of the Private Key. If the Private Key and domain information have not changed, the Subscriber may renew the SSL/TLS Server Certificate using a previously issued Certificate or provided CSR.

### 4.6.4. Notification of New Certificate Issuance to Subscriber

DMTS may deliver the Certificate in any secure fashion, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the Certificate.

### 4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted 30 days after the Certificate's renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

### 4.6.6. Publication of the Renewal Certificate by the CA

DMTS publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are published in DMTS's repository.

### 4.6.7. Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

## *4.7. CERTIFICATE RE-KEY*

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same.

### 4.7.1. Circumstance for Certificate Rekey

Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

After re-keying a Certificate, DMTS may revoke the old Certificate but may not further re-key, renew, or modify the previous Certificate. Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

### 4.7.2. Who May Request Certification of a New Public Key

DMTS will only accept re-key requests from the subject of the Certificate, an authorized representative for an Organizational certificate, or the PKI sponsor. DMTS may initiate a certificate re-key at the request of the certificate subject or at DMTS's own discretion.

### 4.7.3. Processing Certificate Rekey Requests

DMTS will only accept re-key requests from the subject of the Certificate, an authorized representative for an Organizational certificate, or the PKI sponsor. If the Private Key and any identity and domain information in a Certificate have not changed, then DMTS can issue a replacement Certificate using a previously issued Certificate or previously provided CSR.

DMTS re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if DMTS believes that the information has become inaccurate.

### 4.7.4. Notification of Certificate Rekey to Subscriber

DMTS notifies the Subscriber within a reasonable time after the Certificate issues.

### 4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

Issued Certificates are considered accepted 30 days after the Certificate is rekeyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

### 4.7.6. Publication of the Issued Certificate by the CA

DMTS publishes rekeyed Certificates by delivering them to Subscribers.

### 4.7.7. Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's rekey if the RA was involved in the issuance process.

## *4.8. CERTIFICATE MODIFICATION*

### 4.8.1. Circumstances for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new Certificate may have the same or a different subject Public Key.

### 4.8.2. Who May Request Certificate Modification

DMTS modifies Certificates at the request of certain certificate subjects or in its own discretion. DMTS does not make certificate modification services available to all Subscribers.

### 4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, DMTS verifies any information that will change in the modified Certificate. DMTS will only issue the modified Certificate after completing the verification process on all modified information. DMTS will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

RAs are required to perform identification and authentication of all modified Subscriber information in terms of Section 3.2.

### 4.8.4. Notification of Certificate Modification to Subscriber

DMTS notifies the Subscriber within a reasonable time after the Certificate issues.

### 4.8.5. Conduct Constituting Acceptance of a Modified Certificate

Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

### 4.8.6. Publication of the Modified Certificate by theCA

DMTS publishes modified Certificates by delivering them to Subscribers.

### 4.8.7. Notification of Certificate Modification by the CA to Other Entities

RAs may receive notification of a Certificate's modification if the RA was involved in the issuance process.

## *4.9. CERTIFICATE REVOCATION AND SUSPENSION*

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, DMTS and Issuer CAs verify that a revocation request was initiated by Subscribers, an RA, an Issuing CA, and other entities listed in section 4.9.2 of this CPS and the CP. Other parties may submit Certificate Problem Reports to DMTS to report reasonable cause to revoke the Certificate. . Issuer CAs are required to provide evidence of the revocation authorization to DMTS upon request.

### 4.9.1. Circumstances for Revocation

DMTS will revoke a Certificate within 24 hours after receipt and confirming one or more of the following occurred:

1. The Subscriber requests in writing that DMTS revoke the Certificate;
2. The Subscriber notifies DMTS that the original Certificate request was not authorized and does not retroactively grant authorization;
3. DMTS obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. DMTS is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);or
5. DMTS obtains evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon.

DMTS may revoke a certificate within 24 hours and will revoke a Certificate within 5 days after receipt and confirming that one or more of the following occurred:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CAB forum baseline requirements or any section of the Mozilla Root Store policy;
2. DMTS obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
3. The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
4. DMTS confirms any circumstance indicating that use of a FQDN, IP address, or email address 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. For code signing, the Application Software Supplier requests revocation and DMTS does not intend to pursue an alternative course ofaction;
6. For code signing, the certificate is being used to sign Suspect Code;
7. DMTS confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
8. DMTS confirms a material change in the information contained in theCertificate;
9. DMTS confirms that the Certificate was not issued in accordance with the CAB forum requirements or relevant browser policy;
10. DMTS determines or confirms that any of the information appearing in the Certificate is inaccurate;
11. DMTS's right to issue Certificates under the CAB forum requirements expires or is revoked or terminated, unless DMTS has made arrangements to continue maintaining the CRL/OCSP Repository;
12. Revocation is required by the DMTS CP and/or this CPS;or
13. DMTS confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key wasflawed.

DMTS may revoke any Certificate in its sole discretion, including if DMTS believes that:

1. Either the Subscriber's or DMTS's obligations under the CP or this CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. DMTS received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. DMTS ceased operations and did not arrange for another Certificate authority to provide revocation support for the Certificates;
4. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;
5. The Subscriber was added as a denied party or prohibited person to a blocklist or is operating from a destination prohibited under the laws of the United States;
6. For Adobe Signing Certificates, Adobe has requested revocation; or
7. For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

DMTS always revokes a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

DMTS will revoke a Subordinate CA Certificate within seven (7) days after receiving and confirming one or more of the following occurred:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies DMTS that the original Certificate request was not authorized and does not retroactively grant authorization;
3. DMTS 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 of the CAB forum baseline requirements or any section of the Mozilla Root Store policy;
4. DMTS obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevantagreement;
5. DMTS confirms that the CA 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. DMTS determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. DMTS or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CACertificate;
8. DMTS's or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless DMTS has made arrangements to continue maintaining the CRL/ OCSP Repository;
9. Revocation is required by DMTS's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

DMTS will revoke a cross-Certificate if the cross-certified entity (including DMTS) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross-Certificate.

### 4.9.2. Who Can Request Revocation

Any appropriately authorized party, such as a recognized representative of a subscriber or cross-signed partner, may request revocation of a Certificate. DMTS may revoke a Certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

DMTS provides Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions on how they can report suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of possible fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates on the following website: https://pki.davidmiller.top/ and other resources as indicated in section
1.5.2 of this CPS.

### 4.9.3. Procedure for Revocation Request

DMTS processes a revocation request as follows:

1. DMTS logs the request or problem report and the reason for requesting revocation based on the list in section 4.9.1, including contact information of the requestor. DMTS may also include its own reasons for revocation in the log.
2. DMTS may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber or an authorized party, DMTS revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
4. For requests from third parties, DMTS personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on thefollowing criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate orwebsite,
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered),and
    d. relevant legislation.
5. If DMTS determines that revocation is appropriate, DMTS personnel revoke the Certificate and update the Certificate Status.

If DMTS deems appropriate, DMTS may forward the revocation reports to law enforcement. DMTS maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports on the following website: https://pki.davidmiller.top/ and other resources as indicated in section 1.5.2 of this CPS.

### 4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. DMTS may grant and extend revocation grace periods on a case-by-case basis. DMTS reports the suspected compromise of its CA Private Key and requests revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

### 4.9.5. Time within which CA Must Process the Revocation Request

DMTS will revoke a CA Certificate within one hour after receiving clear instructions from the DCPA.

Within 24 hours after receiving a Certificate problem report or a revocation request, DMTS investigates the facts and circumstances involved with the report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, DMTS works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which DMTS will revoke the certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by DMTS will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate problem reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered);and
5. Relevant legislation.

Under normal operating circumstances, DMTS will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1.

DMTS follows the revocation timeframes specified for malware in the Minimum Requirements for Issuance and Management of Publicly Trusted Code Signing Certificates in section 13.1.5.

### 4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

### 4.9.7. CRL Issuance Frequency

For publicly-trusted TLS Subscriber certificates:

DMTS updates and reissues CRLs at least once every seven days, and the value of the nextUpdate field is not be more than ten days beyond the value of the thisUpdate field.

For publicly-trusted TLS Subordinate CA certificates:

DMTS updates and reissues 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 is not more than twelve months beyond the value of the thisUpdate field.

For all other Certificates in this CPS:

DMTS uses its offline root CAs to publish CRLs for its intermediate CAs at least every 6 months. All other CRLS are published at least every seven days.

### 4.9.8. Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

### 4.9.9. On-line Revocation/Status Checking Availability

DMTS makes certificate status information available via OCSP for SSL/TLS Server Certificates. OCSP may not be available for other kinds of Certificates. Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time.

OCSP responses conform to RFC 5019 and/or RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked,or
2. Are 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 contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

### 4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

DMTS supports an OCSP capability using the GET method for Certificates issued in accordance with the Baseline Requirements. OCSP Responders under DMTS's direct control will not respond with a "good" status for a certificate that has not been issued.

For Publicly Trusted SSL Subscriber Certificates:
Prior to 2020-09-30:
DMTS update information was provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service have a maximum expiration time of ten days.

Effective 2020-09-30:
1. OCSP responses have a validity interval greater than or equal to eight hours;
2. OCSP responses have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, then DMTS updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then DMTS updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For Publicly Trusted SSL Subordinate CA or Intermediate CA Certificates: DMTS updates 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 should not respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5 of the Baseline Requirements, this CPS and the CP, the responder must not respond with a "good" status for such requests. "unused" if neither of the previous conditions are met.

