Microsoft

Microsoft PKI Services

Certification Practice Statement (CPS)

Version 3.1
June 12, 2018

Table of Contents

1. INTRODUCTION

1.1 OVERVIEW

This document is the Certification Practice Statement (CPS) that defines the procedural and operational requirements governing the lifecycle management of Microsoft PKI Services' Certification Authority (CA) solutions and services for affiliated entities, Applicants, Subscribers, and Relying Parties. Microsoft PKI Services requires entities to adhere to this CPS when issuing and managing digital certificates within Microsoft PKI Services PKI hierarchy. This may include services managed by Microsoft PKI Services as well as other groups within Microsoft responsible for managing trusted and untrusted CAs. Each PKI service is required to have an associated Certification Practice Statement (CPS) that adheres to the presiding CP.

Microsoft PKI Services has two CPS documents to differentiate its internal (not publicly trusted) from its external (publicly trusted) CA operations, as they are regulated by separate compliance authorities and/or levels. This CPS is for the external (publicly trusted) CA operations.

Other important documents that accompany this CPS include the CP and associated Subscriber and Relying Party Agreements. Microsoft may publish additional Certificate Policies or Certification Practice Statements, as necessary, to describe other products or service offerings.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 standards for the creation of Certificate Policy (CP) and Certification Practices Statement (CPS) documents and complies with the current Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements"), and the Guidelines For The Issuance And Management Of Extended Validation Certificates ("EV Guidelines") from the Certificate Authority and Browser Forum (CAB Forum) at http://www.cabforum.org.

In the event of an inconsistency between this document and the governing industry requirements, those requirements take precedence.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is formally referred to as the Microsoft PKI Services "Certification Practice Statement" ("CPS"). CAs SHALL issue certificates in accordance with the policy and practice requirements of this document. The Object Identifier (OID) for the CPS is: 1.3.6.1.4.1.311.76.509.1.1

The following Object Identifiers are assigned for use by Microsoft CAs as a means of asserting compliance with CAB Forum's Baseline Requirements and Extended Validation Guidelines:

Digitally Signed Object	**Object Identifier (OID)**
SSL Domain Validated (DV) Certificates	2.23.140.1.2.1
SSL Organization Validated (OV) Certificates	2.23.140.1.2.2
SSL Individual Validated Certificates	2.23.140.1.2.3
Extended Validation SSL Certificates	2.23.140.1.1
Minimum Requirements for Code Signing	2.23.140.1.4.1

Extended Validation Code Signing	2.23.140.1.3

1.2.1 Revisions

Change Control Log

Revision Date	Revision Reason	Revision Explanation	New Revision	Supersedes
1/27/2010	New	Established	1.0	N/A
1/2/2013	Revised	Updated to support PKI Steering Committee, Microsoft Legal and Audit partner recommendations	1.1	1.0
4/2/2013	Revised	Updated to support the practice of online CA operations	2.0	1.1
4/30/2014	Revised	Updated to incorporate findings from FY13 WebTrust Audit and internal review.	2.1	2.0
2/28/2018	Revised	Major update/rewrite to factor changes in CAB Forum's Baseline Requirements and EV Guidelines.	3.0	2.1
6/12/2018	Revised	Minor updates to factor section revisions in CAB Forum's Baseline Requirements v1.5.7.	3.1	3.0

1.2.2 Relevant Dates

The CAB Forum's Baseline Requirements document should be referenced for relevant dates on industry practice or policy changes.

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

The term Certification Authority (CA) collectively refers to an entity or organization that is responsible for the authorization, issuance, revocation, and life cycle management of a certificate. The term equally applies to Roots CAs and Subordinate CAs.

Microsoft PKI Services operates as the Root CA and administers all CA functions within its PKI hierarchy.

The two main categories of CAs that exist within the Microsoft PKI Services' PKI hierarchy are the Root CAs and Subordinate CAs. An up-to-date enlistment of these CA's is maintained by Microsoft PKI Services.

Obligations of CAs operating within the Microsoft PKI Services' PKI hierarchy include:

- Generating, issuing and distributing Public Key certificates, in accordance with this CPS.
- Distributing CA certificates
- Generating and publishing certificate status information (such as CRLs)
- Maintaining the security, availability, and continuity of the certificate issuance and CRL signing functions
- Providing a means for Subscribers to request revocations
- Ensuring that changes in certificate status are reflected in their own repositories and those of authorized certificate validation authorities within the times specified in Section 4 of this CPS.
- Demonstrating internal or external audited compliance, in accordance with this CPS, the CP, and/or CAB Forum Baseline Requirements and EV Guidelines.

1.3.2 Registration Authorities

No RA functions are delegated to third parties by Microsoft PKI Services.

1.3.3 Subscribers

A Subscriber, as defined in Section 1.6, is the end entity whose name or identifier appears as the subject in a certificate, and who uses its key and certificate in accordance with this CPS. Subscribers within the CA's hierarchy MAY be issued certificates for assignment to devices, groups, organizational roles or applications, provided the responsibility and accountability are attributable to the organization.

Obligations of Subscribers within the CA's hierarchy include:

- Reading and accepting the terms and conditions of the Subscriber Agreement
- Being responsible for the generation of the key pair for their certificate
- Submitting Public Keys and credentials for registration
- Providing information to the RA that is accurate and complete to the best of the Subscribers' knowledge and belief regarding information in their certificates and identification and authentication information
- Taking appropriate measures to protect their Private Keys from compromise
- Promptly reporting loss or compromise of Private Key(s) and inaccuracy of certificate information

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance on a Certificate or digital signature associated with a Certificate.

1.3.5 Other Participants

Other participants include entities or groups that have participated in the development of this CPS and presiding CP, and any authorities that have contributed to the requirements and guidelines governing the issuance and management of publicly-trusted certificates.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The CA has established policy and technical constraints to define appropriate uses for issued certificates and provides reasonable controls to ensure the certificates are used for their intended purpose.

Certificates issued by the CA are used in accordance with the key usage extensions and extended key usage of the respective Certificates and adhere to the terms and conditions of this CPS, the accompanying CP, any agreements with subscribers, and applicable laws.

Relying Parties SHALL evaluate the application environment and associated risks before deciding on whether to use certificates issued under this CPS.

1.4.2 Prohibited Certificate Uses

Use of certificates in violation of this CPS, applicable laws, and/or key usage constraints, is unauthorized and prohibited. The CA reserves the right to revoke certificates that violate their designated usage.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

This organization responsible for the CPS is:

Microsoft PKI Services
One Microsoft Way
Redmond, WA 98052-6399

1.5.2 Contact Person

Contact information is listed below:

PKI Service Manager
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
Email: certificateauthority@microsoft.com

1.5.3 Person Determining CPS Suitability for the Policy

Microsoft PKI Policy Authority determines suitability and applicability of the CPS, in accordance with the CP.

1.5.4 CPS Approval Procedures

The Microsoft PKI Policy Authority reviews and approves any changes to this CPS, in compliance with the CP. Updates to CP or CPS documents SHALL be made available by publishing new versions at https://www.microsoft.com/pkiops/docs/repository.htm.

1.6 DEFINITIONS AND ACRONYMS

Capitalized terms and acronyms, not specified herein, are defined in the CAB Forum's Baseline Requirements (BR) and if not specified in the BR, are defined in the Extended Validation (EV) Guidelines.

