Microsoft DSR PKI

Certificate Policy/Certification Practice Statement For TLS CAs
(DSR CP/CPS)

Version 2.12
Effective Date: February 14, 2023

Change Control Log

Revision Date	Revision Reason	Revision Explanation	New Rev	Super-sedes	Revision By
12/16/2013	New	• Initial version documented	1.0	N/A	Microsoft IT
03/21/2014	Update	• Minor corrections to 7.1, 7.2	1.1	1.0	Microsoft IT
05/08/2014	Update	• Section 4.1 & 4.2 to include certificate request pre-approval workflow • Updated appropriate sections to include addition of OCSP service. OCSP service is expected to be in place on or before 30th May 2014. • Removed reference to PAIX • Minor updates in section 7.1	1.2	1.1	Microsoft IT
01/28/2015	Update	• Revise section 5.4.1 of the CP/CPS to clarify collected events	1.3	1.2	Microsoft IT
12/20/2016	Update	• Added of names and profiles of new SSL/TLS CAs • Updated maximum key usage and certificate validity period for Issuing CAs • Updated to remove reference to certificate	1.4	1.3	Microsoft IT

		issuance for short names, internal server names, and reserved IP address			
10/30/2017	Update	• Added info regarding verification of CAA records	1.5	1.4	Microsoft IT
04/16/2018	Update	• Removed references to deprecated SHA-1 CA • 1.6 – Multiple changes to definitions that were mostly cosmetic • 4.4.3 – Added reference to CT • 4.6.3 – Replace "last 39 months" with "800 days" • 5.1.1 – Removed references to physical location of servers • 5.1.6 – Replace "Corporate HBI" with "Microsoft Highly Confidential" • 5.2.1 – Expanded role definitions • 5.2.4 – Removed separation of duty requirement for activation materials • 6.3.2 – Maximum Key Usage Period for Certificate Signing changed to 8 years • 6.3.2 & 7.1 – Replaced end-entity certificate maximum validity to be 800 days instead of 2 years (or 24 months) • 7.1 – Clarified that the Signature Algorithm is SHA256RSA for multiple templates • 7.1.2.9 – Added reference to CT and pre-certificates • Replaced multiple instances of "SSL" with "TLS" • Replaced "Microsoft IT" with DSRE throughout entire document, including title. • Made some cosmetic changes throughout document	2.0	1.5	DSRE PKI Team
01/07/2019	Update	• 1.1 and 1.3.1 and 6.1.5 removed Microsoft IT SSL SHA2 CA • 3.2.3.2 Removed "any other method of confirmation" • 4.2.2 updated Approver for End-entity Certificate column	2.1	2.0	DSRE PKI Team

		to be more explicit on roles for approval • 5.2.1 Broke out roles by Trusted and Authorized • 6.7 removed physical location as all systems use same physical security now • 7.1 removed profile for SSL SHA-2 Issuing CA Certificate Profile and references to sanitized CDP and AIA locations in End Entity Certificate Profile • 9.4.1 update hyperlink to Microsoft Privacy statement			
3/15/2019	Update	• 3.2.3.2 removed relying on a domain authorization document	2.2	2.1	DSRE PKI Team
05/22/2019	Update	• 4.9.7 & 7.2 Updated CRL validity to not exceed 10 days	2.3	2.2	DSRE PKI Team
03/31/2020	Update	• 1 Added text that this CP relies on DigiCert CP and adheres to Mozilla Root Policy • 1.5.2 Replaced contact email • 3.2.3.2 Added domain validation process • 4.9.1 Updated revocation reasons and timeline based on BR 4.9.1.1 • 5.7.1 Added Bugzilla details for incidents • 6.1.5 Updated end-entity certificate requirement language based on Mozilla requirement • 7.1 Added serial number size requirements • 8.4 Added clarification to audit period language and Mozilla requirements • 9.11 Added notification details in case of merger or ownership change.	2.4	2.3	DSRE PKI Team
07/23/2020	Update	• 1 Specifically referenced the DigiCert CP OID • 1.1 Added new CA names and updated CA Type names • 1.3.1 Added new CA names • 3.2.3.2 Deleted text that had strikethrough • 6.1.5 Added new CA names	2.5	2.4	DSRE PKI Team

		• 7.1 Added new DV and OV templates for legacy and new CAs. Added new CA profiles. Corrected some older template language.				
10/22/2020	Update	• Cosmetic updates throughout document • 1.5.4 Clarified process for document review period • 2.3 Document version tracking clarification • 3.3.2 Updated to reference §3.2 • 3.4 Added missing section • 4.2.4 Corrected CAA record value and updated process • 4.9.10 Updated On-Line Revocation Checking • 4.10 Updated to reference §4.9.6 - §4.9.9 • 5.2.1 Added PRSS team as Trusted Role • 5.2.3 Updated and added reference to §5.3 • 5.5.4 and 5.5.6 added detail about backup system and processes • 6.2.2 Update definitions for m and for n because they were reversed • 6.3.2 Clarification to explain that we reduced the validity period • 7.1.4.1 Update to Name Encoding • 7.2.2 CRL extension details added • 7.3.2 Clarify OCSP Extensions • 9.4.7 Added missing section	2.6	2.5	DSRE PKI
03/5/2021	Update	• 1 Removed reference to DigiCert CPS and kept the reference to DigiCert CP • 1.1 Removed references to decommissioned CAs • 1.3 Removed references to decommissioned CAs • 4.2.4 Removed DNS Operator exemption from CAA check • 6.1.5 Removed references to decommissioned CAs	2.7	2.6	DSRE PKI

		• 6.3.2 Reduced Periods to match Microsoft Corporate Policy • 7.1 Removed templates that were retired with the recent CA infrastructure retirement • 7.1.2.1 Key Usage SHALL be marked as critical			
04/29/2021	Update	• 3.2.2 Added validation re-use details. Added statement that IP addresses are not supported in certificates. • 4.6.3 Removed extraneous details that were already covered in 3.2.2 • 4.9.12 Expanded description for handling key compromise, including adding details for how to prove key compromise • Replaced multiple references of old DSRE org name and changed to DSR • Modified multiple references of numbers to represent a consistent formatting	2.8	2.7	DSR PKI Team
03/01/2022	Update	• Various grammatical and formatting corrections • 1.3.5 Updated CST to CSPA due to organizational name change • 1.4.1 Removed MSIT reference • 1.6 Updated CAA RFC reference • 3.4 Corrected section reference • 4.2.4 Updated CAA RFC reference • 4.9.7 Updated CRL publication frequency to 7 days to align with BRs • 4.9.9 Updated to align with BRs and remove redundant information covered in later sections • 4.10.1 Updated revocation response removal information to align with BRs • 4.10.2 Added additional Service Availability information • 5.4.3 Updated retention periods to align with updated BRs	2.9	2.8	DSR PKI Team

Date	Type	Changes	New	Old	Author
		• 5.5.2 Added information on archive retention period due to updates in 5.4.3 negating the existing section reference • 6.2.1 Removed non-applicable information regarding subscriber keys • 6.2.8 Removed non-applicable information regarding subscriber keys • 6.3.2 Increased Maximum Key Usage Period For Certificate Signing from 3 to 4 years • 7.1 Removed references to IP Addresses as IP Address subjects are not supported by DSR PKI TLS CAs, Clarified that subscriber keys may be larger than 2048 bits • 7.1.2.3 Removed IP Addresses as supported SANs • 7.2.2 Updated CRL Revocation reason codes to remove cACompromise (2) and add privilegeWithdrawn (9) • 7.3 Updated OCSP RFC reference from 2560 to 6960 • 9.11 Generalized notification procedures for Application Software Vendors			
08/16/2022	Update	• 4.9.10 – Removed an implementation date that was in the past • 5.4.1, 5.4.3, 5.5.1, 5.5.2 – Updated these sections to align with latest audit and archive standards for data types and retention • 7.1 – Removed OU as a supported subject attribute on the WTTLSOV template	2.10	2.9	DSR PKI Team
10/28/2022	Update	• 1.3.5 – Updated definition of DSR PKI PMA	2.11	2.10	DSR PKI Team
02/14/2023	Update	• 1.6 – Add definition for Terms of Use • 1.6 – Updated a Subscriber definition • 4.1.2, 4.4, 4.5.1, 4.9.1 – minor update to add Terms of Use reference	2.12	2.11	DSR PKI Team

		• 3.2.2, 3.2.3.2 – Added additional domain validation details			

Table of Contents

1. Introduction

This Certificate Policy/Certification Practice Statement (CP/CPS) governs the operations of Microsoft Digital Security + Resilience (DSR) Public Key Infrastructure (PKI) Transport Layer Security (TLS) Certificate Authority (CA) services and sets forth the business, legal, and technical practices for approving, issuing, managing, using, and revoking digital Certificates within the DSR TLS CA hierarchy. The effective date for implementation of the practices disclosed in this document is the date of publication of the Certificate Policy and Certification Practice Statement (CP/CPS) and will apply to all future CA related activities performed by DSR PKI.

