Microsoft PKI Services

Corporate Certification Practice Statement (CPS)

Version 3.1.7
May 22, 2023

Table of Contents

1. INTRODUCTION 10

1.1 OVERVIEW 10
1.2 DOCUMENT NAME AND IDENTIFICATION 10
1.2.1 Revisions 10
1.2.2 Relevant Dates 10
1.3 PKI PARTICIPANTS 10
1.3.1 Certification Authorities 10
1.3.1.1 Root CAs 11
1.3.1.2 Subordinate CAs 11
1.3.1.3 Issuing CAs 11
1.3.2 Registration Authorities 11
1.3.3 Subscribers 11
1.3.4 Relying Parties 12
1.3.5 Other Participants 12
1.4 CERTIFICATE USAGE 12
1.4.1 Appropriate Certificate Uses 12
1.4.2 Prohibited Certificate Uses 12
1.5 POLICY ADMINISTRATION 13
1.5.1 Organization Administering the Document 13
1.5.2 Contact Person 13
1.5.3 Person Determining CPS Suitability for the Policy 13
1.5.4 CPS Approval Procedures 13
1.6 DEFINITIONS AND ACRONYMS 13
1.6.1 Definitions 13
1.6.2 Acronyms 17
1.6.3 References 17
1.6.4 Conventions 18

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 18

2.1 REPOSITORIES 18
2.2 PUBLICATION OF CERTIFICATION INFORMATION 18
2.3 TIME OR FREQUENCY OF PUBLICATION 19
2.4 ACCESS CONTROLS ON REPOSITORIES 19

3. IDENTIFICATION AND AUTHENTICATION 19

3.1 NAMING 19
3.1.1 Type of Names 19
3.1.2 Need for Names to be Meaningful 19
3.1.3 Anonymity or Pseudonymity of Subscribers 19
3.1.4 Rules for Interpreting Various Name Forms 19
3.1.5 Uniqueness of Names 19

3.1.6 Recognition, Authentication, and Role of Trademarks **19**
3.2 INITIAL IDENTITY VALIDATION **20**
3.2.1 Method to Prove Possession of Private Key **20**
3.2.2 Authentication of Organization Identity **20**
3.2.2.1 Identity 20
3.2.2.2 DBA/Tradename 20
3.2.2.3 Verification of Country 20
3.2.2.4 Validation of Domain Authorization or Control 20
3.2.2.4.1 Validating the Applicant as a Domain Contact 20
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact 20
3.2.2.4.3 Phone Contact with Domain Contact 20
3.2.2.4.4 Constructed Email to Domain Contact 20
3.2.2.4.5 Domain Authorization Document 20
3.2.2.4.6 Agreed-Upon Change to Website 21
3.2.2.4.7 DNS Change 21
3.2.2.4.8 IP Address 21
3.2.2.4.9 Test Certificate 21
3.2.2.4.10 TLS Using a Random Number 21
3.2.2.4.11 Any Other Methods 21
3.2.2.4.12 Validating Applicant as a Domain Contact 21
3.2.2.5 Authentication for an IP Address 21
3.2.2.6 Wildcard Domain Validation 21
3.2.2.7 Data Source Accuracy 21
3.2.2.8 CAA Records 21
3.2.3 Authentication of Individual Identity **21**
3.2.4 Non-Verified Subscriber Information **21**
3.2.5 Validation of Authority **21**
3.2.6 Criteria for Interoperation **22**
3.2.7 Criteria for PKI Operating Groups **22**
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS **22**
3.3.1 Identification and Authentication for Routine Re-Key **22**
3.3.2 Identification and Authentication for Re-Key After Revocation **22**
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST **22**
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS **22**
4.1 CERTIFICATE APPLICATION **22**
4.1.1 Who Can Submit a Certificate Application **22**
4.1.2 Enrollment Process and Responsibilities **23**
4.2 CERTIFICATE APPLICATION PROCESSING **23**
4.2.1 Performing Identification and Authentication Functions **23**
4.2.2 Approval or Rejection of Certificate Applications **23**
4.2.3 Time to Process Certificate Applications **23**
4.3 CERTIFICATE ISSUANCE **23**
4.3.1 CA Actions During Certificate Issuance **23**
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate **24**
4.4 CERTIFICATE ACCEPTANCE **24**
4.4.1 Conduct Constituting Certificate Acceptance **24**

4.4.2 Publication of the Certificate by the CA 24
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 24
4.5 KEY PAIR AND CERTIFICATE USAGE 24
4.5.1 Subscriber Private Key and Certificate Usage 24
4.5.2 Relying Party Public Key and Certificate Usage 24
4.6 CERTIFICATE RENEWAL 24
4.6.1 Circumstance for Certificate Renewal 24
4.6.2 Who May Request Renewal 25
4.6.3 Processing Certificate Renewal Requests 25
4.6.4 Notification of New Certificate Issuance to Subscriber 25
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 25
4.6.6 Publication of the Renewal Certificate by the CA 25
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 25
4.7 CERTIFICATE RE-KEY 25
4.7.1 Circumstance for Certificate Re-Key 25
4.7.2 Who May Request Certification of a New Public Key 25
4.7.3 Processing Certificate Re-keying Requests 25
4.7.4 Notification of New Certificate Issuance to Subscriber 25
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 26
4.7.6 Publication of the Re-keyed Certificate by the CA 26
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 26
4.8 CERTIFICATE MODIFICATION 26
4.8.1 Circumstance for Certificate Modification 26
4.8.2 Who May Request Certificate Modification 26
4.8.3 Processing Certificate Modification Requests 26
4.8.4 Notification of New Certificate Issuance to Subscriber 26
4.8.5 Conduct Constituting Acceptance of Modified Certificate 26
4.8.6 Publication of the Modified Certificate by the CA 26
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 26
4.9 CERTIFICATE REVOCATION AND SUSPENSION 26
4.9.1 Circumstances for Revocation 26
4.9.1.1 Reasons for Revoking a Subscriber Certificate 27
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate 27
4.9.2 Who Can Request Revocation 27
4.9.3 Procedure for Revocation Request 27
4.9.4 Revocation Request Grace Period 27
4.9.5 Time Within Which CA Must Process the Revocation Request 28
4.9.6 Revocation Checking Requirement for Relying Parties 28
4.9.7 CRL Issuance Frequency 28
4.9.8 Maximum Latency for CRLs 28
4.9.9 On-Line Revocation/Status Checking Availability 28
4.9.10 On-Line Revocation Checking Requirements 28
4.9.11 Other Forms of Revocation Advertisements Available 28
4.9.12 Special Requirements re Key Compromise 28
4.9.13 Circumstances for Suspension 28

