Microsoft

Microsoft PKI Services

Public TLS Certification Practice Statement (CPS)

Version 3.3.0
April 21, 2025

Table of Contents

1. INTRODUCTION 11

1.1 OVERVIEW 11
1.2 DOCUMENT NAME AND IDENTIFICATION 13
1.2.1 Revisions 14
1.2.2 Relevant Dates 14
1.3 PKI PARTICIPANTS 14
1.3.1 Certification Authorities 14
1.3.2 Registration Authorities 14
1.3.3 Subscribers 14
1.3.4 Relying Parties 15
1.3.5 Other Participants 15
1.4 CERTIFICATE USAGE 15
1.4.1 Appropriate Certificate Uses 15
1.4.2 Prohibited Certificate Uses 15
1.5 POLICY ADMINISTRATION 16
1.5.1 Organization Administering the Document 16
1.5.2 Contact Person 16
1.5.3 Person Determining CPS Suitability for the Policy 16
1.5.4 CPS Approval Procedures 16
1.6 DEFINITIONS AND ACRONYMS 16
1.6.1 Definitions 16
1.6.2 Acronyms 28
1.6.3 References 29
1.6.4 Conventions 30

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 31

2.1 REPOSITORIES 31
2.2 PUBLICATION OF CERTIFICATION INFORMATION 31
2.3 TIME OR FREQUENCY OF PUBLICATION 31
2.4 ACCESS CONTROLS ON REPOSITORIES 32

3. IDENTIFICATION AND AUTHENTICATION 32

3.1 NAMING 32
3.1.1 Type of Names 32
3.1.2 Need for Names to be Meaningful 32
3.1.3 Anonymity or Pseudonymity of Subscribers 32
3.1.4 Rules for Interpreting Various Name Forms 32
3.1.5 Uniqueness of Names 32
3.1.6 Recognition, Authentication, and Role of Trademarks 32
3.2 INITIAL IDENTITY VALIDATION 33
3.2.1 Method to Prove Possession of Private Key 33

3.2.2 Authentication of Organization Identity 33
3.2.2.1 Identity 33
3.2.2.2 DBA/Tradename 34
3.2.2.3 Verification of Country 34
3.2.2.4 Validation of Domain Authorization or Control 34
3.2.2.5 Authentication for an IP Address 34
3.2.2.6 Wildcard Domain Validation 34
3.2.2.7 Data Source Accuracy 35
3.2.2.8 CAA Records 35
3.2.3 Authentication of Individual Identity 35
3.2.4 Non-Verified Subscriber Information 35
3.2.5 Validation of Authority 35
3.2.6 Criteria for Interoperation 36
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 36
3.3.1 Identification and Authentication for Routine Re-Key 36
3.3.2 Identification and Authentication for Re-Key After Revocation 36
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST. 36
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 36
4.1 CERTIFICATE APPLICATION 36
4.1.1 Who Can Submit a Certificate Application 36
4.1.2 Enrollment Process and Responsibilities 37
4.2 CERTIFICATE APPLICATION PROCESSING 37
4.2.1 Performing Identification and Authentication Functions 37
4.2.2 Approval or Rejection of Certificate Applications 38
4.2.3 Time to Process Certificate Applications 38
4.2.4 Verification of CAA Records 38
4.3 CERTIFICATE ISSUANCE 40
4.3.1 CA Actions During Certificate Issuance 40
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 40
4.4 CERTIFICATE ACCEPTANCE 41
4.4.1 Conduct Constituting Certificate Acceptance 41
4.4.2 Publication of the Certificate by the CA 41
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 41
4.5 KEY PAIR AND CERTIFICATE USAGE 41
4.5.1 Subscriber Private Key and Certificate Usage 41
4.5.2 Relying Party Public Key and Certificate Usage 41
4.6 CERTIFICATE RENEWAL 41
4.6.1 Circumstance for Certificate Renewal 41
4.6.2 Who May Request Renewal 41
4.6.3 Processing Certificate Renewal Requests 42
4.6.4 Notification of New Certificate Issuance to Subscriber 42
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 42
4.6.6 Publication of the Renewal Certificate by the CA 42
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 42
4.7 CERTIFICATE RE-KEY 42

4.7.1 Circumstance for Certificate Re-Key 42
4.7.2 Who May Request Certification of a New Public Key 42
4.7.3 Processing Certificate Re-keying Requests 42
4.7.4 Notification of New Certificate Issuance to Subscriber 42
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 42
4.7.6 Publication of the Re-keyed Certificate by the CA 43
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 43
4.8 CERTIFICATE MODIFICATION **43**
4.8.1 Circumstance for Certificate Modification 43
4.8.2 Who May Request Certificate Modification 43
4.8.3 Processing Certificate Modification Requests 43
4.8.4 Notification of New Certificate Issuance to Subscriber 43
4.8.5 Conduct Constituting Acceptance of Modified Certificate 43
4.8.6 Publication of the Modified Certificate by the CA 43
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 43
4.9 CERTIFICATE REVOCATION AND SUSPENSION **43**
4.9.1 Circumstances for Revocation 43
4.9.1.1 Reasons for Revoking a Subscriber Certificate 43
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate 45
4.9.2 Who Can Request Revocation 45
4.9.3 Procedure for Revocation Request 45
4.9.4 Revocation Request Grace Period 48
4.9.5 Time Within Which CA Must Process the Revocation Request 48
4.9.6 Revocation Checking Requirement for Relying Parties 48
4.9.7 CRL Issuance Frequency 48
4.9.8 Maximum Latency for CRLs 49
4.9.9 On-Line Revocation/Status Checking Availability 49
4.9.11 Other Forms of Revocation Advertisements Available 50
4.9.12 Special Requirements re Key Compromise 50
4.9.13 Circumstances for Suspension 50
4.9.14 Who Can Request Suspension 50
4.9.15 Procedure for Suspension Request 50
4.9.16 Limits on Suspension Period 50
4.10 CERTIFICATE STATUS SERVICES **50**
4.10.1 Operational Characteristics 50
4.10.2 Service Availability 51
4.10.3 Optional Features 51
4.11 END OF SUBSCRIPTION **51**
4.12 KEY ESCROW AND RECOVERY **51**
4.12.1 Key Escrow and Recovery Policy and Practices 51
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 51
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS **51**
5.1 PHYSICAL CONTROLS **52**
5.1.1 Site Location and Construction 52

5.1.2 Physical Access 52
5.1.3 Power and Air Conditioning 53
5.1.4 Water Exposures 53
5.1.5 Fire Prevention and Protection 53
5.1.6 Media Storage 53
5.1.7 Waste Disposal 53
5.1.8 Off-Site Backup 53
5.2 PROCEDURAL CONTROLS **53**
5.2.1 Trusted Roles 53
5.2.2 Number of Persons Required per Task 54
5.2.3 Identification and Authentication for Each Role 54
5.2.4 Roles Requiring Separation of Duties 54
5.3 PERSONNEL CONTROLS 54
5.3.1 Qualifications, Experience, and Clearance Requirements 54
5.3.2 Background Check Procedures 54
5.3.3 Training Requirements 54
5.3.4 Retraining Frequency and Requirements 54
5.3.5 Job Rotation Frequency and Sequence 55
5.3.6 Sanctions for Unauthorized Actions 55
5.3.7 Independent Contractor Requirements 55
5.3.8 Documentation Supplied to Personnel 55
5.4 AUDIT LOGGING PROCEDURES **55**
5.4.1 Types of Events Recorded 55
5.4.2 Frequency of Processing Log 56
5.4.3 Retention Period for Audit Log 56
5.4.4 Protection of Audit Log 57
5.4.5 Audit Log Backup Procedures 57
5.4.6 Audit Collection System (Internal vs. External) 57
5.4.7 Notification to Event-Causing Subject 57
5.4.8 Vulnerability Assessments 57
5.5 RECORDS ARCHIVAL **57**
5.5.1 Types of Records Archived 57
5.5.2 Retention Period for Archive 57
5.5.3 Protection of Archive 58
5.5.4 Archive Backup Procedures 58
5.5.5 Requirements for Time-Stamping of Records 58
5.5.6 Archive Collection System (Internal or External) 58
5.5.7 Procedures to Obtain and Verify Archive Information 58
5.6 KEY CHANGEOVER **58**
5.7 COMPROMISE AND DISASTER RECOVERY **58**
5.7.1 Incident and Compromise Handling Procedures 58
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 58
5.7.3 Entity Private Key Compromise Procedures 58
5.7.4 Business Continuity Capabilities After a Disaster 59
5.8 CA OR RA TERMINATION **59**

6. TECHNICAL SECURITY CONTROLS.....59
6.1 KEY PAIR GENERATION AND INSTALLATION..... 59
6.1.1 Key Pair Generation.....59
6.1.1.1 CA Key Pair Generation..... 59
6.1.1.3 Subscriber Key Pair Generation..... 60
6.1.2 Private Key Delivery to Subscriber.....60
6.1.4 CA Public Key Delivery to Relying Parties.....61
6.1.5 Key Sizes.....61
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field).....62
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS..... 62
6.2.1 Cryptographic Module Standards and Controls.....62
6.2.2 Private Key (m out of n) Multi-Person Control.....62
6.2.3 Private Key Escrow.....62
6.2.4 Private Key Backup.....62
6.2.5 Private Key Archival.....63
6.2.6 Private Key Transfer into or from a Cryptographic Module.....63
6.2.7 Private Key Storage on Cryptographic Module.....63
6.2.8 Method of Activating Private Key.....63
6.2.9 Method of Deactivating Private Key.....63
6.2.10 Method of Destroying Private Key.....63
6.2.11 Cryptographic Module Rating.....63
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT..... 63
6.3.1 Public Key Archival.....63
6.3.2 Certificate Operational Periods and Key Pair Usage Periods.....63
6.4 ACTIVATION DATA..... 64
6.4.1 Activation Data Generation and Installation.....64
6.4.2 Activation Data Protection.....64
6.4.3 Other Aspects of Activation Data.....64
6.5 COMPUTER SECURITY CONTROLS..... 65
6.5.1 Specific Computer Security Technical Requirements.....65
6.5.2 Computer Security Rating.....65
6.6 LIFE CYCLE TECHNICAL CONTROLS..... 65
6.6.1 System Development Controls.....65
6.6.2 Security Management Controls.....65
6.6.3 Life Cycle Security Controls.....65
6.7 NETWORK SECURITY CONTROLS..... 65
6.8 TIME-STAMPING..... 65
7. CERTIFICATE, CRL, AND OCSP PROFILES.....65
7.1 CERTIFICATE PROFILE..... 65
7.1.1 Version Number(s).....66
7.1.2 Certificate Extensions.....66
7.1.2.1 Root CA Certificate Profile..... 66
7.1.2.1.1 Root CA Validity..... 66

7.1.2.1.2 Root CA Extensions ... 66
7.1.2.1.3 Root CA Authority Key Identifier ... 66
7.1.2.1.4 Root CA Basic Constraints ... 66
7.1.2.2 Cross-Certified Subordinate CA Certificate Profile ... 66
7.1.2.2.1 Cross-Certified Subordinate CA Validity ... 66
7.1.2.2.2 Cross-Certified Subordinate CA Naming ... 67
7.1.2.2.3 Cross-Certified Subordinate CA Extensions ... 67
7.1.2.2.4 Cross-Certified Subordinate CA Extended Key Usage – Unrestricted ... 67
7.1.2.2.5 Cross-Certified Subordinate CA Extended Key Usage – Restricted ... 67
7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile ... 67
7.1.2.3.1 Technically Constrained Non-TLS Subordinate CA Extensions ... 67
7.1.2.3.2 Technically Constrained Non-TLS Subordinate CA Certificate Policies ... 67
7.1.2.3.3 Technically Constrained Non-TLS Subordinate CA Extended Key Usage ... 67
7.1.2.4.1 Technically Constrained Precertificate Signing CA Extensions ... 68
7.1.2.4.2 Technically Constrained Precertificate Signing CA Extended Key Usage ... 68
Microsoft PKI Services does not issue Technically Constrained Precertificate Signing CA certificates. ... 68
7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile ... 68
7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions ... 68
7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints ... 68
7.1.2.6 TLS Subordinate CA Profile ... 68
7.1.2.6.1 TLS Subordinate CA Extensions ... 68
7.1.2.7 Subscriber (Server) Certificate Profile ... 68
7.1.2.7.1 Subscriber Certificate Types ... 68
7.1.2.7.2 Domain Validated ... 68
7.1.2.7.3 Individual Validated ... 68
7.1.2.7.4 Organization Validated ... 68
7.1.2.7.5 Extended Validation ... 68
7.1.2.7.6 Subscriber Certificate Extensions ... 68
7.1.2.7.7 Subscriber Certificate Authority Information Access ... 68
7.1.2.7.8 Subscriber Certificate Basic Constraints ... 69
7.1.2.7.9 Subscriber Certificate Certificate Policies ... 69
7.1.2.7.10 Subscriber Certificate Extended Key Usage ... 69
7.1.2.7.11 Subscriber Certificate Key Usage ... 69
7.1.2.8 OCSP Responder Certificate Profile ... 69
7.1.2.8.1 OCSP Responder Validity ... 69
7.1.2.8.2 OCSP Responder Extensions ... 69
7.1.2.8.3 OCSP Responder Authority Information Access ... 69
7.1.2.8.4 OCSP Responder Basic Constraints ... 69
7.1.2.8.5 OCSP Responder Extended Key Usage ... 69
7.1.2.8.7 OCSP Responder Key Usage ... 70
7.1.2.8.8 OCSP Responder Certificate Policies ... 70
7.1.2.9.1 Precertificate Profile Extensions – Directly Issued ... 70
7.1.2.9.2 Precertificate Profile Extensions – Precertificate CA Issued ... 71
7.1.2.9.3 Precertificate Poison ... 71
7.1.2.9.4 Precertificate Authority Key Identifier ... 71
7.1.2.10 Common CA Fields ... 71
7.1.2.10.1 CA Certificate Validity ... 71