This CP/CPS relies upon the following DigiCert CP: 2.16.840.1.114412.0.1.4

Note: Please refer to earlier versions of the DigiCert CP for CA Policy Definitions valid from the time period that those CAs were issued. DigiCert policy version history can be found here: https://www.digicert.com/legal-repository/.

This CP/CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. CAs within the DSR PKI hierarchy conform to the current version of the CA/Browser Forum (CABF) requirements including:

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

This CP/CPS adheres to Mozilla Root Store Policy Requirements:

https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

In the event of any inconsistency between this document, the CABF Requirements, and those Requirements, those Mozilla Root Store Policy Requirements take precedence.

1.1 Overview

Microsoft Corporation DSR PKI has been established to provide TLS digital certificate services to support operations of various Microsoft functions and business units. DSR PKI functions as the Certification Authority, Registration Authority (RA), and manages TLS Certificates for Microsoft. The TLS Certificates provide consumers with assurance regarding the authenticity and integrity of Microsoft owned domains and servers.

The following CAs, that are used to issue public key TLS Certificates, are within the scope of this CP/CPS referred to here after as "DSR TLS CAs."

CA Type	CA Name	Description of Function
Microsoft RSA TLS Issuing CA	Microsoft RSA TLS CA 01	Issues SHA2 TLS web server/client Certificates to authenticated individuals

CA Type	CA Name	Description of Function
Microsoft RSA TLS Issuing CA	Microsoft RSA TLS CA 02	Issues SHA2 TLS web server/client Certificates to authenticated individuals

1.2 Document Name and Identification

This document is formally referred to as the "DSR PKI Certificate Policy/Certification Practice Statement for TLS CAs" (DSR PKI CP/CPS). DSR TLS CAs issue Certificates in accordance with the policy and practice requirements of this document. The "Certificate Policies" field for each end-entity (leaf) certificate must reference the OID for the CP/CPS under which it was issued. Certificates issued by DSR TLS CAs must include the following Object Identifier (OID) in the "Certificates Policies" field 1.3.6.1.4.1.311.42.1.

1.3 PKI Participants

1.3.1 Certification Authorities

The following CAs are supported by this CP/CPS:

- Microsoft RSA TLS CA 01

  Microsoft RSA TLS CA 01 is part of the DSR TLS CA hierarchy and issues SHA2 end-entity certificates. This CA has been issued a certificate from the Baltimore CyberTrust Root CA.

- Microsoft RSA TLS CA 02

  Microsoft RSA TLS CA 02 is part of the DSR TLS CA hierarchy and issues SHA2 end-entity certificates. This CA has been issued a certificate from the Baltimore CyberTrust Root CA.

DSR TLS CAs issue end-entity TLS Certificates for Microsoft owned domains. In limited circumstances, DSR TLS CAs also issue end-entity TLS Certificates for domains owned by partners for purposes of conducting business with Microsoft. DSR PKI TLS CAs are operated by the DSR PKI team.

1.3.2 Registration Authorities

Registration Authorities (RAs) perform identification and authentication of subscribers for certificate issuance and revocation requests, and pass along such requests to the Certification Authorities. RA activities are operated by the DSR PKI team for all Certificates issued under the DSR TLS CA hierarchy.

1.3.3 Subscribers

Subscribers within the DSR TLS PKI CA hierarchy include Microsoft employees (full-time, part-time and contingent staff) and may be issued Certificates for assignment to

devices or applications, provided that responsibility and accountability is attributable to the organization.

1.3.4 Relying Parties

A Relying Party is the entity who relies on the validity and binding of the Subscriber with the public key associated with the Certificate. Relying Parties typically include entities that may rely upon a Subscriber Certificate for purposes of a) authenticating identity or b) encrypting communications.

1.3.5 Other Participants

DSR PKI Policy Management Authority (PMA)

The DSR PKI Policy Management Authority (PMA) manages and approves policy and practice statement documents for DSR PKI and oversees DSR PKI compliance and operations. It consists of representatives from various operational and compliance organizations throughout Microsoft.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued within the DSR TLS CA hierarchy can be used for server authentication, client authentication, and SSL/TLS Secure Sessions. Certificates issued to Microsoft's external partners shall only be used for conducting business with Microsoft.

Certificate Type	Assurance Level	Description and Assurance Level
TLS Certificate	High Assurance	CAs operating under this policy are hosted and managed by DSR PKI using FIPS 140-2 Level 3 validated hardware security modules (HSMs) and employ pre-defined and approved fulfillment practices which include identification and authentication of the subscriber and verification of the subject information included in the end-entity certificate prior to issuance.

1.4.2 Prohibited Certificate Uses

Certificates must only be used to the extent consistent with applicable law and for the purposes specified in §1.4.1. CA Certificates must not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP/CPS is administered by the DSR PKI PMA at Microsoft Corporation.

1.5.2 Contact Information

Contact information is listed below:

DSR PKI Practices Administrator

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052-6399

centralpki@microsoft.com

1.5.3 Person Determining CPS Suitability for the Policy

The DSR PKI PMA, as defined in §1.3.5, determines suitability of CPS for the policy.

1.5.4 CP/CPS Approval Procedures

The CP/CPS will be maintained in a repository available to the public. The CP/CPS shall be reviewed by the DSR PKI PMA at least annually or in the event of a major change. The version number of the document will be updated at least annually. The DSR CP/CPS is prepared and reviewed by Microsoft DSR PKI team and submitted to the DSR PKI PMA for their approval. Conditions for approval by the PMA include:

- All voting members (or their delegates) shall review proposed changes to this document. Changes will not be implemented unless approved unanimously by voting members, although members may waive approval if the proposed change does not relate to their area(s) of operation. Waivers may be delivered via e-mail.

1.6 Definitions and Acronyms

- **Certificate** – An electronic document that uses a digital signature to bind a public key and an identity.
- **Certification Authority (CA)** – An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
- **Certification Authority Authorization (CAA)** – From RFC 8659 (https://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify 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."
- **Certificate Policy/Certificate Practice Statement –** A set of rules governing the operation, applicability, and use of a named set of Certificates for a defined set of users.
- **Certificate Revocation List (CRL)** – A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

- **Certificate Signing Request (CSR)** – A message sent to the certification authority containing the information required to issue a digital Certificate.
- **Certificate Transparency (CT)** – Provides an auditing and monitoring system that lets any domain owner or Certification Authority (CA) determine whether their certificates have been mistakenly issued or maliciously used.
- **Compromise** - A loss, theft, disclosure, modification, unauthorized use, or other breach of security related to a Private Key.
- **Distinguished Name (DN)** – The Distinguished Name (DN) is used on Certificates and in the Repository to uniquely represent a Subject identified in a Certificate.
- **Hardware Security Module (HSM)** –A specialized hardware system designed to securely store cryptographic keys and perform cryptographic operations.
- **Object Identifier (OID)** – A unique alphanumeric/numeric identifier registered under the International Standards Organization's applicable standard for a specific object or object class.
- **Online Certificate Status Protocol (OCSP) –** An online Certificate-checking protocol that enables an OCSP Responder to determine the status of an identified Certificate by contacting the Repository.
- **Policy Management Authority (PMA)** – The DSR PKI Policy Management Authority which creates and maintains the policies related to the DSR Public Key Infrastructure.
- **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 is intended to be publicly shared with recipients of digitally signed electronic records and that is used by such recipients to verify Digital Signatures created with the corresponding Private Key and/or to encrypt electronic records so that they can be decrypted only with the 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.
- **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.
- **Relying Party** – Any natural person or Legal entity that relies on a Valid Certificate. An Application Software Supplier is not considered a **Relying Party** when software distributed by such Supplier merely displays information relating to a Certificate.
- **Repository** – An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies/Certification Practice Statements) and Certificate status information in the form of a CRL.

- **Subscriber** – A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
- **Subscriber Agreement** – An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
- **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.
- **Transport Layer Security(TLS)/Secure Socket layer (SSL)** – Security protocol that is widely used in the internet for authentication and establishing secure sessions.

2. Publication and Repository Responsibilities

2.1 PKI Repository

The Microsoft DSR PKI team maintains a public repository located at http://www.microsoft.com/pki/mscorp/cps

2.2 Publication of Certification Information

DSR PKI shall publish this CP/CPS, DSR TLS CA Certificates, and current CRLs for the DSR TLS CAs, and other information relevant to Subscribers and Relying Parties in the online PKI repository http://www.microsoft.com/pki/mscorp/cps. The DSR PKI team also maintains a database of issued TLS Certificates to which access is restricted to authorized Microsoft personnel.

2.3 Time or Frequency of Publication

In the event of a change to this CP/CPS, an updated version of this document with an incremented version number will be published in accordance with §1.5.4 after approval from the PMA. The new version of this CP/CPS will become effective immediately for all participants listed in §1.3. CRLs are published in accordance with §4.9.7.

2.4 Access Controls on Repositories

Information published in the Microsoft Corporation Internet website repository is publicly accessible information. Physical and logical access controls are used to restrict write access to authorized Microsoft personnel.