DMTS may monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

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

Not applicable.

### 4.9.12. Special Requirements Related to Key Compromise

DMTS uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. DMTS will transition any revocation reason code in a CRL to “key compromise” upon discovery of such reason or as required by an applicable CP.

Reports to DMTS of key compromise must include:
Proof of key compromise in either of the following formats:

- A CSR signed by the compromised private key with the Common Name “Proof of Key Compromise for DMTS”; or
- The private key itself.
- A valid email address so that you can receive confirmation of your problem report and associated certificate revocations.

DMTS provides specific instructions and support for Key compromise on the following website: https://pki.davidmiller.top/ and other resources as indicated in section 1.5.2 of this CPS.

### 4.9.13. Circumstances for Suspension

Not applicable.

### 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

Certificate status information is available via CRL and OCSP responder. For publicly-trusted TLS certificates, revocation entries on a CRL or OCSP Response are not removed until after the expiration of the revoked Certificate. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate’s validity period, except for revoked Code Signing Certificates and EV Code Signing Certificates, which remain on the CRL for at least 10 years following the Certificate’s validity period. OCSP information for subscriber Certificates is updated at least every four days. OCSP information for subordinate CA Certificates is updated at least every 12 months and within 24 hours after revoking the Certificate.

### 4.10.2. Service Availability

Certificate status services are available 24x7 for publicly-trusted TLS and generally for all other services. This includes the online repository that application software can use to automatically check the current status of all unexpired Certificates issued by DMTS operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

DMTS also maintains a 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

OCSP Responders may not be available for all certificate types.

## *4.11. END OF SUBSCRIPTION*

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

## *4.12. KEY ESCROW AND RECOVERY*

### 4.12.1. Key Escrow and Recovery Policy Practices

DMTS never escrows CA Private Keys under this CPS.

DMTS may escrow Subscriber key management keys to provide key recovery services. If done, DMTS encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key. Enterprise customers utilizing key escrow software provided by DMTS may escrow keys within their or DMTS's infrastructure.

DMTS or Issuer CAs allow Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. DMTS uses multi-person controls during key recovery to prevent unauthorized access to a Subscriber's escrowed Private Keys. DMTS accepts key recovery requests:

1. From the Subscriber or Subscriber's organization, if the Subscriber has lost or damaged the private-key token;
2. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with DMTS for Private Key escrow;
3. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
4. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
5. From a requester authorized by law or governmental regulation; or
6. From an entity contracting with DMTS for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities using DMTS's key escrow services are required to:

1. Notify Subscribers that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
4. Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and
5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

### 4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

# 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## *5.1. PHYSICAL CONTROLS*

### 5.1.1. Site Location and Construction

DMTS performs its CA and TSA operations from secure data centers. The data centers are equipped with logical and physical controls that make DMTS's CA and TSA operations inaccessible to non-trusted personnel. DMTS operates under a security policy designed to detect, deter, and prevent unauthorized access to DMTS's operations.

### 5.1.2. Physical Access

#### *5.1.2.1. Data Centers*

Systems providing online certificate issuance (e.g. Issuer CAs) are located in secure data centers. DMTS protects such online equipment (including certificate status servers and CMS equipment) from unauthorized access and implements physical controls to reduce the risk of equipment tampering. Access to the data centers housing the CA and TSA platforms requires two-factor authentication by DMTS staff in trusted roles to meet two-person physical access control. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module.
Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer DMTS's Private Keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

The DMTS data centers are continuously attended. However, if DMTS ever becomes aware that a data center is to be left unattended or has been left unattended for an extended period of time, DMTS personnel will perform a security check of the data center to verify that:

1. DMTS's equipment is in a state appropriate to the current mode of operation,
2. Any security containers are properly secured,
3. Physical security systems (e.g., door locks) are functioning properly,and
4. The area is secured against unauthorized access.

DMTS's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

#### *5.1.2.2. RA Operations Areas*

DMTS's RA operations are protected against access from non-authorized individuals. DMTS securely stores all removable media and paper containing sensitive plain-text information related to its CA or RA operations in secure containers.

#### *5.1.2.3. Offline CA Key Storage Rooms*

DMTS securely stores the cryptomodules used to generate and store offline CA Private Keys. Access to the rooms used for key storage is controlled and logged. When not in use during a key ceremony, CA cryptomodules are locked in a safe that provides two-person physical access control. Activation data is protected in accordance with section 6.4. Cryptomodule activation keys are stored under dual control in a secured environment when not in use.

#### *5.1.2.4. CA Key Generation and Signing Rooms*

CA key generation and signing occurs either in the secure storage room described in section 5.1.2.3 or in a room of commensurate security in close proximity thereto. DMTS's CA Administrators retrieve cryptographic materials necessary to perform key generation and certificate signing. At no time are cryptographic materials left unattended by fewer than two persons serving in trusted roles as specified in section 5.2.2.

### 5.1.3. Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and generators provide redundant backup power.

### 5.1.4. Water Exposures

The cabinets housing DMTS's CA and TSA systems are designed to prevent and protect against water exposure.

### 5.1.5. Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

### 5.1.6. Media Storage

DMTS protects its media from accidental damage, environmental hazards, and unauthorized physical access. Backup files are created on a daily basis. DMTS's backup files are maintained separately from DMTS's primary data operations facility.

### 5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are physically destroyed or are overwritten multiple times to prevent the recovery of the data.

### 5.1.8. Off-site Backup

DMTS makes regular backup copies of any information necessary to recover from a system failure. Backup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site and are accessible only by trusted personnel.

### 5.1.9. Certificate Status Hosting, CMS and External RA Systems

All physical control requirements under Section 5.1 apply equally to any Certificate Status Hosting, CMS, or external RA system.

## *5.2. PROCEDURAL CONTROLS*

### 5.2.1. Trusted Roles

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

#### *5.2.1.1. CA Administrators*

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue Certificates to Subscribers.

#### *5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel*

The Registration Officer role is responsible for issuing and revoking Certificates.

#### *5.2.1.3. System Administrators/ System Engineers(Operator)*

The System Administrator / System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / System Engineer also keeps critical systems updated with software patches and other maintenance needed for system stability and recoverability.

#### *5.2.1.4. Internal Auditors*

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DMTS is operating in accordance with this CPS or an RA's Registration Practices Statement.

#### *5.2.1.5. RA Administrators*

RA Administrators are responsible for the RA software.

### 5.2.2. Number of Persons Required per Task

DMTS requires that at least two people acting in a trusted role take action for the most sensitive tasks, such as activating DMTS's Private Keys, generating a CA Key Pair, or backing up a DMTS Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access. Physical access to the CAs does not constitute a task as defined in this section, but is defined in section 5.1.

### 5.2.3. Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA, TSA, and RA systems before they are allowed access to systems necessary to perform their trusted roles.

### 5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keepingfunctions;
3. Those performing audit, review, oversight, or reconciliation functions;and
4. Those performing duties related to CA/TSA key management or CA/TSA administration.

To accomplish this separation of duties, DMTS specifically designates individuals to the trusted roles defined in Section 5.2.1 above. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. DMTS's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles at the same time.

## *5.3. PERSONNEL CONTROLS*

### 5.3.1. Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for DMTS's PKI operations and ensures compliance with this CPS and the CP. Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor, DMTS verifies the identity and trustworthiness of such person.

Management and operational support personnel involved in time-stamp operations possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. DMTS determines that all individuals assigned to trusted roles perform their prospective job responsibilities competently and satisfactorily as required.

### 5.3.2. Background Check Procedures

DMTS verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. DMTS requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks may include a combination of the following as required; verification of individual identity, employment history, education, character references, social security number, previous residences, driving records, professional references, and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. These procedures shall be subject to any limitations on background checks imposed by local law.

To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity shall utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned. Background checks are refreshed and re-adjudication occurs at least every five years.

These procedures are subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met by DMTS due to a prohibition or limitation in local law, DMTS utilizes a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

### 5.3.3. Training Requirements

DMTS provides relevant skills training in DMTS's PKI and TSA operations for the personnel performing information verification duties including: :

1. basic Public Key Infrastructure (PKI) knowledge;
2. software versions used by DMTS;
3. authentication and verification policies and procedures;
4. DMTS security principles and mechanisms;
5. disaster recovery and business continuity procedures;
6. common threats to the validation process, including phishing and other social engineering tactics; and
7. CAB forum guidelines and other applicable industry and government guidelines.

DMTS maintains records of who received training. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Registration Officers are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of such Certificates.

### 5.3.4. Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with DMTS industry-relevant training and performance programs in order to continue acting in trusted roles. DMTS makes employees acting in trusted roles aware of any changes to DMTS's operations as necessary for them to perform their role. If DMTS's operations change, DMTS will provide documented training, in accordance with an executed training plan, to all employees acting in relevant trusted roles to those changes.

### 5.3.5. Job Rotation Frequency and Sequence

Not applicable.

### 5.3.6. Sanctions for Unauthorized Actions

DMTS employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to internally maintained processes specifying guidance on administrative or disciplinary actions, up to and including termination of employment or agency and criminal sanctions.

### 5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

### 5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties.

## *5.4. AUDIT LOGGING PROCEDURES*

### 5.4.1. Types of Events Recorded

DMTS's systems require identification and authentication at system logon. Important system actions are logged to establish the accountability of the operators who initiate such actions.