4.9.14 Who Can Request Suspension **28**
4.9.15 Procedure for Suspension Request **28**
4.9.16 Limits on Suspension Period **29**
4.10 CERTIFICATE STATUS SERVICES **29**
4.10.1 Operational Characteristics **29**
4.10.2 Service Availability **29**
4.10.3 Optional Features **29**
4.11 END OF SUBSCRIPTION **29**
4.12 KEY ESCROW AND RECOVERY **29**
4.12.1 Key Escrow and Recovery Policy and Practices **29**
4.12.2 Session Key Encapsulation and Recovery Policy and Practices **29**
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS **29**
5.1 PHYSICAL CONTROLS **29**
5.1.1 Site Location and Construction **29**
5.1.2 Physical Access **29**
5.1.3 Power and Air Conditioning **30**
5.1.4 Water Exposures **30**
5.1.5 Fire Prevention and Protection **30**
5.1.6 Media Storage **30**
5.1.7 Waste Disposal **30**
5.1.8 Off-Site Backup **30**
5.2 PROCEDURAL CONTROLS **30**
5.2.1 Trusted Roles **30**
5.2.2 Number of Persons Required per Task **31**
5.2.3 Identification and Authentication for Each Role **31**
5.2.4 Roles Requiring Separation of Duties **31**
5.3 PERSONNEL CONTROLS **31**
5.3.1 Qualifications, Experience, and Clearance Requirements **31**
5.3.2 Background Check Procedures **31**
5.3.3 Training Requirements **31**
5.3.4 Retraining Frequency and Requirements **31**
5.3.5 Job Rotation Frequency and Sequence **32**
5.3.6 Sanctions for Unauthorized Actions **32**
5.3.7 Independent Contractor Requirements **32**
5.3.8 Documentation Supplied to Personnel **32**
5.4 AUDIT LOGGING PROCEDURES **32**
5.4.1 Types of Events Recorded **32**
5.4.2 Frequency of Processing Log **33**
5.4.3 Retention Period for Audit Log **33**
5.4.4 Protection of Audit Log **34**
5.4.5 Audit Log Backup Procedures **34**
5.4.6 Audit Collection System (Internal vs. External) **34**
5.4.7 Notification to Event-Causing Subject **34**

5.4.8 Vulnerability Assessments 34
5.5 RECORDS ARCHIVAL 34
5.5.1 Types of Records Archived 34
5.5.2 Retention Period for Archive 34
5.5.3 Protection of Archive 34
5.5.4 Archive Backup Procedures 34
5.5.5 Requirements for Time-Stamping of Records 35
5.5.6 Archive Collection System (Internal or External) 35
5.5.7 Procedures to Obtain and Verify Archive Information 35
5.6 KEY CHANGEOVER 35
5.7 COMPROMISE AND DISASTER RECOVERY 35
5.7.1 Incident and Compromise Handling Procedures 35
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 35
5.7.3 Entity Private Key Compromise Procedures 35
5.7.4 Business Continuity Capabilities After a Disaster 35
5.8 CA OR RA TERMINATION 35
6. TECHNICAL SECURITY CONTROLS 36
6.1 KEY PAIR GENERATION AND INSTALLATION 36
6.1.1 Key Pair Generation 36
6.1.1.1 CA Key Pair Generation 36
6.1.1.2 RA Key Pair Generation 36
6.1.1.3 Subscriber Key Pair Generation 36
6.1.2 Private Key Delivery to Subscriber 36
6.1.3 Public Key Delivery to Certificate Issuer 36
6.1.4 CA Public Key Delivery to Relying Parties 36
6.1.5 Key Sizes 36
6.1.6 Public Key Parameter Generation and Quality Checking 38
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 38
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 38
6.2.1 Cryptographic Module Standards and Controls 38
6.2.2 Private Key (m out of n) Multi-Person Control 38
6.2.3 Private Key Escrow 38
6.2.4 Private Key Backup 38
6.2.5 Private Key Archival 38
6.2.6 Private Key Transfer into or From a Cryptographic Module 39
6.2.7 Private Key Storage on Cryptographic Module 39
6.2.8 Method of Activating Private Key 39
6.2.9 Method of Deactivating Private Key 39
6.2.10 Method of Destroying Private Key 39
6.2.11 Cryptographic Module Rating 39
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 39
6.3.1 Public Key Archival 39
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 39

6.4 ACTIVATION DATA 40
6.4.1 Activation Data Generation and Installation 40
6.4.2 Activation Data Protection 40
6.4.3 Other Aspects of Activation Data 40
6.5 COMPUTER SECURITY CONTROLS 40
6.5.1 Specific Computer Security Technical Requirements 40
6.5.2 Computer Security Rating 40
6.6 LIFE CYCLE TECHNICAL CONTROLS 40
6.6.1 System Development Controls 40
6.6.2 Security Management Controls 40
6.6.3 Life Cycle Security Controls 40
6.7 NETWORK SECURITY CONTROLS 40
6.8 TIME-STAMPING 41
7. CERTIFICATE, CRL, AND OCSP PROFILES 41
7.1 CERTIFICATE PROFILE 41
7.1.1 Version Number(s) 41
7.1.2 Certificate Extensions 41
7.1.2.1 Root CA Certificate 41
7.1.2.2. Subordinate CA Certificate 43
7.1.2.3 Subscriber Certificate 43
7.1.2.4 All Certificates 45
7.1.2.5 Application of RFC 5280 45
7.1.3 Algorithm Object Identifiers 45
7.1.4 Name Forms 45
7.1.4.1. Issuer Information 45
7.1.4.2. Subject Information – Subscriber Certificates 45
7.1.4.2.1. Subject Alternative Name Extension 45
7.1.4.2.2. Subject Distinguished Name Fields 45
7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates 45
7.1.4.3.1. Subject Distinguished Name Fields 45
7.1.5 Name Constraints 46
7.1.6 Certificate Policy Object Identifier 46
7.1.6.1 Reserved Certificate Policy Object Identifiers 46
7.1.6.2 Root CA Certificates 46
7.1.6.3 Subordinate CA Certificates 46
7.1.6.4 Subscriber Certificates 46
7.1.7 Usage of Policy Constraints Extension 46
7.1.8 Policy Qualifiers Syntax and Semantics 46
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 46
7.2 CRL PROFILE 46
7.2.1 Version Number(s) 46
7.2.2 CRL and CRL Entry Extensions 46
7.3 OCSP PROFILE 46
7.3.1 Version Number(s) 47
7.3.2 OCSP Extensions 47