3. Identification and Authentication

3.1 Naming

3.1.1 Type of Names

Certificates are issued in accordance with the X.509 standard. All Certificates require a Distinguished Name in the subject field or a set of Subject Alternative Name values in the Subject Alternative Name extension. In the case where subject identity information is contained solely in the Subject Alternative Name extension, the Subject field of the Certificate may be empty.

The Issuer and Subject fields for Certificates issued by DSR PKI are populated in accordance with §7.1.

3.1.2 Need for Names to be Meaningful

The Distinguished Names assigned to the DSR TLS CAs and Subscribers shall be meaningful and shall have a reasonable association with DSR TLS CAs and organization.

3.1.3. Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

No stipulation.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Subscriber's Certificate request shall contain the public key to be certified and be digitally signed with the corresponding private key.

3.2.2 Authentication of Organization Identity

All Microsoft employees may submit requests for Certificates to be issued by DSR TLS CAs. Where the organization name is included in the Certificate request, the identity of the organization and other enrollment information provided by Certificate applicants is confirmed in accordance with the procedures set forth in DSR PKI operations procedures.

DSR PKI authenticates Organization information in each request in compliance with CA/Browser Forum's TLS Baseline Requirements.

DSR PKI determines that the organization information submitted in the request is accurate by validating against a qualified independent information source, or alternatively, an Attestation Letter to confirm the existence of the organization.

DSR PKI does not support issuance of subscriber certificates with IP addresses.

Each dnsName in a SAN or commonName in server certificates will be validated following subsection 3.2.2.4.2 or 3.2.2.4.4 of the CA/Browser Forum's TLS Baseline Requirements no more than 398 days prior to issuing the Certificate..

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Microsoft Employee

All Microsoft employees may submit requests for Certificates to be issued by DSR TLS CAs. Subscriber identity is authenticated by the RA application using the Windows Authentication against the enterprise directory. For each domain name included in the Certificate application, DSR PKI authenticates the Subscriber's right to request a Certificate for the domain based on an approval from the requester's manager who shall be a fulltime employee of Microsoft.

3.2.3.2 Authentication of Domain Name

DSR PKI issues Certificates only for the domains that are owned by Microsoft, and in limited circumstances, to domains that are owned by partners for conducting business with Microsoft.

No more than 398 days prior to certificate issuance, Microsoft verifies the Applicant's control over each FQDN listed in the Certificate by using at least one of the following approved methods as defined in the CA/Browser Forum's TLS Baseline Requirements at the time of validation:

- 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
- 3.2.2.4.4 Constructed Email to Domain Contact

The domain contact for Microsoft owned domains is identified from the Domain Name Registrar used by Microsoft. Any other domain contact is identified from public whois information. If domain contact is not available from the Domain Name Registrar or public whois data, the contact will be created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name. An email with a random value is sent to the domain contact from the previous steps. The domain contact must provide the random value to prove ownership.

3.2.4 Non-Verified Subscriber Information

Not Applicable.

3.2.5 Validation of Authority

All Microsoft employees are authorized to submit requests for Certificates to be issued by DSR TLS CAs. Requests for Certificates shall be approved by the Certificate applicant's direct Manager or a Manager up to two levels higher in the organization chain.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Requests for routine re-key of Subscriber Certificates are treated as new certificate requests and DSR PKI performs the same identification and authentication checks as described in §3.2. Routine re-key of the DSR TLS issuing CA certificates shall be performed in accordance with DSR PKI Key Generation process and the third-party Root CA re-key procedures.

3.3.2 Identification and Authentication for Re-Key After Revocation

Requests for re-key of Subscriber Certificates after revocation are treated as new certificate requests and DSR PKI performs the same identification and authentication checks as described in §3.2.

A Subscriber Certificate revocation request is valid if it complies with one of the following requirements:

- The request is raised through the RA application or
- If a revocation request is not raised through the RA application, the DSR PKI shall perform sufficient procedures to manually authenticate the Subscriber's request.

Revocation service requests for DSR TLS CA Certificates are required to be approved by the DSR PKI PMA prior to being processed.

3.4 Identification and Authentication for Revocation Request

See §3.2.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Prior to an end-entity certificate being issued, the Subscriber submits a Certificate application through the RA application.

Certificate requests for OCSP responder certificates are submitted to the CA application by authorized DSR PKI personnel.

4.1.1 Who Can Submit a Certificate Application

All Microsoft employees can submit Certificate applications for subscriber end-entity certificates.

4.1.2 Enrollment Process and Responsibilities

Authorized applicants shall begin the enrollment process by submitting a Certificate application through the enrollment website. Certificate fields are to be populated in accordance with DSR Certificate profile requirements. The requestor and subject information in the Certificate are validated as per §3.2. Upon completion of the validation steps, the Certificate application shall be approved by a Microsoft full-time

employee who is a manager in the management chain of the applicant requesting the Certificate. The applicant has the option of selecting an approver in direct line of management above the applicant (up to three levels) within the same organization. Managers or authorized individuals representing a user group within Microsoft may provide pre-approval for certificate requests made by members of that group, via individual user or service accounts, for a pre-determined list of Microsoft-owned domains. Approvals are documented and are required to be re-authorized on a periodic basis.

Subscribers are required to sign a Subscriber agreement or agree to the Terms of Use regarding the usage of an issued TLS Certificate in accordance with CP/CPS.

4.2 Certificate Application Processing

Certificates are generated, issued, and distributed only after the required identification and authentication steps are completed in accordance with §3 and DSR's PKI Operations Guide.

4.2.1 Performing Identification and Authentication Functions

See §3.

4.2.2 Approval or Rejection of Certificate Applications

The following approvals shall be obtained prior to Certificate issuance and are dependent on the Certificate type and assurance level.

	CERTIFICATE LEVELS WITHIN THE DSR PKI TLS CA HIERARCHY	
CERTIFICATE ASSURANCE	Approver for Issuing CA Certificate	Approver for End-entity (i.e., non-CA) Certificate
High Assurance	PKI Policy Management Authority (PMA)	• Applicant's Manager in the management chain or authorized individuals representing a user group • DSR PKI Team (where applicable for banned domain exception processing) • Microsoft Domains Administration Team (where applicable for domain exception processing)

4.2.3 Time to Process Certificate Applications

Certificate applications, where possible, shall be processed within three (3) business days.

4.2.4 Verification of CAA Records

CAA record verification is done in conformance with Baseline Requirements for Issuance and Management of Publicly Trusted certificates set forth by the CA/Browser Forum.

For all other FQDNs, CAA records are checked. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659.

The Certification Authority CAA identifying domain for CAs that Microsoft recognizes is "microsoft.com".

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Certificates are generated, issued, and distributed only after required approvals have been obtained and the required identification and authentication steps have been successfully completed in accordance with §3.2.2, §3.2.3, §3.3, and §3.4. Once the registration process is completed and the requestor is approved for a certificate, the CA will take reasonable steps to:

- Authenticate the source of the request before issuing the certificate
- Verify that certificate fields and extensions are populated in accordance with the approved certificate template
- Generate a certificate containing appropriate public keys, OIDs, dates, etc.
- Notify the RA application that the certificate is available for distribution

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Subscribers are notified of Certificate creation upon issuance via email and are provided access to their Certificates for download and installation.

4.4 Certificate Acceptance

By accepting a Certificate, the Subscriber:

- Agrees to be bound by the continuing responsibilities, obligations and duties imposed by the DSR PKI CP/CPS;
- Agrees to be bound by the DSR PKI Subscriber Agreement or Terms of Use;
- Represents and warrants that to its knowledge no unauthorized person has had access to the private key associated with the Certificate; and
- Represents and warrants that the Certificate information it has supplied during the registration process is truthful and accurate.

Upon receipt of a Certificate, the Subscriber is responsible for verifying that the information contained within the Certificate is accurate and complete and that the Certificate is not damaged or otherwise corrupted. In the event the Certificate is inaccurate, damaged, or corrupted, the Subscriber should contact the CA to have the Certificate replaced as determined by the CA.

4.4.1 Conduct Constituting Certificate Acceptance

A Subscriber's receipt of a Certificate and subsequent use of the key pair and Certificate constitute Certificate acceptance.

4.4.2 Publication of the Certificate by the CA

DSR TLS CA Certificates will be published within the DSR repository (see §2.1). Subscriber Certificates can be downloaded by Subscribers from the RA application.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Microsoft may notify the public of the issuance of a certificate by adding it to one or more publicly accessible Certificate Transparency (CT) Logs.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of a TLS Certificate is permitted once the Subscriber has agreed to the Subscriber Agreement or Terms of Use. The Certificate shall be used in accordance with the Subscriber Agreement or Terms of Use and with the terms of this CP/CPS.

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

Subscribers are required to protect their private keys from unauthorized use and discontinue use of the private key following expiration or revocation of the Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall use public key Certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, certificate policies, etc.) in the Certificates. A Relying Party is responsible for verifying the validity of the Certificate prior to relying on any Certificate.

4.6 Certificate Renewal

DSR TLS CAs support certificate renewals as specified in the following sections.

4.6.1 Circumstance for Certificate Renewal

Renewal requests may be submitted for certificates issued by DSR TLS CAs as long as the existing certificate is valid (i.e., not expired or revoked).