DMTS enables all essential event auditing capabilities of its CA and TSA applications in order to record the events listed below. If DMTS's applications cannot automatically record an event, DMTS implements manual procedures to satisfy the requirements. For each event, DMTS records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. DMTS records the precise time of any significant TSA events. All event records are available to auditors as proof of DMTS's practices. Logs are maintained to the standard per the requirements of the relevant policies and programs.

DMTS records at least the following events:

1. CA Certificate and key lifecycle events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction
    b. Certificate requests, renewal, and re-key requests, and revocation;
    c. Approval and rejection of certificate requests
    d. Cryptographic device lifecycle management events;
    e. Generation of Certificate Revocation Lists and OCSP entries;
    f. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in the CABF Requirements, the DMTS CP, and this CPS;
    c. Approval and rejection of certificate requests;
    d. Issuance of Certificates; and
    e. Generation of Certificate Revocation Lists and OCSPentries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. Installation, update and removal of software on a Certificate System;
    e. System crashes, hardware failures, and other anomalies;
    f. Firewall and router activities; and
    g. Entries to and exits from the CAfacility.

Log entries include the following elements:

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

### 5.4.2. Frequency of Processing Log

As required, generally within at least once every two months, a DMTS administrator reviews the logs generated by DMTS's systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) (if necessary) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to DMTS's operations management committee and are made available to DMTS's auditors upon request. DMTS documents any actions taken as a result of a review.

### 5.4.3. Retention Period for Audit Log

Audit logs related to publicly trusted SSL/TLS Certificates are retained for at least two (2) years or in accordance with section 5.5.2. DMTS retains audit logs on-site until after they are reviewed. DMTS makes the audit logs available to auditors, as defined in section 8, available upon request.

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) of the CABF

Baseline Requirements after the later occurrence of:

- the destruction of the CA Private Key; or
- 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 its Qualified Auditor upon requesttrue 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)) of the CABF Baseline Requirements after the revocation or expiration of the Subscriber Certificate;

3. Any security event records (as set forth in Section 5.4.1 (3)) of the CABF Baseline Requirements after the event occurred.

### 5.4.4 Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. DMTS's CA and TSA systems are configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. DMTS's off-site storage location is a safe and secure location.

DMTS makes time-stamping records available when required to prove in a legal proceeding that DMTS's time-stamping services are operating correctly. Audit logs are made available to auditors upon request.

### 5.4.5 Audit Log Backup Procedures

DMTS makes regular backup copies of audit logs and audit log summaries and saves a copy of the audit log to a secure, off-site location on at least a monthly basis.

Where required, DMTS creates incremental backups of audit logs daily and full backups weekly.

### 5.4.6 Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, DMTS's Administrators and the DCPA shall be notified and the DCPA will consider suspending the CA's or RA's operations until the problem is remedied.

### 5.4.7 Notification to Event-causing Subject

No stipulation.

### 5.4.8 Vulnerability Assessments

To meet requirements of the CAB baseline requirements section 5. DMTS performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. DMTS also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DMTS has in place to control such risks.

Based on the Risk Assessment, DMTS develops, implements, and maintains 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 includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan takes into account available technology and the cost of implementing the specific measures, and implements 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.

DMTS's Internal Auditors review the security audit data checks for continuity. DMTS's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

## *5.5 RECORDS ARCHIVAL*

DMTS complies with all record retention policies that apply by law and retrieved as necessary by request of authorized parties. DMTS includes sufficient detail in all archived records to show that a Certificate or time-stamp token was issued in accordance with this CPS.

### 5.5.1 Types of Records Archived

DMTS retains the following information in its archives (as such information pertains to DMTS's CA / TSA operations):

1. Accreditations of DMTS,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA /TSA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Certificate issuance, rekey, renewal, and revocation requests,
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
8. Any documentation related to the receipt or acceptance of a Certificate or token,
9. Subscriber Agreements,
10. Issued Certificates,
11. A record of certificate re-keys,
12. Data or applications necessary to verify an archive's contents,
13. Compliance auditor reports,
14. Changes to DMTS's audit parameters,
15. Any attempt to delete or modify audit logs,
16. CA Key generation and destruction,
17. Access to Private Keys for key recovery purposes,
18. Changes to trusted Public Keys,
19. Export of Private Keys,
20. Approval or rejection of a revocation request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP or CPS.

### 5.5.2 Retention Period for Archive

DMTS, or the RA supporting issuance, archives data for other certificate types for at least 7 years or according to their respective requirements and as contractually agreed upon.

### 5.5.3 Protection of Archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the DCPA or as required by law. DMTS maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If DMTS needs to transfer any media to a different archive site or equipment, DMTS will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

### 5.5.4 Archive Backup Procedures

On at least an annual basis, DMTS creates an archive of the data listed in section 5.5.1. Each archive is stored separately and available for integrity verification at a later date. DMTS stores the archive in a secure location for the duration of the set retention period.

### 5.5.5 Requirements for Time-stamping of Records

DMTS automatically time-stamps archived records with system time (non-cryptographic method) as they are created. DMTS synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

### 5.5.6 Archive Collection System (internal or external)

Archive information is collected internally by DMTS.

### 5.5.7 Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the DMTS PKI, DMTS may elect to retrieve the information from archival. The integrity of archive information is verified by comparing a hash of the archive disk with the hash originally stored for that disk, as described in Section 5.5.4. DMTS may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with thedata.

## *5.6 KEY CHANGEOVER*

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, DMTS ceases using the expiring CA Private Key to sign Certificates and uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4. Where DMTS has cross-certified another CA that is in the process of a key rollover, DMTS obtains a new CA Public Key (PKCS#10) or new CA Certificate from the other CA and distributes a new CA cross Certificate following the procedures described above.

## *5.7 COMPROMISE AND DISASTER RECOVERY*

### 5.7.1 Incident and Compromise Handling Procedures

DMTS maintains an internal incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. DMTS documents in these internal procedures how it will notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

DMTS reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

### 5.7.2 Computing Resources, Software, and/or Data Are Corrupted

DMTS makes regular system backups weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, separate location. If DMTS discovers that any of its computing resources, software, or data operations have been compromised, DMTS assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If DMTS determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, DMTS suspends such operation until it determines that the risk is mitigated.

### 5.7.3 Entity Private Key Compromise Procedures

If DMTS suspects that one of its CA Private Keys has been compromised or lost then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. Specifically, DMTS will meet the requirements of 1.1 , but those steps generally include the following:

1. Collect information related to the incident;
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. Notify any cross-certified entities of the compromise so that they can revoke theircross-Certificates;
6. Incorporate lessons learned into the implementation of long term solutions and the Incident

Response Plan.

DMTS may generate a new Key Pair and sign a new Certificate. If a disaster physically damages DMTS's equipment and destroys all copies of DMTS's signature keys then DMTS will provide notice to affected parties at the earliest feasible time.

### 5.7.4 Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, DMTS implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving DMTS's primary facility and that DMTS be capable of maintaining other services or resuming them as quickly as possible following a disaster. DMTS reviews, tests, and updates the BCMP and supporting procedures at least annually.

DMTS's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes DMTS's primary CA or TSA operations to become inoperative, DMTS will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

## *5.8 CA OR RA TERMINATION*

Unless otherwise addressed in an applicable agreement between DMTS and a counterparty, before terminating its CA or TSA activities, DMTS may:

1. Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors, and cross-certifying entities and by posting such information on DMTS's web site; and
2. Transfer all responsibilities to a qualified successor entity.

Unless otherwise addressed in an applicable agreement between DMTS and a counterparty, if a qualified successor entity does not exist, DMTS may:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CPS.

DMTS has made arrangements to cover the costs associated with fulfilling these requirements in case DMTS becomes bankrupt or is unable to cover the costs. Any requirements of this section that are varied by contract apply only the contracting parties.

# 6. TECHNICAL SECURITY CONTROLS

## *6.1. KEY PAIR GENERATION AND INSTALLATION*

### 6.1.1. Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

DMTS's CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony in the environments described in section 5.1 and logged in accordance with section 5.4. The cryptographic hardware is evaluated to FIPS 140-2 Level 3 or higher. Activation of the hardware requires the use of two-factor authentication tokens. DMTS creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process. DMTS requires that an external auditor witness the generation of or review a recording of any CA keys to be used as publicly trusted root Certificates or to sign EV Certificates. For other CA key pair generation ceremonies, an Internal Auditor, external auditor, or independent third party attends the ceremony, or an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.

Subscribers must generate their keys in a manner that is appropriate for the certificate type. DMTS never creates key pairs for publicly trusted SSL/TLS Server Certificates and will not accept a certificate request using a Key Pair previously generated by DMTS. Certificates issued at Level 3 Hardware or at Level 4 Biometric must be generated on validated hardware cryptographic modules using a FIPS-approved method. For publicly-trusted TLS Certificates, DMTS rejects a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 of CA/Browser Baseline Requirements, DMTS has been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1 of the CA/Browser Baseline Requirements, if it has a known weak Private Key that is easily computed (such as a Debian weak key, see http://wiki.debian.org/SSLkeys). DMTS will not generate the key pair on behalf of the Subscriber if the Subscriber Certificate request has an extendedKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280].

For Adobe Signing Certificates, Subscribers must generate their Key Pairs in a medium that prevents exportation or duplication and that meets or exceeds FIPS 140-2 Level 3 certification standards.

