Microsoft

Microsoft PKI Services

Certificate Policy (CP)

Version 3.1.2
August 5, 2019

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

This document is the Certification Policy (CP) that defines the procedure 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 CP 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 this CP.

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

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

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is formally named the "Microsoft PKI Services Certificate Policy" (referred to as "CP"). Microsoft CAs issue certificates in accordance with the policy and practice requirements of this document. The Object Identifier (OID) for this CP is: 1.3.6.1.4.1.311.76.509.1.2

1.2.1 Revisions

Change Control Log

Revision Date	Revision Reason	Revision Explanation	New Rev	Supersedes
1/27/2010	New	Established	1.0	N/A
1/2/2013	Updated	Updated to support PKI Steering committee, Microsoft legal and Audit partner recommendations	1.1	1.0
4/2/2013	Updated	Updated to support the practice of "Online" CA Operations.	2.0	1.1
4/30/2014	Revised	Updated to incorporate findings from FY13 WebTrust Audit and internal review.	2.1	2.0
2/28/2018	Revised	Major update/rewrite to factor changes in CAB Forum's Baseline Requirements and EV Guidelines.	3.0	2.1
6/12/2018	Revised	Minor updates to factor section revisions in CAB Forum's Baseline Requirements v1.5.7.	3.1	3.0
7/10/2018	Revised	Minor clarifying updates	3.1.1	3.1
8/5/2019	Revised	Minor clarifying updates	3.1.2	3.1.1

1.2.2 Relevant Dates

Refer to the current version of the CAB Forum's Baseline Requirements document for relevant dates of industry practice or policy changes.

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

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

The CA hierarchy structure and specific practices SHALL be specified within the relevant Certification Practice Statement (CPS).

1.3.2 Registration Authorities

A Registration Authority (RA) is 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.

1.3.3 Subscribers

A Subscriber is an individual or end-entity (person, device, or applications) that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate.

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 groups that have participated in the development of this Certificate Policy and respective Certification Practice Statement (CPS).

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Certificates issued under this Certificate Policy SHALL only be used for the purposes identified by the Issuing CA in its Certification Practice Statement and for the purposes designated in the key usage and/or extended key usage fields found in the certificate.

All end-entity certificates issued within this CA hierarchy are technically constrained for use. This is done either by the inclusion of at least one extended key usage extension in the end-entity certificate, or by inclusion of one or more extended key usage extensions in the issuing CA's certificate.

The following certificate class options and assurance levels are available to Applicants in the form of CA and end-entity Certificates issued by the Microsoft PKI CAs. The Issuing CA will assess the risk and apply the appropriate rating.

Assurance Level	Description and Assurance Level
Low Assurance	Certificates of this class provide a low level of assurance to publicly available products and services.

Assurance Level	Description and Assurance Level
Medium Assurance	This level is relevant where risks and consequences of compromise are significant. Medium assurance CAs include but are not limited to intermediate production CAs (i.e. non-root CAs). CAs operating under this policy are hosted and managed by Microsoft PKI Services and employ pre-defined and approved fulfillment practices to provision CA and end-entity production certificates to Applicants.
High Assurance	This level is relevant where risks and consequences of compromise are high. High assurance CAs include but are not limited to root and intermediate CAs. CAs operating under this policy are hosted and managed by Microsoft PKI Services and employ pre-defined and approved fulfillment practices to provision CA production certificates to Applicants.

1.4.2 Prohibited Certificate Uses

Use of certificates in violation of Section 1.4.1 is unauthorized and prohibited.

Certificates must only be used to the extent permitted with applicable laws. CA Certificates MAY not be used for any functions except CA functions. In addition, end-user Subscriber Certificates SHALL not be used as CA Certificates.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

Contact information is listed below:

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

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

1.5.3 Person Determining CPS Suitability for the Policy

The Microsoft PKI Policy Authority determines the suitability and applicability of the CPS to this CP.

1.5.4 CPS Approval Procedures

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

1.6 DEFINITIONS AND ACRONYMS

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

1.6.1 Definitions

- **Affiliate –** A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
- **Applicant** – a natural person or Legal Entity that applies for (or seeks renewal of) a Certificate by a CA.
- **Application Software Supplier** – A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
- **Baseline Requirements (BR)** – An integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements issued by the CA/Browser Forum and available at cabforum.org.
- **CA/Browser Forum (CAB Forum)** – A consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of digital certificates. Details are available at: cabforum.org.
- **Certificate** – digital record that contains information such as the Subscriber's distinguished name and Public Key, and the signer's signature and data.
- **Certificate Application –** a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.