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 47
8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT 47
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 47
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 47
8.4 TOPICS COVERED BY ASSESSMENT 47
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 47
8.6 COMMUNICATION OF RESULTS 48
8.7 SELF-AUDITS 48
9. OTHER BUSINESS AND LEGAL MATTERS 48
9.1 FEES 48
9.1.1 Certificate Issuance or Renewal Fees 48
9.1.2 Certificate Access Fees 48
9.1.3 Revocation or Status Information Access Fees 48
9.1.4 Fees for Other Services 48
9.1.5 Refund Policy 48
9.2 FINANCIAL RESPONSIBILITY 48
9.2.1 Insurance Coverage 48
9.2.2 Other Assets 49
9.2.3 Insurance or Warranty Coverage for End-Entities 49
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 49
9.3.1 Scope of Confidential Information 49
9.3.2 Information Not Within the Scope of Confidential Information 49
9.3.3 Responsibility to Protect Confidential Information 49
9.4 PRIVACY OF PERSONAL INFORMATION 49
9.4.1 Privacy Plan 49
9.4.2 Information Treated as Private 50
9.4.3 Information Not Deemed Private 50
9.4.4 Responsibility to Protect Private Information 50
9.4.5 Notice and Consent to Use Private Information 50
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 50
9.4.7 Other Information Disclosure Circumstances 50
9.5 INTELLECTUAL PROPERTY RIGHTS 50
9.6 REPRESENTATIONS AND WARRANTIES 50
9.6.1 CA Representations and Warranties 51
9.6.2 RA Representations and Warranties 51
9.6.3 Subscriber Representations and Warranties 51
9.6.4 Relying Party Representations and Warranties 51
9.6.5 Representations and Warranties of Other Participants 51
9.7 DISCLAIMERS OF WARRANTIES 51
9.8 LIMITATIONS OF LIABILITY 51
9.9 INDEMNITIES 52
9.9.1 Indemnification by CAs 52

9.9.2 Indemnification by Subscribers **52**
9.9.3 Indemnification by Relying Parties **52**
9.10 TERM AND TERMINATION **53**
9.10.1 Term **53**
9.10.2 Termination **53**
9.10.3 Effect of Termination and Survival **53**
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS **53**
9.12 AMENDMENTS **53**
9.12.1 Procedure for Amendment **53**
9.12.2 Notification Mechanism and Period **53**
9.12.3 Circumstances under which OID must be changed **53**
9.13 DISPUTE RESOLUTION PROVISIONS **54**
9.14 GOVERNING LAW **54**
9.15 COMPLIANCE WITH APPLICABLE LAW **54**
9.16 MISCELLANEOUS PROVISIONS **54**
9.16.1 Entire Agreement **54**
9.16.2 Assignment **54**
9.16.3 Severability **54**
9.16.4 Enforcement (attorneys' fees and waiver of rights) **55**
9.16.5 Force Majeure **55**
9.17 OTHER PROVISIONS **55**

1. INTRODUCTION

1.1 OVERVIEW

This Certification Practice Statement (CPS) is the principle document that governs the minimum requirements for the public and private lifecycle management of Microsoft PKI Services' Certification Authority (CA) solutions and services for Microsoft Product Groups and affiliated entities operating within the Public Key Infrastructure (PKI) Certification Authority (CA) hierarchies.

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

Other important documents that accompany this CPS include the presiding CP and associated subscriber and relying party agreements. Microsoft may publish additional Certificate Policies or Certification Practice Statements, as necessary, to describe other products or service offerings.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 standards for the creation of Certificate Policy (CP) and Certification Practices Statement (CPS) documents.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is formally referred to as the "Microsoft PKI Services Certification Practice Statement" (referred to as "CPS"). Microsoft CAs SHALL issue certificates in accordance with the policy and practice requirements of this document. The Object Identifier (OID) for this CPS is: 1.3.6.1.4.1.311.76.509.1.3

1.2.1 Revisions

See Appendix A

1.2.2 Relevant Dates

No Stipulation

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

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

The two main categories of CAs that exist within the Microsoft PKI Services' PKI hierarchy are the Root CAs and Subordinate CAs. Up-to-date records of CAs are maintained by Microsoft PKI Services.

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

- Generating, issuing and distributing public key certificates in accordance with this CPS;
- Distributing CA certificates;
- Generating and publishing certificate status information (such as CRLs);
- Maintaining the security, availability, and continuity of the certificate issuance and CRL signing functions;
- Providing a means for Subscribers to request revocation;
- Ensuring that changes in certificate status are reflected in their own repositories and those of authorized certificate validation authorities within the times specified in Section 4 of this CPS.
- Ensuring that changes in certificate status are reflected in its own repositories and those of authorized certificate validation authorities within the times specified in Section 4 of this CPS.

1.3.1.1 Root CAs

Root CAs serve as the "trust anchors" for the Microsoft PKI Services CA hierarchy and issue any new CAs for different types of PKI services.

1.3.1.2 Subordinate CAs

The primary function of Subordinate CAs is to issue additional CAs and/or Subscriber certificates.

1.3.1.3 Issuing CAs

The primary function of an Issuing CA is to issue Subscriber certificates to internal Microsoft Product Groups or approved 3rd Party entities. Issuing CAs are further classified in the following categories:

- **Microsoft PKI Services managed CAs:** this category consists of CAs hosted and managed by the Microsoft PKI Services team.
- **Microsoft PKI Operating Group (POG) managed CAs**: this category consists of CAs that are hosted and managed by affiliated Microsoft Product Groups Roots and are subordinate to Root CAs managed by the Microsoft PKI Services team.

1.3.2 Registration Authorities

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

1.3.3 Subscribers

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

accountability is attributable to the organization.

Obligations of Subscribers within the Microsoft PKI Services PKI hierarchy include:

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

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

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

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

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

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

1.4.2 Prohibited Certificate Uses

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

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The Microsoft PKI Policy Authority is responsible for the maintenance of this CPS

1.5.2 Contact Person

Contact information is listed below:

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

To request certificate revocation or to report security issues such as suspected key compromise, certificate misuse, fraud or other matters, contact CentralPKI@microsoft.com.

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

The Microsoft PKI Policy Authority reviews and approves any changes to this CPS, in compliance with the CP.

1.6 DEFINITIONS AND ACRONYMS

Capitalized terms and acronyms, not included herein, MAY be specified in the Certificate Policy.