### 6.1.2. Private Key Delivery to Subscriber

If DMTS, a CMS, or an RA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases:

1. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber's Private Key afterdelivery,
2. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process,
3. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate, and
4. The key generator must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it,and
    b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

SSL/TLS and S/MIME email signature certificates shall not be distributed as PKCS#12 packages. S/MIME encryption certificates can be distributed as PKCS#12 packages using secure channels. If generated on a physical token, it will also require a sufficiently secure passwords sent out of band from the package containing the hardware.

### 6.1.3. Public Key Delivery to Certificate Issuer

Not Applicable.

### 6.1.4. CA Public Key Delivery to Relying Parties

DMTS's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs. All accreditation authorities supporting DMTS Certificates and all application software providers are permitted to redistribute DMTS's root anchors.

DMTS may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may obtain DMTS's self- signed CA Certificates from DMTS's web site or by email.

### 6.1.5. Key Sizes

DMTS generally follows the NIST timelines in using and retiring signature algorithms and key sizes.

DMTS generates and uses at least the following minimum key sizes, signature algorithms, and hash algorithms for signing Certificates, CRLs, and certificate status server responses for policy OID arcs of 2.16.840.1.114535.1, 2.16.840.1.114535.2, and under specific circumstances the legacy arcs in section 1.1.

- 2048-bit or greater RSA Key (with a modulus size in bits divisible by 8);
- 256--bit ECDSA Key or greater with the matching Secure Hash Algorithm as required and a valid point on the elliptic curve; or
- a hash algorithm that is equally or more resistant to a collision attack allowed by the references in sections 1.1 and 1.6.3.

Signatures on CRLs, OCSP responses, and OCSP responder Certificates that provide status information for Certificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm if it is compliant with all applicable programs listed in section 1.1.

All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

DMTS requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms.

DMTS may require higher bit keys in its sole discretion if it is compliant with references in section 1.1 and 1.6.3.

Any Root Certificates participating in the AATL program issued after July 1, 2017 must be at least 3072-bit for RSA and 256-bit for ECDSA.

DMTS and Subscribers may fulfill the transmission security requirements under the CP and this CPS using TLS or another protocol that provides similar security, provided the protocol requires at least AES 128 bits or equivalent for the symmetric key and at least 2048-bit RSA or equivalent for the asymmetric keys.

### 6.1.6. Public Key Parameters Generation and Quality Checking

DMTS uses a cryptomodule that conforms to FIPS 186-2 and provides random value generation and on-board generation of Public Keys and a wide range of ECC curves. Key Usage Purposes (as per X.509 v3 key usage field).

DMTS's Certificates include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.

The use of a specific key is determined by the key usage extension in the X.509 Certificate.

Private Keys corresponding to Root CA Certificates are not 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;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates; and
4. Certificates for OCSP Response verification

Subscriber Certificates assert key usages based on the intended application of the Key Pair and cannot include anyExtendedKeyUsage.

Key usage bits and extended key usages are specified in the certificate profile for each type of Certificate DMTS's CA Certificates have at least two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the digitalSignature bit is also set.

Except for legacy applications using Level 1-3 and requiring a single key for dual use with both encryption and signature, DMTS does not issue Certificates with key usage for both signing and encryption. Instead, DMTS issues Subscribers two Key Pairs—one for key management and one for digital signature and authentication. For Certificates at Levels 1, 2 and 3 that are used for signing and encryption in support of legacy applications, they must:

1. be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CPS,
2. never assert the non-repudiation key usage bit, and
3. not be used for authenticating data that will be verified on the basis of the dual-use Certificate at a future time.

No Level 4 Certificates may have such dual-use Key Pairs.

## *6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHICMODULEENGINEERING CONTROLS*

### 6.2.1. Cryptographic Module Standards and Controls

DMTS's cryptographic modules for all of its CA and OCSP responder Key Pairs are validated to the FIPS 140- 2 Level 3. IGTF Certificate Subscribers must protect their Private Keys in accordance with the applicable Guidelines on Private Key Protection, including the use of strong pass phrases to protect Private Keys.

Cryptographic module requirements for subscribers and registration authorities are shown in the table below.

| Assurance Level | Subscriber | Registration Authority |
|---|---|---|
| **EV Code Signing** | FIPS 140-2 Level 2<br>(Hardware) | FIPS 140-2 Level 2<br>(Hardware) |
| **Adobe Signing** | FIPS 140-2 Level 2<br>(Hardware) | FIPS 140-2 Level 2<br>(Hardware) |
| **Rudimentary** | N/A | FIPS 140-2 Level 1<br>(Hardware or Software) |
| **Level 1 - Rudimentary** | N/A | FIPS 140-2 Level 1<br>(Hardware or Software) |
| **Level 2 – Basic** | FIPS 140-2 Level 1<br>(Hardware or Software) | FIPS 140-2 Level 1<br>(Hardware or Software) |

| | | |
|---|---|---|
| **Level 3 - Medium** | FIPS 140-2 Level 1 (Software)<br>FIPS 140-2 Level 2 (Hardware) | FIPS 140-2 Level 2 (Hardware) |
| **Medium** | FIPS 140-2 Level 1 (Software)<br>FIPS 140 Level 2 (Hardware) | FIPS 140-2 Level 2 (Hardware) |
| **Medium Hardware, Biometric /Hardware Authentication** | FIPS 140-2 Level 2 (Hardware) | FIPS 140-2 Level 2 (Hardware) |

DMTS ensures that the Private Key of an EV Code Signing Certificate is properly generated, used, and stored in a cryptomodule that meets or exceeds the requirements of FIPS 140-2 level 2 by (i) shipping conforming cryptomodules with preinstalled Key Pairs, (ii) communicating via PKCS#11 crypto APIs of cryptomodules that DMTS has verified meet or exceed requirements, or (iii) obtaining a suitable IT audit from the Subscriber that indicates compliance with FIPS 140-2 level 2 or the equivalent.

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

DMTS's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

Backups of CA Private Keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

### 6.2.3. Private Key Escrow

DMTS does not escrow its signature keys. Subscribers may not escrow their private signature keys. DMTS may provide escrow services for other types of Certificates in order to provide key recovery as described in section 4.12.1.

### 6.2.4. Private Key Backup

DMTS's Private Keys are generated and operated inside DMTS's cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. DMTS's CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and video-recorded key backup process as described in section 5.2.

DMTS may provide backup services for Private Keys that are not required to be kept on a hardware device. Access to back up Certificates is protected in a manner that only the Subscriber can control the Private Key. Backed up keys are never stored in a plain text form outside of the cryptographic module.

### 6.2.5. Private Key Archival

DMTS does not archive Private Keys.

### 6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, DMTS encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access. If DMTS 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 DMTS will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If DMTS pre-generates private keys and transfers them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, it will securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

### 6.2.7. Private Key Storage on Cryptographic Module

DMTS's Private Keys are generated and stored inside DMTS's cryptographic module, which has been evaluated to at least FIPS 140-2 Level 3, which includes requirements to protect the Private Key and other assets against known threats as described in section 5. Root Private Keys are stored offline in cryptographic modules or backup tokens as described above in Sections 6.2.2, 6.2.4, and 6.2.6.

### 6.2.8. Method of Activating Private Keys

DMTS's Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. Subscribers should also take commercially reasonable measures for the physical protection of their workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. When deactivated, private keys shall be kept in encrypted form only and secured. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys. *See also* Section 6.4.

### 6.2.9. Method of Deactivating Private Keys

DMTS's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. DMTS never leaves its HSM devices in an active unlocked or unattended state.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

### 6.2.10. Method of Destroying Private Keys

DMTS personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

DMTS may destroy a Private Key by deleting it from all known storage partitions. DMTS also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, DMTS will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

### 6.2.11. Cryptographic Module Rating

See Section 6.2.1.

## *6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT*

### 6.3.1. Public Key Archival

DMTS archives copies of Public Keys in accordance with Section 5.5.

### 6.3.2. Certificate Operational Periods and Key Pair Usage Periods

DMTS Certificates have maximum validity periods of:

| Type | Private Key Use[3] | Certificate Term |
|---|---|---|
| Publicly Trusted Root CAs | No stipulation | 25 years |
| Root CAs Not Otherwise Restricted | No stipulation | 100 years |

[3] CA Private Keys may continue to be used to sign CRLs and OCSP response s.

| | | |
|---|---|---|
| Publicly Trusted Sub CAs / Issuer CAs | No stipulation | 15 years |
| IGTF Cross-certified Sub CA[4] | 6 years | 15 years |
| CRL and OCSP responder signing | 3 years | No Stipulation[5] |
| DV SSL/TLS Server | No stipulation | 398 days |
| OV SSL/TLS Server | No stipulation | 398 days |
| EV SSL/TLS Server | No stipulation | 398 days |
| Time Stamping Authority | 15 months | 135 months |
| Object Signing Certificate and Document Signing | No stipulation | 123 months |
| Code Signing Certificate or EV Code Signing Certificate issued to Subscriber under the Minimum Requirements for Code Signing Certificates | No stipulation | 39 months |
| EV Code Signing Certificate issued to Signing Authority | 123 months | 123 months |
| Adobe Signing Certificate | 39 months | 5 years |
| IGTF End Entity Client used for signatures | 36 months | 36 months |
| IGTF Client used for key management. | 36 months | 36 months |
| End Entity Client for all other purposes (FBCA or IGTF compliant) | 36 months | 36 months |
| End Entity / Client for all other purposes (non-IGTF certs) | No Stipulation | 123 months |
| IGTF on hardware | 60 months | 13 months |
| Hotspot 2.0 OSU Server Certificates | No stipulation | 2 years |

Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day.