- **Certificate Request** – an application for a new Certificate or a renewal of a Certificate.
- **Certificate Revocation List (CRL)** – periodically published listing of all certificates that have been revoked for use by Relying Parties
- **Certificate Signing Request (CSR)** – a message sent to the certification authority containing the information required to issue a digital certificate
- **Certification Authority (CA)** – an entity or organization that is responsible for the authorization, issuance, revocation, and management of a certificate. The term equally applies to Roots CAs and Subordinate CAs.
- **Certificate Owner** – Parties designated by business process owners to be associated with and/or have responsibility for specified issued certificates.
- **Certificate Policy (CP)** – A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- **Certification Practice Statement (CPS) –** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- **Distinguished Name (DN)** – a globally unique identifier representing a Subject that is used on Certificates and in the Repository
- **EV Certificate –** a certificate that contains subject information specified and validated in accordance with the EV Guidelines.
- **EV Certificate Beneficiaries –** Persons to whom the CA and its Root CA make specified EV Certificate Warranties.
- **EV Guidelines –** Guidelines for the Issuance and Management of Extended Validation Certificates, as defined by the CA/Browser Forum.
- **Extended Key Usage –** an extension in an X.509 certificate to indicate the allowed purpose(s) for the use of the Public Key. Also referenced or known as "Enhanced Key Usage".
- **Issuing CA** – the first digital certificate issuing authority who issues certificates signed by the root certificate authority (CA).
- **Legal Entity** – An association, corporation, partnership, proprietorship, trust, or government entity that has legal standing in a country's legal system.
- **Microsoft PKI Policy Authority –** combination of Microsoft's Steering and Oversight Committees.
- **Online CA (OCA)** – a certification authority system which signs end-entity Subscriber Certificates that are operated and maintained in an online state so as to provide continually available certificate signing services. Online CAs reside in segmented, secured, and functionally dedicated networks.

- **Private Key –** The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- **Public Key –** The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- **Public Key Infrastructure (PKI) –** A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
- **Registration Authority (RA)** – any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate Application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- **Registration Identifier** – the unique code assigned to an Applicant by the Incorporating or Registration Agency in such entity's Jurisdiction of Incorporation or Registration.
- **Relying Party** – a Relying Party is an individual or entity that acts in reliance on a Certificate or digital signature associated with a Certificate.
- **Relying Party Agreement** – an agreement which specifies the stipulations under which a person or organization acts as a Relying Party.
- **Repository** – an online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- **Root CA** – The top-level CA whose root certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- **Signing Service** – an organization that signs an Object on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.
- **Subscriber** – an individual or end-entity (person, device, or application) that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate.
- **Subscriber Agreement –** an agreement containing the terms and conditions that the authorized Subscriber consented to for the use of their issued certificate, containing the Private Key and corresponding Public Key.
- **Suspect Code** – code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or

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

- **Takeover Attack** – an attack where a Signing Service or Private Key associated with the Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.
- **Technically Constrained Subordinate CA Certificate** – a Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate MAY issue Subscriber or additional Subordinate CA Certificates**.**
- **TimeStamp Authority –** a service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via secure hashing algorithm) existed at the specific time.
- **Transport Layer Security (TLS)/Secure Socket Layer (SSL) –** a **s**ecurity protocol that is widely used in the Internet, for the purpose of authentication and establishing secure sessions.
- **Trusted Role –** an employee or contractor of a CA or Delegated Third Party who has authorized access to or control over a Secure Zone or High Security Zone.

1.6.2 Acronyms

Term	Definition
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module

IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTL	Time to Live

1.6.3 References

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

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

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

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

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

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

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

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

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

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

1.6.4 Conventions

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

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

2.2 PUBLICATION OF INFORMATION

A web-based repository, referenced in Section 2.1, provides Relying Parties access to this CP. The repository SHALL contain the current version of this CP, CPS, a fingerprint of the established Root CAs, current CRLs, and other information relevant to Subscribers and Relying Parties.