1.6.1 Definitions

- **Affiliate –** A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
- **Applicant** – a natural person or Legal Entity that applies for (or seeks renewal of) a Certificate by a CA.
- **Application Software Supplier** – A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
- **Authorized Ports:** One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

- **Baseline Requirements (BR)** – An integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements issued by the CA/Browser Forum and available at cabforum.org.
- **CA/Browser Forum (CAB Forum)** – A consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of digital certificates. Details are available at: cabforum.org.
- **Certificate** – A digital record that contains information such as the Subscriber's distinguished name and public key, and the signer's signature and data.
- **Certificate Application –** a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
- **Certificate Request** – an application for a new Certificate or a renewal of a Certificate.
- **Certificate Revocation List (CRL)** – periodically published listing of all certificates that have been revoked for use by Relying Parties
- **Certificate Signing Request (CSR)** – a message sent to the certification authority containing the information required to issue a digital certificate
- **Certification Authority (CA)** – an entity or organization that is responsible for the authorization, issuance, revocation, and management of a certificate. The term equally applies to Roots CAs and Subordinate CAs.
- **Certificate Owner** – Parties designated by business process owners to be associated with and/or have responsibility for specified issued certificates.
- **Certificate Policy (CP)** – A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- **Certification Practice Statement (CPS) –** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- **Distinguished Name (DN)** – a globally unique identifier representing a Subject that is used on Certificates and in the Repository
- **Extended Key Usage –** An extension in an X.509 certificate to indicate the allowed purpose(s) for the use of the public key. Also referenced or known as "Enhanced Key Usage".
- **Issuing CA** – The first digital certificate issuing authority who issues certificates signed by the root certificate authority (CA).
- **Legal Entity** – An association, corporation, partnership, proprietorship, trust, or government entity that has legal standing in a country's legal system.
- **Microsoft PKI Oversight Committee –** The overseer of the Microsoft PKI Services Policy

Authority (PA) and consists of the Vice Presidents from at least three appropriate groups across Microsoft.

- **Microsoft PKI Operating Group (POG) –** a group of cross-company or divisional teams that manage a PKI hierarchy, which includes as least one CA.
- **Microsoft PKI Policy Authority –** consists of two governing bodies. The Microsoft PKI Steering Committee and the Microsoft PKI Oversight Committee.
- **Microsoft PKI Services –** the Microsoft PKI Certification and Registration Authority that manages keys, certificates, and the provisioning of certificates.
- **Microsoft PKI Standards –** A collection of policies and procedures that any Microsoft organization must follow to operate PKI services. All PKI Operating Groups (POGs) at Microsoft must demonstrate compliance with these standards.
- **Microsoft PKI Steering Committee –** the primary decision-making body that exercises its authority in support of Microsoft PKI Service's endeavors, maintaining alignment between business strategy and technical governance. It consists of PKI subject matter experts from across Microsoft.
- **Online CA** – a certification authority system which signs end-entity Subscriber Certificates that are operated and maintained in an online state so as to provide continually available certificate signing services. Online CAs reside in segmented, secured, and functionally dedicated networks.
- **Offline CA** – A root CA, subordinate CA, or issuing CA that are maintained offline for security reasons in order to protect them from possible attacks by intruders over the network.
- **Private Key –** The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- **Public Key –** The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- **Public Key Infrastructure (PKI) –** A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
- **Registration Authority (RA)** – Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- **Registration Identifier –** the unique code assigned to an Applicant by the Incorporating or

Registration Agency in such entity's Jurisdiction of Incorporation or Registration.

- **Relying Party** – a Relying Party is an individual or entity that acts in reliance on a Certificate or digital signature associated with a Certificate.
- **Relying Party Agreement** – an agreement which specifies the stipulations under which a person or organization acts as a Relying Party
- **Repository** – an online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- **Root CA** – The top-level CA whose root certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- **Signing Service** – an organization that signs an Object on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.
- **Subscriber** – an individual or end-entity (person, device, or application) that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate
- **Subscriber Agreement –** an agreement containing the terms and conditions that the authorized Subscriber consented to for the use of their issued certificate, containing the private key and corresponding public key.
- **Suspect Code –** code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes**.**
- **Takeover Attack** – an attack where a Signing Service or Private Key associated with the Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.
- **Technically Constrained Subordinate CA Certificate –** a Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate MAY issue Subscriber or additional Subordinate CA Certificates**.**
- **TimeStamp Authority –** a service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via secure hashing algorithm) existed at the specific time.
- **Transport Layer Security (TLS)/Secure Socket Layer (SSL) –** a **s**ecurity protocol that is widely used in the Internet, for the purpose of authentication and establishing secure sessions
- **Trusted Role –** An employee or contractor of a CA or Delegated Third Party who has

authorized access to or control over a Secure Zone or High Security Zone.

- **WebTrust for Certification Authorities (WTCA)** - a program that helps ensure proper procedures are followed by Certification Authorities (CAs) for activities involving e-commerce transactions, public key infrastructure (PKI), and cryptography.

1.6.2 Acronyms

Term	Definition
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTL	Time to Live

1.6.3 References

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

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

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

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

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

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

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

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

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

1.6.4 Conventions

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

A repository of Microsoft PKI Services CA information and associated policy documents is maintained by Microsoft PKI Services and SHALL be made available upon request.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

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

2.3 TIME OR FREQUENCY OF PUBLICATION

Microsoft PKI Services SHALL annually review this CPS for any changes to internal PKI practices or the presiding Certificate Policy.

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

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

Microsoft PKI Services offers CRLs showing the revocation status of Microsoft PKI Services Certificates. CRLs will be published in accordance with Section 4.9.6 and Section 4.9.7.

2.4 ACCESS CONTROLS ON REPOSITORIES

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Type of Names

Certificates SHALL be issued in accordance with the X.509 v3 standard. The certificate profiles for specifying names SHALL conform with requirements in Section 7.

3.1.2 Need for Names to be Meaningful

Distinguished names SHALL identify both the entity (i.e. person, organization, device, or object) that is the subject of the certificate and the entity that is the issuer of the certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

No Stipulation

3.1.4 Rules for Interpreting Various Name Forms

No Stipulation

3.1.5 Uniqueness of Names

No Stipulation

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The Registration and/or Issuance process SHALL involve procedures in which the applicant demonstrates possession of the Private Key by using a method approved by Microsoft PKI Services.

In cases where a key pair is generated by the CA on behalf of a Subscriber, proof of possession of the private key is not required.

3.2.2 Authentication of Organization Identity

All Microsoft employees (full-time and part-time) may submit requests for Certificates/Keys to be issued by CAs managed and hosted by Microsoft PKI Services. The Subscriber's employment with Microsoft shall be verified with the existence of a valid Microsoft issued smart-card employee badge, in order to submit requests. A smart-card or other multi-factor authentication method is not required in the case of automated/systematic request.