1.6.1 Definitions

- **Affiliate –** A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
- **Applicant** – a natural person or Legal Entity that applies for (or seeks renewal of) a Certificate by a CA.
- **Applicant Representative** – A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA**.**
- **Application Software Supplier** – A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
- **Attestation Letter:** A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
- **Audit Report** – A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
- **Authorization Domain Name** – The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until

encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

- **Authorized Port –** One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).
- **Base Domain Name** – The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
- **Baseline Requirements (BR)** – An integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements issued by the CA/Browser Forum and available at cabforum.org.
- **CAA** – From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."
- **CA/Browser Forum (CAB Forum)** – A consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of digital certificates. Details are available at: cabforum.org.
- **Certificate -** digital record that contains information such as the Subscriber's distinguished name and public key, and the signer's signature and data.
- **Certificate Application –** a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
- **Certificate Request** – an application for a new Certificate or a renewal of a Certificate.
- **Certificate Revocation List (CRL)** – periodically published listing of all certificates that have been revoked for use by Relying Parties
- **Certificate Signing Request (CSR)** – a message sent to the certification authority containing the information required to issue a digital certificate
- **Certification Authority (CA)** – an entity or organization that is responsible for the authorization, issuance, revocation, and management of a certificate. The term equally applies to Roots CAs and Subordinate CAs.
- **Certificate Policy (CP)** – A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- **Certification Practice Statement (CPS) –** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- **CSPRNG** – A random number generator intended for use in cryptographic system.
- **Domain Authorization Document** – Documentation provided by, or a CA's documentation

of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

- **Domain Contact** – The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
- **Domain Name** – The label assigned to a node in the Domain Name System.
- **Domain Namespace** – The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
- **Domain Name Registrant** – Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
- **Domain Name Registrar** – A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
- **Distinguished Name (DN)** – a globally unique identifier representing a Subject that is used on Certificates and in the Repository
- **EV Certificate –** A certificate that contains subject information specified and validated in accordance with the EV Guidelines.
- **EV Certificate Beneficiaries –** Persons to whom the CA and its Root CA make specified EV Certificate Warranties.
- **EV Guidelines –** Guidelines for the Issuance and Management of Extended Validation Certificates, as defined by the CA/Browser Forum.
- **Extended Key Usage –** An extension in an X.509 certificate to indicate the allowed purpose(s) for the use of the public key. Also referenced or known as "Enhanced Key Usage".
- **Fully-Qualified Domain Name (FQDN)** – A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
- **Government Entity** – A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
- **Issuing CA** – The first digital certificate issuing authority who issues certificates signed by the root certificate authority (CA).

- **Legal Entity** – An association, corporation, partnership, proprietorship, trust, or government entity that has legal standing in a country’s legal system.
- **Microsoft PKI Policy Authority –** Combination of Microsoft’s Steering and Oversight Committees.
- **Online CA (OCA) -** a certification authority system which signs end-entity Subscriber Certificates that are operated and maintained in an online state so as to provide continually available certificate signing services. Online CAs reside in segmented, secured, and functionally dedicated networks.
- **Private Key –** 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 –** 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 corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding Private Key.
- **Public Key Infrastructure (PKI) –** A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
- **Random Value** – A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
- **Registration Authority (RA)** – Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- **Registration Identifier --** the unique code assigned to an Applicant by the Incorporating or Registration Agency in such entity’s Jurisdiction of Incorporation or Registration.
- **Reliable Data Source** – An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
- **Relying Party** – a Relying Party is an individual or entity that acts in reliance on a Certificate or digital signature associated with a Certificate.
- **Relying Party Agreement** – an agreement which specifies the stipulations under which a person or organization acts as a Relying Party

- **Repository** – an online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- **Request Token** – A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

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

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

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

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

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

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

  The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
- **Required Website Content** – Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
- **Root CA** – The top-level CA whose root certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- **Signing Service** – an organization that signs an Object on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.
- **Subject** – The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- **Subject Identity Information** – Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.
- **Subscriber** – an individual or end-entity (person, device, or application) that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate
- **Subscriber Agreement –** an agreement containing the terms and conditions that the authorized Subscriber consented to for the use of their issued certificate, containing the private key and corresponding public key.
- **Suspect Code -** code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or

resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes**.**

- **Takeover Attack** - an attack where a Signing Service or Private Key associated with the Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.
- **Technically Constrained Subordinate CA Certificate --** a Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate MAY issue Subscriber or additional Subordinate CA Certificates**.**
- **Terms of Use** – Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
- **Test Certificate** – A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID (2.23.140.2.1), or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.
- **TimeStamp Authority –** a service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via secure hashing algorithm) existed at the specific time. If the TimeStamp Authority is delegated to a third party, the CA is responsible that the delegated authority complies with the CAB Code Signing Requirements.
- **Transport Layer Security (TLS)/Secure Socket Layer (SSL) –** a security protocol that is widely used in the Internet, for the purpose of authentication and establishing secure sessions
- **Trusted Role –** An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over CA Operations.
- **Wildcard Domain Name** – A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

1.6.2 Acronyms

Term	**Definition**
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTL	Time to Live

1.6.3 References

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”)

Digital Signature Standard, FIPS 186-4 (http://csrc.nist.gov/publications/pubsfips.html).

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

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

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

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

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

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

WebTrustforCertificationAuthorities,SSLBaselinewithNetworkSecurity,Version2.0,available at http://www.webtrust.org/homepage-documents/item79806.pdf.

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

1.6.4 Conventions

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

A public Repository of CA information and associated policy documents is located at https://www.microsoft.com/pkiops/docs/repository.htm.

2.2 PUBLICATION OF INFORMATION

A web-based repository is available to all Relying Parties who wish to access to this CPS and other information from Microsoft PKI Services. The repository SHALL contain the current versions of this CPS and accompanying CP, a fingerprint of the established Root CAs, current CRLs, qualified Auditor Reports, Subscriber and Relying Party Agreements, a Privacy Statement, and other Terms of Use information.

The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

2.3 TIME OR FREQUENCY OF PUBLICATION

The CA SHALL annually review their CP and CPS and compare it with the CAB Forum's Baseline Requirements and EV Guidelines for any modifications.

Updates SHALL be published annually, in accordance with Section 1.5, and the document version number SHALL be incremented to account for the annual review and potential content revisions.

New versions of this CPS and respective CP documents will become effective immediately for all participants listed in Section 1.3.

The CA offers CRLs showing the revocation of Microsoft PKI Services Certificates and offers status checking through the online repository. CRLs will be published in accordance with Section 4.9.6 and Section 4.9.7.

2.4 ACCESS CONTROLS ON REPOSITORIES

CAs SHALL not limit access to this CP, their CPS, Certificates, CRLs and Certificate status information. CAs SHALL however implement controls to prevent unauthorized adding, modifying or deleting of repository entries.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Type of Names

Certificates SHALL be issued in accordance with the X.509 standard. CA Certificates SHALL generate and sign certificates containing a compliant distinguished name (DN) in the Issuer and Subject name fields; the DN MAY contain domain component elements. The Subject Alternative Name (SAN) MAY be used. Naming values for EV SSL, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform with the governing CA/Browser Forum Guidelines published at www.cabforum.org. The certificate profiles for specifying names SHALL conform with requirements in Section 7.

3.1.2 Need for Names to be Meaningful

Distinguished names SHALL 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.

3.1.3 Anonymity or Pseudonymity of Subscribers

No Stipulation

3.1.4 Rules for Interpreting Various Name Forms

No Stipulation

3.1.5 Uniqueness of Names

No Stipulation

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Application or Certificate Request that infringes upon the intellectual property rights of entities outside of their authority.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The Registration and/or Issuance process SHALL involve procedures in which the Applicant demonstrates possession of the Private Key by using a self-signed PKCS#10 request, an equivalent cryptographic mechanism, or a different method approved by the CA.

3.2.2 Authentication of Organization and Domain Identity

The CA SHALL verify the identity of an organization or domain, and the Applicant's authority to request Certificates on behalf of the organization or domain, in accordance with procedures set forth in this CPS and the CAB Forum's Baseline Requirements.

If an Applicant requests an Extended Validation (EV) or a Code Signing Certificate, the CA SHALL conform to the CAB Forum's respective EV Guidelines.

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third-party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or

4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant’s identity and address.

Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

3.2.2.2 DBA/Tradename

If the Subject Identity information includes a DBA or tradename, the CA SHALL use the same verification procedures and criteria as in Section 3.2.2.1 to verify the Applicant’s right to use the DBA/tradename.

3.2.2.3 Verification of Country

If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using any method in Section 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

The CA SHALL confirm that, before a Certificate gets issued, the Fully-Qualified Domain Name (FQDN) and/or its accompanying Domain Namespace MUST be validated for use in the Certificate by one or more of the below sections’ methods. The validation process must be initiated within the allowed time-period specified in the relevant requirement, such as Section 3.3.1 of this CPS.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

- The CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, OR
- The CA authenticates the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR
- The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names. For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The

Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

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

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

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

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

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

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

Confirming the Applicant's control over the FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space. For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or

2. The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

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

Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M sha256sum <r2.csr | sed "s/[-]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with Section 3.2.2.5.

Note: Note: Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9 Test Certificate

Confirming the Applicant's control over the FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorization Domain Name and which is accessible by the CA via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.10 TLS Using a Random Number

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by the CA via TLS over an Authorized Port.

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

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

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

No Stipulation

3.2.2.6 Wildcard Domain Validation

No Stipulation

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

The criteria for this evaluation SHOULD include:

1. The age of the information provided
2. The frequency of updates to the information source
3. The data provider and purpose of the data collection
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.2.

3.2.2.8 CAA Records

This section is effective as of 8 September 2017.

As part of the issuance process, Microsoft PKI Services MUST check for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued, as specified in the procedures of RFC 6844 as amended by Errata 5065 (Appendix A). If Microsoft PKI Services issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

This stipulation does not prevent Microsoft PKI Services from checking CAA records at any other time.

When processing CAA records, Microsoft PKI Services MUST process the issue, issuewild, and iodef property tags as specified in RFC 6844, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported but MUST NOT conflict with or supersede the mandatory property tags set out in this document. Microsoft PKI Services MUST respect the critical flag and not issue a Certificate if they encounter an unrecognized property with this flag set.

RFC 6844 requires that Microsoft PKI Services "MUST NOT issue a certificate unless either (1) the Certificate request is consistent with the applicable CAA Resource Record set or (2) an exception specified in the relevant Certificate Policy or Certification Practices Statement applies."

Microsoft PKI Services MAY decide to not rely on any exceptions specified in their CP or CPS unless they are one of the following:

- CAA checking is optional for Certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
- CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
- CAA checking is optional if Microsoft PKI Services or associated Affiliate is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

Microsoft PKI Services is permitted to treat a record lookup failure as permission to issue if:

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

Microsoft PKI Services MUST document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. URL schemes in the iodef record other than mailto: or https: are not supported.

3.2.3 Authentication of Individual Identity

No Stipulation

3.2.4 Non-Verified Subscriber Information

No Stipulation

3.2.5 Validation of Authority

Validation of authority (i.e. the determination of whether an Applicant or Subscriber has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate) is the responsibility of the Issuing CA or CA-appointed Registration Authorities (RA). Validation procedures SHALL be conducted as described in the Issuing CA's CPS document and in accordance to the CAB Forum's Baseline Requirements and EV Guidelines.

3.2.6 Criteria for Interoperation or Certification

The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

CAs SHALL treat certificate re-key requests identical to applications for new certificates and perform the same identity-proofing processes as described in Section 3.2.2. Routine re-key of the CA Certificates SHALL be performed in accordance with the established Key Generation process in Section 6.1 of this CPS.

Re-keys of Extended Validation Subscriber Certificates require no additional verification, provided that the data used to support issuance complies with Section 11.14 of the Guidelines for the Issuance and Management of Extended Validation Certificates.

3.3.2 Identification and Authentication for Re-Key After Revocation

Revoked or Expired Certificates SHALL require a new enrollment. Applicants MUST submit a new Certificate Request and be subject to the same Identification and Authentication requirements as first-time Applicants, as specified in Section 3.2.2 of this CPS.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

A Certificate Revocation Request that is submitted electronically MAY be authenticated and approved, providing the request comes from the subscriber or an approved authority. The identity of the person or end-entity submitting a revocation request in any other manner SHALL be authenticated per Section 3.2.2.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

No individual or entity listed on a government denied list, list of prohibited persons or other list that prohibits doing business with such organization or person under the laws of the United States may submit an application for a Certificate.

Applicants or authorized Certificate Requestors who are not included in any of the previous lists MAY submit a Certificate Application provided the Certificate Request meets the requirements set forth in the CP, this CPS, and the CA/Browser Forum's Baseline Requirements and EV Guidelines published at www.cabforum.org.

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

4.1.2 Enrollment Process and Responsibilities

Prior to the issuance of a Certificate, an Applicant SHALL undergo an enrollment process which, at minimum, includes:

1. Completing and submitting a digitally signed Certificate Request;
2. Consenting to a Subscriber Agreement, which MAY be an electronic acknowledgement;
3. Paying any applicable fees.

Certificate Applicants are required to fully comply with the requirements for the requested products prior to Certificate issuance.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

Certificate Applications are reviewed and processed, per the Identification and Authentication requirements in Section 3.2.2.

Certificate requests MAY be subject to additional verification activities, as outlined in documented procedures, prior to approving the request.

4.2.2 Approval or Rejection of Certificate Applications

Submitted Certificate applications MUST be reviewed and approved by the CA or appointed RA prior to issuance. Certificate Applications MAY be approved if the requirements of Section 3.2.2 and CAB Forum Requirements and Guidelines are met.

The Certificate Application MAY be rejected for any of, but not limited to, the following reasons:

- Applicant or Subscriber information is unable to be verified, per Section 3.2.2;
- The CA deems the certificate issuance MAY negatively impact the CA's business or reputation;
- Failure to consent to the Subscriber Agreement;
- Failure to provide Payment;
- Requests for EV Certificates contain entity information that are on a government deny list;
- The Certificate Request contains an internal name with a gTLD that ICANN has either announced or MAY consider making operational, per information from the following location: https://gtldresult.icann.org/application-result/applicationstatus/viewstatus.

The CA reserves the right to not disclose reasons for refusal.

EV Certificate requests SHALL be validated by Trusted Role personnel.

4.2.3 Time to Process Certificate Applications

Certification applications SHALL be processed within a commercially reasonable time frame. The CA SHALL not be responsible for processing delays initiated by the Applicant or from events outside of the CA's control.

4.2.4 Verification of CAA Records

Microsoft PKI Services supports CAA record checking, as described in Section 3.2.2.8. Subscribers who wish to authorize Microsoft PKI Services to issue Certificates for their FQDNs should include a CAA record property "issue" or "issuewild", which contains the value "microsoft.com" in their respective DNS zone.

Subscribers who already have CAA entries in their respective DNS zone and need a Certificate from Microsoft PKI Services must add a CAA record property "issue" or "issuewild", which includes the value "microsoft.com".

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

The source of the Certificate Request SHALL be verified before issuance. Certificates are generated, issued and distributed only after the CA or RA performs the required identification and authentication steps in accordance with Section 3. Certificates SHALL be checked to ensure that all fields and extensions are properly populated. Exceptions to defined Certificate Policies MUST be approved by the Microsoft PKI Policy Authority.

4.3.2 Notification of Certificate Issuance

Upon issuance, Subscribers SHALL be notified via an email or another agreed upon method, with information about the issued Certificate.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

A Subscriber's receipt of a Certificate and subsequent use of the Certificate and its key pair constitutes Certificate acceptance. It is the sole responsibility of the Subscriber to install the issued Certificate on their designated system.

4.4.2 Publication of the Certificate by the CA

Certificates SHALL be published in the Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the Public Key in the Certificate SHALL only be permitted once the Subscriber has agreed to the Subscriber agreement and accepted the Certificate.

Subscribers and CAs SHALL use their Private Keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the Certificates issued to them.

Subscribers SHALL protect their Private Keys from unauthorized use and discontinue use of the Private Key following expiration or revocation of the Certificate.