Effective as of 8 September 2017, section 4.2 of a CA’s Certificate Policy and/or Certification Practice Statement SHALL state whether the CA reviews CAA Records, and if so, the CA’s policy or practice on processing CAA Records for Fully Qualified Domain Names. It shall clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or “issuewild” records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.

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 them with the CAB Forum’s Baseline Requirements and EV Guidelines for any modifications.

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

New versions of this CP and respective CPS documents will become effective immediately

for all participants listed in Section 1.3. The CA offers CRLs showing the revocation of Microsoft PKI Services Certificates and offers status checking through the online repository. CRLs will be published in accordance with Section 4.9.6 and Section 4.9.7.

2.4 ACCESS CONTROLS ON REPOSITORIES

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Type of Names

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

3.1.2 Need for Names to be Meaningful

No Stipulation

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 infringe upon the intellectual property rights of entities outside of their authority.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization and Domain Identity

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

3.2.2.1 Identity

No Stipulation

3.2.2.2 DBA/Tradename

No Stipulation

3.2.2.3 Verification of Country

No Stipulation

3.2.2.4 Validation of Domain Authorization or Control

No Stipulation

3.2.2.4.1 Validating the Applicant as a Domain Contact

No Stipulation

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

No Stipulation

3.2.2.4.3 Phone Contact with Domain Contact

No Stipulation

3.2.2.4.4 Constructed Email to Domain Contact

No Stipulation

3.2.2.4.5 Domain Authorization Document

No Stipulation

3.2.2.4.6 Agreed-Upon Change to Website

No Stipulation

3.2.2.4.7 DNS Change

No Stipulation

3.2.2.4.8 IP Address

No Stipulation

3.2.2.4.9 Test Certificate

No Stipulation

3.2.2.4.10 TLS Using a Random Number

No Stipulation

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

No Stipulation

3.2.2.5 Authentication for an IP Address

No Stipulation

3.2.2.6 Wildcard Domain Validation

No Stipulation

3.2.2.7 Data Source Accuracy

No Stipulation

3.2.2.8 CAA Records

No Stipulation

3.2.3 Authentication of Individual Identity

No Stipulation

3.2.4 Non-Verified Subscriber Information

No Stipulation

3.2.5 Validation of Authority

Validation of authority (i.e. the determination of whether an Applicant or Subscriber has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate) is the responsibility of the CA or CA-appointed Registration Authority (RA).

3.2.6 Criteria for Interoperation or Certification

No Stipulation

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

Issuing 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. Routine re-key of

the issuing CA certificates SHALL be performed in accordance with the established Key Generation process in Section 6.1 of this CP.

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

3.3.2 Identification and Authentication for Re-Key After Revocation

Revoked or Expired Certificates SHALL require a new enrollment. Applicants MUST submit a new Certificate Request and be subject to the same Identification and Authentication requirements as first-time Applicants, as specified in Section 3 of this CP.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

A Certificate Revocation Request that is submitted electronically MAY be authenticated and approved, providing the request comes from the Subscriber or an approved authority.

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 this CP and respective CPS.

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, the CA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic;
2. An executed Subscriber Agreement or Terms of Use, which may be electronic; and
3. Pay fee, if applicable.

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 3.3.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

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 the CA to obtain from the Applicant in order to comply with the Baseline Requirements, CP and CPS. In cases where the Certificate Request does not contain all the necessary information about the Applicant, the CA 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 or IP address to be included in the Certificate's SubjectAltName extension.

Certificate Applications are reviewed and processed, per the Identification and Authentication requirements in Section 3.2. The CA MAY use the documents and data acquired in Section 3.2 to verify certificate information or reuse previous validations, provided that:

1. Prior to March 1, 2018, the CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 39 months prior to issuing the Certificate; and
2. On or after March 1, 2018, the CA 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.

Certificate requests that are identified as "High Risk" SHALL be subject to additional verification activities, as outlined in documented procedures, prior to approving the request.

The CA MAY delegate the performance of all or any part of a requirement of this CP to an Affiliate, a RA, or subcontractor, provided that the process employed by the CA fulfills all of the requirements of Section 11.12 and 11.13 of the EV Guidelines. Affiliates and/or RAs must comply with the qualification requirements of Sections 5.2.4, 5.3.2, and 5.3.3 in this CP.

The CA SHALL verify that the RA or subcontractor personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15 of the EV Guidelines.

4.2.2 Approval or Rejection of Certificate Applications

Submitted Certificate Applications, MUST be reviewed and approved by the issuing CA or appointed RA prior to issuance.