7.1.2.10.3 CA Certificate Authority Information Access 71
7.1.2.10.4 CA Certificate Basic Constraints 71
7.1.2.10.5 CA Certificate Certificate Policies 71
7.1.2.10.6 CA Certificate Extended Key Usage 71
7.1.2.10.7 CA Certificate Key Usage 72
7.1.2.11 Common Certificate Fields 72
7.1.2.11.1 Authority Key Identifier 72
7.1.2.11.2 CRL Distribution Points 72
7.1.2.11.4 Subject Key Identifier 72
7.1.2.11.5 Other Extensions 72
7.1.3 Algorithm Object Identifiers 73
7.1.3.1 SubjectPublicKeyInfo 73
7.1.3.1.1 RSA 73
7.1.3.1.2 ECDSA 73
7.1.3.2 Signature AlgorithmIdentifier 73
7.1.3.2.1 RSA 74
7.1.3.2.2 ECDSA 75
7.1.4 Name Forms 76
7.1.4.1. Name Encoding 76
7.1.4.2 Subject Attribute Encoding 76
7.1.4.3. Subscriber Certificate Common Name Attribute 77
7.1.4.4 Other Subject Attributes 78
7.1.6 Certificate Policy Object Identifier 78
7.1.6.1 Reserved Certificate Policy Object Identifiers 78
7.1.7 Usage of Policy Constraints Extension 78
7.1.8 Policy Qualifiers Syntax and Semantics 78
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 78
7.2 CRL PROFILE **78**
7.2.1 Version Number(s) 80
7.2.2 CRL and CRL Entry Extensions 80
7.3 OCSP PROFILE **84**
7.3.1 Version Number(s) 84
7.3.2 OCSP Extensions 84
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS **84**
8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT **84**
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR **85**
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY **85**
8.4 TOPICS COVERED BY ASSESSMENT **85**
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY **86**
8.6 COMMUNICATION OF RESULTS **86**
8.7 SELF-AUDITS **87**
9. OTHER BUSINESS AND LEGAL MATTERS **88**
9.1 FEES **88**

9.1.1 Certificate Issuance or Renewal Fees 88
9.1.2 Certificate Access Fees 88
9.1.3 Revocation or Status Information Access Fees 88
9.1.4 Fees for Other Services 88
9.1.5 Refund Policy 88
9.2 FINANCIAL RESPONSIBILITY **89**
9.2.1 Insurance Coverage 89
9.2.2 Other Assets 89
9.2.3 Insurance or Warranty Coverage for End-Entities 89
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION **89**
9.3.1 Scope of Confidential Information 89
9.3.2 Information Not Within the Scope of Confidential Information 89
9.3.3 Responsibility to Protect Confidential Information 89
9.4 PRIVACY OF PERSONAL INFORMATION **90**
9.4.1 Privacy Plan 90
9.4.2 Information Treated as Private 90
9.4.3 Information Not Deemed Private 90
9.4.4 Responsibility to Protect Private Information 90
9.4.5 Notice and Consent to Use Private Information 90
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 90
9.4.7 Other Information Disclosure Circumstances 90
9.5 INTELLECTUAL PROPERTY RIGHTS **90**
9.6 REPRESENTATIONS AND WARRANTIES **91**
9.6.1 CA Representations and Warranties 91
9.6.2 RA Representations and Warranties 92
9.6.3 Subscriber Representations and Warranties 92
9.6.4 Relying Party Representations and Warranties 94
9.6.5 Representations and Warranties of Other Participants 94
9.7 DISCLAIMERS OF WARRANTIES **94**
9.8 LIMITATIONS OF LIABILITY **94**
9.9 INDEMNITIES **95**
9.9.1 Indemnification by CAs 95
9.9.2 Indemnification by Subscribers 96
9.9.3 Indemnification by Relying Parties 96
9.10 TERM AND TERMINATION **96**
9.10.1 Term 96
9.10.2 Termination 96
9.10.3 Effect of Termination and Survival 96
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS **97**
9.12 AMENDMENTS **97**
9.12.1 Procedure for Amendment 97
9.12.2 Notification Mechanism and Period 97
9.12.3 Circumstances under which OID must be changed 97
9.13 DISPUTE RESOLUTION PROVISIONS **97**
9.14 GOVERNING LAW **97**

9.15 COMPLIANCE WITH APPLICABLE LAW 97
9.16 MISCELLANEOUS PROVISIONS 98
9.16.1 Entire Agreement 98
9.16.2 Assignment 98
9.16.3 Severability 98
9.16.4 Enforcement (attorneys' fees and waiver of rights) 98
9.16.5 Force Majeure 99
9.17 OTHER PROVISIONS 99
APPENDIX A: Document History 100
APPENDIX B: Certificate Profiles 103

1. INTRODUCTION

1.1 OVERVIEW

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

Microsoft PKI Services has three CPS documents to differentiate its internal first-party (not publicly trusted) from its external first-party (publicly trusted) CA operations and its third-party issued Code signing certificates, as they are regulated by separate compliance authorities and/or levels. This CPS is for the external first-party (publicly trusted) CA operations.

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

This CPS specifically governs the following Root and Subordinate CAs:

Root CAs	**Root CA Serial Numbers**	**Issue Date**	**Expiration Date**	**SHA2 Thumbprint**
Microsoft RSA Root Certificate Authority 2017	1ed397095fd8b4b347701eaabe7f45b3	12/18/2019	7/18/2042	c741f70f4b2a8d88bf2e71c14122ef53ef10eba0cfa5e64cfa20f418853073e0
Microsoft ECC Root Certificate Authority 2017	66f23daf87de8bb14aea0c573101c2eC	12/18/2019	7/18/2042	358df39f764af9e1b766e9c972df352ee15cfac227af6ad1d70e8e4a6edcba02
Issuing and Intermediate CAs	**Issuing and Intermediate CAs Serial Numbers**	**Issue Date**	**Expiration Date**	**SHA2 Thumbprint**
Microsoft Azure TLS Issuing CA 01	330000001DBE9496F3DB8B8DE700000000001D	1/17/2020	6/27/2024	0437AB2EC2C2B4890296C135034B21DB146434B8317EE703AA8AA943C5EA51AE
Microsoft Azure TLS Issuing CA 01	0AAFA6C5CA63C45141EA3BE1F7C75317	7/29/2020	6/27/2024	24C7299864E0A2A6964F551C0E8DF2461532FA8C48E4DBBB6080716691F190E5
Microsoft Azure TLS Issuing CA 02	330000001EC6749F058517B4D000000000001E	1/17/2020	6/27/2024	D39CE39FF6F449D4F3391EE2004D705EC22F99CFFCA40A88F85DB26454ADDBD1
Microsoft Azure TLS Issuing CA 02	0C6AE97CCED599838690A00A9EA53214	7/29/2020	6/27/2024	15A98761EBE011554DA3A46D206B0812CB2EB69AE87AAA11A6DD4CB84ED5142A
Microsoft Azure TLS Issuing CA 05	330000001F9F1FA2043BC28DB900000000001F	1/17/2020	6/27/2024	AB3203B3EA2017D509726A1D82293EFFCB8C42CEB52C9AF1C0EEE96B5C02BCBA
Microsoft Azure TLS Issuing CA 05	0D7BEDE97D8209967A52631B8BDD18BD	7/29/2020	6/27/2024	D6831BA43607F5AC19778D627531562AF55145F191CAB5EFAFA0E0005442B302

Microsoft Azure TLS Issuing CA 06	3300000020A2F1491A37FBD31F000000000020	1/17/2020	6/27/2024	7DF4D3EF45798F8C4384FC702BA52A44CE7BD6298B141628D4ABABC7678F6467
Microsoft Azure TLS Issuing CA 06	02E79171FB8021E93FE2D983834C50C0	7/29/2020	6/27/2024	48FF8B494668C752304B48BFE818758987DEF6582E5F09B921F4B60BB3D6A8DD
Microsoft RSA TLS Issuing AOC CA 01	33000000265ee5cbef101479fb000000000026	3/11/2021	3/11/2026	7484F2F1618D35F6F239C05BAD30B8B7AD93C7024D4000D387141417EE3DDBF4
Microsoft RSA TLS Issuing AOC CA 02	3300000027c7deaf47d6c012fe000000000027	3/11/2021	3/11/2026	F19A176BC779C77609427F441B995F14CAB9A19D87CDDD92725E4997CB0878BC
Microsoft RSA TLS Issuing EOC CA 01	33000000289b1be7b00f9743910000000000028	3/11/2021	3/11/2026	1F1D8E7685CE8255088F791BFD3FB927F50AC1007091B5BBC3347EFBC5D9A80C
Microsoft RSA TLS Issuing EOC CA 02	3300000029d905146635d54ebd000000000029	3/11/2021	3/11/2026	89E1EF9BD893880FCA4C2D0BA71EC93DAF6C0AC14D5A9996F3E16F9763995076
Microsoft Azure ECC TLS Issuing CA 01	330000001AA9564F44321C54B900000000001A	1/17/2020	6/27/2024	2CAEFBB55E70DF5A8985FE9BC10DD56A40C3DEDAB3DA1530A29682015C5B7C66
Microsoft Azure ECC TLS Issuing CA 01	09DC42A5F574FF3A389EE06D5D4DE440	8/12/2020	6/27/2024	949D6B4B761CA134AD3E7A8571186F580EE887F2C6B568B5140F4157F98D68DD
Microsoft Azure ECC TLS Issuing CA 02	330000001B498D6736ED5612C200000000001B	1/17/2020	6/27/2024	4EC439672A443401A66E27947CC3B5897F132B667F712CC1A37018A3CC85B16A
Microsoft Azure ECC TLS Issuing CA 02	0E8DBE5EA610E6CBB569C736F6D7004B	8/12/2020	6/27/2024	9C64A9A43E990E98FBCE8317B2D4C1C07FFE6E032DA8BB6D60A696E2FF038F1F
Microsoft Azure ECC TLS Issuing CA 05	330000001CC0D2A3CD78CF2C10000000000001C	1/17/2020	6/27/2024	624D5576A652B2130768BFE84B965EEFFFD91603D25CD5F7155A7DC2789DAC38
Microsoft Azure ECC TLS Issuing CA 05	0CE59C30FD7A83532E2D0146B332F965	8/12/2020	6/27/2024	003F71DC4820216575FC5AACFE3B1AEB76F72AEA5B8E8FCEFC80B9F517A4A612
Microsoft Azure ECC TLS Issuing CA 06	330000001D0913C309DA3F05A600000000001D	1/17/2020	6/27/2024	151A3E5969C6616EB637A8722B174CFD95387AACE78D57C3BD23F0CB3008186A
Microsoft Azure ECC TLS Issuing CA 06	066E79CD7624C63130C77ABEB6A8BB94	8/12/2020	6/27/2024	2975BAB51D00D862D0E16EEDEF8306A759C65CD4B9F00DAF50ECDFCB4EC396E4
Microsoft ECC TLS Issuing AOC CA 01	330000002378f1186465d367c2000000000023	3/11/2021	3/11/2026	A9DF77A5BFB79FA34CDB975D964A30D9FE7FC4E670BD39BF1B8C2605E843DB54
Microsoft ECC TLS Issuing AOC CA 02	330000002404e553405f2daad3000000000024	3/11/2021	3/11/2026	85FA29EB740D90CE77EDDBE3AB6C66A5DE3FC8BA94D6B2955FB7D33B04231601
Microsoft ECC TLS Issuing EOC CA 01	330000002571afe0d5aee7a2f500000000025	3/11/2021	3/11/2026	EDE152DA0C19D6C3BB3168D11E40901919646BB6998CD5E7D0FBE6537FFF42EF
Microsoft ECC TLS Issuing EOC CA 02	33000000269ab02dde29abbcf7000000000026	3/11/2021	3/11/2026	21CD47E3200B2D7F13567DF9E698EC21ACAC77A8F4A2A1173F4EAB23B2048967
Microsoft Azure ECC TLS Issuing CA 03	330000003322a2579b5e698bcc000000000033	5/25/2023	5/25/2028	2EC9A5BA68B60F81E5F8662F7645743CCE1EDCE06AF686C775431F7BBB69ABD4
Microsoft Azure ECC TLS Issuing CA 03	01529ee8368f0b5d72ba433e2d8ea62d	06/07/2023	08/25/2026	BBD27139C5302C63D903F570F173AD4DC06C974B9EBE292C90FFCCAB5D6FA54E