3.2.2.1 Identity

No Stipulation

3.2.2.2 DBA/Tradename

No Stipulation

3.2.2.3 Verification of Country

No Stipulation

3.2.2.4 Validation of Domain Authorization or Control

No Stipulation

3.2.2.4.1 Validating the Applicant as a Domain Contact

No Stipulation

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

No Stipulation

3.2.2.4.3 Phone Contact with Domain Contact

No Stipulation

3.2.2.4.4 Constructed Email to Domain Contact

No Stipulation

3.2.2.4.5 Domain Authorization Document

No Stipulation

3.2.2.4.6 Agreed-Upon Change to Website

No Stipulation

3.2.2.4.7 DNS Change

No Stipulation

3.2.2.4.8 IP Address

No Stipulation

3.2.2.4.9 Test Certificate

No Stipulation

3.2.2.4.10 TLS Using a Random Number

No Stipulation

3.2.2.4.11 Any Other Methods

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

No Stipulation

3.2.2.5 Authentication for an IP Address

No Stipulation

3.2.2.6 Wildcard Domain Validation

No Stipulation

3.2.2.7 Data Source Accuracy

No Stipulation

3.2.2.8 CAA Records

No Stipulation

3.2.3 Authentication of Individual Identity

No Stipulation

3.2.4 Non-Verified Subscriber Information

No Stipulation

3.2.5 Validation of Authority

No Stipulation

3.2.6 Criteria for Interoperation

No Stipulation

3.2.7 Criteria for PKI Operating Groups

At least one of the following criteria options SHALL be used to determine if a third party and/or Microsoft PKI Operating Group (POG) should receive a Subordinate CA from Microsoft PKI Services.

- A signed contractual agreement between Microsoft and the entity operating the CA
- The entity operating the CA maintains an annual WTCA certification of their CA services and provides sufficient evidence of such certification to Microsoft PKI Services
- A Microsoft PKI Operating Group (POG) receiving the CA has completed an internal compliance assessment against Microsoft PKI Standards
- The Microsoft PKI Steering Committee and the team performing an internal compliance assessment against the Microsoft PKI Standards have approved issuance of Subordinate CA(s) to the third party or Microsoft PKI Operating Group (POG)

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

Microsoft PKI Services CAs SHALL treat certificate re-key requests identical to applications for new certificates.

3.3.2 Identification and Authentication for Re-Key After Revocation

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

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

Certificate Applications MAY be submitted by an Applicant or authorized Certificate Requestor, provided the Certificate Request meets the requirements set forth in this CPS and/or CP.

Requests MAY be submitted from designated business users from Microsoft product groups or by the Microsoft PKI Services team on behalf of customers.

4.1.2 Enrollment Process and Responsibilities

Prior to the issuance of a certificate, an Applicant SHALL perform the following:

1. Complete and submit a digitally signed certificate request.
2. Have an approved Subscriber Agreement, which MAY be an electronic acknowledgement.
3. Consent to any other terms and conditions, which MAY be an electronic acknowledgement.

Certificate Applicants are required to fully comply with the aforementioned prior to certificate issuance.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

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

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

4.2.2 Approval or Rejection of Certificate Applications

Submitted Certificate applications, MUST be reviewed and approved by Microsoft PKI Services or appointed RA prior to issuance. Certificate Applications MAY be approved if the requirements of Section 3.2.2 are met.

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

- Applicant or Subscriber information is unable to be verified, per Section 3.2.2;
- Microsoft PKI Services deems the certificate issuance MAY negatively impact their business or reputation;
- Failure to consent to the Subscriber Agreement;
- Failure to consent to any other terms and conditions

Microsoft PKI Services reserves the right to not disclose reasons for refusal.

4.2.3 Time to Process Certificate Applications

Certification applications SHALL be processed within a commercially reasonable time frame. Microsoft PKI Services SHALL NOT be responsible for processing delays initiated by the applicant or from events outside of the CA's control.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

The source of the certificate request SHALL be verified before issuance. Certificates are generated, issued and distributed only after the CA or RA performs the required identification

and authentication steps in accordance with Section 3. Certificates SHALL be checked to ensure that all fields and extensions are properly populated. Exceptions to defined Certificate Policies MUST be approved by the Microsoft PKI Policy Authority.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

Certificates SHALL be published in the Microsoft PKI Services repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate SHALL only be permitted once the Subscriber has agreed to the Subscriber agreement and accepted the certificate.

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

Subscribers SHALL protect their private keys from unauthorized use and discontinue use of the private key following expiration or revocation of the certificate.

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

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties SHALL use public key certificates and associated public keys for the sole purposes as constrained by this CPS or the CP and Certificate extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates. Relying Parties are subject to the terms of the Relying Party Agreement.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

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

4.6.2 Who May Request Renewal

Certificate Renewals MAY be requested by the Subscriber or an authorized agent, providing the renewal request meets the requirements set forth in this CPS and the presiding CP.

4.6.3 Processing Certificate Renewal Requests

Renewal requests follow the same validation and authentication procedures as a new certificate request and MAY re-use the information provided with the original certificate request, for means of verification; however, new key pairs are required.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6 Publication of the Renewal Certificate by the CA

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

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

4.7 CERTIFICATE RE-KEY

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

4.7.1 Circumstance for Certificate Re-Key

No stipulation

4.7.2 Who May Request Certification of a New Public Key

No stipulation

4.7.3 Processing Certificate Re-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

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

4.8.1 Circumstance for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

No stipulation

4.8.3 Processing Certificate Modification Requests

No stipulation

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation

4.8.6 Publication of the Modified Certificate by the CA

No stipulation

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

Revocation MAY take place at the discretion of Microsoft PKI Services upon receiving information of a security or integrity threat to the certificate, a Subscriber, or Relying Party.

Any subscriber can request a revocation, but they are required to provide justification. Microsoft PKI Services, if approved, will process revocation. In some cases, PKI Policy Authority approval MAY be required.

4.9.1.1 Reasons for Revoking a Subscriber Certificate

A Subscriber Certificate revocation request SHALL commence an investigation and plan for revocation within 24 hours if any of the circumstances in Section 4.9.1 occur.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

A Subordinate CA Certificate revocation request SHALL commence an investigation and plan for revocation within seven (7) days if any of the circumstances in Section 4.9.1 occur.

4.9.2 Who Can Request Revocation

Certificate revocation can be requested by Subscribers or Certificate Owners. Revocation can also be initiated at the discretion of Microsoft PKI Services.