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;
- 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 CA reserves the right not to disclose reasons for refusal.

4.2.3 Time to Process Certificate Applications

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

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notification of Certificate Issuance

Upon issuance, Subscribers SHALL be notified via an email or another agreed upon method with information about their 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 key pair and Certificate constitutes Certificate acceptance.

4.4.2 Publication of the Certificate by the CA

Certificates SHALL be published in a database and/or a publicly accessible 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 respective 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, as long as the renewal request meets the requirements set forth in this CP, the supporting CPS, 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

Issuing 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, and the same acceptance methods, as described in Section 4.4. Routine re-key of the issuing CA certificates SHALL be performed in accordance with the established Key Generation process of Section 6.1 in this CP.

4.7.1 Circumstance for Certificate Re-Key

No stipulation

4.7.2 Who May Request Certification of a New Public Key

No stipulation

4.7.3 Processing Certificate Re-Key Requests

No stipulation

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 CERTIFICATE MODIFICATION

Modification to an issued Certificate's details is not permitted. The certificate MUST first be revoked, core Subscriber information must remain the same (domain name, DUNS/SSN, etc.), and only inconsequential information must have changed (email address, phone number, etc.), before modifications to Subscriber information are allowed. The replacement certificate (i) requires a new issuance process that doesn't require the same identity and authentication procedures as a new Applicant (as in Section 4.2.1), (ii) MAY or MAY not retain the same key pair, and (iii) SHALL have new validity dates.

4.8.1 Circumstance for Certificate Modification

No stipulation

4.8.2 Who May Request Certificate Modification

No stipulation

4.8.3 Processing Certificate Modification Requests

No stipulation

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation

4.8.6 Publication of the Modified Certificate by the CA

No stipulation

4.8.7 Notification of Certificate Issuance by the CA to other entities

No stipulation

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

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

1. Certificate revocation is requested in writing and in accordance with Section 4.9.3;
2. The CA acquires evidence that the Certificate or key pairs were compromised or misused.
3. The Subscriber can be shown to have violated obligations under the Subscriber

Agreement;

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

4.9.1.1 Reasons for Revoking a Subscriber Certificate

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

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

The issuing CA SHALL provide Revocation Request instructions that are noted in the respective CPS to parties and maintain a 24x7 availability to accept and respond to requests by steps outlined in Section 3.4. A manual process SHALL be used to approve high assurance CA requests for Certificate revocation.

Issuing CAs and/or RAs will take the appropriate actions to process the Certificate revocation, per Section 4.9.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

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

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

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

4.9.6 Revocation Checking Requirement for Relying Parties

No Stipulation.

4.9.7 CRL Issuance Frequency

No Stipulation.

4.9.8 Maximum Latency for CRLs

Issuing CAs SHALL ensure that the response time for CRL or OCSP requests do not exceed ten (10) seconds under normal operating conditions.

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

4.9.9 On-Line Revocation/Status Checking Availability

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

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

4.9.10 On-Line Revocation Checking Requirements

No Stipulation

4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation

4.9.12 Special Requirements Related to Key Compromise

See Section 4.9.1

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

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

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

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

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

4.10.3 Optional Features

No Stipulation

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

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

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

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

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

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

Physical access to cryptographic systems, hardware, and activation materials are restricted by

multiple access control mechanisms, which are logged, monitored, and video recorded on a 24x7 basis.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

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

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Trusted Roles consist of vetted and approved employees, contractors, or consultants that require access to or control over the CA's PKI operations. Trusted Role positions are subject to a clearly defined set of responsibilities that maintain a strict "separation of duties"; such that, no single person is able to perform both validation duties and certificate issuance fulfillment without a secondary review by another "trusted" team member. The personnel considered for Trusted Role positions MUST successfully pass the screening and training requirements of CPS Section 5.3.

Trusted Role positions MAY include, but are not limited to, system administrators, operators, engineers, and certain executives who are designated to oversee CA operations.