DMTS may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. DMTS does not issue Subscriber Certificates with an expiration date that exceeds the Issuer CA's public key term stated in the table above or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

## *6.4. ACTIVATION DATA*

### 6.4.1. Activation Data Generation and Installation

DMTS activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. For roots and public issuing CAs, this method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. DMTS will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All DMTS personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords that meet the requirements specified by the CAB forum network security requirements and other relevant requirements to meet best practices. If DMTS uses passwords as activation data for a signing key, DMTS will change the activation data change upon rekey of the CACertificate.

[4] IGTF signing Certificates must have a lifetime that is at least twice the maximum lifetime of an end entity Certificate.
[5] Restrictions will be based on program requirements as listed in section 1.1 of this CPS.

### 6.4.2. Activation Data Protection

DMTS protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All DMTS personnel are instructed to memorize and not to write down their password or share it with another individual. DMTS locks accounts used to access secure CA processes if a certain number of failed password attempts occur as specified in the internal security policies, procedures, and relevant requirements in references listed in Section 1.6.3.

End-user Subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

### 6.4.3. Other Aspects of Activation Data

Not applicable.

## *6.5. COMPUTER SECURITY CONTROLS*

### 6.5.1. Specific Computer Security Technical Requirements

DMTS secures its CA systems and authenticates and protects communications between its systems and trusted roles. DMTS's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses. Inactivity log out timeframes are set and enforced through internal information security policies and procedures to ensure security.

RAs must ensure that the systems maintaining RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

RAs must logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs must use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs must require the use of passwords with a minimum character length and a combination of alphanumeric and special characters.

DMTS's CA systems are configured to:

1. authenticate the identity of users before permitting access to the system or applications;
2. manage the privileges of users and limit users to their assigned roles;
3. generate and archive audit records for all transactions;
4. enforce domain integrity boundaries for security critical processes; and
5. support recovery from key or system failure.

All Certificate Status Servers:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage privileges to limit users to their assigned roles,
3. enforce domain integrity boundaries for security critical processes, and
4. support recovery from key or system failure.

DMTS enforces multi-factor authentication on any account 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

DMTS has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. DMTS only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by DMTS are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to DMTS's operations is scanned for malicious code on first use and periodically thereafter.

### 6.6.2. Security Management Controls

DMTS has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, DMTS verifies that the software is the correct version and is supplied by the vendor free of any modifications.

### 6.6.3. Life Cycle Security Controls

No stipulation.

## *6.7. NETWORK SECURITY CONTROLS*

DMTS and RA functions are performed using networks secured in accordance with the standards documented in the DMTS CP to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

DMTS documents and controls the configuration of its systems, including any upgrades or modifications made. DMTS's CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). DMTS's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

DMTS's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. DMTS's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

## *6.8. TIME-STAMPING*

The system time on DMTS's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to a real time value distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body. DMTS maintains an internal NTP server that synchronizes with cellular telephone networks and maintains the accuracy of its clock within one second or less. However, Relying Parties should be aware that all times included in a time-stamp token are synchronized with UTC within the accuracy defined in the time-stamp token itself, if present.

DMTS will not issue a time-stamp token using any clock that is detected as inaccurate. All clocks used for time-stamping are housed in the DMTS's secure facilities and are protected against threats that could result in an unexpected change to the clock's time. DMTS's facilities automatically detect and report any clock that drifts or jumps out of synchronization with UTC. Clock adjustments are auditable events.

TST Requesters request time-stamp tokens by sending a request to DMTS. After the TST Requester receives a response from DMTS, it must verify the status error returned in the response. If an error was not returned, the TST Requester must then verify the fields contained in the time-stamp token and the validity of the time-stamp token's digital signature. In particular, the TST Requester must verify that the time-stamped data corresponds to what was requested and that the time-stamp token contains the correct certificate identifier, the correct data imprint, and the correct hash algorithm OID. The TST Requester must also verify the timeliness of the response by verifying the response against a local trusted time reference. The TST Requester is required to notify DMTS immediately if any information cannot be verified.

Time Stamp Verifiers shall verify the digital signature on the time-stamp token and confirm that the data corresponds to the hash value in the time-stamp token.

# 7. CERTIFICATE, CRL, AND OCSP PROFILES

DMTS uses the ITU X.509, version 3 standard to construct digital Certificates for use within the DMTS PKI. DMTS adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

DMTS meets the technical requirements set forth in sections 2.2, 6.1.5, and 6.1.6 of the CA/Browser Baseline Requirements, the CP, and this CPS for publicly-trusted TLS certificates.

DMTS generates non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG.

## *7.1. CERTIFICATE PROFILE*

### 7.1.1. Version Number(s)

All Certificates are X.509 version 3 Certificates.

### 7.1.2. Certificate Extensions

IGTF Certificates comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

For Root CA, Subordinate CA, and Subscriber certificates used for publicly-trusted TLS, DMTS abides by the Baseline Requirements and configures the Certificate extensions to those requirements.
Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross- certificates that share a private key with a corresponding root certificate: will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId, and DMTS no longer includes both the id-kp- serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate**.**

For TLS certificates, the subjectAltName extension is populated in accordance with RFC 5280. For all web server certificates, the SubjectAltName extension is populated with the authenticated value in the Common Name field of the subject DN (domain name or public iPAddress). The SubjectAltName extension may contain additional authenticated domain names or public iPAddresses.

For internationalized domain names, the Common Name is represented as a puny-code value and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.

DMTS's Technically Constrained Subordinate CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly trusted certificates.

### 7.1.3. Algorithm Object Identifiers

DMTS Certificates are signed using relevant algorithms approved by the requirements listed in section 1.1. Some of those include one of the following:

| | |
|---|---|
| sha-1WithRSAEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5] |
| sha256WithRSAEncryption[6] | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11] |

[6] Legacy applications include the following algorithm ObjectIdentifier: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

| | |
|---|---|
| sha384WithRSAEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12] |
| sha512WithRSAEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13] |
| ecdsa-with-SHA256 | [iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 ] |
| ecdsa-with-SHA384 | [iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3] |

DMTS does not currently sign Certificates using RSA with PSS padding. SSL/TLS Server Certificates and OCSP Certificates are not signed with sha-1WithRSAEncryption.
DMTS and Subscribers may generate Key Pairs using the following:

| | |
|---|---|
| id-dsa | [iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1] |
| RsaEncryption | [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1] |
| Dhpublicnumber | [iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1] |
| id-keyExchangeAlgorithm | [joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22] |
| id-ecPublicKey | [ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 ] |

Elliptic curve Public Keys submitted to DMTS for inclusion in end entity Certificates should all be based on NIST “Suite B” curves.

As described in section 1.2 DMTS uses the keys and hash algorithms specified in the CAB forum Baseline Requirements and other requirements. DMTS does not issue publicly trusted SSL/TLS Certificates to a Reserved IP address or Internal Name.

### 7.1.4. Name Forms

Each Certificate includes a unique serial number. Optional subfields in the subject of an SSL Certificate must either contain information verified by DMTS or be left empty. SSL/TLS Server Certificates cannot contain metadata such as ‘.’, ‘-‘ and ‘ ‘ characters or and/or any other indication that the value/field is absent, incomplete, or not applicable. For CABF requirements as listed in section 1.1 DMTS has a process that limits information in OU fields from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless DMTS has verified this information in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.

For CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.

Certificates are populatedwith the Issuer Name and Subject Distinguished Name required under Section 3.1.1.
Issuer DNs meet the requirements in the CAB forum baseline requirements.
The contents of the fields in EV Certificates must meet the requirements in Section 8.1 of the EV Guidelines.

### 7.1.5. Name Constraints

DMTS may include name constraints in the nameConstraints field when appropriate.
For publicly-trusted TLS certificates, DMTS will follow the requirements of section 7.1.5 of the Baseline Requirements and as the following sections specify.

[3] Legacy applications include the following algorithm ObjectIdentifier: {iso(1) member-body(2) us(840)ansi-X9- 62(10045) signatures(4) ecdsa-with-SHA2 (3)2}

[4] Legacy applications include the following algorithm ObjectIdentifier: {iso(1) member-body(2) us(840)ansi-X9- 62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}

#### *7.1.5.1. Name-Constrained serverAuth CAs*

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then a technically constrained Subordinate CA Certificate includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

(a) For each dNSName in permittedSubtrees, the DMTS confirms that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements section3.2.2.4.

(b) For each iPAddress range in permittedSubtrees, DMTS confirms that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.

(c) For each DirectoryName in permittedSubtrees the DMTS confirms the Applicant’s and/or Subsidiary’s Organizational name(s) and location(s) such that end entity certificates issued from the subordinate CA Certificate will comply with section 7.1.2.4 and 7.1.2.5 of the Baseline Requirements. If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate specifies the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate includes within excludedSubtrees an iPAddress GeneralName of8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate also includes within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate includes at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate includes a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate includes at least one dNSName in permittedSubtrees.