Microsoft Azure ECC TLS Issuing CA 04	33000000322164aedab61f509d000000000032	5/25/2023	5/25/2028	4D0F5DA23B099209B048E1871B4BB1C4B4E812E3FA0249BB8D19E00FFA9E91BC
Microsoft Azure ECC TLS Issuing CA 04	02393d48d702425a7cb41c000b0ed7ca	06/07/2023	08/25/2026	7A3AE4F12920D5A8129BE1183FBEC4370EF10B8B3AD41EAE4A58D5385AA94D33
Microsoft Azure ECC TLS Issuing CA 07	3300000034c732435db22a0a2b000000000034	5/25/2023	5/25/2028	BD3816423553ED993FA44A02F5562470C0CFB0D3B00532E3526A4A3AEC87522F
Microsoft Azure ECC TLS Issuing CA 07	0f1f157582cdcd33734bdc5fcd941a33	06/07/2023	08/25/2026	BE23414A42E74886E7C72A861BA2DDDA0175ED829223D894C5D272651FC0C189
Microsoft Azure ECC TLS Issuing CA 08	330000003152697984479 8bbb8000000000031	5/25/2023	5/25/2028	2C99B917B7A068578F7EFB4FB8E60B9CB5A0E73BF300E0E1DC112E5654C5AE52
Microsoft Azure ECC TLS Issuing CA 08	0ef2e5d83681520255e92c608fbc2ff4	06/07/2023	08/25/2026	89AADE767B7BA43F8DDE8E9E74A2FCBBEA40D57155F7E1F2259C88835601FAED
Microsoft Azure RSA TLS Issuing CA 03	330000003968ea517d8a7e30ce000000000039	5/25/2023	5/25/2028	3D3F4B440F933FFD269565EDA9E20E8DF863C9CBE3651D3B476C5B4F4AF5CE28
Microsoft Azure RSA TLS Issuing CA 03	05196526449a5e3d1a38748f5dcfebcc	06/07/2023	08/25/2026	9D1BC5D2DD75BF8B64F35E7F919E2546C225BE888C1A8CBE82C0E9579234A7ED
Microsoft Azure RSA TLS Issuing CA 04	330000003cd7cb44ee579961d000000000003c	5/25/2023	5/25/2028	FD39FFC48F148354262162A2F55DD46DC2564CFC1499309AD53F09C10981DCCA
Microsoft Azure RSA TLS Issuing CA 04	09f96ec295555f24749eaf1e5dced49d	06/07/2023	08/25/2026	33F9731BE910A66DC6ACD07D9D9CA212EE8D0A9A5C78C8BF3E89BB74DF8FB936
Microsoft Azure RSA TLS Issuing CA 07	330000003bf980b0c837834317000000000003b	5/25/2023	5/25/2028	FBB7926A451BADF516BE518614A77E6E325E29819908796D807F59320F918EE2
Microsoft Azure RSA TLS Issuing CA 07	0a43a9509b01352f899579ec7208ba50	06/07/2023	08/25/2026	724247794951C93F3E41711617E95CE143263E3196C345A1DA78F6639749EC03
Microsoft Azure RSA TLS Issuing CA 08	330000003a5dc2ffc321c16d9b000000000003a	5/25/2023	5/25/2028	CFDD061FCD4CFF3BB9E133264CA7FDE45CA49B70CFAA977AE0DC422B4330A8C1
Microsoft Azure RSA TLS Issuing CA 08	0efb7e547edf0ff1069aee57696d7ba0	06/07/2023	08/25/2026	511C1C41CB7EB2A10078C32C82F17925BA786DE46C633921D038E7409E15A5EA

1.2 DOCUMENT NAME AND IDENTIFICATION

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

The following Object Identifiers are assigned for use by Microsoft CAs as a means of asserting compliance with CA/B Forum's Baseline Requirements:

Digitally Signed Object	Object Identifier (OID)
TLS Organization Validated (OV) Certificates	2.23.140.1.2.2

1.2.1 Revisions

See Appendix A.

1.2.2 Relevant Dates

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

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

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

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

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

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

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

1.3.2 Registration Authorities

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

1.3.3 Subscribers

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

groups, organizational roles or applications, provided the responsibility and accountability are attributable to the organization.

Obligations of Subscribers within the CA's hierarchy include:

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

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

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

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

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

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

1.4.2 Prohibited Certificate Uses

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

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

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 please refer to Section 4.9.3

For suspected key compromise please refer to Section 4.9.12.

To report other issue such as 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 the CPS, in accordance with the CP.

1.5.4 CPS Approval Procedures

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

1.6 DEFINITIONS AND ACRONYMS

Capitalized terms and acronyms, not specified herein, are defined in the CA/B Forum's Baseline Requirements (BR) and if not specified in the BR, are defined in the Network and Certificate System Security Requirements (the "NCSSRs"), also referred to as the Network Security Requirements ("NSRs").

1.6.1 Definitions

- **Air-Gapped** – Physically and logically separated, disconnected, and isolated from all other Systems.
- **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** – The natural person or Legal Entity that applies for (or seeks renewal of) a

Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

- **Applicant Representative** – A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA**.**
- **Application Software Supplier** – A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
- **Attestation Letter:** A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
- **Audit Report** – A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
- **Authorization Domain Name** – The FQDN used to obtain authorization for certificate issuance for a given FQDN to be included in a Certificate. The CA MAY use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "'*.*'" from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA MAY prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and MAY use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.
- **Authorized Port –** One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).
- **Base Domain Name** – The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself MAY be used as the Base Domain Name.
- **Baseline Requirements (BR)** – An integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements issued by the CA/Browser Forum and available at cabforum.org.
- **CAA** – From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

- **CA/Browser Forum (CA/B 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.
- **CA Infrastructure** – Collectively the infrastructure used by the CA or Delegated Third Party which qualifies as a:
    - Certificate System; or
    - Root CA System (Air-Gapped and otherwise)
- **Certificate** - An electronic document that uses a digital signature to bind a public key and an identity.
- **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 Data** – Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
- **Certificate Management Process** – Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
- **Certificate Management System:** A system used by a CA of Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.
- **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.
- **Certificate Problem Report –** Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
- **Certificate Profile –** A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.
- **Certificate Request** – an application for a new Certificate or a renewal of a Certificate.
- **Certificate Revocation List (CRL)** – A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
- **Certificate Signing Request (CSR)** – a message sent to the certification authority containing the information required to issue a digital certificate
- **Certificate System –** A system used by a CA or Delegated Third Party to access, process, or manage data or provide services related to:
    1. identity validation;
    2. identity authentication;

3. account registration;
4. certificate application;
5. certificate approval;
6. certificate issuance;
7. certificate revocation;
8. authoritative certificate status; or
9. key escrow.

- **Certification Authority (CA)** – An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.
- **Certification Practice Statement (CPS) –** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- **Common Vulnerability Scoring System (CVSS)** – A quantitative model used to measure the base level severity of a vulnerability (see http://nvd.nist.gov/vuln-metrics/cvss).
- **Control** – "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.
- **Country** – Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.
- **Critical Security Event** – An event, set of circumstances, or anomalous activity that could lead to a circumvention of CA Infrastructure security controls or compromise of CA Infrastructure integrity or operational continuity, including, but not limited to, excessive login attempts, attempts to access prohibited resources, DoS/DDoS attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or physical compromise of component integrity.
- **Critical Vulnerability** – A system vulnerability that has a CVSS v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see https://nvd.nist.gov/vuln-metrics/cvss), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.
- **Cross-Certified Subordinate CA Certificate** – A certificate that is used to establish a trust relationship between two CAs.
- **CSPRNG** – A random number generator intended for use in cryptographic system.
- **Delegated Third Party** – A natural person or legal entity that is not the CA and that operates

any part of a Certificate System.

- **Delegated Third Party System** – Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.
- **Domain Authorization Document** – Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
- **Domain Contact** – The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) for a Base Domain Name.
- **Domain Label** – From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names.
- **Domain Name** – An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
- **Domain Namespace** – The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
- **Domain Name Registrant** – Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
- **Domain Name Registrar** – A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
- **Distinguished Name (DN)** – a globally unique identifier representing a Subject that is used on Certificates and in the Repository
- **Enterprise RA** – An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.
- **Expiry Date –** The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
- **Extended Key Usage –** An extension in an X.509 certificate to indicate the allowed purpose(s) for the use of the public key. Also referenced or known as "Enhanced Key Usage".
- **Fully-Qualified Domain Name (FQDN)** – A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

- **Government Entity** – A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
- **High Risk Certificate Request:** A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which MAY include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.
- **IP Address** – A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
- **Issuing CA** – In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
- **Issuing System** – A system used to sign certificates or validity status information.
- **Key Compromise** – A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
- **Key Generation Script** – A documented plan of procedures for the generation of a CA Key Pair.
- **Key Pair** – The Private Key and its associated Public Key.
- **LDH Label** – From RFC 5890 (http://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, it's total length MUST NOT exceed 63 octets."
- **Legal Entity** – An association, corporation, partnership, proprietorship, trust, or government entity that has legal standing in a country's legal system.
- **Linting** – A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in the Baseline Requirements.
- **Microsoft PKI Policy Authority –** Combination of Microsoft's Steering and Oversight Committees.
- **Multi-Factor Authentication** – An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction:
    1. something the user knows (knowledge factor);
    2. something the user has (possession factor); and
    3. something the user is (inherence factor). Each factor is independent of the other(s).

- **Multi-Party Control** – An access control mechanism which requires two or more separate, authorized users to successfully authenticate with their own unique credentials prior to access being granted.
- **National Vulnerability Database (NVD)** – A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see http://nvd.nist.gov/).
- **Network Equipment** – Hardware devices and components that facilitate communication and data transfer within the CA Infrastructure.
- **Non-Reserved LDH Label** – From RFC 5890 (hhtp://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '- -' in the third and fourth positions."
- **Object Identifier** – A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
- **OCSP Responder** – An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
- **Onion Domain Name** – A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.
- **Online CA (OCA) -** a certification authority system which signs end-entity Subscriber Certificates that are operated and maintained in an online state so as to provide continually available certificate signing services. Online CAs reside in segmented, secured, and functionally dedicated networks.
- **Online Certificate Status Protocol** – An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.
- **OWASP Top Ten** – A list of application vulnerabilities published by the Open Web Application Security Project (see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
- **Parent Company** – A company that Controls a Subsidiary Company.
- **Penetration Test –** A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.
- **Physically Secure Environment** – A controlled and protected physical space consisting minimally of a physical environment which is:

1. protected by security controls which address the topics outlined in section 4.5.1 of RFC3647; and
2. designed, built, and maintained in accordance with Risk Assessments conducted by the CA.

- **P-Label** – A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3942, Section 6.3) from the fifth and subsequent positions.
- **Pending Prohibition** – The use of a behavior described with this label is highly discouraged, as it is planned to be deprecated and will likely be designated as MUST NOT in the future.
- **Principle of Least Privilege** – The principle that users, devices, and software should only have the minimum necessary access and privileges to complete their functions.
- **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.
- **Publicly-Trusted Certificate** – A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
- **P-Label** – A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.
- **Random Value** – A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
- **Registration Authority (RA)** – Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- **Registration Identifier --** the unique code assigned to an Applicant by the Incorporating or Registration Agency in such entity's Jurisdiction of Incorporation or Registration.
- **Reliable Data Source** – An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the

Applicant obtaining a Certificate.

- **Relying Party** – Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.
- **Relying Party Agreement** – an agreement which specifies the stipulations under which a person or organization acts as a Relying Party.
- **Repository** – An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- **Request Token** – A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

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

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

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

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

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

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

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

- **Required Website Content** – Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
- **Reserved IP Address** – An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:
  1. https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
  2. https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml
- **Risk Assessment** – A formal process that:
  1. Identifies and documents foreseeable internal and external threats to the CA Infrastructure that could result in:
     1. unauthorized access to the CA Infrastructure;
     2. disclosure of data stored in the CA Infrastructure;
     3. misuse of the CA Infrastructure; or
     4. unapproved alteration or destruction of any part of the CA Infrastructure;

2. Assesses and documents the likelihood and potential damage of each identified threat, taking into consideration minimally the sensitivity and criticality of the CA Infrastructure; and
3. Assesses and documents the sufficiency of the policies, procedures, controls, information systems, technology, and other arrangements that the CA has in place to counter each identified threat.

- **Root CA** – The top-level CA whose root certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- **Root CA Certificate** – A self-signed and self-issued certificate where:
    1. the issuer and subject of the certificate are the same; and
    2. the digital signature of the certificate is:
        - generated using the Private Key of a Key Pair whose corresponding Public Key is bound to the certificate; and
        - verified using the Public Key contained in the certificate.
- **Root CA Private Key** – The Private Key associated with a Root CA Certificate.
- **Root CA System** – A system used to:
    1. generate a Key Pair whose Private Key is or will be a Root CA Private Key;
    2. store a Root CA Private Key; or
    3. create digital signatures using a Root CA Private Key.
- **SANS Top 25** – A list created with input from the SysAdmin, Audit, Network, and Security (SANS) Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 Most Dangerous Software Errors that lead to exploitable vulnerabilities (see http://www.sans.org/top25-software-errors/).
- **Security Support System** – A system or set of systems supporting the security of the CA Infrastructure, which minimally includes:
    1. authentication;
    2. network boundary control;
    3. audit logging;
    4. audit log reduction and analysis;
    5. vulnerability scanning;
    6. physical intrusion detection;
    7. host-based intrusion detection; and
    8. network-based intrusion detection.
- **Short-lived Subscriber Certificate** – A Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

- **Signing Service** – an organization that signs an Object on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.
- **Sovereign State** – A state or country that administers its own government, and is not dependent upon, or subject to, another power.
- **Subject** – The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- **Subject Identity Information** – Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the 'subjectAltName' extension or the Subject 'commonName' field.
- **Subscriber** – an individual or end-entity (person, device, or application) that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate .
- **Subordinate CA** – A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
- **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.
- **Subsidiary Company** – A company that is controlled by a Parent Company.
- **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**.**
- **System** – One or more pieces of equipment or software that stores, transforms, or communicates data.
- **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 or Name Constraint extensions, as defined within the relevant Certificate Profiles of this document, to limit the scope within which the Subordinate CA Certificate MAY issue Subscriber or additional Subordinate CA Certificates**.**
- **Terms of Use** – Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
- **TimeStamp Authority –** a service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root,

thereby asserting that the data (or the data from which the data were derived via secure hashing algorithm) existed at the specific time. If the TimeStamp Authority is delegated to a third party, the CA is responsible that the delegated authority complies with the CAB Code Signing Requirements.

- **Transport Layer Security (TLS)/Secure Socket Layer (SSL) –** a security protocol that is widely used in the Internet, for the purpose of authentication and establishing secure sessions
- **Trusted Role –** An employee or contractor of a CA or Delegated Third Party who has authorized access to any component of CA Infrastructure.
- **Trustworthy System** – Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
- **Unregistered Domain Name** – A Domain Name that is not a Registered Domain Name.
- **Valid Certificate** – A Certificate that passes the validation procedure specified in RFC 5280.
- **Validation Specialist** – Someone who performs the information verification duties specified by these Requirements.
- **Validity Period** – From RFC 5280 (http://tools.ietf.org/html/rfc5280): "The period of time from notBefore through notAfter, inclusive."
- **Vulnerability Scan** – A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.
- **WHOIS** – Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
- **Wildcard Certificate** – A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.
- **Wildcard Domain Name** – A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.
- **Workstation** – A device, such as a phone, tablet, or desktop or laptop computer, which is capable of accessing CA Infrastructure and/or Network Equipment with elevated privileges compared to any given point on the general internet.
- **XN-Label** – From RFC 5890 (http://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix "xn- -" (case independent), but otherwise conform to the rules for LDH Labels."