Subscribers SHALL contact the issuing entity if the Private Key is compromised.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties SHALL use Public Key certificates and associated Public Keys for the sole purposes as constrained by the CP or this CPS and Certificate extensions (such as key usage, extended key usage, certificate policies, etc.) in the Certificates. Relying Parties are subject to the terms of the Relying Party Agreement on the public repository and responsibly verify the validity of the Certificate, including revocation status, prior to trusting any Certificate.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

Subscribers are responsible for the renewal of Certificates to maintain service continuity.

4.6.2 Who May Request Renewal

Certificate Renewals MAY be requested by the Subscriber or an authorized agent, providing the Renewal Request meets the requirements set forth in this CPS, the governing CP, and the CA/Browser Forum's Baseline Requirements and EV Guidelines published at www.cabforum.org.

4.6.3 Processing Certificate Renewal Requests

Renewal requests follow the same validation and authentication procedures as a new Certificate Request and MAY re-use the information provided with the original Certificate Request, for means of verification. If for any reason re-verification fails, the certificate SHALL not be renewed and be subject to new key generation, in accordance with Section 6.1.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

Certificate Renewals SHALL follow the same notification method as a new certificate, in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of Renewal Certificate

Certificate Renewals SHALL follow the same acceptance method as a new certificate, in accordance with Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Certificate Renewals SHALL follow the same publication method as a new certificate, in accordance with Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate notifications to other entities SHALL follow the same entity notification method as a new certificate, in accordance with Section 4.4.3.

4.7 CERTIFICATE RE-KEY

CAs SHALL treat certificate re-key requests identical to applications for new certificates and perform the same identity-proofing processes, as described in Section 3.2.2, and the same acceptance methods, as described in Section 4.4. Routine re-key of the CA certificates SHALL be performed in accordance with the established key generation process of Section 6.1 in this CPS.

4.7.1 Circumstance for Certificate Re-Key

No Stipulation

4.7.2 Who May Request Certification of a New Public Key

No Stipulation

4.7.3 Processing Certificate Re-Key Requests

No Stipulation

4.7.4 Notification of New Certificate Issuance to Subscriber

No Stipulation

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No Stipulation

4.7.6 Publication of the Re-keyed Certificate by the CA

No Stipulation

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation

4.8 CERTIFICATE MODIFICATION

Modification to an issued Certificate’s details is not permitted. The certificate MUST first be revoked, core subscriber information must remain the same (domain name, DUNS/SSN, etc.), and only inconsequential information must have changed (email address, phone number, etc), before modifications to the Subscriber information are allowed. The replacement certificate doesn’t require the same identity and authentication procedures as a new Applicant (as in Section 4.2.1) and SHALL be issued with new validity dates.

4.8.1 Circumstance for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

No stipulation

4.8.3 Processing Certificate Modification Requests

No stipulation

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation

4.8.6 Publication of the Modified Certificate by the CA

No stipulation

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

The CA SHALL revoke Subscriber or Subordinate CA Certificates if one or more of the following circumstances occur:

1. Certificate revocation is requested in writing and in accordance with Section 4.9.3;
2. The CA acquires evidence that the Certificate or key pairs were compromised or misused.
3. The Subscriber can be shown to have violated obligations under the Subscriber Agreement;
4. The CA is notified that the original Certificate request was not authorized and does not grant retroactive authorization;
5. The Natural Person Subscriber has been terminated or the organization goes out of business;
6. The Issuing or Subordinate CA ceases operation for any reason and has not arranged for another CA to provide revocation support for the Certificate;
7. The Issuing or Subordinate CA's right to issue Certificates has expired, is revoked or terminated, unless the CA arranged to continue maintaining the CRL/OCSP Repository;
8. Any information in the certificate is inaccurate, not legally permitted, or presents an unacceptable risk to Microsoft, Relying Parties, or Application Software Suppliers;
9. Revocation is required per guidelines in this CPS;
10. The Certificate was not issued in accordance with this CPS, CP, corresponding CAB Guidelines, or other arising factors per applicable laws or regulations.

4.9.1.1 Reasons for Revoking a Subscriber Certificate

A Subscriber Certificate SHALL be revoked within 24 hours if any of the circumstances in Section 4.9.1 or additional items specified in the CAB Forum Baseline Requirements and EV Guidelines occur.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

A Subordinate CA Certificate SHALL be revoked within seven (7) days if one or more of the circumstances in Section 4.9.1 or additional items specified in the CAB Forum Baseline Requirements and EV Guidelines occur.

4.9.2 Who Can Request Revocation

Certificate revocations MAY be requested from the authorized Subscribers, RAs, or the CA. Third parties MAY also submit Certificate Problem Reports to the Issuing CA, if one or more of the circumstances in 4.9.1 occur that suggests reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

The CA MAY process revocation requests using at least the following steps:

1. CA SHALL log the identity of the entity submitting the request or Certificate Problem Report and the reason for requesting revocation; to include, CA's reasons for revocation;
2. CA MAY request authorization of the revocation request from the Subscriber or designated contact;
3. CA SHALL authenticate the entity making the request, per Section 4.9.2;
4. If a request is received from a third party, CA personnel SHALL initiate an investigation within 24 hours of receipt of the request to determine if a revocation is applicable, based the criteria in Section 4.9.5;
5. CA SHALL verify the requested revocation reason aligns with those in Section 4.9.1.1 or 4.9.1.2;
6. If CA determines that revocation is appropriate; CA personnel MAY revoke the certificate and update the CRL.

CA SHALL maintain a 24x7 availability to internally respond to any high priority revocation requests. If appropriate, CA MAY forward complaints to law enforcement.

Instructions for requesting a revocation is provided in the PKI Repository.

4.9.4 Revocation Request Grace Period

Subscribers are required to request revocation within a commercially reasonable amount of time after detecting the loss or compromise of the Private Key (within 24 hours is recommended).

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocation requests SHALL initiate an investigation within 24 business hours of receiving the request.

CAs and/or RAs SHALL consider whether revocation or other actions are warranted based on at least following criteria:

1. The entity submitting the complaint;
2. The nature of the alleged problem;
3. The number of reports received about a certain Certificate or Subscriber problem; or
4. Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties SHALL verify a Certificate's validity and revocation status prior to relying on the Certificate.

4.9.7 CRL Issuance Frequency

The CA SHALL post new CRL entries, as soon as a revocation request is fulfilled.

Subscriber Certificate CRLs SHALL be updated and issued at least once every seven (7) days and record the date and time of the transaction in the CRL's *ThisUpdate* field. The CRL's *NextUpdate* field value identifies the point in time when the CRL expires and MUST NOT be more than ten (10) days after the value of the *ThisUpdate* field.

CRLs for Subordinate CA Certificates SHALL be updated and issued at least once every twelve (12) months, within 24 hours after revoking a Subordinate CA Certificate, and the CRL's *NextUpdate* field value MUST NOT be more than twelve (12) months after the value of the *ThisUpdate* field.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable amount of time after generation.

CRL responses for an EV certificate chain MUST be downloaded in three (3) seconds or less over an analog telephone line under normal operating conditions.

4.9.9 On-Line Revocation/Status Checking Availability

In accordance with RFC6960 and/or RFC5019, CAs MUST ensure that OCSP responses are signed by one of the following:

1. The Issuing CA of the Certificate whose revocation status is being checked, or
2. An OCSP Responder whose Certificate is signed by the Issuing CA of the Certificate whose revocation status is being checked.
    a. In this instance, the OCSP signing Certificate MUST contain an extension type of id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

The CA SHALL support an OCSP capability using the GET method for certificates issued in accordance with RFC 6960 and CA/Browser Forum Baseline Requirements.

For the status of Subscriber Certificates: The CA SHALL update information via OCSP at least every four (4) days and the responses from this service MUST have a maximum expiration time of ten (10) days.