4.6.2 Who May Request Renewal

Renewal requests shall be submitted by the subscriber, certificate owner (can be the same person as the subscriber), or a delegate. Such requests must be signed using the existing certificate (key based renewal).

4.6.3 Processing Certificate Renewal Requests

DSR TLS CAs performs all identification, authorization, and validation checks specified in §3.2 during renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

Subscribers are notified of new certificate issuance through emails.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Refer to §4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

Refer to §4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.7 Certificate Re-Key

Any certificate re-key request shall be treated as initial certificate issuance. Refer to §4.3.

4.7.1 Circumstance for Certificate Re-Key

No Stipulation.

4.7.2 Who May Request Certification of a New Public Key

No Stipulation.

4.7.3 Processing Certificate Re-Keying Requests

No Stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No Stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No Stipulation.

4.7.6 Publication of the Re-Keyed Certificate by the CA

No Stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.8 Certificate Modification

Any certificate modification request shall be treated as initial certificate issuance. Refer to §4.3

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

No Stipulation.

4.9 Certificate Revocation and Suspension

DSR PKI supports Certificate revocation for all DSR TLS CAs. DSR PKI does not support Certificate suspension for DSR TLS CAs.

DSR PKI, through the RA application, maintains a continuous 24x7 ability to accept and respond to revocation requests. Inquiries related to Certificate revocations are sent to an e-mail address monitored by the DSR PKI Team.

DSR TLS CAs publicly disclose to Subscribers, Relying Parties, Application Software Suppliers, and other Third Parties, instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.

When a revocation request or Certificate problem is reported through email, DSR PKI will begin investigation within twenty-four (24) hours of receipt of such a request to decide whether revocation or other appropriate action is warranted.

DSR PKI maintains a continuous 24x7 ability to accept and respond internally to a high-priority certificate problem report and where appropriate, forward such a complaint to law enforcement authorities and/or revoke a Certificate that is the subject of such a complaint.

4.9.1 Circumstances for Revocation

Revocation may take place at the discretion of the DSR PKI in the event that the security or integrity of the Certificate (or information contained within it) is compromised. When confirmed, DSR PKI shall revoke a TLS Certificate within twenty-four (24) hours if one or more of the following circumstances occur:

- The Subscriber requests in writing that DSR PKI revoke the Certificate;
- The Subscriber notifies DSR PKI that the original Certificate request was not authorized and does not retroactively grant authorization;

- DSR PKI obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused;
- DSR PKI obtains evidence that the validation of domain authorization or control for any Fully Qualified Domain Name or IP address in the Certificate should not be relied upon.

When confirmed, DSR PKI shall revoke a TLS Certificate within five (5) days if one or more of the following circumstances occur:

- DSR PKI is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- DSR PKI is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- DSR PKI is made aware of a material change in the information contained in the Certificate;
- DSR PKI is made aware that the Certificate was not issued in accordance with this CP/CPS or CA/Browser Forum's TLS Baseline Requirements;
- DSR PKI determines that any of the information appearing in the Certificate is inaccurate or misleading;
- DSR PKI ceases operations for any reason and has not planned to continue to provide revocation support for the Certificate;
- DSR PKI's right to issue Certificates is revoked or terminated, unless DSR PKI has planned to continue maintaining the CRL/OCSP Repository;
- Revocation is required as per this CP/CPS;
- As required by the law; or
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

DSR PKI may invoke its incident handling procedures if it considers a compromised subscriber certificate to have significant impact to the security of Microsoft platform customers. In such a situation, DSR PKI may revoke the certificate using "disallowed CTLs" method in addition to publishing CRLs.

4.9.2 Who Can Request Revocation

Certificate revocation can be requested by Subscribers, Subscriber's Manager, or delegates (See §4.9.3) as identified in the RA application. Revocation can also be initiated at the discretion of DSR PKI.

4.9.3 Procedure for Revocation Request

Each Certificate has at least one owner (can be the same as the Subscriber) and two delegates, one of which is the Subscriber's Manager as assigned in the RA application. Revocations requests are submitted by either the Certificate owner or a delegate through the RA application. A notification mail is sent to the Certificate owner and custodians informing them of the revocation request. The revocation request has to be

approved by the owner or one of the delegates and the approver cannot be the same person as the requestor.

Fulfillment of the revocation is done by marking a Certificate as revoked in the CA system and then submitting a CRL service request to the system to generate the appropriate CRLs. Depending upon how the revocation request was received, the fulfillment is performed either automatically by the RA application (for requests received in the RA application) or by the DSR PKI Team (for requests received through emails).

The CRLs are then posted and distributed by the DSR PKI as per § 4.9.7.

4.9.4 Revocation Request Grace Period

No stipulations.

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocation requests submitted through the RA application are revoked immediately following necessary approvals. Revocation requests submitted through emails are investigated and fulfilled as per §4.9 and §4.9.1.

4.9.6 Revocation Checking Requirements for Relying Parties

A Relying Party shall use the validation service (i.e., CRL or OCSP) prior to relying on any Certificate. Reliance without using the validation service will be considered an unreasonable reliance on the Certificate in question.

4.9.7 CRL Issuance Frequency

CRLs for Subscriber TLS Certificates shall be issued at least once every seven (7) days and shall be valid not more than ten (10) days. CRLs may be issued more frequently at the discretion of DSR PKI.

4.9.8 Maximum Latency for CRLs

DSR PKI will publish CRLs no later than the time specified in the "nextUpdate" field of the previously published CRL.

4.9.9 On-Line Revocation/Status Checking Availability

Status information for certificates issued by the DSR CAs is available using OCSP. Responses can be submitted through http://ocsp.msocsp.com. OCSP responses conform to RFC6960 and/or RFC5019.

4.9.10 On-Line Revocation Checking Requirements

1. OCSP responses MUST have a validity interval greater than or equal to eight (8) hours;
2. OCSP responses MUST have a validity interval less than or equal to ten (10) days;
3. For OCSP responses with validity intervals less than sixteen (16) hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

4. For OCSP responses with validity intervals greater than or equal to sixteen (16) hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight (8) hours prior to the nextUpdate, and no later than four (4) days after the thisUpdate.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

In an event or suspected or actual CA key compromise, Subscribers must immediately notify Microsoft DSR PKI. The subscriber is responsible for investigating the compromise circumstances.

DSR PKI management, in conjunction with the PKI PMA, will assess the situation and determine the appropriate course of action to confirm and address the compromise. If deemed necessary by Microsoft, Microsoft shall use commercially reasonable efforts to notify potential Relying Parties if DSR PKI discovers, or has reason to believe, that there has been a compromise of a TLS CA private key. In any case of compromise, the certificate will be revoked and an updated CRL will be published.

Reports to Microsoft DSR PKI of key compromise must include:

- Proof of key compromise in either of the following formats:
  - A CSR signed by the compromised private key with the Common Name "Proof of Key Compromise for Microsoft DSR PKI"; or
  - The private key itself.
- A valid email address so that you can receive confirmation of your problem report and associated certificate revocations.

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

See §4.9.6, §4.9.7, §4.9.8, and §4.9.9.

4.10.1 Operational Characteristic

Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

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

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

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

4.10.3 Optional Feature

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

The escrow of CA and Subscriber TLS private keys, for purposes of access by law enforcement or any other reason, is not supported by DSR PKI.

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. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The locations of the production and disaster recovery DSR PKI facilities, housing CA equipment and cryptographic materials, are consistent with facilities used to house high value, sensitive information.

All CA operations are conducted within physically protected environments that deter, prevent, and detect unauthorized use of, access to, or disclosure of sensitive information and systems.

DSR TLS CA systems are hosted and managed within secure facilities, that are constructed to have multiple tiers of physical security and employ a variety of controls to

prevent and detect the unauthorized use of and access to sensitive DSR assets. Physical access to production DSR TLS CA systems is restricted to authorized personnel using dual controlled, two-factor authentication access control mechanisms; is logged; and is monitored and video recorded on a 24x7 basis.

DSR PKI has implemented a backup facility in an alternate location to address the recovery of the DSR PKI service and systems in the case of a disaster scenario.

5.1.2 Physical Access

DSR TLS CA systems are protected by dual controlled, two-factor authentication systems, including biometrics. Access is restricted to a limited number of authorized individuals with an approved business need to access DSR systems and cryptographic materials.

Furthermore, access to these facilities is reviewed on a periodic basis to determine compliance.

Cryptographic hardware and activation materials are protected through the use of locked racks and safes. Access to cryptographic systems, hardware, and activation materials is restricted in accordance with §5.2.2. Participation of a minimum of two (2) trusted individuals is required to obtain access to the quorum of activation materials needed to activate CA keys.

5.1.3 Power and Air Conditioning

DSR TLS CA facilities are equipped with primary and backup power systems, including uninterruptible power supply (UPS) systems and backup generators. Also, these secure facilities are equipped with climate control systems, as appropriate, to maintain optimal levels of temperature and humidity.

5.1.4 Water Exposures

DSR maintains controls to minimize the risk of water exposure and damage for CA systems and cryptographic materials.

5.1.5 Fire Prevention and Protection

CA facilities are equipped with smoke detection and fire suppression systems.