1.6.2 Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure

RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extension)
SSL	Secure Socket Layer
TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol

1.6.3 References

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

CA/Browser Forum Network and Certificate Systems Security Requirements (“NCSSRs”) or Network Security Requirements (“NSRs”)

FIPS 140-3, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019.

FIPS 186-5, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, February 3, 2023.

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

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

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure:

Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for

Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.

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

RFC3912, Request for Comments: 3912, WHOIS Protocol Specification, Daigle,

September 2004.

RFC3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic

Syntax. T. Berners-Lee, et al. January 2005.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions,

Blake-Wilson, et al, April 2006.

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

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

RFC5890, Request for Comments: 5890, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. J. Klensin. August 2010.

RFC5952, Request for Comments: 5952, A Recommendation for IPv6 Address Text Representation. S. Kawamura, et al. August 2010.

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

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

RFC7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, R. Fielding, J. Reschke. June 2014.

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

RFC7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect), J. Reschke. April 2015.

RFC8499, Request for Comments: 8499, DNS Terminology. P. Hoffman, et al. January 2019.

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

RFC8738, Request for Comments: 8738, Automated Certificate Management Environment (ACME) IP Identifier Validation Extension. R.B.Shoemaker, Ed. February 2020.

RFC8954, Request for Comments: 8954, Online Certificate Status Protocol (OCSP) Nonce Extension. M. Sahni, Ed. November 2020.

WebTrust for Certification Authorities, SSL Baseline with Network Security, available at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust Principles and Criteria for Certification Authorities – SSL Baseline

X.509, Recommendation ITU-T X.509 (10/2023) | ISO/IEC 9594-8/Core2 (Common), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

1.6.4 Conventions

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 standards for the creation of Certificate Policy (CP) and Certification Practices Statement (CPS) documents and complies with the current Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“Baseline Requirements”) from the Certificate Authority and Browser Forum (CA/B Forum) at http://www.cabforum.org.

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

A web-based repository is available on a 24x7 basis to all Relying Parties who wish to access this CPS or other information from Microsoft PKI Services. The repository SHALL contain the current versions of this CPS and accompanying CP, a fingerprint of the established Root CAs, current CRLs, qualified Auditor Reports, Subscriber and Relying Party Agreements, a Privacy Statement, and other Terms of Use information.

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

2.3 TIME OR FREQUENCY OF PUBLICATION

The CA SHALL annually review their CP and CPS and compare it with the CA/B Forum’s Baseline Requirements for any modifications.

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

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

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

2.4 ACCESS CONTROLS ON REPOSITORIES

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Type of Names

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

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

No Stipulation

3.1.4 Rules for Interpreting Various Name Forms

No Stipulation

3.1.5 Uniqueness of Names

No Stipulation

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Application or Certificate Request that infringes upon the intellectual property and commercial rights of entities outside of their authority. Microsoft PKI Services does not determine whether Certificate Applicants have intellectual property rights in the name used in a Certificate Application, nor does Microsoft PKI Services resolve any dispute concerning the ownership of a domain name or trademark. Microsoft PKI Services MAY reject any Certificate Application and revoke any Certificate because of such a dispute.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization Identity

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the `countryName` field, then the MS PKI SHALL verify the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3 and that is described in MS PKI's Certificate Policy and/or Certification Practice Statement. If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then MS PKI SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of this Section 3.2.2.1 and that is described in MS PKI's Certificate Policy and/or Certification Practice Statement. MS PKI SHALL inspect any document relied upon under this Section for alteration or falsification.

All DNS queries conducted in the course of satisfying the requirements of Section 3.2.2.4 (Validation of Domain Authorization or Control) and Section 3.2.2.8 (CAA Records) are made from the CA to authoritative nameservers, i.e. without the use of recursive resolvers operated outside the CA's audit scope.

All contact information for Domain Contacts comes from a DNS SOA record or direct contact with the Domain Name Registrar of the Base Domain Name, and SHALL be obtained directly by MS PKI. MS PKI does not validate IP addresses.

3.2.2.1 Identity

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

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

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

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

3.2.2.2 DBA/Tradename

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

3.2.2.3 Verification of Country

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

3.2.2.4 Validation of Domain Authorization or Control

Microsoft PKI Services SHALL confirm that, before a Certificate gets issued, the Fully-Qualified Domain Name (FQDN) and/or its accompanying Domain Namespace MUST be validated for use in the Certificate by one or more of the methods listed below.

Microsoft PKI Services does not issue certificates for FQDNs that contain "onion" as the rightmost Domain Label.

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

Microsoft PKI Services currently utilizes the following methods as detailed in the Baseline Requirements:

- 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact;
- 3.2.2.4.7 DNS Change

When issuing Subscriber Certificates, Microsoft PKI Services SHALL NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period. When obtaining Domain Contact information for a requested Domain Name, Microsoft PKI Services SHALL NOT use the WHOIS protocol (RFC 3912) or Registry Data Access Protocol (RFC 7482).

For each method Microsoft PKI Services will follow a documented process and maintain records noting the method(s) used for each issuance.

3.2.2.5 Authentication for an IP Address

Microsoft PKI Services does not issue to IP Addresses from CAs governed by this CPS.

3.2.2.6 Wildcard Domain Validation

Using a documented process, Microsoft PKI Services SHALL refuse issuance if a wildcard character in a CN or subjectAltName of type DNS-ID occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. ".com","co.uk"). Upon receiving an application for a wildcard certificate as described in the previous sentence, if the FQDN portion of the Wildcard Domain Name is "registry-controlled" or is a "public suffix, Microsoft PKI Services SHALL only allow issuance after an applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7 Data Source Accuracy

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

The criteria for this evaluation SHOULD include:

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

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

3.2.2.8 CAA Records

Microsoft PKI Services policy on checking CAA records is stated in Section 4.2.4.

3.2.3 Authentication of Individual Identity

Microsoft PKI Services does not issue certificates to natural persons from CAs governed by this CPS.

3.2.4 Non-Verified Subscriber Information

Microsoft PKI Services does not verify the following subscriber information:

- Organization identity for Domain Validated certificates;
- Any other information not designated as verified.

3.2.5 Validation of Authority

Microsoft PKI Services SHALL verify authority for all certificate requests using a Reliable Method of Communication as described in the Baseline Requirements. For Domain Validated or Organization Validated requests, Microsoft PKI Services SHALL verify this authority utilizing one or more methods as described in the Baseline Requirements.

Microsoft PKI Services will allow an Applicant to limit authority to a list of authorized individuals. The limitation to authorized individuals is complete once Microsoft PKI Services notifies Applicant that the specified limitations have been approved. Microsoft PKI Services SHALL NOT accept any certificate requests that are outside of the Applicant's specification.

Microsoft PKI Services SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation

The CA SHALL disclose, in our public repository, all Cross Certificates that identify a Microsoft PKI Services CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

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

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 (e.g. via API) MAY be authenticated and approved, providing the request comes from the subscriber or an approved authority.

Revocation requests which are not made electronically are evaluated on a case by case basis. If identification and authentication are required, Microsoft PKI Services selects these procedures based on the circumstances of the request and follows a documented process (such as per Section 3.2.2 of this CPS).

Identification and authentication is not required in cases where the revocation request is made by Microsoft PKI Services or where the request is made by reference to a revocation reason that is independent of the requester's identity.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

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

Applicants or authorized Certificate Requestors who are not included in any of the previous lists MAY submit a Certificate Application provided the Certificate Request meets the requirements

set forth in the CP, this CPS, and the CA/Browser Forum's Baseline Requirements published at www.cabforum.org.

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

4.1.2 Enrollment Process and Responsibilities

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

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

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

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

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

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

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

Section 6.3.2 limits the validity period of Subscriber Certificates. MS PKI Services MAY use the documents and data provided in Section 3.2.2 to verify certificate information, or MAY reuse previous validations themselves, provided that MS PKI Services obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 825 days prior to issuing the Certificate.

For validation of Domain Names according to Section 3.2.2.4 any reused data, document, or completed validation MUST be obtained no more than 398 days prior to issuing the Certificate.

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

After the change to any validation method specified in the Baseline Requirements, MS PKI Services MAY continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in the BR Section 4.2.1 unless otherwise specifically provided in a ballot.

Microsoft PKI Services SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

Microsoft PKI Services does not use Delegated Third Parties to fulfill any of the obligations under this section of the BR.

4.2.2 Approval or Rejection of Certificate Applications

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

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

- Applicant or Subscriber information is unable to be verified, per Section 3.2.2;
- The CA deems the certificate issuance MAY negatively impact the CA's business or reputation;
- Failure to consent to the Subscriber Agreement;
- Failure to provide Payment;
- The Certificate Request contains an Internal Name with a gTLD that ICANN has either announced or MAY consider making operational, per information from the following location: https://gtldresult.icann.org/application-result/applicationstatus/viewstatus.
- The Certificate Request contains an IP Address (see Section 3.2.2.5).

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

Applications for subordinate CAs are not approved unless the CA in question is operated by Microsoft or one of its affiliates and SHALL be governed by the CP and this CPS.

Microsoft PKI Services SHALL NOT issue publicly trusted Certificates to Internal Names or Reserved IP Addresses.

4.2.3 Time to Process Certificate Applications

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

4.2.4 Verification of CAA Records

As part of the issuance process, Microsoft PKI Services checks for a CAA record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the

procedure in RFC 8659, following the processing instructions set down in RFC 8659 for any records found. This stipulation does not prevent Microsoft PKI Services from checking CAA records at any other time.

If Microsoft PKI Services issues, it does so within the TTL of the CAA record, or 8 hours, whichever is greater.

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

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

When processing CAA records, Microsoft PKI Services MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag.

Additional property tags MAY be supported but MUST NOT conflict with or supersede the mandatory property tags set out in this document.

Microsoft PKI Services MUST respect the critical flag and not issue a Certificate if they encounter an unrecognized property with this flag set.

RFC 8659 requires that MS PKI Services MUST NOT issue a certificate unless the CA determines that either:

(1) the certificate request is consistent with the applicable CAA RRset or

(2) an exception specified in the relevant CP or CPS applies.

Microsoft PKI Services MAY decide not to check for a CAA record:

- For certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked;
- For certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant;

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

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

Microsoft PKI Services documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/B Forum on the circumstances.

CAA record checking results are logged in certificate lifecycle management event logs (see Section 5.4.1).

URL schemes in the iodef record other than mailto: or https: are not supported.

Microsoft PKI Services MAY choose to limit issuance according to RFC 8657.

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 SHALL be approved by the Microsoft PKI Policy Authority.

4.3.1.1 Manual authorization of certificate issuance for Root CAs

Certificate issuance by the Root SHALL require an individual authorized by Microsoft PKI Services (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.1.2 Linting of to-be-signed Certificate content

Microsoft PKI Services SHALL implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that Microsoft PKI Services has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962, Section 3.2.

Methods used to produce a certificate containing the to-be-signed Certificate content include, but are not limited to:

1. Sign the tbsCertificate with a "dummy" Private Key whose Public Key component is not certified by a Certificate that chains to a publicly-trusted CA Certificate; or
2. Specify a static value for the signature field of the Certificate ASN.1 SEQUENCE.

Microsoft PKI Services MAY implement first-party certificate Linting tools and/or use the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

4.3.1.3 Linting of issued Certificates

Microsoft PKI Services MAY use a Linting process to test each issued Certificate.

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 Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

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

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

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

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

4.5.2 Relying Party Public Key and Certificate Usage

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

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

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

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of 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

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 SHALL NOT 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

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Microsoft PKI Services SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs (and Microsoft PKI Services gains actual knowledge of it):

1. The Subscriber requests in writing, without specifying a CRLreason, that the MS PKI Services revoke the Certificate (CRLReason "unspecified (0)" which results in no

reasonCode extension being provided in the CRL);

2. The Subscriber notifies MS PKI Services that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. MS PKI Services obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. MS PKI Services is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);
5. MS PKI Services obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

Microsoft PKI Services SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days and use the corresponding CRLReason if one or more of the following occurs (and Microsoft PKI Services gains actual knowledge of it):

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #4, superseded);
7. MS PKI Services obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. MS PKI Services is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
9. MS PKI Services is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
10. MS PKI Services is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
11. MS PKI Services is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
12. MS PKI Services is made aware that the Certificate was not issued in accordance with the BRs, MS PKI's Certificate Policy or this Certification Practice Statement (CRLReason #4, superseded);

13. MS PKI determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. MS PKI's right to issue Certificates under the BR expires or is revoked or terminated, unless MS PKI has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. Revocation is required by MS PKI's Certificate Policy or this Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

A Subordinate CA Certificate SHALL be revoked within seven (7) days if one or more of the circumstances in Section 4.9.1.1 or additional items specified in the CA/B Forum Baseline Requirements occur.

4.9.2 Who Can Request Revocation

Certificate revocations MAY be requested from the authorized Subscribers, RAs, or the CA. Third parties MAY also submit Certificate Problem Reports to the Issuing CA, if one or more of the circumstances in 4.9.1.1 occur that suggests reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

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

1. MS 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. MS PKI Services MAY request authorization of the revocation request from the Subscriber or designated contact;
3. MS PKI Services SHALL authenticate the entity making the request, per Section 4.9.2;
4. If a request is received from a third party, MS 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. MS PKI Services SHALL verify the requested revocation reason aligns with those in Section 4.9.1.1 or 4.9.1.2;
6. If MS PKI Services determines that revocation is appropriate; CA personnel MAY revoke the certificate and update the CRL.

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

Instructions for requesting a revocation:

- Microsoft PKI Services provides revocation request instructions directly to subscribers.
- For everyone else please contact via email at CentralPKI@microsoft.com.

Please refer to Section 1.5.2 for other information on contacting Microsoft PKI Services.