For the status of Subordinate CA Certificates: the CA SHALL update information via OCSP at least (i) every twelve (12) months and (ii) within twenty-four (24) hours after revoking a Subordinate CA Certificate.

An OCSP responder that receives a request for status of a certificate which has not been issued, SHOULD NOT respond with a "good" status. The CA SHOULD monitor the responder for such requests as part of its security response procedures.

OCSP responders for CAs that are not Technically Constrained, per Section 7.1.5, MUST NOT respond with a "good" status for such certificates.

4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation

4.9.12 Special Requirements Related to Key Compromise

See Section 4.9.1

4.9.13 Circumstances for Suspension

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

No Stipulation

4.10.2 Service Availability

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

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

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

4.10.3 Optional Features

No Stipulation

4.11 END OF SUBSCRIPTION

Certificate Subscriptions end when the certificate has either been revoked or expires.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

The CA SHALL develop, implement, and maintain a comprehensive security program which includes an annual Risk Assessment that:

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

Based on the outcome of the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and cost of implementing the specific measures and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 Site Location and Construction

CA and RA operations are conducted within physically protected environments designed to detect and prevent unauthorized use or disclosure of, or access to sensitive information and systems. The CA maintains multiple business resumption facilities for CA and RA operations. Business resumption facilities are protected with comparable physical and logical security controls. Business resumption facilities are at geographically disparate locations, so that operations MAY continue if one or more locations are disabled.

5.1.2 Physical Access

CA facilities are protected from unauthorized access, through the required use of multi-factor authentication solutions. Facility security systems electronically log ingress and egress of authorized personnel.

Physical access to cryptographic systems, hardware, and activation materials are restricted by multiple access control mechanisms, which are logged, monitored, and video recorded on a 24x7 basis.

5.1.3 Power and Air Conditioning

CA facilities are equipped with redundant power and climate control systems to ensure continuous and uninterrupted operation of CA systems.

5.1.4 Water Exposures

Commercially reasonable safeguards and recovery measures have been taken to minimize the risk of damage from water exposure.

5.1.5 Fire Prevention and Protection

Commercially reasonable fire prevention and protection measures are in place to detect and extinguish fires and prevent damage from exposure to flames or smoke.

5.1.6 Media Storage

Media containing production software, data, audit, and archival backup information SHALL be securely stored within facilities with appropriate physical and logical access controls, consistent with Sections 5.1.2 – 5.1.5, that prevent unauthorized access and provide protection from environmental hazards.

5.1.7 Waste Disposal

Sensitive waste material or PKI information SHALL be shredded and destroyed by an approved service. Removable media containing sensitive information SHALL be rendered unreadable before secure disposal. Cryptographic devices, smart cards, and other devices that may contain Private Keys or keying material SHALL be physically destroyed or zeroized in accordance with the manufacturers' waste disposal guidelines.

5.1.8 Off-Site Backup

Alternate facilities have been established for the storage and retention of PKI systems/data backups. The facilities are accessible by authorized personnel on a 24x7 basis with physical security and environmental controls comparable to those of the primary CA facility.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Trusted Roles consist of vetted and approved employees, contractors, or consultants that require access to or control over the CA's PKI operations. Trusted Role positions are subject to a clearly defined set of responsibilities that maintain a strict "separation of duties"; such that, no single person is able to perform both validation duties and certificate issuance fulfillment without a secondary review by another "trusted" team member. The personnel considered for Trusted Role positions MUST successfully pass the screening and training requirements of CPS Section 5.3. Trusted Role positions MAY include, but are not limited to, system administrators, operators, engineers, and certain executives who are designated to oversee CA operations.

Personnel responsible for CA key management, certificate issuance, and management of CA system functions are considered to serve in "Trusted Roles".

5.2.2 Number of Individuals Required per Task

The CA Private Key SHALL be backed up, stored, and recovered only by at least two persons in Trusted Roles using at least dual control (mechanisms) in a physically secured environment.

Systems used to process and approve EV Certificate Requests MUST require actions by at least two persons in Trusted Roles before creating an EV Certificate.

Systems used to process and approve EV Code Signing Certificate and EV Signature requests MUST require actions by at least two persons in Trusted Roles before creating an EV Code Signing Certificate or EV Signature.

5.2.3 Identification and Authentication for Trusted Roles

Individuals in a Trusted Role position SHALL be authorized by management to perform CA or RA duties and MUST satisfy the Personnel Controls requirements specified in Section 5.3.

5.2.4 Roles Requiring Separation of Duties

To ensure a separation of duties, as described in Section 5.2.1, PKI responsibilities relating to access, operations, and audit MUST be performed by separate Trusted Roles.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The CA verifies the identity and trustworthiness of all personnel, whether as an employee, agent, or an independent contractor, prior to the engagement of such person(s).

Any personnel occupying a Trusted Role, as defined in 5.2.1, must possess suitable experience and be deemed qualified. Personnel in Trusted Roles shall undergo training prior to performing any duties as part of that role.

5.3.2 Background Check Procedures

Prior to assignment in a Trusted Role position, the prospective CA personnel SHALL undergo and clear the necessary background checks or security screenings requirements, per CA hiring policies, CAB Guidelines, and local laws.

5.3.3 Training Requirements and Procedures

All CA personnel performing information verification duties SHALL receive skills-training and pass an examination prior to commencing their job role that includes:

1. Basic Public Key Infrastructure knowledge,
2. Authentication and vetting policies and procedures (including the CA's CP and CPS),
3. Common threats to the information verification process (including phishing and other social engineering tactics),
4. CA/Browser Forum Guidelines,
5. Applicable functions of the CA's PKI system relative to their assigned Trusted Role

The CA SHALL document records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

5.3.4 Retraining Frequency and Requirements

Trusted Role personnel SHALL receive periodic training to maintain competency with the CA's PKI-related operations and regulatory changes.

The CA SHALL maintain records of all training taken by Trusted Role personnel.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

In accordance with the CA's HR policies, appropriate disciplinary actions SHALL be taken for unauthorized actions or other violations of PKI policies and procedures.

5.3.7 Independent Contractor Controls

The CA MAY employ contractors, as necessary. Contractors SHALL adhere to background checks, training, skills assessment, and audit requirements, as appropriate for their role.

5.3.8 Documentation Supplied to Personnel

CA PKI personnel are required to read this CPS and CP. They are also provided with PKI policies, procedures, and other documentation relevant to their job functions.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

The CA SHALL maintain controls to provide reasonable assurance that significant CA environmental, key management, and certificate management events are accurately and appropriately logged.

The CA and each Delegated Third Party SHALL record details of the actions taken to process a Certificate Request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate Request; the date and time; and the personnel involved. The CA SHALL make these records available to Qualified Auditors, as proof of CA's compliant practices.

The CA SHALL record at least the following events:

1. CA key lifecycle management events, to include: a. Key generation, backup, storage, recovery, archival, and destruction; and b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, to include: a. Certificate requests, renewal, and re-key requests, and revocation; b. All verification activities

stipulated in these Requirements and the CA’s Certification Practice Statement; c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls; d. Acceptance and rejection of Certificate Requests; e. Issuance of Certificates; and f. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, to include: a. Successful and unsuccessful PKI system access attempts; b. PKI and security system actions performed; c. Security profile changes; d. System crashes, hardware failures, and other anomalies; e. Firewall and router activities; and f. CA facility ingress and egress.

Log entries MUST include the following elements:

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

5.4.2 Frequency for Processing and Archiving Audit Logs

Audit logs are reviewed on an as-needed basis.

5.4.3 Retention Period for Audit Logs

Audit logs SHALL be retained for a period of at least seven (7) years and made available to the CA’s Qualified Auditor upon request.

5.4.4 Protection of Audit Log

Audit logs are protected from unauthorized viewing, modification, deletion, or other tampering using a combination of physical and logical security access controls.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up and archived in accordance with business practices.