5.1.6 Media Storage

Media containing production software and system audit information is stored within secure hosting facilities with appropriate physical and logical access controls in accordance with DSR Microsoft Highly Confidential policies.

Media containing copies of production data, i.e., backup of key files etc., is stored within secure hosting facilities that also adhere to appropriate physical and logical access controls in accordance with DSR Microsoft Highly Confidential policies.

5.1.7 Waste Disposal

Sensitive waste material is disposed of in a secure fashion. Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive

information are rendered unreadable before disposal. Other waste is disposed of in accordance with Microsoft's normal waste disposal requirements.

Cryptographic devices, smart cards, and other devices that may contain private keys or key material will be physically destroyed or zeroized, if deemed necessary, in accordance with the manufacturers' guidance prior to disposal. Authorization is required for the disposal of all storage devices that contain key materials. Destruction of CA private keys shall be approved by the PMA and shall be witnessed by at least 2 individuals in trusted roles, and records of all disposals shall be maintained by DSR PKI.

5.1.8 Off-Site Backup

Backups of the CAs, including backups of system configurations and databases required to reconstitute PKI systems in the event of failure, are made and transported, on a periodic basis, to a secured backup location.

5.2 Procedural Controls

5.2.1 Trusted Roles and Authorized Roles

Personnel responsible for CA key management, Certificate issuance, and management of CA system functions are considered to serve in "trusted roles."

Within DSR PKI, the following roles are implemented:

Trusted Roles

- **DSR PKI Core Team** - fulfills and supports PKI systems and services including designing, building, and testing the TLS PKI system, and cryptographic key management operations, providing support to customers (i.e., internal business groups), administration of service requests, and providing support for DSR TLS RA application and underlying infrastructure.
- **Product and Release Solutions (PRSS) Team** – partner team within Microsoft which also supports publicly trusted CAs. Trusted to perform physical tasks on DSR PKI assets upon approval from Service Owner.

Authorized Roles

- **DSR ACE** - provides information security related support for the DSR TLS CA hierarchy, including performing risk and threat assessments, periodic vulnerability assessments, and log review and monitoring.
- **Policy Management Authority (PMA)** - provides guidance for PKI policies.
- **DSR PKI Development Team** - provides development, and testing support for the TLS RA application.
- **Microsoft Domains Team** - provides support for the DSR TLS RA operations by reviewing certificates requests that are flagged for exception due to domain ownership.
- **Site Services/Global Capacity Services** - provides facilities assistance including installation of new hardware and hardware monitoring and support.

- ***Physical Security*** - responsible for the physical security of the data center and storage of the cryptographic materials in safes.
- ***Infrastructure and Networking*** - responsible for managing and maintaining the infrastructure and network components of the DSR TLS hierarchy.

5.2.2 Number of Persons Required per Task

Cryptographically sensitive operations within the DSR PKI such as access to cryptographic materials and systems, CA key generation, CA key recovery, CA key activation and CA system configuration requires the participation of multiple trusted individuals in accordance with §6.2.2. Other operations may require only one trusted or authorized individual.

5.2.3 Identification and Authentication for Each Role

Role members are approved and tracked by the Service Owner upon completion of §5.3 Personnel Controls.

5.2.4 Roles Requiring Separation of Duties

Roles requiring separation of duties include, but may not be limited to, the following:

- Handling of CA key life-cycle management activities, Certificate life-cycle management activities, CA system installation, administration, and maintenance activities
- Independent witness during the key ceremony
- RA application developers
- RA application operational support

5.3 Personnel Controls

The DSR PKI operation relies on Microsoft Corporate HR policies for personnel management to ensure the trustworthiness of its staff.

5.3.1 Qualifications, Experience, and Clearance Requirements

The recruitment and selection practices for Microsoft personnel shall take into account the background, qualifications, and experience requirements of each position, which are compared against the profiles of potential candidates.

5.3.2 Background Check Procedures

DSR PKI trusted personnel undergo background checks prior to their commencement of employment at Microsoft. Such checks include:

- Social Security Number trace;
- County, State, and Federal criminal records search (7 year search, where permitted by resident jurisdiction);
- Employment verification [last seven (7) years or last three employers]; and
- Education verification (highest degree obtained).

DSR PKI employees are required to sign a nondisclosure agreement and are required to adhere to Microsoft corporate policies and procedures.

5.3.3 Training Requirements

DSR PKI personnel in trusted roles receive training as needed to perform assigned job responsibilities relating to CA or RA operations:

- Basic PKI concepts
- Roles and responsibilities
- The policies and practices noted in the CP/CPS
- DSR PKI security and operational policies and procedures

Training curriculum and renewal requirements are determined by DSR PKI management.

5.3.4 Retraining Frequency and Requirements

DSR PKI provides refresher training as needed to ensure a consistently high level of awareness and proficiency.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Unauthorized actions or other violations of DSR PKI policies, procedures, and practices as described in this CP/CPS will result in disciplinary action. Disciplinary actions are taken in accordance with Microsoft corporate policies.

5.3.7 Independent Contractor Requirements

DSR PKI may employ contractors as necessary. Contractors are required to follow a similar background check process as full-time employees.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

DSR PKI and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. DSR PKI SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

DSR PKI SHALL record at least the following events:

1. CA certificate and key lifecycle management events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction;
   b. Certificate requests, renewal, and re-key requests, and revocation;
   c. Approval and rejection of certificate requests;
   d. Cryptographic device lifecycle management events;
   e. Generation of Certificate Revocation Lists;
   f. Signing of OCSP Responses (as described in §4.9 and §4.10); and
   g. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles
2. CA and Subscriber lifecycle management events, including:
   a. Certificate requests, renewals, re-key requests, and revocation;
   b. All verification activities stipulated in this CP/CPS;
   c. Acceptance and rejection of certificate requests;
   d. Issuance of Certificates; and
   e. Generation of Certificate Revocation Lists; and
   f. Signing of OCSP Responses (as described in §4.9 and §4.10).
3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. System crashes, hardware failures, and other anomalies;
   e. Firewall and router activities; and
   f. Entries to and exits from the CA facility.

Log records MUST include the following elements:

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

Audit Logs are either manually recorded or automatically recorded by the system.

5.4.2 Frequency of Processing Log

Audit logs are reviewed on an as-needed basis and significant events may be documented in a review summary. Exception based entries corresponding to alerts or irregularities are highlighted and actions, if any, to resolve noted issues are also documented.

5.4.3 Retention Period for Audit Log

DSR PKI and each Delegated Third Party SHALL retain, for at least two (2) years:

1. CA certificate and key lifecycle management event records (as set forth in §5.4.1 (1)) after the later occurrence of:
   a. the destruction of the CA Private Key; or
   b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA

field set to true and which share a common Public Key corresponding to the CA Private Key;

2. Subscriber Certificate lifecycle management event records (as set forth in §5.4.1 (2)) after the expiration of the Subscriber Certificate;
3. Any security event records (as set forth in §5.4.1 (3)) after the event occurred.

Note: While this is the minimum retention period, the DSR PKI MAY choose to retain audit logs for a longer period as appropriate to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.

5.4.4 Protection of Audit Log

Production and archived logical and physical audit logs are protected using a combination of physical and logical access controls.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up on a periodic basis.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, database, network, and operating system level. Manually generated audit data is recorded.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual or system that caused the event.

5.4.8 Vulnerability Assessments

DSR PKI maintains detection and prevention controls to protect Certificate Systems against viruses and malicious software and document and follows a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.

DSR TLS CA systems will undergo periodic vulnerability scans and penetration testing as determined by DSR PKI.

5.5 Records Archival

5.5.1 Types of Records Archived

DSR PKI and each Delegated Party maintain an archive of logs that include the recorded events specified in §5.4.1.

Additionally, DSR PKI maintains an archive of:

1. Documentation related to the security of the:
   a. Certificate Systems
   b. Certificate Management Systems
   c. Delegated Third Party Systems

2. Documentation related to the verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in §5.5.1 SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per §5.4.3, whichever is longer. Additionally, DSR PKI and each delegated party SHALL retain, for at least two (2) years:

1. All archived documentation related to the security of:
    a. Certificate Systems
    b. Certificate Management Systems
    c. Delegated Third Party Systems (as set forth in §5.5.1)
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in §5.5.1) after the later occurrence of:
    a. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
    b. the expiration of the Subscriber Certificates relying upon such records and documentation

Note: While this is the minimum retention period, the DSR PKI MAY choose to retain audit logs for a longer period as appropriate to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.

5.5.3 Protection of Archive

Archives of relevant records are protected using a combination of physical and logical access controls.

5.5.4 Archive Backup Procedures

All logs specified in §5.4.1 are uploaded to geographically redundant and replicated file storage. This archive is held in the same logical environment as the CA systems.

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)

All logs specified in §5.4.1 are uploaded to geographically redundant and replicated file storage. This archive is held in the same logical environment as the CA systems.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized designated individuals from DSR PKI are able to obtain access to archived records.