4.9.3.1 Revocation Reason Codes

Microsoft PKI Services follows Mozilla's Root Store Policy when populating the reasonCode extension of CRL entries for the revocation of end-entity TLS certificates.

Third parties including Subscribers and Relying Parties are required to select the appropriate reason code as defined in Mozilla' Root Store Policy when submitting a revocation request.

For revocation requests made electronically via API, the reason code can be selected during the API workflow.

4.9.3.1.1 Reason Codes Available to Third Parties

The following reason codes can be selected by third parties.

keyCompromise (RFC 5280, CRLReason #1)

This reason code is used if either of the following applies:

- The Subscriber requests revocation for this revocation reason;
- Microsoft PKI Services obtains verifiable evidence that the certificate subscriber's private key corresponding to the public key in the certificate suffered a key compromise (as outlined in Section 4.9.12).
- There is a demonstrated or proven method that exposes the Subscriber's private key to a key compromise;
- Anyone requesting revocation for keyCompormise has previously demonstrated or can currently demonstrate possession of the private key of the certificate;
- There is clear evidence that that the specific method used to generate the private key was flawed; or
- There is a demonstrated or proven method that can easily compute the certificate subscriber's private key based on the public key in the certificate (e.g Debian weak key).

cessationOfOperation (RFC 5280, CRLReason #5)

This reason code is used if either of the following applies:

- The Subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate;
- The Subscriber will no longer be using the certificate because they are discontinuing their website; or

- There are circumstances indicating that use of a fully qualified domain name in the certificate is no longer legally permitted.

affiliationChanged (RFC 5280, CRLReason #3)

This reason code is used if:

- The subject's name or other subject identity information in the certificate has changed, but there is no cause to suspect that the certificate's private key has been compromised.

Superseded (RFC 5280, CRLReason #4)

This reason code is used if either of the following applies:

- The Subscriber requests revocation for this revocation reason;
- The Subscriber has requested a new certificate to replace an existing certificate;
- There is reasonable evidence that the validation of domain authorization or control for any fully qualified domain name in the certificate should not be relied upon; or
- The certificate does not comply with a relevant root program policy, the CA/Browser Forum's Baseline Requirements, or Microsoft PKI Service's CP or CPS.

No Reason Code

No reason code is included for revocation where none of the reasons in this section apply. If the certificate is revoked for a reason not listed in 4.9.3.1.1 or 4.9.3.1.2 the reasonCode extension MUST NOT be provided in the CRL.

Multiple Revocation Reasons

If the situation is that multiple revocation reasons apply, the revocation reason of higher priority (as per this priority list) should be indicated.

1. keyCompromise (RFC 5280, CRLReason #1)
2. privilegeWithdrawn (RFC 5280, CR Reason #9)
3. cessationOfOperation (RFC 5280, CRLReason #5)
4. affiliationChanged (RFC 5280, CRLReason #3)
5. superseded (RFC 5280, CRLReason #4)

4.9.3.1.2 Reason Codes Only Available to Microsoft PKI Services

In addition to the reason codes listed above, Microsoft PKI Services MAY use the reason code provided below.

privilegeWithdrawn (RFC 5280, CRLReason #9)

This reason code is used if either of the following applies:

- The certificate was misused;
- The Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
- Microsoft PKI Services is made aware of a material change in the information contained in the certificate;

- Microsoft PKI Services determines or is made aware that any of the information appearing in the certificate is inaccurate; or
- Microsoft PKI Services is made aware that the original certificate request was not authorized and that the Subscriber does not retroactively grant authorization.

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

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

After reviewing the facts and circumstances, Microsoft PKI Services SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether the certificate will be revoked, and if so, a date on which the CA will revoke the certificate.

The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1.

The date selected by MS PKI Services SHALL consider the following criteria:

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

CRLs are available via a publicly-accessible HTTP URL (i.e., "published").
Within twenty-four (24) hours of issuing its first Certificate, the CA MUST generate and publish either:
a full and complete CRL; or
partitioned (i.e., "sharded") CRLs that, when aggregated, represent the equivalent of a full and complete CRL.
CAs issuing Subscriber Certificates:
Update and publish a new CRL at least every:

seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod (“AIA OCSP pointer”); or
four (4) days in all other cases;
Update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.
CAs issuing CA Certificates:
Update and publish a new CRL at least every twelve (12) months;
Update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.
CAs continue issuing CRLs until one of the following is true:
all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; or
the corresponding Subordinate CA Private Key is destroyed.

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

The validity interval of an OCSP response is the difference in time between the `thisUpdate` and `nextUpdate` field, inclusive. For purposes of computing differences, a difference of 3,600 seconds SHALL be equal to one hour, and a difference of 86,400 seconds SHALL be equal to one day, ignoring leap-seconds.
A certificate serial is "assigned" if:
a Certificate or Precertificate with that serial number has been issued by the Issuing CA; or
a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with the Issuing CA.
A certificate serial is "unassigned" if it is not "assigned".
The following SHALL apply for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.
OCSP responders operated by Microsoft PKI Services support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. Microsoft PKI Services MAY process the Nonce extension (`1.3.6.1.5.5.7.48.1.2`) in accordance with RFC 8954.
An authoritative OCSP response SHALL be available (i.e. the responder MUST NOT respond with the "unknown" status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.
For OCSP responses with validity intervals less than sixteen hours, Microsoft PKI Services SHALL provide an updated OCSP response prior to one-half of the validity period before the nextUpdate.
For OCSP responses with validity intervals greater than or equal to sixteen hours, Microsoft PKI Services SHALL provide an updated OCSP response at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.
For the status of a Subordinate CA Certificate, Microsoft PKI Services SHALL provide an updated OCSP response at least every twelve months, and within 24 hours after revoking the Certificate.
The following SHALL apply for communicating the status of *all* Certificates for which an OCSP responder is willing or required to respond.
OCSP responses conform to RFC6960 and/or RFC5019. OCSP responses are either:
signed by the CA that issued the Certificates whose revocation status is being checked, or

signed by an OCSP Responder which complies with the OCSP Responder Certificate Profile in Section 7.1.2.8.
OCSP responses for Subscriber Certificates have a validity interval greater than or equal to eight hours and less than or equal to ten days.
If the OCSP responder receives a request for the status of a certificate serial number that is "unassigned", then the responder SHALL NOT respond with a "good" status.

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

In the event of key compromise, Subscribers MUST immediately notify Microsoft PKI Services, via email to CentralPKI@microsoft.com. The Subscriber is responsible for investigating the compromise circumstances.

Reports to Microsoft PKI Services of key compromise MUST include:

1. Proof of key compromise in either of the following formats:
   a. A CSR signed by the compromised private key with the Common Name “Proof of Key Compromise for Microsoft PKI Services”; or
   b. The private key itself.
2. A valid email address so that you can receive confirmation of your problem report and as appropriate associated certificate revocations.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

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

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

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

4.10.3 Optional Features

No Stipulation

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

Microsoft PKI Services SHALL develop, implement, and maintain a comprehensive security program designed to:

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

The Certificate Management Process MUST include:

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

Microsoft PKI Services' security program MUST include an annual Risk Assessment that:

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

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

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

CA facilities are protected from unauthorized access, through the required use of multi-factor

authentication solutions. Facility security systems electronically log ingress and egress of authorized personnel.

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

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

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

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Trusted Roles consist of vetted and approved employees or Delegated Third Parties that require access to or control over Microsoft PKI Service's Certificate Systems.

The personnel considered for Trusted Role positions MUST successfully pass the screening and training requirements of CPS Section 5.3.

5.2.2 Number of Persons Required per Task

Microsoft PKI Services Private Keys SHALL be backed up, stored, and recovered only by personnel in Trusted Roles using at least, dual control in a physically secured environment.

5.2.3 Identification and Authentication for Each Role

Microsoft PKI Services complies with Section 2 of the NCSSRs.

5.2.4 Roles Requiring Separation of Duties

No Stipulation

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

Prior to assignment in a Trusted Role position, the prospective CA personnel SHALL undergo and clear the necessary background checks or security screenings requirements.

5.3.3 Training Requirements

Microsoft PKI Services SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including Microsoft PKI Services Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and the BRs.

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

Microsoft PKI Services SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

Microsoft PKI Services SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the BRs.

Personnel in a Trusted Role SHALL comply with Microsoft Compliance Training standards.

5.3.4 Retraining Frequency and Requirements

All personnel in Trusted roles SHALL maintain skill levels consistent with Microsoft Compliance Training standards , at least annually.
All Validation specialists SHALL maintain skill levels consistent with Section 5.3.3. at least every two years.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Microsoft PKI Services SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.8 Documentation Supplied to Personnel

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

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

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. Relevant router and firewall activities (as described in Section 5.4.1.1); and
   g. Entries to and exits from the CA facility.

Log entries MUST include at least the following elements:

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

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.f MUST at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

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 and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the revocation or expiration of the Subscriber Certificate;
3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

5.4.4 Protection of Audit Log

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

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

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

Additionally, see Section 5 for the annual Risk Assessment requirements.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

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

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

5.5.2 Retention Period for Archive

CA SHALL retain all documentation relating to a Certificate's activities for a period of at least two (2) years after the Certificate ceases to be valid.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 KEY CHANGEOVER

No Stipulation

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

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

The Business Continuity Plan SHALL align with the requirements of the CA/B Forum's Baseline Requirements.

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

See Section 5.7.4.

5.7.3 Entity Private Key Compromise Procedures

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

Subscribers, and coordinate revoking and reissuing the affected certificates.

5.7.4 Business Continuity Capabilities After a Disaster

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

5.8 CA OR RA TERMINATION

In the event that it is necessary to terminate the operation of a CA, CA management SHALL plan and coordinate the termination process with its Subscribers and Relying Parties, such that the impact of the termination is minimized. The CA SHALL 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

For CA Key Pairs that are either:

1. used as a CA Key Pair for a Root Certificate or
2. used as a CA Key Pair for a Subordinate CA Certificate, where the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA,

Microsoft PKI Services SHALL:

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

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

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

In all cases, Microsoft PKI Services SHALL:

1. generate the CA Key Pair in a physically secured environment as described in this Certification Practice Statement;
2. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;

3. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in this Certification Practice Statement;
4. log its CA Key Pair generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this Certification Practice Statement and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No Stipulation

6.1.1.3 Subscriber Key Pair Generation

Microsoft PKI Services SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. Microsoft PKI Services is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. Microsoft PKI Services has previously been notified that the Applicant's Private Key has suffered a Key Compromise using the Microsoft PKI Services' procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key. At least the following precautions are implemented:
    a. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), the Microsoft PKI Services SHALL reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, Microsoft PKI Services SHALL reject Debian weak keys.
    b. In the case of ROCAvulnerability, Microsoft PKI Services SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    c. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), Microsoft PKI Services SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

If the Subscriber Certificate will contain an extKeyUsage extension containing eitherthe values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], Microsoft PKIServices SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using a Key Pair previously generated by the CA.

6.1.2 Private Key Delivery to Subscriber

If a Subscriber generates their own key pairs, Private Key delivery SHALL NOT be performed.

In the event the CA is authorized to generate a Private Key on behalf of a Subscriber, the Private Key SHALL be encrypted prior to transporting to the Subscriber.

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber.

If Microsoft PKI Services become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then Microsoft PKI Services SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

No Stipulation

6.1.4 CA Public Key Delivery to Relying Parties

No Stipulation

6.1.5 Key Sizes

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

Root CA, Subordinate CA, and Subscriber Certificates

Key Algorithm	Values
Digest Algorithm	SHA-256, SHA-384, SHA-512
Minimum RSA Modulus Size (bits)	2048
ECC Curve	NIST P-256, P-384, P-521

Digital Signature Algorithm (DSA) key lengths (L and N) are described in the Digital Signature Standard, FIPS 186-6 (https://csrc.nist.gov/publications/detail/fips/186/6/final).

For RSA key pairs Microsoft PKI Services SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, the CA SHALL:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

No other algorithms or key sizes are permitted.

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.

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

ECDSA: Microsoft PKI Services SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

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); and
4. Certificates for OCSP Response verification.

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 or FIPS 140-3 level 3 hardware cryptographic modules that meet industry standards for random and prime number generation.

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

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

6.2.3 Private Key Escrow

No Stipulation

6.2.4 Private Key Backup

Backup copies of CA Private Keys SHALL be backed up by multiple persons in Trusted Role

positions and only be stored in encrypted form on cryptographic modules that meet the requirements specified in Section 6.2.1.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA.

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

6.2.7 Private Key Storage on Cryptographic Module

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 Trusted 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. (See Section 7.1.2.1.1 for additional Root CA Validity restrictions)

Entity Type	Minimum - notBefore	Maximum - notBefore	Minimum - notAfter	Maximum - notAfter
Root CAs*	One day prior to the time of signing	The time of signing	2922 days (approx - 8 years)	9132 days (approx -25 years)
"Offline" Subordinate CAs	One day prior to the time of signing for Native; or for Cross-Certified, the earlier of one day prior to the time of signing or the earliest notBefore date of the existing CA Certificate(s)	The time of signing	The time of signing	7305 days (approx - 20 years)
"Online" Subordinate CAs	One day prior to the time of signing for Native; or for Cross-Certified, the earlier of one day prior to the time of signing or the earliest notBefore date of the existing CA Certificate(s)	The time of signing	The time of signing	2192 days (approx - 6 years)
Subscriber Certificates	A value within 48 hours of the certificate signing operation	The time of signing	The time of signing	397 days
OCSP Responder Certificates	One day prior to the time of signing	The time of signing	The time of signing	397 days

***Note:** This restriction applies even in the event of generating a new Root CA Certificate for an existing subject and subjectPublicKeyInfo (e.g. reissuance). The new CA Certificate MUST conform to these rules.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds or leap seconds, SHALL represent an additional day. For this reason, Microsoft PKI Services SHALL NOT issue Subscriber Certificates for the maximum permissible time by default, in order to account for such adjustments.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

No Stipulation

6.4.3 Other Aspects of Activation Data

No Stipulation

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

No Stipulation

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

No Stipulation

6.6.2 Security Management Controls

No Stipulation

6.6.3 Life Cycle Security Controls

No Stipulation

6.7 NETWORK SECURITY CONTROLS

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

Microsoft PKI Services CA systems are protected by a set of controls that implement the CA/B Forum's Network and Certificate System Security Requirements (https://cabforum.org/network-security-requirements/).