#### *7.1.5.2. Name-Constrained emailProtection CAs*

If the technically constrained Subordinate CA certificate includes the id-kp-emailProtection extended key usage, it also includes the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.

### 7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy and are included as appropriate in the certificate.

OIDs required by CA/Browser Forum are implemented in accordance with those specifications.

The following is a non-comprehensive list of OIDs including extensions and policies used when issuing DMTS Certificates and time-stamp tokens:

| **Digitally Signed Object** | **DMTS Object Identifier (OID)** | **CABF OID** |
|---|---|---|
| DMTS Arc | 2.16.840.1.114535.<br>2.16.840.1.114535.1<br>2.16.840.1.114535.2 | |
| DMTS Policy Documents | 2.16.840.1.114535.0 | |
| DMTS Certificate Policy | 2.16.840.1.114535.0.1.4 | |
| DMTS Certification Practices Statement | 2.16.840.1.114535.0.2.4 | |
| DMTS Certificate extension identifying the Legal Entity Identifier (LEI) of an entity verified by the certificate authority | 2.16.840.1.114535.133 | |
| DMTS OCSP Responder | 2.16.840.1.114535.36 | |
| DMTS OCSP Responder (Dedicated Signer) | 2.16.840.1.114535.36.1 | |

| | | |
|---|---|---|
| DMTS Level 3 certificates - US | 2.16.840.1.114535.4.3.1 | |
| DMTS Level 3 certificates - Customs and Border Protection (CBP) | 2.16.840.1.114535.4.3.2 | |
| DMTS Level 3 Certificates – NIST LOA | 2.16.840.1.114535.4.3.3 | |
| DMTS PIV-I Content Signing | 2.16.840.1.114535.5.3 | |
| DMTS PIV-I Encryption | 2.16.840.1.114535.5.4 | |
| DMTS Authentication certificate with rudimentary level of verification | 2.16.840.1.114535.6.1 | |
| Federated Device Certificate | 2.16.840.1.114535.1.11 | |
| FPKI Common Devices | 2.16.840.1.101.3.2.1.3.8 | |
| FBCA Basic | 2.16.840.1.101.3.2.1.3.2 | |
| FBCA Address and FBCA Org | 2.16.840.1.101.3.2.1.3.2 | |
| FBCA Device | 2.16.840.1.101.3.2.1.3.37 | |
| FBCA Medium | 2.16.840.1.101.3.2.1.3.14 | |
| Federal Bridge Certification Authority (FBCA) policy for Medium Assurance Commercial Best Practice (CBP) certificates | 2.16.840.1.101.3.2.1.3.14 | |
| FBCA Device | 2.16.840.1.101.3.2.1.3.37 | |
| IGTF | 1.2.840.113612.5.2.2.1<br>1.2.840.113612.5.2.3.3.1<br>1.2.840.113612.5.2.3.3.2 | |
| Grid | 1.2.840.113612.5.2.3.1.2 | |
| Grid OGF | 1.2.840.113612.5.2.3.3.3 | |
| DMTS Grid | 2.16.840.1.114535.19.31.1 | |
| Domain Vetted (DV) SSL/TLS Server Certificates per the Baseline Requirements | 2.16.840.1.114535.1.2 | 2.23.140.1.2.1 |
| Organization Vetted (OV) SSL/TLS Server Certificates per the Baseline Requirements | 2.16.840.1.114535.1.1 | 2.23.140.1.2.2 |
| Individual Vetted (IV) SSL/TLS Server Certificates per the Baseline Requirements | 2.16.840.1.114535.1.1 | 2.23.140.1.2.3 |
| Where allowed based on cert use (primarily Iussing CAs) | 2.5.29.32.0 (anyPolicy) | |
| Extended Validation (EV) SSL/TLS Server Certificates per the EV SSL Guidelines | 2.16.840.1.114535.2.1, 1.3.6.1.4.1.6334.1.100.1 (originally registered by beTRUSTed), and/or 2.16.840.1.113733.1.7.23.6 (originally registered by Verisign) | 2.23.140.1.1 |
| DMTS CA/Browser Forum validation method used to issue a certificate | 2.16.840.1.114535.55 | |
| Object Signing Certificates | 2.16.840.1.114535.3 | |
| Code Signing Certificates | 2.16.840.1.114535.3.1 | |

| | | |
|---|---|---|
| Code Signing per the Baseline Requirements for Code-Signing Certificates | 2.16.840.1.114535.3.1.1 | 2.23.140.1.4.1 |
| Extended Validation Code Signing per the Baseline Requirements for Code-Signing Certificates | 2.16.840.1.114535.3.2 | 2.23.140.1.3 |
| Windows Kernel Driver Signing | 2.16.840.1.114535.3.11 | |
| Adobe Authentic Documents Trust (CDS) | 1.2.840.113583.1.1.5 | |
| Adobe Signing Certificate | 2.16.840.1.114535.3.21 | |
| Adobe Signing Certificate for Individuals | 2.16.840.1.114535.3.21.1 | |
| Adobe Signing Certificate for Organizations | 2.16.840.1.114535.3.21.2 | |
| Non-Adobe Signing Certificate | 2.16.840.1.114535.3.25 | |
| Client Certificate OID Arc | 2.16.840.1.114535.4 | |
| Level 1 Certificates – Personal | 2.16.840.1.114535.4.1.1, 2.16.840.1.114535.4.1.2, or 2.16.840.1.114535.5.1 (maps to 2.16.840.1.113733.1.7.23.1) | |
| Level 1 Certificates – Enterprise | 2.16.840.1.114535.4.1.2 or 2.16.840.1.114535.5.2 (maps to 2.16.840.1.113733.v1.7.23.2) | |
| Level 2 Certificates | 2.16.840.1.114535.4.2 or 2.16.840.1.114535.5.2 (maps to 2.16.840.1.113733.1.7.23.1, 2.16.840.1.113733.1.7.23.2, or 2.16.840.1.113733.1.7.23.3) | |
| Level 3 Certificates – Client | 2.16.840.1.114535.4.3 | |
| Level 4 Certificates | 2.16.840.1.114535.4.4 | |
| DMTS Level 4 Certificates - US | 2.16.840.1.114535.4.4.1 | |
| DMTS Level 4 Certificates - Customs and Border Protection (CBP) | 2.16.840.1.114535.4.4.2 | |
| DMTS CA/Browser Forum validation method used to issue a certificate | 2.16.840.1.114535.55 | |
| DMTS Magnum | 2.16.840.1.114535.5.3<br>1.2.840.113583.1.2.1<br>1.2.840.113583.1.2.3<br>2.16.840.1.113733.1.7.1.6 | |
| Certisur | 1.3.6.1.4.1.12456.1.1.3 | |

| | | |
|---|---|---|
| Grid Certificate OID Arcs | 2.16.840.1.114535.4.31 or 2.16.840.1.114535.31 (Grid-only arc) | |
| IGTF Classic X.509 Authorities with secured infrastructure | 2.16.840.1.114535.4.31.1 (Client w/ Public), 2.16.840.1.114535.31.4.1.1 (Client Grid Only),<br>and/or 1.2.840.113612.5.2.2.1.x (IGTF) | |
| IGTF Member Integrated X.509 Credential Services with Secured Infrastructure Certificates | 2.16.840.1.114535.4.31.5 and/or 1.2.840.113612.5.2.2.5.x (IGTF) | |
| IGTF Grid Host – Public Trust | 2.16.840.1.114535.1.31.1 | |
| IGTF Grid-Only Host Certificate | 2.16.840.1.114535.31.1.1.1,<br>1.2.840.113612.5.2.2.1.x (IGTF),<br>and/or 1.2.840.113612.5.2.2.5.x (IGTF) | |
| Authentication-Only Certificates | 2.16.840.1.114535.6 | |
| Class 1 Authentication-Only Certificates | 2.16.840.1.114535.6.1.1,<br>2.16.840.1.114535.6.1.2, | |
| Class 2 Authentication-Only Certificates | 2.16.840.1.114535.6.2 | |
| Time Stamping Arc | 2.16.840.1.114535.7 | |
| Trusted Time-stamping | 2.16.840.1.114535.7.1 | |
| Legacy arc | 2.16.840.1.114535.81<br>2.16.840.1.113733.1.7<br>2.23.140.1.1,1.3.6.1.4.1.14370<br>1.3.6.1.4.1.14370.1<br>2.16.840.1.113733.1.7.48 | |
| Test arc | 2.16.840.1.114535.99 | |
| Zoom Video Communications, Inc | 1.3.6.1.4.1.57731 | |

SigiCert may include other OIDs as appropriate.

OIDs in this list and in DMTS certificates belong to their respective owners.

### 7.1.7. Usage of Policy Constraints Extension

Not applicable.

### 7.1.8. Policy Qualifiers Syntax and Semantics

DMTS includes brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension. Those Certificates may contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the applicable CPS.

### 7.1.9 Processing Semantics for the Critical Certificate PoliciesExtension

No stipulation.

## *7.2 CRL PROFILE*

For revoked issuing CAs, the CRLReason indicated cannot be unspecified (0) or certificateHold(6). If the reason for revocation is unspecified, DMTS will omit the reasonCode entry extension, when technically not capable of issuance.