5.2.2 Number of Individuals Required per Task

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

5.2.3 Identification and Authentication for Trusted Roles

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

5.2.4 Roles Requiring Separation of Duties

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

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

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

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements and Procedures

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

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Controls

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

5.3.8 Documentation Supplied to Personnel

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

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

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

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

The CA SHALL record at least the following events:

1. CA key lifecycle management events, to include: a. Key generation, backup, storage, recovery, archival, and destruction; and b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, to include: a. Certificate requests, renewal, and re-key requests, and revocation; b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement; c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls; d. Acceptance and rejection of Certificate Requests; e. Issuance of Certificates; and f. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, to include: a. Successful and unsuccessful PKI system access attempts; b. PKI and security system actions performed; c. Security profile changes; d. System crashes, hardware failures, and other anomalies; e. Firewall and router activities; and f. CA facility ingress and egress.

Log entries MUST include the following elements:

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

5.4.2 Frequency for Processing and Archiving Audit Logs

Audit logs are reviewed on an as-needed basis.

5.4.3 Retention Period for Audit Logs

Upon effective date, Audit logs SHALL be retained for a period defined in the respective CPS and made available to the CA's Qualified Auditor upon request.

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Log Accumulation System (Internal vs. External)

No Stipulation

5.4.7 Notification to Event-Causing Subject

No Stipulation

5.4.8 Vulnerability Assessments

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

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

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

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 KEY CHANGEOVER

No Stipulation

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

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

The Business Continuity Plan aligns with the requirements of the CAB Forum's Baseline Requirements.

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

See Section 5.7.4.

5.7.3 Recovery Procedures After Key Compromise

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

5.7.4 Business Continuity Capabilities After a Disaster

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

5.8 CA OR RA TERMINATION

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

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

Additional details of the CA key generation ceremony MAY reside in the respective CPS.

6.1.1.2 RA Key Pair Generation

No Stipulation

6.1.1.3 Subscriber Key Pair Generation

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

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

No Stipulation

6.1.4 CA Public Key Delivery to Relying Parties

No Stipulation

6.1.5 Key Sizes

No Stipulation

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

6.1.7 Key Usage Purposes

Root Certificate Private Keys MUST NOT be used to sign Certificates, except in the following cases:
1. Self-signed Certificates to represent the Root CA;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and

4. Certificates for OCSP Response verification.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

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

6.2.1 Cryptographic Module Standards and Controls

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

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

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

6.2.3 Private Key Escrow

No Stipulation

6.2.4 Private Key Backup

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

6.2.5 Private Key Archival

No Stipulation

6.2.6 Private Key Transfer into or from a Cryptographic Module

No Stipulation

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.1

6.2.8 Activating Private Keys

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

6.2.9 Deactivating Private Keys

No Stipulation

6.2.10 Destroying Private Keys

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

6.2.11 Cryptographic Module Capabilities

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

No Stipulation

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

No stipulation

6.8 TIME-STAMPING

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

CA certificates SHALL be X.509 Version 3 format and conform to RFC 5280 standards: Internet X.509 Public Key Infrastructure Certificate and CRL profile.

7.1.1 Version Number(s)

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

7.1.2 Certificate Content and Extensions; Application of RFC 5280

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

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

7.1.2.1 Root CA Certificate

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

7.1.2.2. Subordinate CA Certificate

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

7.1.2.3. Subscriber Certificate

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

7.1.2.4 All Certificates

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

7.1.2.5 Application of RFC 5280

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

7.1.3 Algorithm Object Identifiers

No stipulation

7.1.4 Name Forms

Issuing CAs SHALL issue Certificates with Name Forms compliant with RFC 5280.

7.1.4.1. Issuer Information

No Stipulation

7.1.4.2. Subject Information – Subscriber Certificates

No Stipulation

7.1.4.2.1. Subject Alternative Name Extension

No Stipulation

7.1.4.2.2. Subject Distinguished Name Fields

No Stipulation

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

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

7.1.4.3.1. Subject Distinguished Name Fields

No Stipulation

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

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

7.1.6.1 Reserved Certificate Policy Object Identifiers

No Stipulation

7.1.6.2 Root CA Certificates

No Stipulation

7.1.6.3 Subordinate CA Certificates

No Stipulation

7.1.6.4 Subscriber Certificates

No Stipulation

7.1.7 Usage of Policy Constraints Extension

No Stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation

7.2 CRL PROFILE

CRL Profiles comply with X.509 V3 standards.