6.8 TIME-STAMPING

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Microsoft PKI Services meets the technical requirements set forth in Section 2.2 – Publication of Information, Section 6.1.5 – Key Sizes, and Section 6.1.6 – Public Key Parameters Generation and Quality Checking of this document.

Microsoft PKI Services issues Certificates in accordance with the profile specified in the BRs.

7.1.1 Version Number(s)

Microsoft PKI Services issues certificates that are compliant with X.509 v3.

7.1.2 Certificate Extensions

Microsoft PKI Services asserts compliance with the BRs, all issued certificates comply with one of the following certificate profiles, which incorporate, and are derived from RFC 5280 (https://datatracker.ietf.org/doc/html/rfc5280). Except as explicitly noted, all normative requirements imposed by RFC 5280 SHALL apply, in addition to the normative requirements imposed by this document. Microsoft PKI Services has examined RFC 5280, Appendix B (https://datatracker.ietf.org/doc/html/rfc5280#appendix-B) for further issues to be aware of.

- CA Certificates
  - Section 7.1.2.1 – Root CA Certificate Profile
  - Section 7.1.2.6 – TLS Subordinate CA Certificate Profile
- Section 7.1.2.7 – Subscriber (End-Entity) Certificate Profile
- Section 7.1.2.8 – OCSP Responder Certificate Profile
- Section 7.1.2.9 – Precertificate Profile

7.1.2.1 Root CA Certificate Profile

See Appendix B for Root CA Profile details.

7.1.2.1.1 Root CA Validity

See Section 6.3.2.

7.1.2.1.2 Root CA Extensions

See Appendix B for Root CA Profile details.

7.1.2.1.3 Root CA Authority Key Identifier

See Appendix B for Root CA Profile details.

7.1.2.1.4 Root CA Basic Constraints

See Appendix B for Root CA Profile details.

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

While Microsoft PKI Services MAY have Subordinate CA certificates cross-certified by other providers, Microsoft PKI Services SHALL NOT cross-certify or cross-sign Subordinate CA certificates.

7.1.2.2.1 Cross-Certified Subordinate CA Validity

While Microsoft PKI Services MAY have Subordinate CA certificates cross-certified by other providers, Microsoft PKI Services does not cross-certify or cross-sign Subordinate CA certificates.

7.1.2.2.2 Cross-Certified Subordinate CA Naming

While Microsoft PKI Services MAY have Subordinate CA certificates cross-certified by other providers, Microsoft PKI Services SHALL NOT cross-certify or cross-sign Subordinate CA certificates.

7.1.2.2.3 Cross-Certified Subordinate CA Extensions

While Microsoft PKI Services MAY have Subordinate CA certificates cross-certified by other providers, Microsoft PKI Services SHALL NOT cross-certify or cross-sign Subordinate CA certificates.

7.1.2.2.4 Cross-Certified Subordinate CA Extended Key Usage – Unrestricted

While Microsoft PKI Services MAY have Subordinate CA certificates cross-certified by other providers, Microsoft PKI Services does not cross-certify or cross-sign Subordinate CA certificates.

7.1.2.2.5 Cross-Certified Subordinate CA Extended Key Usage – Restricted

While Microsoft PKI Services MAY have Subordinate CA certificates cross-certified by other providers, Microsoft PKI Services SHALL NOT cross-certify or cross-sign Subordinate CA certificates.

7.1.2.2.6 Cross-Certified Subordinate CA Certificate Certificate Policies

While Microsoft PKI Services MAY have Subordinate CA certificates cross-certified by other providers, Microsoft PKI Services SHALL NOT cross-certify or cross-sign Subordinate CA certificates.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

Microsoft PKI Services does not issue Technically Constrained Non-TLS Subordinate CA certificates.

7.1.2.3.1 Technically Constrained Non-TLS Subordinate CA Extensions

Microsoft PKI Services does not issue Technically Constrained Non-TLS Subordinate CA certificates.

7.1.2.3.2 Technically Constrained Non-TLS Subordinate CA Certificate Policies

Microsoft PKI Services does not issue Technically Constrained Non-TLS Subordinate CA certificates.

7.1.2.3.3 Technically Constrained Non-TLS Subordinate CA Extended Key Usage

Microsoft PKI Services does not issue Technically Constrained Non-TLS Subordinate CA certificates.

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

Microsoft PKI Services does not issue Technically Constrained Precertificate Signing CA certificates.

7.1.2.4.1 Technically Constrained Precertificate Signing CA Extensions

Microsoft PKI Services does not issue Technically Constrained Precertificate Signing CA certificates.

7.1.2.4.2 Technically Constrained Precertificate Signing CA Extended Key Usage

Microsoft PKI Services does not issue Technically Constrained Precertificate Signing CA certificates.

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

Microsoft PKI Services does not issue Technically Constrained TLS Subordinate CA certificates.

7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions

Microsoft PKI Services does not issue Technically Constrained TLS Subordinate CA certificates.

7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints

Microsoft PKI Services does not issue Technically Constrained TLS Subordinate CA certificates.

7.1.2.6 TLS Subordinate CA Profile

See Appendix B for TLS Subordinate CA Profile details.

7.1.2.6.1 TLS Subordinate CA Extensions

See Appendix B for TLS Subordinate CA Profile details.

7.1.2.7 Subscriber (Server) Certificate Profile

See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.1 Subscriber Certificate Types

Microsoft PKI Services only issues Organization Validated (OV) subscriber certificates. See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.2 Domain Validated

Microsoft PKI Services does not issue DV Subscriber Certificates.

7.1.2.7.3 Individual Validated

Microsoft PKI Services does not issue IV Subscriber Certificates.

7.1.2.7.4 Organization Validated

See Appendix B for Organization Validated TLS Subscriber Certificate Profile details.

7.1.2.7.5 Extended Validation

Microsoft PKI Services does not currently issue EV Subscriber Certificates.

7.1.2.7.6 Subscriber Certificate Extensions

See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.7 Subscriber Certificate Authority Information Access

See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.8 Subscriber Certificate Basic Constraints

See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.9 Subscriber Certificate Certificate Policies

See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.10 Subscriber Certificate Extended Key Usage

See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.11 Subscriber Certificate Key Usage

See Appendix B for Subscriber Certificate Profile details.

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

See Appendix B for Subscriber Certificate Profile details.

7.1.2.8 OCSP Responder Certificate Profile

If the Issuing CA does not directly sign OCSP responses, it MAY make use of an OCSP Authorized Responder, as defined in RFC 6960. The Issuing CA of the Responder MUST be the same as the Issuing CA for the Certificates it provided responses for. See OCSP Responder Certificate Profile details within Appendix B.

7.1.2.8.1 OCSP Responder Validity

See Section 6.3.2.

7.1.2.8.2 OCSP Responder Extensions

See OCSP Responder Certificate Profile details within Appendix B.

7.1.2.8.3 OCSP Responder Authority Information Access

See OCSP Responder Certificate Profile details within Appendix B.

7.1.2.8.4 OCSP Responder Basic Constraints

See OCSP Responder Certificate Profile details within Appendix B.

7.1.2.8.5 OCSP Responder Extended Key Usage

See OCSP Responder Certificate Profile details within Appendix B.

7.1.2.8.7 OCSP Responder Key Usage

See OCSP Responder Certificate Profile details within Appendix B.

7.1.2.8.8 OCSP Responder Certificate Policies

See OCSP Responder Certificate Profile details within Appendix B.

7.1.2.9 Precertificate Profile

A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined byRFC 6962. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by the CA that it MAY issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate. The CA MAY construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs. The CA MAY use the returned Signed Certificate Timestamps to then alter the Certificate's extensions field, adding a Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3 and as permitted by the relevant profile, prior to signing the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from the CA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the `tbsCertificate` contents, as transformed by the process defined in RFC 6962, Section 3.2.

This profile describes the transformations that are permitted to a Certificate to construct a Precertificate. CAs MUST NOT issue a Precertificate unless they are willing to issue a corresponding Certificate, regardless of whether they have done so. Similarly, a CA MUST NOT issue a Precertificate unless the corresponding Certificate conforms to the Baseline Requirements, regardless of whether the CA signs the corresponding Certificate.

A Precertificate is issued directly by the Issuing CA.

See Subscriber Certificate Profile details within Appendix B for profile specific details.

7.1.2.9.1 Precertificate Profile Extensions – Directly Issued

See Subscriber Certificate Profile details within Appendix B for profile specific details.

7.1.2.9.2 Precertificate Profile Extensions – Precertificate CA Issued

Microsoft PKI Services does not issue from a Precertificate Signing CA.

7.1.2.9.3 Precertificate Poison

The Precertificate MUST contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

This extension MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

7.1.2.9.4 Precertificate Authority Key Identifier

Microsoft PKI Services does not issue from a Precertificate Signing CA. The Precertificate SHALL be byte-for-byte identical with the contents of the authorityKeyIdentifier extension of the corresponding Certificate.

7.1.2.10 Common CA Fields

See CA Certificate Profile details within Appendix B.

7.1.2.10.1 CA Certificate Validity

See Section 6.3.2.

7.1.2.10.2 CA Certificate Naming

All subject names MUST be encoded as specified in Section 7.1.4.

7.1.2.10.3 CA Certificate Authority Information Access

See CA Certificate Profile details within Appendix B.

7.1.2.10.4 CA Certificate Basic Constraints

See CA Certificate Profile details within Appendix B.

7.1.2.10.5 CA Certificate Certificate Policies

See CA Certificate Profile details within Appendix B.

7.1.2.10.6 CA Certificate Extended Key Usage

See CA Certificate Profile details within Appendix B.

7.1.2.10.7 CA Certificate Key Usage

See CA Certificate Profile details within Appendix B.

7.1.2.10.8 CA Certificate Name Constraints

Microsoft PKI Services does not use CA Name Constraints when issuing Subordinate CAs.

7.1.2.11 Common Certificate Fields

This section contains several fields that are common among multiple certificate profiles. However, these fields may not be common among all certificate profiles. Before issuing a certificate, Microsoft PKI Services MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.11.1 Authority Key Identifier

See Certificate Profile details within Appendix B.

7.1.2.11.2 CRL Distribution Points

See Certificate Profile details within Appendix B.

7.1.2.11.3 Signed Certificate Timestamp List

See Certificate Profile details within Appendix B.

7.1.2.11.4 Subject Key Identifier

See Certificate Profile details within Appendix B.

7.1.2.11.5 Other Extensions

All extensions and extension values not directly addressed by the applicable certificate profile:

1. MUST apply in the context of the public Internet, unless:
    a. the extension OID falls within an OID arc for which the Applicant demonstrates ownership, or,
    b. the Applicant can otherwise demonstrate the right to assert the data in a public context.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA (such as including an extension that indicates a Private Key is stored on a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).
3. MUST be DER encoded according to the relevant ASN.1 module defining the extension and extension values.

Microsoft PKI Services SHALL NOT include additional extensions or values unless the CA is aware of a reason for including the data in the Certificate.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to subjectPublicKeyInfo field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

Microsoft PKI Services SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL. Microsoft PKI Services SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the AlgorithmIdentifier for RSA keys MUST be byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

7.1.3.1.2 ECDSA

Microsoft PKI Services SHALL indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters MUST use the namedCurve encoding.

- For P-256 keys, the namedCurve MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
- ForP-384 keys, the namedCurve MUST be secp384r1 (OID: 1.3.132.0.34).
- For P-521 keys, the namedCurve MUST be secp521r1 (OID: 1.3.132.0.35).

When encoded, the AlgorithmIdentifier for ECDSA keys MUST be byte-for-byte identical with the following hex-encoded bytes:

- For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107.
- For P-384 keys, 301006072a8648ce3d020106052b81040022.
- For P-521 keys, 301006072a8648ce3d020106052b81040023.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key MUST conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier - derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate or Precertificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).

- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

Microsoft PKI Services SHALL use one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256: Encoding: 300d06092a864886f70d01010b0500.
- RSASSA-PKCS1-v1_5 with SHA-384: Encoding: 300d06092a864886f70d01010c0500.
- RSASSA-PKCS1-v1_5 with SHA-512: Encoding: 300d06092a864886f70d01010d0500.
- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes: Encoding: 304106092a864886f70d01010a3034a00f300d060960864801650304020105000a11c301a06092a864886f70d010108300d060960864801650304020105000a203020120
- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes: Encoding: 304106092a864886f70d01010a3034a00f300d060960864801650304020205000a11c301a06092a864886f70d010108300d060960864801650304020205000a203020130
- RSASSA-PSS with SHA-512, MGF-1with SHA-512, and a salt length of 64 bytes: Encoding: 304106092a864886f70d01010a3034a00f300d060960864801650304020305000a11c301a06092a864886f70d010108300d060960864801650304020305000a203020140

In addition, Microsoft PKI Services MAY use the following signature algorithm and encoding if all of the following conditions are met:

- If used within a Certificate, such as the signatureAlgorithm field of a Certificate or the signature field of a TBSCertificate:
    - The new Certificate is a Root CA Certificate or Subordinate CA Certificate that is a Cross-Certificate; and,
    - There is an existing Certificate, issued by the same issuing CA Certificate, using the following encoding for the signature algorithm; and,
    - The existing Certificate has a serialNumber that is at least 64-bits long; and,
    - The only differences between the new Certificate and existing Certificate are one of the following:

        - A new subjectPublicKey within the subjectPublicKeyInfo, using the same algorithm and key size; and/or,
        - A new serialNumber, of the same encoded length as the existing Certificate; and/or,
        - The new Certificate's extKeyUsage extension is present, has at least one key purpose specified, and none of the key purposes specified are the id-kp-serverAuth (OID:1.3.6.1.5.5.7.3.1) or the anyExtendedKeyUsage (OID:2.5.29.37.0) key purposes; and/or,
        - The new Certificate's basic Constraints extension has a pathLenConstraint that is zero.
- If used within an OCSP response, such as the signatureAlgorithm of a BasicOCSPResponse:
    - The producedAt field value of the ResponseData MUST be earlier than 2022-06-01 00:00:00UTC; and,
    - All unexpired, un-revoked Certificates that contain the Public Key of the CA Key Pair and that have the same Subject Name MUST also contain an extKeyUsage extension with the only key usage present being the id-kp-ocspSigning (OID:1.3.6.1.5.5.7.3.9) keyusage.
- If used within a CRL, such as the signatureAlgorithm field of a CertificateList or the signature field of a TBSCertList:
    - The CRL is referenced by one or more Root CA or Subordinate CA Certificates; and,
    - The Root CA or Subordinate CA Certificate has issued one or more Certificates using the following encoding for the signature algorithm.