5.6 Key Changeover

CAs managed and operated by DSR PKI will stop issuing TLS Certificates and will be re-keyed or terminated before the maximum key usage period for Certificate signing is reached in accordance with §6.3.2. The TLS CAs will continue to sign and publish CRLs until the end of the CA Certificate lifetime. The key changeover or CA termination process will be performed such that it causes minimal disruption to Subscribers and Relying Parties. Affected entities will be notified prior to the planned key changeover.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

DSR PKI follows the Microsoft Corporate Information Security Incident Management Procedure for handling attacks or suspected attacks on the security or integrity of DSR TLS CA systems. Key compromise or suspected key compromise follows procedures listed in §5.7.3.

When DSR PKI fails to comply with the Mozilla Trusted Root Policy - whether it be a mis-issuance, a procedural or operational issue, or any other variety of non-compliance - the event is classified as an incident. At a minimum, DSR PKI will promptly report all incidents through Mozilla's Bugzilla bug reporting tool and will regularly update the Incident Report until the corresponding bug is resolved by a Mozilla representative. Issuance of impacted certificates will cease until the problem has been prevented from reoccurring.

Changes that are motivated by a security concern such as certificate mis-issuance or a root or intermediate compromise will be treated as security-sensitive, and a secure bug will be filed in Bugzilla.

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

See §5.7.4.

5.7.3 Entity Private Key Compromise Procedures

If DSR PKI discovers, or has reason to believe, that there has been a compromise of a DSR TLS CA private key, DSR PMA will immediately convene an emergency incident response team to assess the situation to determine the degree and scope of the incident and take appropriate action as specified in Microsoft's corporate information security incident response plan.

5.7.4 Business Continuity Capabilities after a Disaster

DSR PKI has established and maintains the following business continuity capabilities and practices to address recovery of the DSR PKI service and systems in the event of a disaster:

- Secure storage of backup cryptographic hardware modules containing copies of the private keys for TLS CAs managed and operated by DSR PKI at a Microsoft facility away from the primary location;

- Secure storage of the requisite activation materials at a secured facility away from the primary location;
- Secure storage of daily backups of system, data, and configuration information;
- Secured disaster recovery site at a Microsoft facility away from the primary location where operations can be restored in the event of a disaster at the primary location;
- A business continuity strategy that defines the acceptable Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The RTO is a maximum three (3) days except for the certificate revocation and CRL publishing which shall have an RTO of twenty-four (24) hours. The RPO is at maximum twenty-four (24) hours;
- Disaster recovery plan; and
- Disaster recovery testing performed on at least an annual basis.

5.8 CA or RA Termination

In the event that it is necessary to terminate the operation of a DSR TLS CA, management will plan and coordinate the termination process with its Subscribers and Relying Parties such that the impact of the termination is minimized. DSR PKI will provide as much prior notice as is reasonable to Subscribers and Relying Parties and preserve relevant records for a period of time deemed fit for functional and legal purposes. Relevant Certificates will be revoked no later than the time of the termination.

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

DSR PKI generates CA key pairs for the DSR TLS CAs following a defined key generation process, which is witnessed and performed in the presence of multiple trusted roles.

CA key pair generation is performed in accordance with the "DSR PKI Key Generation Ceremony Process" and "DSR PKI Operations Guide" during formal, pre-scripted ceremonies using hardware cryptographic modules that meet the requirements of §6.2.1. The CA Key Generation Script ("script") defines the specific steps performed during the installation and key generation ceremony and serves as an audit record. The script includes a list of the specific CA hardware and cryptographic materials required to be accessed during the ceremony.

Key ceremonies require the participation of multiple trusted employees, functioning in the capacity of pre-allocated ceremony roles, and are performed in controlled secure facilities. These facilities are secured with multiple tiers of physical security and are used to store production and backup copies of CA systems and key materials required for the key generation activities. Physical access is restricted using dual-controlled, two factor authentication access control systems, including biometrics. Access to and within the facilities is monitored via closed circuit televisions (CCTV) and recorded.

Activation materials are retrieved by assigned shareholders prior to the key ceremony. A log is maintained of all items removed and replaced from their storage location citing the individuals' names, date, time, and purpose of retrieval. Major ceremony activities are witnessed by an independent observer who attests to the integrity of the ceremony and records exceptions to the pre-scripted processes.

6.1.1.2 Subscriber Key Pair Generation

DSR PKI does not generate Subscriber keys. Subscriber key pairs are generated by the end-entity DSR PKI Subscriber.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Issuing CA Certificate requests are generated by the DSR PKI team using a controlled process that requires the participation of multiple trusted individuals. CA Certificate requests are PKCS #10 requests (signing request) and accordingly contain the requesting CA's public key and are digitally signed by the requesting CA's private key. The PKCS #10 requests are sent to third party provider to be digitally signed by the third-party Root CA.

For Subscriber Certificate requests, the Subscriber's public key is submitted to the CA using a Certificate request signed with the Subscriber's private key. This mechanism ensures that:

- The public key has not been modified during transit and
- The sender possesses the private key corresponding to the transferred public key

6.1.4 CA Public Key Delivery to Relying Parties

When DSR PKI updates signature key pairs it shall distribute the new public key in a secure fashion. The new public key may be distributed in a new CA Certificate obtained from the issuer(s) of the current CA Certificate(s). DSR TLS CA Certificates will be published in one or both of the following locations:

- Within the RA database and/or
- Published within the DSR PKI repository (See §2.1).

6.1.5 Key Sizes

Issuing CAs under this CP/CPS that sign end-entity Certificate requests and CRLs shall be generated as defined below:

- Microsoft RSA TLS CA 01 shall be generated with 4096-bit RSA Public Key Modulus
- Microsoft RSA TLS CA 02 shall be generated with 4096-bit RSA Public Key Modulus

End-entity Certificates shall use RSA keys whose modulus size in bits is divisible by 8, and is at least 2048.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Key pairs may be used as follows:

Entity	Permitted Key Usage
Issuing CA	Signing of Subscriber Certificates, CRL Signing, and OCSP Responder Certificates Signing
Subscriber	Server Authentication, Client Authentication Exceptions to the above noted key uses should be approved on a case-by-case basis

The key usage extension is set in accordance with the Certificate profile requirements specified in §7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA key pairs are generated in and protected by hardware security modules certified to FIPS 140 level 3 that meet industry standards for random number and prime number generation.

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

The participation of at least two trusted employees is required to perform sensitive CA private key operations (e.g., signing operations, CA key backup, CA key recovery, etc.) for the Issuing CAs. This is enforced through DSR PKI's allocation among persons or groups with trusted roles of the activation materials required for CA key activation and through physical access controls specified in §5.1.2 over the CA systems and related activation materials.

A threshold (n) number of card sets of the total number (m) of activation materials, created and distributed for each hardware cryptographic module security world, is required to initialize a CA private key. At least one operator card with passphrase shall be required for activating the private key. Production security worlds created after the approval and publication of this CP/CPS shall have an "n out of m" configuration to support distribution of materials to individual key shareholders while maintaining redundancy to achieve operational efficiencies.

Assurance Level	Required Operator Card Set Threshold	Required Administrator Card Set Threshold
High Assurance	1 Operator Card	3 Administrator Cards

Exceptions to these policies require the approval of the DSR PKI Policy Management Authority. Furthermore, DSR PKI production security worlds shall not be shared with non-DSR PKI groups or used to perform signing activities for test CAs.

CA key pairs, managed and hosted by DSR PKI group shall comply with private key multi-person access control requirements defined in this CP/CPS.

6.2.3 Private Key Escrow

The escrow of CA and Subscriber private keys is not supported by DSR PKI.

6.2.4 Private Key Backup

Backups of CA private keys are created to facilitate disaster recovery and business continuity capabilities. Backups of key files are stored in encrypted form and protected in accordance with media handling practices stated in §5.1.6. DSR PKI does not provide private key backup for end-entity Subscriber private keys.

6.2.5 Private Key Archival

DSR TLS CA and Subscriber private keys are not archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA private keys are generated, stored, and backed up in an encrypted form, and used only within industry-standard hardware cryptographic modules meeting the requirements of §6.2.1.

6.2.7 Private Key Storage on Cryptographic Module

See §6.2.6.

6.2.8 Method of Activating Private Key

Cryptographic modules used for CA private key protection utilize a smart card-based activation mechanism (Operator Card) as described in CP/CPS §6.2.2.

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall be secured from unauthorized access. After use, the cryptographic module shall be deactivated by removal of the inserted OCS from the card reader. Hardware cryptographic modules are removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Key

CA private keys shall be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked, in the presence of multiple trusted personnel after approval from the PKI Policy Management Authority (PMA). When CA key destruction is required, CA private keys shall be destroyed through zeroization and/or physical destruction of the device in accordance with manufacturers' guidelines.

6.2.11 Cryptographic Module Rating

See §6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Copies of CA and Subscriber TLS Certificates shall be archived in accordance with §5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For Certificates issued after the effective date of this CP/CPS, the following key and Certificate usage periods shall be deployed.

Entity Type	Maximum Key Usage Period For Certificate signing	Maximum Key Usage Period For CRL signing	Maximum Certificate Validity Period
Issuing CAs	4 Years	6 Years	6 Years
Subscribers	N/A	N/A	398 Days as measured from the notBefore through notAfter, inclusive

Exceptions to the above noted operational and usage periods shall be approved by the PKI Policy Management Authority.