4.9.3 Procedure for Revocation Request

Microsoft PKI Services MAY process revocation requests using at least the following steps:

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

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

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

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

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

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

Microsoft PKI Services SHALL post new CRL entries as soon as a revocation request is fulfilled.

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation/Status Checking Availability

No Stipulation

4.9.10 On-Line Revocation Checking Requirements

No Stipulation

4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation

4.9.12 Special Requirements re Key Compromise

See Section 4.9.1

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

No Stipulation

4.10.2 Service Availability

Certificate Status Services shall be available 24 x 7 without scheduled interruption.

4.10.3 Optional Features

No Stipulation

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

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

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

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

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

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

system administrators, operators, engineers, and certain executives who are designated to oversee CA operations.

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

5.2.2 Number of Persons Required per Task

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

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Roles Requiring Separation of Duties

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

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

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

Any personnel occupying a trusted role, as defined in 5.2.1, MUST possess suitable experience and be deemed qualified. Personnel in trusted roles SHALL undergo training prior to performing any duties as part of that role.

5.3.2 Background Check Procedures

Prior to assignment in a Trusted Role position, the prospective Microsoft PKI Services personnel SHALL undergo and clear the necessary background checks or security screening requirements, per Microsoft hiring policies and local laws.

5.3.3 Training Requirements

All personnel involved with CA operations SHALL receive and pass the required training to perform the duties relative to their assigned Trusted Role. Microsoft PKI Services SHALL retain records of the training completed by such individuals.

5.3.4 Retraining Frequency and Requirements

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

Microsoft PKI Services SHALL maintain records of all training taken by Trusted Role personnel.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Microsoft PKI Services may employ contractors, as necessary. Contractors SHALL adhere to background checks, training, skills assessment, and audit requirements, as appropriate for their role.

5.3.8 Documentation Supplied to Personnel

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

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

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

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

Microsoft PKI Services 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 and OCSP entries;
    f. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Microsoft PKI Services' Subscriber Certificate lifecycle management events,

including:

a. Certificate requests, renewal, and re-key requests, and revocation;
b. All verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement;
c. Approval and rejection of certificate requests;
d. Issuance of Certificates; and
e. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. Installation, update and removal of software on a Certificate System;
   e. System crashes, hardware failures, and other anomalies;
   f. Firewall and router activities; and
   g. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

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

5.4.2 Frequency of Processing Log

Audit logs are reviewed on an as-needed basis.

5.4.3 Retention Period for Audit Log

Microsoft PKI Services SHALL retain, for at least two (2) years after the following conditions:

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

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

No Stipulation

5.4.7 Notification to Event-Causing Subject

No Stipulation

5.4.8 Vulnerability Assessments

Microsoft PKI Services maintains detection and prevention security controls to safeguard Certificate Systems against potential threats or vulnerabilities.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

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

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

Microsoft PKI Services SHALL employ appropriate systems for the collection and maintenance of archived records.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 KEY CHANGEOVER

No Stipulation

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

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

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

See Section 5.7.4.

5.7.3 Entity Private Key Compromise Procedures

Microsoft PKI Services' maintains procedures to address incidents in which a CA Private Key is suspected to be or has been compromised.

5.7.4 Business Continuity Capabilities After a Disaster

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

5.8 CA OR RA TERMINATION

In the event that it is necessary to terminate the operation of a CA, Microsoft PKI Services management will plan and coordinate the termination process with its Subscribers and Relying Parties, such that the impact of the termination is minimized. Microsoft PKI Services will make a commercially reasonable effort to provide prior notice to Subscribers and Relying Parties and

preserve relevant records for a period of time deemed fit for functional and legal purposes.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

6.1.1.2 RA Key Pair Generation

No Stipulation

6.1.1.3 Subscriber Key Pair Generation

The Subscriber may generate their own key pairs, in accordance to the requirements set forth in Section 6.1.5 and 6.1.6. If the Subscriber does not adhere to these requirements or has a known weak private key, Microsoft PKI Services SHALL reject the certificate request.

It is recommended that the subscriber use a FIPS 140-2 certified cryptographic module for key generation.

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

No Stipulation

6.1.4 CA Public Key Delivery to Relying Parties

No Stipulation

6.1.5 Key Sizes

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

Root CA, Subordinate CA, and Subscriber Certificates

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

The following tables contains the minimum key sizes for CA and End Entity certificates issued by the Microsoft PKI Services hierarchy:

(1) Root CA Certificates

Key Algorithm	Certificates Created Before Jan 1, 2014	Certificates Created After Jan 1, 2014	Certificates Expiring Before Dec 31, 2030	Certificates Expiring After Dec 31, 2030
RSA	2048 or greater	4096 or greater	2048 or greater	4096 or greater
ECC	NIST P-256, NIST P-384, NIST P-521	NIST P-384, NIST P-521	NIST P-256, NIST P-384, NIST P-521	NIST P-384, NIST P-521

(2) Subordinate CA Certificates (Primary or Issuing CAs)

Key Algorithm	Certificates Created Before Jan 1, 2014	Certificates Created After Jan 1, 2014	Certificates Expiring Before Dec 31, 2030	Certificates Expiring After Dec 31, 2030
RSA	2048 or greater	4096 or greater	2048 or greater	4096 or greater
ECC	NIST P-256, NIST P-384, NIST P-521	NIST P-384, NIST P-521	NIST P-256, NIST P-384, NIST P-521	NIST P-384, NIST P-521

*NOTE: The CA can only issue SHA-1 certificates for code-signing and timestamping functionality to legacy platforms that do not support SHA-2. Certificates with smaller public key modulus bit sizes must be approved by the PKI Policy Authority. The CA SHALL reject a certificate request if the requested Public Key does not meet the minimum algorithm key sizes specified in this section.

(3) End-Entity (Subscriber Certificates)

Key Algorithm	Certificates Created Before Jan 25, 2013	Certificates Created After Jan 25, 2013	Certificates Expiring Before Dec 31, 2030	Certificates Expiring After Dec 31, 2030
RSA	1024 or greater	2048 or greater	2048 or greater	4096 or greater
ECC	N/A	NIST P-256, NIST P-384, NIST P-521	NIST P-256, NIST P-384, NIST P-521	NIST P-256, NIST P-384, NIST P-521

*NOTE: Certificates with smaller public key modulus bit sizes must be approved by the Microsoft PKI Policy Authority. Any use of SHA-1 MUST only be for legacy platforms that do not support SHA-2. Exceptions require the approval of the Microsoft PKI Policy Authority.

6.1.6 Public Key Parameter Generation and Quality Checking

Microsoft PKI Services SHALL generate Private Keys using secure algorithms and parameters based on current research and industry standards.