If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate. DMTS specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

- unspecified (0)[7],
- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4)[8],
- cessationOfOperation (5)[9],

### 7.2.1 Version number(s)

DMTS issues version 2 CRLs that contain the following fields:

| Field | Value |
|---|---|
| Issuer Signature Algorithm | sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR<br>sha-256WithRSAEncryption [1 2 840 113549 1 1 11];<br>sha-384WithRSAEncryption [1 2 840 113549 1 1];<br>sha-512WithRSAEncryption [1 2 840 113549 1 1 13 ];<br>ecdsa-with-sha256 [1 2 840 10045 4 3 2 ]; OR<br>ecdsa-with-sha384 [1 2 840 10045 4 3 3]. |
| Issuer Distinguished Name | Full subject DN of the issuing CA |
| thisUpdate | CRL issue date in UTC format |
| nextUpdate | Date when the next CRL will issue in UTC format. |
| Revoked Certificates List | List of revoked Certificates, including the serial number and revocation date |
| Issuer’s Signature | [Signature] |

### 7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

| Extension | Value |
|---|---|
| CRL Number | Never repeated monotonically increasing integer |
| Authority Key Identifier | Subject Key Identifier of the CRL issuer certificate |
| Invalidity Date | Optional date in UTC format |

| | |
|---|---|
| Reason Code | Specify reason for revocation in list of reason codes in section 7.2, if included. |

[7] Reason code (0)_unspecified is only used if it is omitted from the CRL and OCSP in accordance with the baseline requirements.

[8] When a reason code is not specified, DMTS will log the revocation as (4) superseded or (5) Cessation of Operation

[9] When a reason code is not specified, DMTS will log the revocation as (4) superseded or (5) Cessation of Operation.

## *7.3 OCSP PROFILE*

Effective 2020-09-30, if an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present and asserted.

Effective 2020-09-30, the CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

### 7.3.1 Version Number(s)

DMTS's OCSP responders conform to version 1 of RFC 6960.

### 7.3.2 OCSP Extensions

Not Applicable. The singleExtension of an OCSP response cannot contain the reasonCode (OID 2.5.29.21) CRL entry extension.

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for Certification Authorities as required by the Mozilla Root Store policy and other programs listed in section 1.1 and 1.6.3.

## *8.2 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT*

DMTS receives an annual period in time audit by an independent external auditor to assess DMTS's compliance with this CPS, referenced requirements, any applicable CPs, and the WebTrust for CA programs criteria.

## *8.3 IDENTITY/QUALIFICATIONS OF ASSESSOR*

WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements.

## *8.4 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY*

DMTS's WebTrust / Federal PKI auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against DMTS.

## *8.5 TOPICS COVERED BY ASSESSMENT*

The audit covers DMTS's business practices disclosure, the integrity of DMTS's PKI operations, and DMTS's compliance with this CPS and referenced requirements. The audit verifies that DMTS is compliant with the CP, this CPS, and any MOA between it and any other PKI.

DMTS undergoes an audit in accordance with one of the following schemes:

1. "WebTrust for CAs v2.1 or newer" AND "WebTrust for CAs SSL Baseline with Network Security v2.3 or newer"; or
2. ETSI EN 319 411-1 v1.2.2, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied).

Whichever scheme is chosen, it incorporates 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 is conducted by a Qualified Auditor, as specified in Section 8.2.

## *8.6 ACTIONS TAKEN AS A RESULT OFDEFICIENCY*

If an audit reports a material noncompliance with applicable law, this CPS, the CP, or any other contractual obligations related to DMTS's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify DMTS, and (3) DMTS will develop a plan to cure the noncompliance. DMTS will submit the plan to the DCPA for approval and to any third party that DMTS is legally obligated to satisfy.
The DCPA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates. DMTS is entitled to suspend and/or terminate of services through revocation or other actions as deemed by the DCPA to address the non- compliant Issuer CA.

## *8.7 COMMUNICATION OF RESULTS*

The results of each audit are reported to the DCPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. Copies of DMTS's conforming WebTrust for CAs audit reports can be found at: https://www.DMTS.com/webtrust-audits. On an annual basis and within three months of completion, DMTS submits copies of relevant audit compliance reports to various parties, such as Mozilla, Adobe, CA licensing bodies, etc.

### *8.8 SELF-AUDITS*

On at least a quarterly basis, DMTS performs regular internal audits against a randomly selected sample of at least three percent of its SSL/TLS Server Certificates and EV Code Signing Certificates issued since the last internal audit. Self-audits on server and code signing Certificates are performed in accordance with Guidelines adopted by the CA B forum. Audits of other certificate types will be at the discretion of DMTS to gain reasonable assurance of compliance to applicable root program requirements.

# 9. OTHER BUSINESS AND LEGAL MATTERS

## *9.1. FEES*

### 9.1.1. Certificate Issuance or Renewal Fees

DMTS charges fees for certificate issuance and renewal. DMTS may change its fees at any time in accordance with the applicable customer agreement.

### 9.1.2. Certificate Access Fees

DMTS may charge a reasonable fee for access to its certificate databases.

### 9.1.3. Revocation or Status Information Access Fees

DMTS does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL.

DMTS may charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. DMTS does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without DMTS's prior express written consent.

### 9.1.4. Fees for Other Services

DMTS does not charge a fee for access to the DMTS CP or this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

### 9.1.5. Refund Policy

Subscribers must request refunds, in writing, within 30 days after a Certificate issues. After receiving the refund request, DMTS may revoke the Certificate and refund the amount paid by the Applicant, minus any applicable application processing fees.

## *9.2. FINANCIAL RESPONSIBILITY*

### 9.2.1. Insurance Coverage

DMTS maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

### 9.2.2. Other Assets

No stipulation.

### 9.2.3. Insurance or Warranty Coverage for End-Entities

DMTS provides a warranty to Subscribers according to the terms of the Netsure Extended Warranty Protection Plan. DMTS provides a limited warranty to Relying Parties in DMTS's Relying Party Agreement.

## *9.3. CONFIDENTIALITY OF BUSINESS INFORMATION*

### 9.3.1. Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;

3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by DMTS as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set foirnththis CPS).

### 9.3.2. Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

### 9.3.3. Responsibility to Protect Confidential Information

DMTS's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

## *9.4. PRIVACY OF PERSONAL INFORMATION*

### 9.4.1. Privacy Plan

DMTS follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws.

### 9.4.2. Information Treated as Private

DMTS treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. DMTS protects private information using appropriate safeguards and a reasonable degree of care.

### 9.4.3. Information Not Deemed Private

Subject to local laws, private information does not include Certificates, CRLs, or their contents.

### 9.4.4. Responsibility to Protect Private Information

DMTS employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

### 9.4.5. Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. DMTS will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

### 9.4.6. Disclosure Pursuant to Judicial or Administrative Process

DMTS may disclose private information, without notice, if DMTS believes the disclosure is required by law or regulation.

### 9.4.7. Other Information Disclosure Circumstances

No stipulation.

## *9.5. INTELLECTUAL PROPERTY RIGHTS*

DMTS and/or its business partners own the intellectual property rights in DMTS's services, including the Certificates, trademarks used in providing the services, and this CPS.

### 9.5.1. Property Rights in Certificates and Revocation Information

DMTS retains all intellectual property rights in and to the Certificates and revocation information that they issue. DMTS and customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. DMTS, and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any otherapplicable agreements.

### 9.5.2. Property Rights in the CP

Issuer CAs acknowledge that DMTS retains all intellectual property rights in and to this CPS.

### 9.5.3. Property Rights in Names

Subscribers and Applicants retain all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate and distinguished name within any Certificate issued to such Subscriber or Applicant.

### 9.5.4. Property Rights in Keys and Key Material

Key Pairs corresponding to Certificates of CAs and end-user Subscribers are the property of DMTS and end-user Subscribers that are the respective subjects of the Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all intellectual property rights in and to these key pairs. Without limiting the generality of the foregoing, DMTS's root Public Keys and the Root Certificates containing them, including all Public Keys and self-signed Certificates, are the property of DMTS licenses software and hardware manufacturers to reproduce such Root Certificates to place copies in trustworthy hardware devices or software.

### 9.5.5. Violation of Property Rights

Issuer CAs shall not knowingly violate the intellectual property rights of any third party.

## *9.6. REPRESENTATIONS AND WARRANTIES*

### 9.6.1. CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, DMTS does not make any representations regarding its products or services. DMTS represents, to the extent specified in this CPS, that:

1. DMTS complies, in all material aspects, with the CP, this CPS, and all applicable laws and regulations,
2. DMTS publishes and updates CRLs and OCSP responses on a regular basis,
3. All Certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the Baseline Requirements,and
4. DMTS will maintain a repository of public information on its website.

To the extent allowed under EU law, DMTS:

1. Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information, including name verification for (1) Certificates intended for email and intranet use, (2) Multi-SAN Certificates, and (3) other Certificates issued to individuals and intranets.
2. Is not responsible for information contained in a Certificate except as stated in this CPS,
3. Does not warrant the quality, function, or performance of any software or hardware device, and
4. Is not responsible for failing to comply with this CPS because of circumstances outside of DMTS's control.

For EV Certificates, DMTS represents to Subscribers, Subjects, Application Software Vendors that distribute DMTS's root Certificates, and Relying Parties that use a DMTS Certificate while the Certificate is valid that DMTS followed the EV Guidelines when verifying information and issuing EV Certificates.

This representation is limited solely to DMTS's compliance with the EV Guidelines (e.g., DMTS may rely on erroneous information provided in an attorney's opinion or accountant's letter that is checked in accordance with the Guidelines).