Note: The above requirements do not permit a CA to sign a Precertificate with this encoding.

- RSASSA-PKCS1-v1_5 with SHA-1: Encoding: 300d06092a864886f70d0101050500

7.1.3.2.2 ECDSA

Microsoft PKI Services SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040302.

If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040303.

If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040304.

7.1.4 Name Forms

This section details encoding rules that apply to all Certificates issued by a CA. Further restrictions MAY be specified within Section 7.1.2, but these restrictions SHALL NOT supersede these requirements.

7.1.4.1. Name Encoding

The following requirements apply to all Certificates listed in Section 7.1.2.

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

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

When encoding a Name, Microsoft PKI Services SHALL ensure that:

- Each Name MUST contain an RDNSequence.
- Each RelativeDistinguishedName MUST contain exactly one AttributeTypeAndValue.
- Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2.
    - For example, a RelativeDistinguishedName that contains a countryName AttributeTypeAndValue pair MUST be encoded within the RDNSequence before a RelativeDistinguishedName that contains a stateOrProvinceName AttributeTypeAndValue.
- Each Name MUST NOT contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in the BRs.

7.1.4.2 Subject Attribute Encoding

This document defines requirements for the content and validation of a number of attributes that MAY appear within the subject field of a tbsCertificate. Microsoft PKI Services SHALL NOT include these attributes unless their content has been validated as specified by, and only if permitted by, the relevant certificate profile specified within Section 7.1.2.

If Microsoft PKI Services includes attributes in the Certificate subject field that are listed in the table below they SHALL encode those attributes in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

Encoding and Order Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max. Length (Bytes)
domainComponent	0.9.2342.19200300.100.1.25	RFC 4519	MUST use IA5String	63
countryName	2.5.4.6	RFC 5280	MUST use PrintableString	2
stateOrProvinceName	2.5.4.8	RFC 5280	MUST use UTF8String or PrintableString	128
localityName	2.5.4.7	RFC 5280	MUST use UTF8String or PrintableString	128
postalCode	2.5.4.17	X.520	MUST use UTF8String or PrintableString	40
streetAddress	2.5.4.9	X.520	MUST use UTF8String or PrintableString	128
organizationName	2.5.4.10	RFC 5280	MUST use UTF8String or PrintableString	64
surname	2.5.4.4	RFC 5280	MUST use UTF8String or PrintableString	64*
givenName	2.5.4.42	RFC5280	MUST use UTF8String or PrintableString	64*
organizationalUnitName	2.5.4.11	RFC 5280	MUST use UTF8String or PrintableString	64
commonName	2.5.4.3	RFC 5280	MUST use UTF8String or PrintableString	64

* **Note:** Although RFC 5280 specifies the upper bound as 32,768 characters, this was a transcription error from X.520 (08/2005). The effective (interoperable) upper bound is 64 characters.

7.1.4.3. Subscriber Certificate Common Name Attribute

If present, this attribute MUST contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.2.7.12). The value of the field MUST be encoded as follows:

- If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value MUST be encoded as a character-for-character copy of the dNSName entry value

from the subjectAltNameextension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name MUST be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.

7.1.4.4 Other Subject Attributes

When explicitly stated as permitted by the relevant certificate profile specified within Section 7.1.2, Microsoft PKI Services MAY include additional attributes within the AttributeTypeAndValue beyond those specified in Section 7.1.4.2.

Before including such an attribute, Microsoft PKI Services SHALL:

- Document the attributes within Section 7.1.4 of our CP or CPS, along with the applicable validation practices.
- Ensure that the contents contain information that has been verified by the CA, independent of the Applicant.

7.1.6 Certificate Policy Object Identifier

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

7.1.6.1 Reserved Certificate Policy Object Identifiers

The following Certificate Policy identifiers are reserved for use by Microsoft PKI Services as an optional means of asserting that a Certificate complies with the BRs.
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)} (2.23.140.1.1)

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

Microsoft PKI Services asserts compliance with the Baseline Requirements, all CRLs that it issues MUST comply with the following CRL profile, which incorporates, and is derived from

RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 SHALL apply, in addition to the normative requirements imposed by this document. Microsoft PKI Services HAS examined RFC 5280, Appendix B for further issues to be aware of.

A full and complete CRL is a CRL whose scope includes all Certificates issued by the CA.

A partitioned CRL (sometimes referred to as a "sharded CRL") is a CRL with a constrained scope, such as all Certificates issued by the CA during a certain period of time ("temporal sharding"). Aside from the presence of the Issuing Distribution Point extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile.

Minimally, Microsoft PKI Services MUST issue either a "full and complete" CRL or a set of "partitioned" CRLs which cover the complete set of Certificates issued by the CA. In other words, if issuing only partitioned CRLs, the combined scope of those CRLs MUST be equivalent to that of a full and complete CRL.

Microsoft PKI Services MUST NOT issue indirect CRLs (i.e., the issuer of the CRL is not the issuer of all Certificates that are included in the scope of the CRL).

CRL Fields

Field	Presence	Description
tbsCertList		
version	PRESENT	MUST be v2(1), see Section 7.2.1
signature	PRESENT	See Section 7.1.3.2
issuer	PRESENT	MUST be byte-for-byte identical to the subject field of the Issuing CA.
thisUpdate	PRESENT	Indicates the issue date of the CRL.
nextUpdate	PRESENT	Indicates the date by which the next CRL will be issued. For CRLs covering Subscriber Certificates, at most 10 days after the thisUpdate. For other CRLs, at most 12 months after the thisUpdate.
revokedCertificates	*	MUST be present if the CA has issued a Certificate that has been revoked and the corresponding entry has yet to appear on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. Microsoft PKI Services removes

		an entry for a corresponding Certificate after it has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. See the "revokedCertificates Component" table for additional requirements.
extensions	PRESENT	See the "CRL Extensions" table for additional requirements.
signatureAlgorithm	PRESENT	Encoded value MUST be byte-for-byte identical to the tbsCertList.signature.
signature	PRESENT	-
Any other value	MAY BE PRESENT	-

7.2.1 Version Number(s)

Certificate Revocation Lists MUST be of type X.509 v2.

7.2.2 CRL and CRL Entry Extensions

CRL Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	PRESENT	N	See Section 7.1.2.11.1
CRLNumber	PRESENT	N	MUST contain an INTEGER greater than or equal to zero (o) and less than 2^{159}, and convey a strictly increasing sequence.
IssuingDistributionPoint	*	Y	See Section 7.2.2.1 CRL Issuing Distribution Point
Any other extension	MAY BE PRESENT	-	-

revokedCertificates Component

Component	Presence	Description
serialNumber	PRESENT	MUST be byte-for-byte identical to the serialNumber contained in the revoked Certificate.
revocationDate	PRESENT	Normally, the date and time revocation occurred. See the footnote following this table for circumstances where backdating is permitted.
crlEntryExtension	*	See the "crlEntryExtension Component" table for additional requirements.

crlEntryExtensions Component

CRL Entry Extension	Presence	Description
reasonCode	*	When present (OID 2.5.29.21), MUST NOT be marked critical and MUST indicate the most appropriate reason for revocation of the Certificate. MUST be present unless the CRL entry is for a Certificate not technically capable of causing issuance and either 1) the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023 or 2) the reason for revocation (i.e., reasonCode) is unspecified (0). See the "CRLReasons" table for additional requirements.
Any other value	MAY BE PRESENT	-

CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
unspecified	0	Represented by the omission of a reasonCode. MUST be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL

		entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023.
keyCompormise	1	Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
affiliationChanged	3	Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
superseded	4	Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the Baseline Requirements or the CA's CP or CPS.
cessationofOperation	5	Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.
certificateHold	6	MUST NOT be included if the CRL entry is for 1) a Certificate subject to the BRs, or 2) a Certificate not subject to the BRs and was either A) issued on-or-after 2020-09-30 or B) has a notBefore on-or-after 2020-09-30.
privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The Subscriber Agreement, or an online resource referenced therein, MUST inform Subscribers about the revocation reason options listed above and provide explanation about when to choose

each option. Tools that the CA provides to the Subscriber MUST allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

When Microsoft PKI Services obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, Microsoft PKI Services SHALL NOT update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension.

7.2.2.1 CRL Issuing Distribution Point

Partitioned CRLs MUST contain an Issuing Distribution Point extension. The distributionPointfield of the Issuing Distribution Point extension MUST be present. Additionally, the fullName field of the DistributionPointName value MUST be present, and its value MUST conform to the following requirements:

1. If a Certificate within the scope of the CRL contains a CRL Distribution Points extension, then at least one of the uniformResourceIdentifiers in the CRL Distribution Points's fullName field MUST be included in the fullName field of the CRL's Issuing Distribution Point extension. The encoding of the uniformResourceIdentifier value in the Issuing Distribution Point extension SHALL be byte-for-byte identical to the encoding used in the Certificate's CRL Distribution Points extension.
2. Other GeneralNames of type uniformResourceIdentifier MAY be included.
3. Non-uniformResourceIdentifier GeneralName types MUST NOT be included.

The indirectCRL and onlyContainsAttributeCerts fields MUST be set to FALSE (i.e.,not asserted).

Microsoft PKI Services MAY set either of the onlyContainsUserCerts and onlyContainsCACerts fields to TRUE, depending on the scope of the CRL.

Microsoft PKI Services MUST NOT assert both of the onlyContainsUserCerts and onlyContainsCACerts fields.

The onlySomeReasons field SHOULD NOT be included; if included, then Microsoft PKI Services MUST provide another CRL whose scope encompasses all revocations regardless of reason code.

This extension is NOT RECOMMENDED for full and complete CRLs.

7.3 OCSP PROFILE

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross-Certified Subordinate CA Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus MUST be present.

The CRLReason indicated MUST contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version Number(s)

No Stipulation

7.3.2 OCSP Extensions

The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Microsoft PKI Services SHALL always:

1. Comply with the requirements in this CPS;
2. Comply with the audit requirements set forth in Section 8 of the BRs; and
3. Be licensed as a CA in each jurisdiction of operation, where required, for the issuance of Certificates.

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with Section 7.1.2.3, Section 7.1.2.4, or Section 7.1.2.5, as well as audited in line with Section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section.

A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods.

An audit period MUST NOT exceed one year in duration.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4.

The point-in-time readiness assessment SHALL be completed no earlier than twelve (12)

months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Microsoft PKI Services' audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

Microsoft PKI Services SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust:
    a. "Principles and Criteria for Certification Authorities" Version 2.2 or newer; and either
    b. "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security" Version 2.7 or newer; or
    c. "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline" Version 2.8 or newer and "WebTrust Principles and Criteria for Certification Authorities – Network Security" Version 1.0 or newer
2. ETSI:

a. ETSI EN 319 411-1 v1.4.1 or newer, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied)

Whichever scheme is chosen, it MUST incorporate periodic monitoring or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

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

For Delegated Third Parties that are not Enterprise RAs, then Microsoft PKI Services SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.4, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then Microsoft PKI Services SHALL not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6 COMMUNICATION OF RESULTS

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1.

Microsoft PKI Services SHALL make the Audit Report publicly available on its repository (https://www.microsoft.com/pkiops/docs/repository.htm).

Microsoft PKI Services MUST make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, Microsoft PKI Services SHALL provide an explanatory letter signed by the Qualified Auditor.

The Audit Report MUST contain at least the following clearly labelled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certified Subordinate CA Certificates, that were in-scope of the audit;

4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date; and
10. (for audits conducted in accordance with any of the ETSI standards) a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part 1 (General Requirements), or Part 2 Requirements for Trust Service Providers).
11. (for audits conducted in accordance with any of the ETSI standards) a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as the BRs, and the version used.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and Microsoft PKI Services SHALL ensure it is publicly available.

The Audit Report MUST be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7 SELF-AUDITS

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

Microsoft PKI Services SHALL use a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous Linting performed during issuance.

Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4, Microsoft PKI Services SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected

sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. Microsoft PKI Services CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with the BRs and the relevant Certificate Policy or Certification Practice Statement.

Microsoft PKI Services SHALL internally audit each Delegated Third Party's compliance with the BRs on an annual basis.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA SHALL monitor adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practice Statement.

On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA SHALL ensure all applicable CP are met.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

Not Applicable

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

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

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

Sensitive Microsoft PKI Services information SHALL remain confidential to Microsoft PKI Services. The following information is considered confidential to Microsoft PKI Services and MAY NOT be disclosed:

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

9.3.2 Information Not Within the Scope of Confidential Information

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

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

This Section 9.3.2 is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Microsoft follows the governing principles established by the Microsoft privacy statement located at 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 SHALL NOT be used without the consent of the party to whom that information applies. This Section 9.4.5 is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 INTELLECTUAL PROPERTY RIGHTS

The following are the property of Microsoft:

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

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

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

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

1. The Subscriber that is a party to the Subscriber Agreement for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contractual relationship for inclusion of its Root Certificate in software distributed by such Application Software Suppliers; and
3. All Relying Parties who reasonably rely on a Valid Certificate. Microsoft PKI Services represents and warrants to the Certificate Beneficiaries, during the period when the Certificate is valid, the CA has complied, in all material aspects and to the best of its knowledge, with the CA/B Forum BRs and the CP or CPS in issuing and managing the Certificate.