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

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

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

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

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

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

6.2.1 Cryptographic Module Standards and Controls

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

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

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

6.2.3 Private Key Escrow

No Stipulation

6.2.4 Private Key Backup

Backup copies of CA private keys SHALL be backed up by multiple persons in trusted role positions and only be stored in encrypted form on cryptographic modules that meet the requirements specified in Section 6.2.1.

6.2.5 Private Key Archival

No Stipulation

6.2.6 Private Key Transfer into or From a Cryptographic Module

No Stipulation

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.1

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

No Stipulation

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. The destruction process shall be performed by multiple Trust Role personnel and documented using verifiable methods.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

Entity Type	Maximum Certificate Validity Period
Root CA	25 Years
Subordinate CAs	20 Years
Online Subordinate CAs	6 Years
Subscribers	15 months

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

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

No Stipulation

6.4.3 Other Aspects of Activation Data

No Stipulation

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

Microsoft PKI Services systems SHALL be secured from unauthorized access using multi-factor authentication security controls.

6.5.2 Computer Security Rating

No Stipulation

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

All in-house developed CA software is built in accordance with documented Microsoft systems development processes. Approvals are required at all stages of development by the management. All code is verified, using digital signatures and hashing, before being deployed into the production CA environment.

6.6.2 Security Management Controls

Microsoft PKI Services has tools and processes in place to control and monitor the configurations of the CA systems, physical and logical access, and performs risk assessments to identify and remediate threats and vulnerabilities.

6.6.3 Life Cycle Security Controls

No Stipulation

6.7 NETWORK SECURITY CONTROLS

Microsoft PKI Services maintains controls to provide reasonable assurance that the following CA system access is limited to authorized individuals:

- network infrastructure access is limited to authorized individuals with predetermined task privileges;
- access to network segments hosting CA systems is limited to authorized individuals, applications and services; and
- CA application use is limited to authorized individuals

6.8 TIME-STAMPING

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Microsoft PKI Services' certificates SHALL be X.509 Version 3 format and conform to RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL profile.

7.1.1 Version Number(s)

Microsoft PKI Services SHALL issue certificates that are compliant with X.509 Version 3.

7.1.2 Certificate Extensions

The extensions defined for Microsoft PKI Services' X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing the certification hierarchy. Each extension in a certificate is designated as either critical or non-critical.

Certificate extensions, their criticality, and cryptographic algorithm object identifiers, are provisioned according to the IETF RFC 5280 standards.

7.1.2.1 Root CA Certificate

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

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA
Signature Algorithm Identifier	See Section 7.1.3
Issuer Distinguished Name	CN = < CA Common Name > OU = < Organizational Unit > (optional) O = < Organization >

Field	Description
	L = < Locality > S = < State > C = < ISO 3166-1 alpha-2 country code >
Valid From	Date and time of certificate issuance. Time is encoded in accordance with RFC 5280.
Valid To	Date and time of certificate expiration. Time is encoded in accordance with RFC 5280. See Section 6.3.2
Subject Distinguished Name	Same as Issuer Distinguished Name for self-signed Root CA certificates
Subject Public Key Information	See Section 6.1.5

7.1.2.2. Subordinate CA Certificate

Subordinate CA Certificates MAY include extensions and values that are pertinent for their intended use, in accordance with this CPS and RFC 5280.

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA to include at least 8 random bytes
Signature Algorithm Identifier	See Section 7.1.3
Issuer Distinguished Name	Subject Distinguished Name of Parent CA
Valid From	Date and time of certificate issuance. Time is encoded in accordance with RFC 5280.
Valid To	Date and time of certificate expiration. Time is encoded in accordance with RFC 5280. See Section 6.3.2
Subject Distinguished Name	CN = < CA Common Name > OU = < Organizational Unit > (optional) O = < Organization > L = < Locality > S = < State > C = < ISO 3166-1 alpha-2 code >
Subject Public Key Information	See Section 6.1.5

7.1.2.3 Subscriber Certificate

Subscriber Certificates MAY include extensions and values that are pertinent for their intended use, in accordance with this CPS and RFC 5280.

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA to include at least 8 random bytes
Signature Algorithm Identifier	See Section 7.1.3
Issuer	Subject Distinguished Name of Parent CA
Valid From	Date and time of certificate issuance. Time is synchronized with a reliable time source. . Time is encoded in accordance with RFC 5280.
Valid To	Date and time of certificate expiration. Time is synchronized with a reliable time source. . Time is encoded in accordance with RFC 5280. See Section 6.3.2
Subject Distinguished Name:	All fields are optional unless specified. E = < Email Address > CN = < Common Name > (required) OU = < Organizational Unit > i.e., Microsoft Product Group or Partner Name (for certificates issued to external 3rd Party customers) O = < Organization > (i.e., Microsoft or Partner Name) L = < Locality > S = < State > DC = < Domain Component > C = < ISO 3166-1 alpha-2 code >
Subject Alternative Name:	If the Subject Alternative Name is present, one or more values such as the below must be present. Alternate values not listed here are acceptable UPN = < User Principal Name > DNS = < Domain Name > email = < Email Address >

Field	Description
	URL = < Uniform Resource Locator > IP = < IP Address > GUID = < Globally Unique Identifier, Hash of ID >
Subject Public Key Information	See Section 6.1.5

7.1.2.4 All Certificates

All other provisions MUST be set in accordance with RFC 5280.

7.1.2.5 Application of RFC 5280

The applicability of RFC 5280 SHALL be governed by the respective requirements and guidelines of the Internet Engineering Task Force (IETF).

7.1.3 Algorithm Object Identifiers

No Stipulation

7.1.4 Name Forms

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

7.1.4.1. Issuer Information

No Stipulation

7.1.4.2. Subject Information – Subscriber Certificates

No Stipulation

7.1.4.2.1. Subject Alternative Name Extension

No Stipulation

7.1.4.2.2. Subject Distinguished Name Fields

No Stipulation

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

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

7.1.4.3.1. Subject Distinguished Name Fields

No Stipulation

7.1.5 Name Constraints

Microsoft PKI Services reserve the right to issue Certificates with Name Constraints and mark them as critical, where necessary. Unless otherwise documented in this CPS the use of Name Constraints SHALL conform with the X.509 V3 standard (RFC 5280).

7.1.6 Certificate Policy Object Identifier

Microsoft PKI Services MAY issue Certificates with policy identifiers, set forth in Section 1.2 herein, and comply with the provisions of this CPS.