6.4 Activation Data

Hardware modules used for CA private key protection utilize a secret sharing mechanism to activate the CA private key under multi-user control as described in §6.2.2. Key material is created during formal key generation ceremonies, used only when needed, and stored in a secure site when not in use.

6.4.1 Activation Data Generation and Installation

See §6.4.

6.4.2 Activation Data Protection

See §6.4.

6.4.3 Other Aspects of Activation Data

See §6.4.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

DSR PKI systems use industry standard CA software, custom developed RA software, commercially available cryptographic modules, and smart cards. DSR PKI systems maintaining CA software and data files are secured from unauthorized access. Authorized access to production servers is limited to those individuals with a valid business reason for such access. Multi-factor authentication is enforced for user accounts capable of directly causing Certificate issuance.

PKI systems comply with Microsoft corporate information security policies.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

Custom developed software is developed, tested, and deployed in accordance with documented Microsoft Systems Development Lifecycle (SDLC) processes. Approvals by management are required for key stages of development, including requirements specifications, design review, user acceptance testing, and deployment.

6.6.2 Security Management Controls

DSR PKI follows Microsoft corporate information security policies for securing and maintaining the DSR TLS PKI systems. Periodic risk assessments and threat analysis are performed by the DSR Security Assessment (ACE) team to identify threats and vulnerabilities in the DSR TLS PKI systems.

Logical access to the DSR TLS CA systems is restricted to authorized individuals in trusted roles. DSR TLS PKI systems are configured by removing/disabling accounts, applications, services, protocols, and ports that are not used in the CA's operations. Anti-virus and malware detection software is installed on CA systems.

6.6.3 Life Cycle Security Control

No stipulation.

6.7 Network Security Controls

DSR PKI segments Certificate systems into zones based on their functional and logical relationship.

The zones, on which the DSR TLS CAs reside, are protected from unauthorized users through a series of network and host-based firewalls and other monitoring and detection systems. Firewalls are configured with rules that support the services, protocols, ports, and communications that DSR PKI has identified as necessary for its operations.

6.8 Time-Stamping

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

CA Certificates within the DSR PKI shall be X.509 Version 3 and shall conform to the RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL profile, dated May 2008. As applicable to the Certificate type, Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

At a minimum the following basic fields and prescribed field attributes are utilized within the CA Certificate profile. Less stringent exceptions to the given basic profile shall be approved on a case-by-case basis by the PKI Policy Management Authority based on a valid documented business case.

Issuer CAs shall generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

WTTLSDV End-entity Certificate Profile

End-user Subscriber Certificates shall be X.509 Version 3.

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA that exhibits at least 8 bytes of entropy
Signature Algorithm	SHA256RSA
Issuer	CN = <Issuing CA's common name> O = Microsoft Corporation C = US
Valid From	Date and time of Certificate issuance. Time synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Valid To	Date and time of Certificate expiration. Time synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.

Field	Description
	Maximum Certificate validity period is 372 Days from issuance for Fully Qualified Domain Names.
Subject	CN = <Subscriber Name> C = Country Code (Optional)
Public Key	RSA (2048 bits or larger)
Subject Alternate Name	<DNS Name(s)>
Certificate Policies	Microsoft IT CPS (1.3.6.1.4.1.311.42.1) Domain Validated (2.23.140.1.2.1)

CRL Distribution Points	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	           URL=
	http://mscrl.microsoft.com/pki/mscorp/crl/<Issuing CA>(n*).crl
	
	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	           URL=
	http://crl.microsoft.com/pki/mscorp/crl/<Issuing CA>(n*).crl
	More than one CRL Distribution Points may be specified in the end-entity certificate.
	*an incremental integer value assigned by Windows Active Directory Certificate Services that represents the version number of the CRL

Authority Information Access	[1]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	        Alternative Name:
	           URL=

Field	Description

	http://www.microsoft.com/pki/mscorp/<Issuing CA name>.crt
	
	[2]Authority Info Access
	   Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
	    Alternative Name:
	      URL=http://ocsp.msocsp.com

Basic Constraints	NOT POPULATED
Key Usage	(Optional)
Extended Key Usage	id-kp-serverAuth id-kp-clientAuth

WTTLSOV End-entity Certificate Profile

End-user Subscriber Certificates shall be X.509 Version 3.

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA that exhibits at least 8 bytes of entropy
Signature Algorithm	SHA256RSA
Issuer	CN = <Issuing CA's common name> O = Microsoft Corporation C = US
Valid From	Date and time of Certificate issuance. Time synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Valid To	Date and time of Certificate expiration. Time synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.

Field	Description
	Maximum Certificate validity period is 372 Days from issuance for Fully Qualified Domain Names
Subject	CN = <Subscriber Name> O = <Subscriber Company Name> i.e., Microsoft or Microsoft Corporation S = State AND/OR L = Locality C = Country Name
Public Key	RSA (2048 bits or larger)
Subject Alternate Name	<DNS Name(s)>
Certificate Policies	Microsoft IT CPS (1.3.6.1.4.1.311.42.1) Organization Validated (2.23.140.1.2.2)

CRL Distribution Points	[1]CRL Distribution Point
	
	    Distribution Point Name:
	
	       Full Name:
	
	          URL=
	
	 http://mscrl.microsoft.com/pki/mscorp/crl/<Issuing CA>(n*).crl
	
	 [1]CRL Distribution Point
	
	    Distribution Point Name:
	
	       Full Name:
	
	          URL=
	
	 http://crl.microsoft.com/pki/mscorp/crl/<Issuing CA>(n*).crl
	
	 More than one CRL Distribution Points may be specified in the end-entity certificate.
	
	 *an incremental integer value assigned by Windows Active Directory Certificate Services that represents the version number of the CRL

Authority Information Access	[1]Authority Info Access

Field	Description
	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.microsoft.com/pki/mscorp/\<Issuing CA name\>.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.msocsp.com
Basic Constraints	NOT POPULATED
Key Usage	(Optional)
Extended Key Usage	id-kp-serverAuth id-kp-clientAuth

7.1.1 Version Number(s)

DSR PKI hierarchy Certificates are X.509 version 3 Certificates.

7.1.2 Certificate Extensions

The extensions defined for DSR IT PKI 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 and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 5280 standards and recommendations and CA / Browser Forum Baseline Requirements. The name forms for Subscribers are enforced through DSR PKI internal policies and the authentication policies described elsewhere in this CP/CPS.

7.1.2.1 Key Usage

The key usage extension defines the purpose (e.g., encipherment, signature, Certificate signing) of the key contained in the Certificate. This extension SHALL appear in Certificates that contain public keys that are used to validate digital signatures on other public key Certificates or CRLs. When this extension appears, it SHALL be marked critical.

7.1.2.2 Certificate Policies Extension

The Certificate Policies extension of DSR PKI X.509 Version 3 Certificates includes a policy identifier, that indicates a Certificate Policy asserting DSR TLS CA's adherence to and compliance with CA/Browser Forum's TLS Baseline Requirements.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of DSR PKI X.509 Version 3 Certificates is utilized. This extension shall contain at least one entry. Each entry shall be a dNSName containing the Fully-Qualified Domain Name.

7.1.2.4 Basic Constraints

BasicConstraints extension shall not be present in DSR TLS CA end-user Subscriber Certificates.

7.1.2.5 Extended Key Usage

DSR PKI shall make use of the ExtendedKeyUsage extension for certain types of X.509 Version 3 Certificates. This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.

7.1.2.6 CRL Distribution Points

DSR PKI X.509 Version 3 end user subscriber certificates include the CRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

Most DSR PKI X.509 Version 3 end user subscriber certificates include the authority key identifier extension to provide a means of identifying the public key corresponding to the private key used to sign the respective Certificate. When used, the criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Most DSR PKI X.509 Version 3 end user Subscriber Certificates include the subject key identifier extension to provide a means of identifying the occurrence of a particular public key. When used, the criticality field of this extension is set to FALSE.

7.1.2.9 Application of RFC 5280

A Pre-certificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under the CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP/CPS shall use signature algorithms indicated by the following OIDs:

Signature Algorithm	OID ASN.1	Status
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}	Acceptable
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}	Acceptable
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}	Acceptable

Certificates created with deprecated signature algorithms adhere to all the requirements of this CP/CPS with the exception that the Certificate is generated with deprecated signature algorithm.

Certificates issued under this CP/CPS shall use the following OIDs to identify the algorithm associated with the subject key:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

Issuing CA and Subscriber Certificates are populated in accordance with Certificate profiles listed in § 7.1.

7.1.4.1 Name Encoding

Effective 2020-09-30, the following requirements SHOULD be met by all newly-issued Subordinate CA Certificates that are not used to issue TLS certificates, as defined in Section 7.1.2.2, and MUST be met for all other Certificates, regardless of whether the Certificate is a CA Certificate or a Subscriber Certificate.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with

the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.

7.1.5 Name Constraints

No additional stipulation other than § 7.1.