5.4.6 Audit Log Accumulation System (Internal vs. External)

No Stipulation

5.4.7 Notification to Event-Causing Subject

No Stipulation

5.4.8 Vulnerability Assessments

The CA MUST maintain detection and prevention security controls to safeguard Certificate Systems against potential threats or vulnerabilities.

Vulnerability assessments and penetration testing on the CA environment SHALL at least be performed in accordance with the CAB Forum Baseline Requirements, EV Guidelines, and Section 4 of the Network Security Requirements.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

The CA SHALL maintain archived backups of application and system data. Archived information MAY include, but are not limited to, the following:

- Audit data, as specified in Section 5.4
- Data related to Certificate requests, verifications, issuances, and revocations
- CA policies, procedures, entity agreements, compliance records,
- Cryptographic device and key life cycle information
- Systems management and change control activities

5.5.2 Retention Period for Archive

CA SHALL retain all documentation relating to a Certificate's activities for a period of at least seven (7) years after the Certificate ceases to be valid.

5.5.3 Protection of Archive

Archives of relevant records are secured using a combination of physical and logical access controls at both the primary and backup locations. Access is restricted to authorized personnel and SHALL be maintained for the period of time specified in Section 5.5.2.

5.5.4 Archive Backup Procedures

Adequate backup procedures SHALL be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a feasible period of time.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other database entries shall contain time and date information.

5.5.6 Archive Collection System (Internal or External)

The CA SHALL employ appropriate systems for the collection and maintenance of archived records.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized CA personnel SHALL have access to primary and backup archives. The CA MAY, at its own discretion, release specific archived information, following a formal request from a Subscriber, a Relying Party, or an authorized agent thereof.

5.6 KEY CHANGEOVER

No Stipulation

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

All CA organizations SHALL have formal Incident Response, Disaster Recovery, and/or Business Continuity Plans that contain documented procedures to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. Business Continuity and Security Plans do not have to be publicly disclosed, but the CA SHALL make them available to auditors upon request and annually test, review, and update the procedures.

The Business Continuity Plan SHALL align with the requirements of the CAB Forum's Baseline Requirements and EV Guidelines.

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

See Section 5.7.4.

5.7.3 Recovery Procedures After Key Compromise

The CA's business continuity plan contains the procedures to address incidents in which a CA Private Key is suspected to be or has been compromised. Upon thorough investigation, appropriate actions will be taken to revoke and generate new key pairs, notify affected Subscribers, and coordinate revoking and reissuing the affected certificates.

5.7.4 Business Continuity Capabilities After a Disaster

In the event of a disaster, the CA has established and maintains business continuity capabilities to address the recovery of PKI services in the event of critical interruptions or outages with CA operations. The recovery procedures align with those identified in Section 5.7.1.

5.8 CA OR RA TERMINATION

In the event that it is necessary to terminate the operation of a CA, CA management will plan and coordinate the termination process with its Subscribers and Relying Parties, such that the impact of the termination is minimized. The CA will make a commercially reasonable effort to provide prior notice to Subscribers and Relying Parties and preserve relevant records for a period of time deemed fit for functional and legal purposes.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The CA SHALL have effective practices and controls in place to reasonably assure that the generation of Root and Subordinate CA key pairs are performed in a physically secured environment, using cryptographic modules that meet the requirements of Section 6.2, by multiple

Trusted Role personnel, following a prepare generated script, and either witnessed in-person or validated from a recorded video of the ceremony by a Qualified Auditor.

6.1.1.2 RA Key Pair Generation

No Stipulation

6.1.1.3 Subscriber Key Pair Generation

The Subscriber MAY generate their own key pairs, in accordance to the requirements set forth in Section 6.1.5 and 6.1.6. If the Subscriber does not adhere to these requirements or has a known weak Private Key, the CA SHALL reject the Certificate Request.

6.1.2 Private Key Delivery to Subscriber

If a Subscriber generates their own key pairs, Private Key delivery is not performed. In the event the CA is authorized to generate a Private Key on behalf of a Subscriber, the Private Key will be encrypted prior to transporting to the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

No Stipulation

6.1.4 CA Public Key Delivery to Relying Parties

No Stipulation

6.1.5 Key Sizes

Certificates issued under this CA hierarchy SHALL meet the following minimum requirements:

Root CA, Subordinate CA, and Subscriber Certificates

Key Algorithm	Values
Digest Algorithm	SHA-256, SHA-384, SHA-512
Minimum RSA Modulus Size (bits)	2048
ECC Curve	NIST P-256, P-384, OR P-512

Digital Signature Algorithm (DSA) key lengths (L and N) are described in the Digital Signature Standard, FIPS 186-4 (http://csrc.nist.gov/publications/pubsfips.html).

Certificate Key configurations SHALL conform with this CPS, the respective CP, and the CAB Forum’s Baseline Requirements and EV Guidelines.

6.1.6 Public Key Parameter Generation and Quality Checking

The CA SHALL generate Private Keys using secure algorithms and parameters based on current research and industry standards.

Quality checks for both RSA and ECC algorithms are performed on generated CA keys.

6.1.7 Key Usage Purposes

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

1. Self-signed Certificates to represent the Root CA;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

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

6.2.1 Cryptographic Module Standards and Controls

CA key pairs are generated and protected by validated FIPS 140-2 level 3 hardware cryptographic modules that meet industry standards for random and prime number generation.

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

The participation of multiple individuals in Trusted Role positions are required to perform sensitive CA Private Key operations (e.g., hardware security module (HSM) activation, signing operations, CA key backup, CA key recovery, etc.).

6.2.3 Private Key Escrow

No Stipulation

6.2.4 Private Key Backup

Backup copies of CA Private Keys SHALL be backed up by multiple persons in Trusted Role positions and only be stored in encrypted form on cryptographic modules that meet the requirements specified in Section 6.2.1.

6.2.5 Private Key Archival

No Stipulation

6.2.6 Private Key Transfer into or from a Cryptographic Module

No Stipulation

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.1

6.2.8 Activating Private Keys

Cryptographic modules used for CA Private Key protection utilize a smart card based activation mechanism by multiple Trusted Role personnel using multi-factor authentication.

6.2.9 Deactivating Private Keys

No Stipulation

6.2.10 Destroying Private Keys

CA Private Keys SHALL be destroyed when they are no longer needed or when the Certificates, to which they correspond, expire or are revoked. The destruction process shall be performed by multiple Trust Role personnel and documented using verifiable methods.

6.2.11 Cryptographic Module Capabilities

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

Copies of CA and Subscriber certificates and Public Keys SHALL be archived in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For Certificates issued after the publication of this CPS, the following key and certificate operational periods SHALL be deployed.

Entity Type	Maximum Certificate Validity Period
Root CA	25 Years
Subordinate CAs	20 Years
Subscribers	Issued between 7/1/2016 – 3/1/2018 = 39 months Issued after March 1, 2018 = 825 days

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

CA shall protect activation data from compromise or disclosure. Appropriate cryptographic and physical access controls shall be implemented to prevent unauthorized use of any CA Private Key activation data.

6.4.2 Activation Data Protection

No Stipulation

6.4.3 Other Aspects of Activation Data

No Stipulation

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

CA systems SHALL be secured from unauthorized access using multi-factor authentication security controls.

6.5.2 Computer Security Rating

No Stipulation

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

No Stipulation

6.6.2 Security Management Controls

No Stipulation

6.6.3 Life Cycle Security Controls

No Stipulation

6.7 NETWORK SECURITY CONTROLS

CA systems SHALL reside in highly segmented networks constrained from both the Internet and corporate networks via multiple levels of firewalls. Interaction with outside entities shall only be performed with servers located in a demilitarized zone (DMZ). All networks associated with CA operations SHALL be monitored by a network intrusion detection system. All systems associated with CA activities shall be hardened with services restricted to only those necessary for CA operations. Changes SHALL be documented and approved via a change management system. Logical and physical access to CA systems and facilities requires two trusted and qualified Microsoft employees.