7.1.6.1 Reserved Certificate Policy Object Identifiers

No Stipulation

7.1.6.2 Root CA Certificates

No Stipulation

7.1.6.3 Subordinate CA Certificates

No Stipulation

7.1.6.4 Subscriber Certificates

No Stipulation

7.1.7 Usage of Policy Constraints Extension

No Stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation

7.2 CRL PROFILE

CRL Profiles comply with X.509 V3 standards.

7.2.1 Version Number(s)

No Stipulation

7.2.2 CRL and CRL Entry Extensions

No Stipulation

7.3 OCSP PROFILE

No Stipulation

7.3.1 Version Number(s)

No Stipulation

7.3.2 OCSP Extensions

No Stipulation

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Microsoft PKI Services SHALL at all times:

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

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

Microsoft PKI Services SHALL have an independent auditor annually assess the CA's compliance to the stated requirements and practices of this CPS and presiding CP. The results of the audit SHALL be provided in an Audit Report indicating compliance status with the applicable standards under the audit scheme herein.

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The entity that performs the annual audit SHALL be completely independent of Microsoft PKI Services.

8.4 TOPICS COVERED BY ASSESSMENT

Annual audits SHALL be performed by an independent certified Auditor that assesses Microsoft PKI Services PKI operations in accordance with the stipulations documented in their CP, CPS, and applicable Auditors' Principles and Criteria for Certification Authorities.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Significant deficiencies identified during the compliance audit will result in a determination of

actions to be taken. The Microsoft PKI Services group makes this determination with input from the auditor. Microsoft PKI Services 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 COMMUNICATION OF RESULTS

Audit results are provided to the PKI Policy Authority, who will distribute to the necessary parties, as required.

8.7 SELF-AUDITS

Microsoft PKI Services SHALL perform periodic self-audits of its PKI business practices, in accordance with this CPS and presiding CP.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

Not Applicable

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

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

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

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

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

9.3.2 Information Not Within the Scope of Confidential Information

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

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

This Section 9.3.2 is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Microsoft follows the governing principles established by the Microsoft privacy statement located at https://privacy.microsoft.com/en-us/privacystatement

when handling personal information.

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

See Section 9.3.2.

9.4.4 Responsibility to Protect Private Information

See Section 9.3.3.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 INTELLECTUAL PROPERTY RIGHTS

The following are the property of Microsoft:

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

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

9.6 REPRESENTATIONS AND WARRANTIES

Microsoft warrants and promises to provide certification authority services substantially in compliance with this CPS and the relevant Microsoft Certificate Policies. Microsoft makes no

other warranties or promises and has no further obligations to Subscribers or Relying Parties, except as set forth under this CPS.

9.6.1 CA Representations and Warranties

See Section 9.6

9.6.2 RA Representations and Warranties

See Section 9.6

9.6.3 Subscriber Representations and Warranties

See Section 9.6

9.6.4 Relying Party Representations and Warranties

See Section 9.6

9.6.5 Representations and Warranties of Other Participants

See Section 9.6

9.7 DISCLAIMERS OF WARRANTIES

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

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

9.8 LIMITATIONS OF LIABILITY

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE A CERTIFICATE, INCLUDING AS A RESULT OF (I) ANY TERMINATION OR SUSPENSION OF THIS AGREEMENT OR THE CPS OR REVOCATION OF A CERTIFICATE, (II) OUR DISCONTINUATION OF ANY OR ALL SERVICE OFFERINGS IN CONNECTION WITH THIS AGREEMENT, OR, (III) ANY DOWNTIME OF ALL OR A

PORTION OF CERTIFICATE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (C) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO MICROSOFT'S CERTIFICATE SERVICES; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, MICROSOFT AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IN CONNECTION WITH THIS AGREEMENT AND ALL CERTIFICATES ISSUED HEREUNDER, IS THE LESSER OF THE AMOUNT PAID BY YOU FOR THE CERTIFICATE(S) AT ISSUE OR THE AMOUNTS PAID FOR THE CERTIFICATE SERVICES FOR THE CERTIFICATE(S) AT ISSUE IN THE LAST TWELVE (12) MONTHS BEFORE THE CLAIM AROSE; PROVIDED, HOWEVER, THAT FOR ANY EV CERTIFICATE ISSUED UNDER THIS AGREEMENT EXEPT FOR AS EXPRESSLY EXCLUDED PER SECTION 8(c), OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IS LIMITED TO $2000 US DOLLARS PER SUBSCRIBER OR RELYING PARTY PER EV CERTIFICATE.

9.9 INDEMNITIES

9.9.1 Indemnification by CAs

See Section 9.9

9.9.2 Indemnification by Subscribers

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

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, Relying Party indemnifies Microsoft, Microsoft's partners, and any cross-signed entities, and their respective employees, directors, agents, and representatives from, and any third-party Certificate Authority or RA providing services to Microsoft or any of its affiliates in relation to the Certificate and defend the indemnified parties against, any loss,

damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by Microsoft or its affiliates and used by the Relying Party, the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a certificate or any constituent elements of it; or (iii) failure to check the certificate's status prior to use.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS becomes effective upon publication in the Repository.

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

No Stipulation

9.12.3 Circumstances under which OID must be changed

No Stipulation

9.13 DISPUTE RESOLUTION PROVISIONS

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

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

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

9.16.2 Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of Microsoft. Unless specified otherwise in a contract with a party, Microsoft does not provide notice of assignment. This CPS shall be binding on all successors of the parties.

9.16.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. It is expressly agreed that every provision of this CPS that provides for a limitation of liability or exclusion of damages, disclaimer or limitation of any warranties, promises or other obligations, is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force Majeure

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

9.17 OTHER PROVISIONS

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

Appendix A – Change Control Log

Revision Date	New Revision	Revision Explanation
5/20/23	3.1.7	Update Change Log location and layout, Update to Privacy Statement Link in 9.4.1, Update to various Section Titles to align with RFC3647
1/7/22	3.1.6	Minor clarifying updates
10/19/21	3.1.5	Minor clarifying updates
7/28/20	3.1.4	Minor clarifying updates, updated email contact
8/5/2019	3.1.3	Minor clarifying updates
7/31/2018	3.1.2	Minor clarifying updates
7/10/2018	3.1.1	Minor clarifying updates
6/12/2018	3.1	Minor clarifying updates
2/28/2018	3.0	Major update/rewrite corresponding to changes made to CP.
4/30/2014	2.1	Updated to incorporate findings from FY13 WebTrust Audit and internal review.
4/2/2013	2.0	Updated to support the practice of online CA operations
1/2/2013	1.1	Updated to support PKI Steering Committee, Microsoft Legal and Audit partner recommendations
1/27/2010	1.0	Established