7.2.1 Version Number(s)

No Stipulation

7.2.2 CRL and CRL Entry Extensions

No Stipulation

7.3 OCSP PROFILE

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

7.3.1 Version Number(s)

No Stipulation

7.3.2 OCSP Extensions

No Stipulation

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

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

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

Annual audits SHALL be performed by an independent certified Auditor that assesses the CA's PKI operations in accordance with the stipulations documented in the CP and respective CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6 COMMUNICATION OF RESULTS

Audit results are provided to the PKI Policy Authority, who will distribute to the necessary parties, as required. General audit findings that do not impact the overall audit opinion are not required to be publicized.

8.7 SELF-AUDITS

No Stipulation

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No Stipulation

9.1.2 Certificate Access Fees

No Stipulation

9.1.3 Revocation or Status Information Access Fees

No Stipulation

9.1.4 Fees for Other Services

The CA does not charge a fee for accessing this CP. However, any use of the CP 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

No Stipulation

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Each CA SHALL maintain the following insurance related to their respective performance and obligations under these Guidelines:

(A) Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and

(B) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Such insurance MUST be with a company rated no less than A- as to Policy Holder’s Rating in the current edition of Best’s Insurance Guide (or with an association of companies each of the members of which are so rated).

A CA MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that it has at least five hundred million US dollars in liquid

assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

9.2.2 Other Assets

No Stipulation

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

No Stipulation

9.3.2 Information Not Within the Scope of Confidential Information

No Stipulation

9.3.3 Responsibility to Protect Confidential Information

No Stipulation

9.4 PRIVACY OF PERSONAL INFORMATION

No Stipulation

9.4.1 Privacy Plan

No Stipulation

9.4.2 Information Treated as Private

No Stipulation

9.4.3 Information Not Deemed Private

No Stipulation

9.4.4 Responsibility to Protect Private Information

No Stipulation

9.4.5 Notice and Consent to Use Private Information

No Stipulation

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No Stipulation

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 INTELLECTUAL PROPERTY RIGHTS

The following are the property of Microsoft:

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

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

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.

The CA represents and warrants to the Certificate Beneficiaries, during the period when the Certificate is valid, the CA has complied, in all material aspects, with the CAB Baseline Requirements and the CP/CPS in issuing and maintaining the Certificate.

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.

For Extended Validation certificates, the CA represents and warrants to the EV Certificate Beneficiaries, during the period when the EV Certificate is valid, the CA has complied, in all material aspects, with the EV Guidelines requirements and the CP/CPS in issuing and maintaining the EV Certificate.

9.6.2 RA Representations and Warranties

No Stipulation

9.6.3 Subscriber Representations and Warranties

The CA 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.

The CA 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. The CA 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 CP, the CA disclaims all other warranties, promises and other obligations. In addition, the CA 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 the CA, or use of Certificates beyond the prescribed use defined by this CP;
- Arising from the negligent or fraudulent use of Certificates or CRLs issued by the CA; and
- Due to disclosure of personal information contained within Certificates, CRLs or OCSP responses.

9.8 LIMITATIONS OF LIABILITY

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

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA 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/or

Certification Practice Statement. If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA 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 the CA desires. If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement.

A CA MAY NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV Certificate.

9.9 INDEMNITIES

9.9.1 Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA 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, the CA 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 the CA, 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 the CA 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 the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

No Stipulation

9.9.3 Indemnification by Relying Parties

No Stipulation

9.10 TERM AND TERMINATION

9.10.1 Term

This CP becomes effective upon publication in the Repository.

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

No Stipulation

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Microsoft accepts notices related to this CP 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 CP MAY be made by the Microsoft PKI Services and SHALL be approved by the Microsoft PKI Policy Authority, as per Section 1.5.4.

9.12.2 Notification Mechanism and Period

No Stipulation

9.12.3 Circumstances under which OID must be changed

No Stipulation

9.13 DISPUTE RESOLUTION PROVISIONS

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

9.14 GOVERNING LAW

THE LAWS OF THE STATE OF WASHINGTON STATE GOVERN THE INTERPRETATION, CONSTRUCTION, AND ENFORCEMENT OF THIS CP,

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 CP.

9.15 COMPLIANCE WITH APPLICABLE LAW

See Section 9.14

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No Stipulation

9.16.2 Assignment

No Stipulation

9.16.3 Severability

If a court or government body with jurisdiction over the activities covered by the Baseline Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Requirements accordingly.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No Stipulation

9.16.5 Force Majeure

No Stipulation

9.17 OTHER PROVISIONS

No Stipulation