7.1.6 Certificate Policy Object Identifier

The DSR PKI CP/CPS will use a Policy Identifier of 1.3.6.1.4.1.311.42.1 in all Certificates it issues from the effective date of this version of the CP/CPS.

7.1.7 Usage of Policy Constraints Extension

The DSR PKI CP/CPS will be hot linked from the Certificate Policies in all Certificates it issues from the publication of this version of the CP/CPS.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies

No stipulation.

7.2 CRL Profile

The following CRL profile is used by Issuing CAs within the DSR TLS CA hierarchy.

Field	Description
Version	V2
Signature	SHA2
Issuer	Subject of Issuer
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	10 days (not to exceed)
Revoked Certificates	List of information regarding revoked Certificates. CRL entries include: • **_Serial Number_**, identifying the revoked Certificate • **_Revocation Date_**, including the date and time of Certificate revocation
CRL Entry Extensions	Not used.

7.2.1 Version Number(s)

See §7.2.

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Specify reason for revocation in list of reason codes: • keyCompromise (1) • affiliationChanged (3) • superseded (4) • cessationOfOperation (5) • privilegeWithdrawn (9)

7.3 OCSP Profile

The profile for OCSP responses issued by the DSR PKI conforms to the standards as described in RFC 6960.

7.3.1 Version Number(s)

DSR Issuing CAs shall issue Version 1 OCSP responses.

7.3.2 OCSP Extensions

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

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

CAs within the DSR TLS CA hierarchy are subject to an annual examination to assess compliance with the DSR PKI TLS policies and procedures (including the DSR PKI TLS CP/CPS), the American Institute of Certified Public Accountants (AICPA) & Canadian Institute of Chartered Accountants (CICA) WebTrust for Certification Authorities (WebTrust for CAs) examination criteria, and the WebTrust for CAs TLS Baseline Requirements examination criteria.

8.2 Identity/Qualifications of Assessor

Auditors demonstrating proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function shall perform the annual examination.

8.3 Assessor's Relationship to Assessed Entity

The entity that performs the annual examination is organizationally independent of DSR PKI.

8.4 Topics Covered by Assessment

The scope of the annual "period-of-time" examination shall include the requirements of the DSR PKI CP/CPS, CA environmental controls, CA key management, and Certificate life-cycle management.

The CAs are audited in accordance with Mozilla's Root Store Policy. If the CA has a currently valid audit report at the time of creation of the certificate, then the new certificate will appear on the CA's next periodic audit reports.

Newly added Intermediate CA certificates will be publicly disclosed in the CCADB within a week of Intermediate CA certificate creation, and before any such subordinate CA is allowed to issue certificates. All disclosure will be made freely available and without additional requirements, including, but not limited to, registration, legal agreements, or restrictions on redistribution of the certificates in whole or in part.

All CA certificates that are capable of being used to issue new certificates, and which directly or transitively chain to a certificate included in Mozilla's CA Certificate Program, will be operated in accordance with Mozilla Trusted Root Program policy and will either be technically constrained or be publicly disclosed and audited.

8.5 Actions Taken as a Result of Deficiency

Significant deficiencies identified during the compliance examination will result in a determination of actions to be taken. DSR PKI makes this determination with input from the auditor. Management is responsible for ensuring that corrective action plans are promptly developed, and corrective action is taken within a period of time commensurate with the significance of such matters identified.

8.6 Communications of Results

Compliance examination results are communicated to DSR PKI management and others deemed appropriate by management.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

DSR PKI currently does not charge Certificate issuance or Certificate revocation fees and reserves the right to charge fees for these or other DSR PKI provided services in the future.

9.1.2 Certificate Access Fees

DSR PKI 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

DSR PKI does not charge a fee as a condition of making the CRLs and OCSP status checking available as required by §4.9 and §4.10 available in a repository or otherwise available to Relying Parties. DSR PKI 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

DSR PKI does not charge a fee for accessing this CP/CPS. However, any use of the CP/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

Not Applicable.

9.2.2 Other Assets

DSR PKI customers that maintain assets outside the realm of the DSR PKI environment shall have access to sufficient financial resources to support operations and perform duties in accordance with the DSR PKI CP/CPS.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not Applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

- DSR PKI policies, procedures and technical documentation supporting this CP/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 DSR TLS CA hierarchy; and

- Compliance audit results except for WebTrust for CAs audit reports which may be published at the discretion of DSR PKI Management.

9.3.2 Information Not Within the Scope of Confidential Information

This CP/CPS and the Certificates and CRLs issued by DSR PKI are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

See §9.3.1.

9.4.1 Privacy Plan

DSR PKI shall follow the governing principles established by the Microsoft privacy statement located at https://privacy.microsoft.com/en-us/ with regards to the collection, handling, and storage of private information during the provision of DSR TLS CA services.

9.4.2 Information Treated as Private

Any 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

Subject to local laws, all information made public in a Certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

DSR PKI participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CP/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 is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

DSR PKI shall be entitled to disclose Confidential/Private Information if, in good faith, DSR PKI 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 CP/CPS;
- Policies and procedures supporting the operation of DSR PKI;
- Certificates and CRLs issued by DSR PKI managed CAs;
- Distinguished Names (DNs) used to represent entities within the DSR TLS CA hierarchy; and
- CA infrastructure and Subscriber key pairs.

DSR PKI participants acknowledge that DSR PKI retains all Intellectual Property Rights in and to this CP/CPS.

9.6 Representations and Warranties

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

9.6.1 CA Representations and Warranties

See §9.6

9.6.2 RA Representations and Warranties

See §9.6

9.6.3 Subscriber Representations and Warranties

See §9.6

9.6.4 Relying Party Representations and Warranties

See §9.6

9.6.5 Representations and Warranties of Other Participants

See §9.6

9.7 Disclaimers of Warranties

Except for express warranties stated in this CP/CPS, DSR PKI disclaims all other warranties, promises and other obligations. In addition, DSR PKI 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 DSR PKI, or use of Certificates beyond the prescribed use defined by this CP/CPS;
- Arising from the negligent or fraudulent use of Certificates or CRLs issued by the DSR PKI; and
- Due to disclosure of personal information contained within Certificates, CRLs or OCSP responses.

9.8 Limitations of Liability

In no event shall DSR PKI be liable for any indirect, consequential, incidental, special or punitive damages, or for any loss of profits, loss of data, or other indirect or consequential damages arising from or in connection with the use, delivery, license, availability or non-availability, performance or nonperformance of Certificates, digital signatures, the repository, or any other transactions or services offered or contemplated by this CP/CPS, even if DSR PKI has been advised of the possibility of such damages.

9.9 Indemnities

By their applying for and being issued Certificates, or otherwise relying upon such Certificates, Subscribers, and Relying Parties, agree to indemnify, defend, and hold harmless the CA, and its personnel, organizations, entities, subcontractors, suppliers, vendors, representatives, and agents from any errors, omissions, acts, failures to act, or negligence resulting in liability, losses, damages, suits, or expenses of any kind, due to or otherwise proximately caused by the use or publication of a Certificate that arises from the Subscriber's failure to provide the CA with current, accurate, and complete information at the time of Certificate application or the Subscriber's errors, omissions, acts, failures to act, and negligence.

The CA and its RAs are not the agents, fiduciaries, trustees, or other representatives of Subscribers or Relying Parties.

9.10 Term and Termination

9.10.1 Term

The CP/CPS becomes effective upon publication in the DSR PKI documentation repository.

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

9.10.2 Termination

No stipulation.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communications with Participants

Severance or merger may result in changes to the scope, management, and/or operations of this CA. In such an event, this CP/CPS may require modification as well.

Changes to the operations will occur consistent with the CA's disclosed CP/CPS management processes.

Notices to Application Software Vendors shall be sent in accordance with the respective requirements.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CP/CPS may be made by the DSR PKI and shall be approved by the DSR PKI Policy Management Authority as per §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 CP/CPS, the aggrieved party shall notify a member of DSR PKI management regarding the dispute. DSR PKI management will involve the appropriate Microsoft personnel to resolve the dispute.

9.14 Governing Law

This CP/CPS is governed by the laws in force in the State of Washington and the United States of America.

9.15 Compliance with Applicable Law

See §9.14.

9.16 Miscellaneous Provisions

This CP/CPS shall be binding on all successors of the parties.

If any provision of this CP/CPS is found to be unenforceable, the remaining provisions shall be interpreted to best carry out the reasonable intent of the parties. It is expressly agreed that every provision of this CP/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.

This CP/CPS shall be interpreted consistently with what is commercially reasonable in good faith under the circumstances and considering its international scope and uniform application. Failure by any person to enforce a provision of this CP/CPS will not be deemed a waiver of future enforcement of that or any other provision.

Any notice, demand, or request pertaining to this CP/CPS shall be communicated either using digitally signed messages consistent with this CP/CPS, or in writing. Electronic communications shall be effective when received by the intended recipient.

9.16.1 Entire Agreement

See §9.16

9.16.2 Assignment

See §9.16

9.16.3 Severability

See §9.16

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

See §9.16

9.16.5 Force Majeure

See §9.16

9.17 Other provisions

See §9.16