6.8 TIME-STAMPING

Certificates, CRLs, and other revocation database entries SHALL contain time and date information.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

CA certificates SHALL be X.509 Version 3 format, conform to RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL profile, and adhere to the CAB Forum's Baseline Requirements and EV Guidelines.

7.1.1 Version Number(s)

CAs SHALL issue certificates that are compliant with X.509 Version 3.

7.1.2 Certificate Content and Extensions; Application of RFC 5280

The extensions defined for the CA's X.509 v3 certificates provide methods for associating additional attributes with users or Public Keys and for managing the certification hierarchy. Each extension in a certificate is designated as either critical or non-critical.

Certificate extensions, their criticality, and cryptographic algorithm object identifiers, are provisioned according to the IETF RFC 5280 standards and/or comply with CAB Forum Baseline Requirements and EV Guidelines.

7.1.2.1 Root CA Certificate

Root CAs SHALL ensure that the content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining, as specified in RFC 5280.

7.1.2.2 Subordinate CA Certificate

Subordinate CA Certificates MAY include extensions and values that are pertinent for their intended use, in accordance with this CPS and RFC 5280, and the CAB Forum's Baseline Requirements and EV Guidelines.

7.1.2.3 Subscriber Certificate

Subscriber Certificates MAY include extensions and values that are pertinent for their intended use, in accordance with this CPS, RFC 5280, and the CAB Forum's Baseline Requirements and EV Guidelines.

7.1.2.4 All Certificates

All other provisions MUST be set in accordance with RFC 5280 and/or CAB Forum Baseline Requirements and EV Guidelines, as appropriate.

7.1.2.5 Application of RFC 5280

The applicability of RFC 5280 SHALL be governed by the respective Requirements and Guidelines of the Internet Engineering Task Force (IETF) and the CA/Browser Forum (CAB Forum).

7.1.3 Algorithm Object Identifiers

No Stipulation

7.1.4 Name Forms

CAs SHALL issue Certificates with Name Forms in accordance with RFC 5280 and Section 3.1.1 of this CPS.

7.1.4.1. Issuer Information

No Stipulation

7.1.4.2. Subject Information – Subscriber Certificates

No Stipulation

7.1.4.2.1. Subject Alternative Name Extension

No Stipulation

7.1.4.2.2. Subject Distinguished Name Fields

No Stipulation

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in this CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1. Subject Distinguished Name Fields

No Stipulation

7.1.5 Name Constraints

CAs reserve the right to issue Certificates with Name Constraints and mark them as critical, where necessary. Unless otherwise documented in this CPS the use of Name Constraints SHALL conform with the X.509 V3 standard (RFC 5280) and the CAB Forum's Baseline Requirements and EV Guidelines.

7.1.6 Certificate Policy Object Identifier

CAs SHALL issue Certificates with policy identifiers set forth in Section 1.2 herein, and comply with the provisions of this CPS and the CAB Forum Baseline Requirements and EV Guidelines.

7.1.6.1 Reserved Certificate Policy Object Identifiers

No Stipulation

7.1.6.2 Root CA Certificates

No Stipulation

7.1.6.3 Subordinate CA Certificates

No Stipulation

7.1.6.4 Subscriber Certificates

No Stipulation

7.1.7 Usage of Policy Constraints Extension

No Stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation

7.2 CRL PROFILE

CRL Profiles comply with X.509 V3 standards.

7.2.1 Version Number(s)

No Stipulation

7.2.2 CRL and CRL Entry Extensions

No Stipulation

7.3 OCSP PROFILE

The profile for OCSP responses issued under this PKI System conforms to RFC 5019 and RFC 6960 standards.

7.3.1 Version Number(s)

No Stipulation

7.3.2 OCSP Extensions

No Stipulation

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

1. Be licensed as a CA in each jurisdiction of operation, where required, for the issuance of Certificates;
2. Operate its PKI and issue Certificates in accordance with all applicable laws and guidelines in every jurisdiction of operation;
3. Comply with the audit requirements set forth in this Section 8.
4. Comply with these requirements

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The CA must have an independent auditor annually assess the CA’s compliance to the stated requirements and practices of this CPS, the CP, and/or the CAB Forum’s Baseline Requirements and EV Guidelines. The results of the audit SHALL be provided in an Audit Report indicating compliance status with the applicable standards under the audit scheme herein.

Any changes to the CA business practices are subject to and SHALL require Self Audits, as described in Section 8.7. Any audit deficiencies SHALL be addressed and remedied, in accordance with Section 8.5. The annual audit SHALL include items mentioned in Section 8.4.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The CA SHALL have an annual audit conducted by an independent licensed Auditor that demonstrates proficiency in the criteria specified in Section 8.4 and maintains a Professional Liability/Errors, & Omissions insurance policy with a minimum coverage of one million US dollars.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The entity that performs the annual audit SHALL be completely independent of the CA.

8.4 TOPICS COVERED BY ASSESSMENT

Annual audits SHALL be performed by an independent certified Auditor that assesses the CA’s PKI operations in accordance with the stipulations documented in their CPS, the CP, applicable Auditors’ Principles and Criteria for Certification Authorities, and the CA/Browser Forum’s Baseline Requirements and EV Guidelines.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Deficiencies identified by the auditor during the compliance audit will determine the actions to be taken. The PKI Policy Authority is responsible for ensuring that remediation plans are promptly developed, documented, and corrective actions are taken within an adequate timeframe corresponding to the significance of identified matters.

8.6 COMMUNICATION OF RESULTS

Audit results are provided to the PKI Policy Authority, who will distribute to the necessary parties, as required. General audit findings that do not impact the overall audit opinion are not required to be publicized. The CA SHALL make the annual Audit Reports publicly available in the PKI repository referenced in Section 2.1.

8.7 SELF-AUDITS

The CA SHALL perform quarterly self-audits of its PKI business practices, in accordance with its CPS, the Microsoft PKI Services CP, and the respective CAB Forum Requirements and EV Guidelines.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

Microsoft reserves the right to charge Subscribers fees for Certificate issuance and renewals.

9.1.2 Certificate Access Fees

Microsoft PKI Services reserves the right to charge a fee for making a Certificate available in a repository or otherwise.

9.1.3 Revocation or Status Information Access Fees

Microsoft PKI Services does not charge a fee to Relying Parties for access to revocation or status information in accordance with Section 2.s. Microsoft PKI Services reserves the right to charge a fee for providing customized CRLs or other value-added revocation and status information services.

9.1.4 Fees for Other Services

Microsoft PKI Services does not charge a fee for accessing this CPS. However, any use of the CPS for purposes other than viewing the document, including reproduction, redistribution, modification, or creation of derivative works, may be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

Not Applicable

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Microsoft maintains insurance or self-insures in accordance with Section 9.2.1 of the CP.

9.2.2 Other Assets

Customers shall have access to sufficient financial resources to support operations and perform duties in accordance with the Microsoft PKI Services CP and shall be able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

Sensitive Microsoft PKI Services information shall remain confidential to Microsoft PKI Services. The following information is considered confidential to Microsoft PKI Services and may not be disclosed:

- Microsoft PKI Services policies, procedures and technical documentation supporting this CPS;
- Subscriber registration records, including: Certificate applications, whether approved or rejected, proof of identification documentation and details;
- Certificate information collected as part of the registration records, beyond that which is required to be included in Subscriber Certificates;
- Audit trail records;
- Any Private Key within the Microsoft PKI Services CA hierarchy; and
- Compliance audit results except for WebTrust for CAs audit reports which may be published at the discretion of Microsoft PKI Policy Authority.

9.3.2 Information Not Within the Scope of Confidential Information

This CPS, Certificates and CRLs issued by Microsoft PKI Services and any information that the CA has explicitly authorized to disclose are not considered confidential.