The certificate warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address:** That, at the time of issuance, Microsoft PKI Services
    a. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
2. **Authorization for Certificate:** That, at the time of issuance, Microsoft PKI Services
    a. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
3. **Accuracy of Information:** That, at the time of issuance, Microsoft PKI Services
    a. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate;
    b. followed the procedure when issuing the Certificate; and
    c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
4. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, Microsoft PKI Services

   a. implemented a procedure to verify the identity of the Applicant in accordance with the CP/CPS Section 3.2 and CP/CPS Section 7.1.4.2.2;
   b. followed the procedure when issuing the Certificate; and
   c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
5. **Subscriber Agreement:** That, if Microsoft PKI Services and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Subscriber Agreement/Terms of Use;
6. **Status:** That Microsoft PKI Services maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
7. **Revocation:** That the CA SHALL revoke the Certificate for any of the reasons specified in the BRs or this CP or accompanying CPS, but only to the extent the CA gains actual, undisputed knowledge that one of these reasons has arisen.

The foregoing representations and warranties regarding procedures relate solely to facts surrounding the establishment and documentation of the procedures and that Microsoft PKI Services followed them. They expressly do not relate to, and Microsoft PKI Services expressly disclaim any representations and warranties regarding, the outcome or results of having followed such procedures.

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

9.6.2 RA Representations and Warranties

No Stipulation

9.6.3 Subscriber Representations and Warranties

Microsoft PKI Services SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

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

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

Microsoft PKI Services SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request.

Microsoft PKI Services MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

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

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;

2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;

5. Reporting and Revocation: An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying Party Representations and Warranties
No Stipulation

9.6.5 Representations and Warranties of Other Participants
No Stipulation

9.7 DISCLAIMERS OF WARRANTIES

Except for express warranties stated in this CPS, Microsoft PKI Services disclaims all other warranties, promises and other obligations (express, implied, statutory, or otherwise). In addition and without limiting the foregoing, Microsoft PKI Services is not liable for any loss:

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

9.8 LIMITATIONS OF LIABILITY

For delegated tasks, Microsoft PKI Services and any Delegated Third-Party MAY allocate liability between themselves contractually as they determine, but Microsoft PKI Services SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

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

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY 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 CONTENT OF ANY CERTIFICATE (INCLUDING ANY ALLEGEDLY ERRONEOUS CONTENT) OR YOUR RELIANCE ON SUCH CONTENT; (C) THE PROCESS OF ISSUING, REPORTING THE STATUS OF, OR REVOKING ANY CERTIFICATE (INCLUDING ANY ALLEGEDLY FLAWED PROCESS) OR YOUR RELIANCE ON SUCH PROCESS; (D) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (E) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO MICROSOFT'S CERTIFICATE SERVICES; OR (F) 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 LIMITED TO DIRECT DAMAGES INCURRED IN REASONABLE RELIANCE IN AN AMOUNT NOT EXCEEDING 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 (UNLESS THE FOREGOING AMOUNT IS ZERO, IN WHICH CASE SUCH DIRECT DAMAGES LIMIT WILL BE DEEMED TO BE FIVE U.S. DOLLARS).

9.9 INDEMNITIES

9.9.1 Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, Microsoft PKI Services understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, Microsoft PKI Services SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by Microsoft PKI Services, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by Microsoft PKI Services where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has

expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from Microsoft CA Services online, and the application software either failed to check such status or ignored an indication of revoked status).

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 will defend these indemnified parties against, any and all third party claims, including by Relying Parties, to the extent arising from or related to: (a) Subscriber's failure to perform any of Subscriber's 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 any Certificate, and will defend these indemnified parties against, any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by Microsoft or its affiliates and used by the Relying Party, the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a certificate or any constituent elements of it; or (iii) failure to check the certificate's status prior to use.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS becomes effective upon publication in the Repository.

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

No Stipulation

9.12.3 Circumstances under which OID must be changed

No Stipulation

9.13 DISPUTE RESOLUTION PROVISIONS

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

9.14 GOVERNING LAW

The laws of 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 SHALL NOT provide notice of assignment. This CPS SHALL be binding on all successors of the parties.

9.16.3 Severability

In the event of a conflict between the CA/B Forum BRs and a law, regulation, or government order (hereinafter 'Law') of any jurisdiction in which Microsoft PKI Services operates or issues certificates, Microsoft PKI Services MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law.

In such an event, Microsoft PKI Services SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of Microsoft PKI Services' CPS or CP a detailed reference to the Law requiring a modification of the CA/B Forum BRs under BRs Section 9.16.3, and the specific modification to the CA/B Forum BRs implemented by Microsoft PKI Services.

Microsoft PKI Services MUST also (prior to issuing a certificate under the modified requirement) notify the CA/B Forum of the relevant information newly added to its CPS or CP by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/B Forum MAY consider possible revisions to these Requirements accordingly.

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

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 SHALL 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: Document History

Change Control Log

New Revision	Revision Date (YYYY/MM/DD)	Revision Explanation
3.3.0	2025/04/21	Title – Added Public TLS to clearly distinguish this CPS from the others 1.1 - Removed retired Root CAs 1.6.1 - Multiple changes to definitions to conform to CA/B Forum documentation. 1.6.3 - Updated the reference links to current standards. 3.2.2 - Replaced entire section to align with SC-070. 3.2.2.4 - Changes to replace validation method 3.2.2.4.4 with 3.2.2.4.7 language. 4.3.1 – Add subsections to include Linting details to align with SC-075. 4.9.7 – Changes to CRL issuance frequency language to closer align to current Baseline Requirements 4.9.9 and 4.9.10 – Changes to revocation details to align with SC-076. 5.4.1 and 5.4.1.1 – Router and firewall log details to align with SC-069. 6.1.1.3 – Updated language to align with SC-073. 7.1 and subsections – Many changes to this section as much of the information was moved to Appendix B and remaining text was streamlined. 8.4 – Updated audit schemes to align with SC-077. 8.7 – Stated that Linting will also occur after issuance against the sample to align with SC-075. Appendix B - Moved Certificate details to this new appendix section. Entire document - There were multiple formatting and cosmetic changes throughout document that did not materially change the content such as extra spaces or different variations of the CA (i.e. Microsoft PKI Services). This included multiple changes to words to align closer to RFC 2119 including capitalization of words.

3.2.4	2024/07/03	Minor updates to revisions and dates, Updates to existing and Added Definitions, Clarified Trusted Role requirements, updated Section 7 to reflect explicit statements of Certificate, CRL and OCSP profiles.
3.2.3	2023/07/26	Minor updates to revisions and dates, Updates and Added Definitions, Clarified Repository is available 24x7, Clarified Use of Random Value for Domain Validation, Updated use of RFC 8659, Updated identification and authorization requirements, Clarified need for a direct command from a Root CA, Updated revocation instructions and revocation timelines, Clarify validity intervals for OCSP responses, Update security program requirements, Update key pair generation and audit reporting requirements, Clarify RSA and ECC quality checks, clarify certificate validity dates, Update audit qualifications, Update Certificate warranties, Clarify severability requirements.
3.2.2	2023/02/22	Update Change Log, Minor updates to revision and dates, Updated link to privacy statement, removed remaining EV language, updates contact information for revocation, clarification on Trademarks, updated Revocation Reason Codes, clarified certificate Subject Information, clarified Domain Validation methods, clarified Domain Name information, updates to align with RFC3647.
3.2.1	2022/01/07	Minor updates and added CA's
3.2.0	2021/07/12	Minor updates
3.1.9	2021/03/30	Minor updates and added CA's
3.1.8	2021/02/15	Minor clarifying updates
3.1.7	2020/11/05	Minor clarifying updates
3.1.6	2020/08/25	Added a process for Domain Validation
3.1.5	2020/07/28	Minor clarifying updates
3.1.4	2020/04/06	Minor clarifying updates
3.1.3	2019/08/05	Minor clarifying updates
3.1.2	2018/10/12	Minor clarifying updates
3.1.1	2018/07/10	Minor clarifying updates
3.1	2018/06/12	Minor updates to factor section revisions in CA/B Forum's Baseline Requirements v1.5.7.

3.0	2018/02/28	Major update/rewrite to factor changes in CA/B Forum's Baseline Requirements and EV Guidelines.
2.1	2014/04/30	Updated to incorporate findings from FY13 WebTrust Audit and internal review.
2.0	2013/04/02	Updated to support the practice of online CA operations
1.1	2013/01/02	Updated to support PKI Steering Committee, Microsoft Legal and Audit partner recommendations
1.0	2010/01/27	Established

APPENDIX B: Certificate Profiles

This section defines profile details within each certificate type issued by Microsoft PKI Services. Any fields or extensions not listed below SHALL be defined according to RFC 5280.

Root CA Certificate (Related to Section 7.1.2.1)

Field	Content
version	v3
serialNumber	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	Byte-for-byte identical to the encoded subject
validity:not after	See Section 6.3.2
subject	Contains countryName, organizationName and commonName. commonName attribute identifies the publisher and SHOULD be unique.
subjectPublicKeyInfo	See Section 7.1.3.1
extension:basicConstraints	marked critical, cA is TRUE, pathLenConstraint is NOT CONSTRAINED
extension:keyUsage	marked critical, keyCertSign and cRLSign are set, digitalSignature MAY be set, other bits are NOT set
extension:subjectKeyIdentifier	Defined within RFC 5280 Section 4.2.1.2. Unique within the scope of all Certificates issued by the CA. 160-bit SHA-1 hash of subjectPublicKey [RFC 5280]
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.

TLS Subordinate CA Certificate (Related to Section 7.1.2.6)

Field	Content
version	v3
serialNumber	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
validity:not before	Not earlier than one day before the time of signing; not later than the time of signing.
validity:not after	Not earlier than the time of signing.
subject	Contains countryName, organizationName and commonName.
extension:authorityKeyIdentifier	Not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present.
extension:basicConstraints	Marked critical, cA is TRUE, pathLenConstraint field MAY be present.
extension:certificatePolicies	Not marked critical, contains at least one reserved policyIdentifier.
extension:cRLDistributionPoints	Not marked critical, contains HTTP URL of CRL service.
extension:keyUsage	Marked critical, keyCertsign, and cRLSign bits are set, digitalSignature MAY be set, all other bits are not set.
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey [RFC 5280].
extension:extkeyUsage	Not marked critical and contains id-kp-serverAuth; MAY include id-kp-clientAuth; SHALL NOT include other values [RFC 5280].
extension:authorityInfoAccess	Not marked critical; if present, it MAY contain the HTTP URL of an Issuing CA's certificate and MAY contain the HTTP URL of Issuing CA's OCSP responder.

Organization Validated TLS Subscriber Certificate (Related to Section 7.1.2.7)

Field	**Content**
version	v3
serialNumber	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
validity:not after	See Section 6.3.2.
subject	Contains organizationName, localityName, stateOrProvinceName, countryName. MAY contain commonName, If the subject contains a commonName attribute, the value MUST be one of the values in the subjectAlternativeName extension.
extension:authorityInformationAccess	Not marked critical, contains the HTTP URL of an Issuing CA's certificate and MAY contain the HTTP URL of Issuing CA's OCSP responder.
extension:authorityKeyIdentifier	Not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present.
extension:basicConstraints	Marked critical and cA is FALSE.
extension:certificatePolicies	Not marked critical, contains at least one reserved policyIdentifier.
policyQualifiers:policyQualifierId	Optional. If present, not marked critical and id-qt 1 [RFC 5280]. Must include at least the Reserved Certificate Policy Identifier of 2.23.140.1.2.2, see section 7.1.6.1.
extension:cRLDistributionPoints	Not marked critical, contains HTTP URL of CRL service.
extension:subjectAltName	Not marked critical, contains at least one name and all names are of type dNSName

extension:keyUsage	Marked critical, digitalSignature bit MUST be set, keyEncipherment MAY be set, other bits are NOT set.
extension:subjectKeyIdentifier	Not marked critical and contains 160-bit SHA-1 hash of subjectPublicKey [RFC 5280].
extension:extkeyUsage	Not marked critical, includes id-kp-serverAuth and MAY include id-kp-clientAuth [RFC 5280].
extension:signedCertificateTimestampList	Optional. If present, NOT marked critical, only in final certificates, contains one or more Signed Certificate Timestamps (SCTs) per RFC 6962.
extension:Microsoft Application Policies	Optional. If present, NOT marked critical.
extension:Microsoft Certificate Template	Optional. If present, NOT marked critical.
extension:ctPoison	Optional. if present, marked critical, indicates that this is a precertificate which contains the OID: 1.3.6.1.4.1.11129.2.4.3. The extension SHALL be used to get SCTs for the final certificate per RFC 6962. Contains an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

OCSP Responder Certificate (Related to Section 7.1.2.8)

Field	**Content**
version	v3
serialNumber	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	Is byte-for-byte identical to the subject field of the Issuing CA.
validity	See Section 6.3.2
subject	Contains countryName, organizationName and commonName. commonName attribute identifies the publisher and SHOULD be unique. May contain localityName and stateOrProvinceName.
subjectPublicKeyInfo	See Section 7.1.3.1
extension:authorityKeyIdentifier	Not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:basicConstraints	Marked critical, Subject Type is End Entity and Path Length Constraint is None
extension:applicationPolicies	Not marked critical and Policy identifier is OCSP Signing
extension:extKeyUsage	Not marked critical and contains id-kp-OCSPSigning; SHALL NOT include other values [RFC 5280]
extension:id-pkix-ocsp-nocheck	Contains an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.

extension:subjectKeyIdentifier	Not marked critical and contains 160-bit SHA-1 hash of subjectPublicKey [RFC 5280].
extension:keyUsage	Marked critical and digitalSignature set, all other bits are not set
signatureAlgorithm	Encoded value is byte-for-byte identical to the tbsCertificate.signature.