Subscriber Agreements may include additional representations and warranties that do not contradict or supersede this CPS.

### 9.6.2. RA Representations and Warranties

RAs represent that:

1. The RA's certificate issuance and management services conform to the DMTS CP and this CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information,and
4. All Certificates requested by the RA meet the requirements of this CPS.

DMTS's agreement with the RA may contain additional representations.

Subscriber Agreements may include additional representations and warranties.

### 9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify DMTS and any applicable RA if a change occurs that could affect the status of the Certificate.

DMTS requires, as part of the Subscriber Agreement or Terms of Use for TLS, that the Applicant make the commitments and warranties in this section for the benefit of DMTS and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, DMTS will obtain, for the express benefit of DMTS and the Certificate Beneficiaries, either:

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

Subscribers represent to DMTS, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys fromcompromise,
2. Provide accurate and complete information when communicating with DMTS,
3. Confirm the accuracy of the certificate data prior to using theCertificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify DMTS if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate,
6. Use the Certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL/TLS Server Certificates on servers accessible at the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent, and
7. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

Subscriber Agreements may include additional representations and warranties

### 9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a DMTS Certificate, it:

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,
2. Studied the applicable limitations on the usage of Certificates and agrees to DMTS's limitations on liability related to the use of Certificates,
3. Has read, understands, and agrees to the DMTS Relying Party Agreement and this CPS,
4. Verified both the DMTS Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a DMTS Certificate if the Certificate has expired or been revoked and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a DMTS Certificate after considering:
   a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
   b) the intended use of the Certificate as listed in the certificate or this CPS,
   c) the data listed in the Certificate,
   d) the economic value of the transaction orcommunication,
   e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
   f) the Relying Party's previous course of dealing with theSubscriber,
   g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
   h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

Relying Party Agreements may include additional representations and warranties.

### 9.6.5. Representations and Warranties of Other Participants

No stipulation.

## *9.7. DISCLAIMERS OF WARRANTIES*

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DMTS DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DMTS DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. DMTS does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

## *9.8. LIMITATIONS OF LIABILITY*

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM DMTS's NEGLIGENCE OR (II) FRAUD COMMITTED BY DMTS. EXCEPT AS STATED ABOVE, ANY ENTITY USING A DMTS CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF DMTS RELATED TO SUCH USE, PROVIDED THAT DMTS HAS MATERIALLY COMPLIED WITH THIS CPS IN PROVIDING THE CERTIFICATE OR SERVICE. DMTS's LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CPS IS LIMITED AS SET FORTH IN THE NETSURE EXTENDED WARRANTY PROTECTION PLAN AND THE DMTS RELYING PARTY AGREEMENT.

All liability is limited to actual and legally provable damages. DMTS is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if DMTS is aware of the possibility of suchdamages;
2. Liability related to fraud or willful misconduct of the Applicant;
3. Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CPS;

4. Liability related to the security, usability, or integrity of products not supplied by DMTS, including the Subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether DMTS failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of DMTS's Certificates and services.

To the extent DMTS has issued and managed the Certificate(s) at issue in compliance with this CP and its CPS, DMTS shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit DMTS's and the applicable Affiliates' liability outside the context of any extended warranty protection program. Limitations of liability shallinclude an exclusionof indirect, special,incidental,andconsequentialdamages.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber Agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in theagreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

## *9.9. INDEMNITIES*

### 9.9.1. Indemnification by DMTS

To the extent permitted by applicable law, DMTS shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an EV Certificate issued by DMTS, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

### 9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify DMTS, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key.

The applicable Subscriber Agreement may include additional indemnity obligations.

### 9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify DMTS, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

## *9.10. TERM AND TERMINATION*

### 9.10.1. Term

This CPS and any amendments to the CPS are effective when published to DMTS's online repository and remain in effect until replaced with a newer version.

### 9.10.2. Termination

This CPS as amended from time to time, shall remain in effect until replaced by a newer version.

### 9.10.3. Effect of Termination and Survival

DMTS will communicate the conditions and effect of this CPS's termination via the DMTS Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the Certificate is revoked or expired, even if this CPS terminates.

## *9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITHPARTICIPANTS*

DMTS accepts notices related to this CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from DMTS. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. DMTS may allow other forms of notice in its Subscriber Agreements.

Notices to Application Software Vendors are sent out in accordance with the respective requirements.

## *9.12. AMENDMENTS*

### 9.12.1. Procedure for Amendment

This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the DCPA.

### 9.12.2. Notification Mechanism and Period

DMTS posts CPS revisions to its website. DMTS does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number. Major changes affecting accredited Certificates are announced and approved by the accrediting agency prior to becoming effective. The DCPA is responsible for determining what constitutes a material change of the CPS.

### 9.12.3. Circumstances under which OID Must Be Changed

The DCPA is solely responsible for determining whether an amendment to the CPS requires an OID change.

## *9.13. DISPUTE RESOLUTION PROVISIONS*

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Unless otherwise approved by DMTS, the procedure to resolve disputes involving DMTS require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Salt Lake County, Utah, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration

Parties are required to notify DMTS and attempt to resolve disputes directly with DMTS before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

## *9.14. GOVERNING LAW*

The laws of the state of Utah govern the interpretation, construction, and enforcement of this CPS and all proceedings related to DMTS's products and services, including tort claims, without regard to any conflicts of law principles. The state of Utah, and Salt Lake County, has non-exclusive venue and jurisdiction over any proceedings related to the CPS or any DMTS product or service.

## *9.15. COMPLIANCE WITH APPLICABLE LAW*

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, DMTS meets the requirements of the European data protection laws and has established appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

## *9.16. MISCELLANEOUS PROVISIONS*

### 9.16.1. Entire Agreement

DMTS contractually obligates each RA to comply with this CPS and applicable industry guidelines. DMTS also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

### 9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of DMTS. Unless specified otherwise in a contact with a party, DMTS does not provide notice of assignment.

### 9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

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

DMTS may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. DMTS's failure to enforce a provision of this CPS does not waive DMTS's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by DMTS.

### 9.16.5. Force Majeure

DMTS is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond DMTS's reasonable control. The operation of the Internet is beyond DMTS's reasonable control.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting DMTS.

## *9.17. OTHER PROVISIONS*

No stipulation.

# APPENDIX A: SAMPLE OPINION LETTER

**[*Date*]**

To: David Miller Trust Services

Email: dmcert@outlook.com

Digital Certificate for *[Exact company name of client – see footnote 1]*(“**Client**”)

Re:

This firm represents Client, who asked that I, as its [*accountant ,lawyer, solicitors, barrister, advocate, etc.*], attest to the following information solely as related to the Client’s application for a digital certificate.

After reviewing the Client’s records and based on my investigation, my professional opinion is that:

1. Client is a duly formed [*corporation, LLC, etc.*] under the laws of the [*state/province*] of [*name of governing jurisdiction where Client is incorporated or registered*]; is “active,” “valid,” “current,” or the equivalent; and is not under any known legal disability.

2. [*If applicable*] The Romanized transliteration of Client’s formal legal name is: [*Romanized name]*.

3. [*If applicable*] Client conducts business under the [*assumed/DBA/trade*] name of *[assumed name of Client].* Client has a currently valid registration of the name with the government agency that has jurisdiction over the place of business listed below.

4. The address where [*Client, Client’s parent, or Client’s subsidiary – select one*] conducts business operations is:
*[Insert place of business – this should match the address on the certificate application]*

5. A main telephone number at Client’s place of business is:
*[Insert primary telephone number of business]*

6. *[Name of Client’s Representative – see footnote 2]* is an individual (or are individuals) with the authority to act on behalf of Clientto:
   a) Provide information about the Client contained in the referenced application,
   b) Request one or more digital certificates and designate other persons to request digital certificates, and
   c) Agree to the contractual obligations contained in DMTS’s agreements.

7. *[Name and title of Client’s Representative],* who is Client’s *[Title of Client Representative]*, can be contacted at:
Email: *[Email address of Client Representative]*
Phone: *[Phone number of Client Representative]*

8. Client has either operated as a business for three or more years or has an active deposit account held at a bank or other financial institution where funds deposited are payable ondemand.

Although we did not find any exceptions to the above identification procedures, these procedures do not constitute an audit or opinion of Client's application for a digital certificate. We are not expressing an opinion on Client's digital certificate application and have provided this letter solely for the benefit of DMTS in connection with Client's application for a digital certificate. No other person or entity may rely on this letter without my express written consent. This letter shall not be quoted in whole or in part, used, published or otherwise referred to or relied upon in any manner, including, without limitation, in any financial statement or other document.

Signature:________________________________________________________
Print Accountant/Attorney Name: ________________________________________
Phone Number: _________________________________
Email:______________________________________
Firm Name: _________________________________
Licensed in: __________________________
License number, ifany: __________________________
Contact information for licensing agency where this accountant's/attorney's license information may be verified: ________________________________________________

Note 1: This must be the Client’s exact corporate name as registered with the relevant Incorporating Agency in the Client’s Jurisdiction of Incorporation.
Note 2: A Power of Attorney from an officer of the Client who has the power to delegate authority is sufficient to establish the Client Representative’s actual authority. Multiple representatives may be listed.
Note 3: In-house counsel of the Client may submit this letter if permitted by the rules of your jurisdiction.
Note 4: This letter may be submitted by mail, fax, or email.