Microsoft may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to Microsoft a license to do so, including the right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf.

This Section 9.3.2 is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

Microsoft PKI Services PKI participants receiving private information shall secure it from compromise and disclosure to third parties.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Microsoft follows the governing principles established by the Microsoft privacy statement located at http://privacy.microsoft.com/en-us/default.aspx when handling personal information.

9.4.2 Information Treated as Private

Information about Subscribers that is not publicly available through the content of the issued Certificate and CRLs is treated as private.

9.4.3 Information Not Deemed Private

See Section 9.3.2.

9.4.4 Responsibility to Protect Private Information

See Section 9.3.3.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy, or by agreement, private information will not be used without the consent of the party to whom that information applies. This Section 9.4.5 is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Microsoft PKI Services shall be entitled to disclose Confidential/Private Information if, in good faith, Microsoft PKI Services believes that:

- Disclosure is necessary in response to subpoenas and search warrants
- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 INTELLECTUAL PROPERTY RIGHTS

The following are the property of Microsoft:

- This CPS;
- Policies and procedures supporting the operation of Microsoft PKI Services;
- Certificates and CRLs issued by Microsoft PKI Services managed CAs;
- Distinguished Names (DNs) used to represent entities within the Microsoft PKI Services CA hierarchy; and
- CA infrastructure and Subscriber key pairs.

Microsoft PKI Services PKI participants acknowledge that Microsoft PKI Services retains all Intellectual Property Rights in and to this CPS.

9.6 REPRESENTATIONS AND WARRANTIES

Microsoft PKI Services warrants and promises to provide certification authority services substantially in compliance with this CPS and the relevant Microsoft Certificate Policies. Microsoft PKI Services makes no other warranties or promises and has no further obligations to Subscribers or Relying Parties, except as set forth under this CPS.

9.6.1 CA Representations and Warranties

See Section 9.6

9.6.2 RA Representations and Warranties

See Section 9.6

9.6.3 Subscriber Representations and Warranties

See Section 9.6

9.6.4 Relying Party Representations and Warranties

See Section 9.6

9.6.5 Representations and Warranties of Other Participants

See Section 9.6

9.7 DISCLAIMERS OF WARRANTIES

Except for express warranties stated in this CPS, Microsoft PKI Services disclaims all other warranties, promises and other obligations. In addition, Microsoft PKI Services is not liable for any loss:

- To CA or RA services due to war, natural disasters or other uncontrollable forces;
- Incurred between the time a Certificate is revoked and the next scheduled issuance of a CRL;
- Due to unauthorized use of Certificates issued by Microsoft PKI Services, or use of Certificates beyond the prescribed use defined by this CPS;
- Arising from the negligent or fraudulent use of Certificates or CRLs issued by the Microsoft PKI Services; and
- Due to disclosure of personal information contained within Certificates, CRLs or OCSP responses.

9.8 LIMITATIONS OF LIABILITY

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE A CERTIFICATE, INCLUDING AS A RESULT OF (I) ANY TERMINATION OR SUSPENSION OF THIS AGREEMENT OR THE CPS OR REVOCATION OF A CERTIFICATE, (II) OUR DISCONTINUATION OF ANY OR ALL SERVICE OFFERINGS IN CONNECTION WITH THIS AGREEMENT, OR, (III) ANY DOWNTIME OF ALL OR A PORTION OF CERTIFICATE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (C) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO MICROSOFT'S CERTIFICATE SERVICES; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, MICROSOFT AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IN CONNECTION WITH

THIS AGREEMENT AND ALL CERTIFICATES ISSUED HEREUNDER, IS THE LESSER OF THE AMOUNT PAID BY YOU FOR THE CERTIFICATE(S) AT ISSUE OR THE AMOUNTS PAID FOR THE CERTIFICATE SERVICES FOR THE CERTIFICATE(S) AT ISSUE IN THE LAST TWELVE (12) MONTHS BEFORE THE CLAIM AROSE; PROVIDED, HOWEVER, THAT FOR ANY EV CERTIFICATE ISSUED UNDER THIS AGREEMENT EXEPT FOR AS EXPRESSLY EXCLUDED PER SECTION 8(c), OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IS LIMITED TO $2000 US DOLLARS PER SUBSCRIBER OR RELYING PARTY PER EV CERTIFICATE.

9.9 INDEMNITIES

9.9.1 Indemnification by CAs

See Section 9.9

9.9.2 Indemnification by Subscribers

To the extent permitted by law, Subscriber indemnifies Microsoft, Microsoft's partners, and any cross-signed entities, and their respective employees, directors, agents, and representatives from, and defend the indemnified parties against, any and all third party claims, including Relying Parties, to the extent arising from or related to: (a) Subscriber's failure to perform any of your warranties, representations, and obligations under this Agreement; (b) any omissions, falsehoods or misrepresentations of fact, regardless of whether the misrepresentation or omission was intentional or unintentional, Subscriber makes on the Certificate or in connection with this Agreement; (c) any infringement of an intellectual property right of any person or entity in information or content provided by Subscriber; (d) Subscriber's misuse of a Certificate or private key; or (e) failure to protect the private key, credentials, or use a trustworthy system, or to take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the private key under the terms of this Agreement. The CA and its RAs are not the agents, fiduciaries, trustees, or other representatives of Subscribers or Relying Parties.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, Relying Party indemnifies Microsoft, Microsoft's partners, and any cross-signed entities, and their respective employees, directors, agents, and representatives from, and any third-party Certificate Authority or RA providing services to Microsoft or any of its affiliates in relation to the Certificate and defend the indemnified parties against, any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by Microsoft or its affiliates and used by the Relying Party, the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a certificate or any constituent elements of it; or (iii) failure to check the certificate's status prior to use.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS becomes effective upon publication in the Repository.

This CPS, as amended from time to time, shall remain in force until it is replaced by a new version. Amendments to this CPS become effective upon publication in the Repository.

9.10.2 Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, participants are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Any notice, demand, or request pertaining to this CPS shall be communicated either using digitally signed messages consistent with this CPS, or in writing. Microsoft 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 Microsoft. 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. Microsoft may allow other forms of notice in its Subscriber Agreements.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Amendments to this CPS may be made by Microsoft PKI Services Service Manager and shall be approved by the Microsoft PKI Policy Management Authority as per Section 1.5.4.

9.12.2 Notification Mechanism and Period

No Stipulation

9.12.3 Circumstances under which OID must be changed

No Stipulation

9.13 DISPUTE RESOLUTION PROVISIONS

In the event of any dispute involving the services or provisions covered by this CPS, the aggrieved party shall notify a member of Microsoft PKI Policy Authority regarding the dispute. Microsoft PKI Policy Authority will involve the appropriate Microsoft personnel to resolve the dispute.

9.14 GOVERNING LAW

The laws of the state of Washington State govern the interpretation, construction, and enforcement of this CPS, including tort claims, without regard to any conflicts of law principles. The state or federal courts located in King County, Washington have nonexclusive venue and jurisdiction over any proceedings related to the CPS. Microsoft may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of our, our affiliates, or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply to this CPS.

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.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

Microsoft contractually obligates each RA to comply with this CPS and applicable industry guidelines. Microsoft 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 Microsoft. Unless specified otherwise in a contract with a party, Microsoft does not provide notice of assignment. This CPS shall be binding on all successors of the parties.

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. It is expressly agreed that every provision of this CPS that provides for a limitation of liability or exclusion of damages, disclaimer or limitation of any warranties, promises or other obligations, is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Microsoft may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Microsoft's failure to enforce a provision of this CPS does not waive Microsoft'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 Microsoft.

9.16.5 Force Majeure

Microsoft 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 Microsoft's reasonable control. The operation of the Internet is beyond Microsoft's reasonable control.

9.17 OTHER PROVISIONS

This CPS shall be interpreted consistently with what is commercially reasonable in good faith under the circumstances and considering its international scope and uniform application.