Microsoft

Product Release & Security Services (PRSS) PKI

Certificate Policy (CP)

Version 2.1
April 30, 2014

Change Control Log

Revision Date	Revision Reason	Revision Explanation	New Rev	Supersedes	Revision By
1/27/2010	New	Established	1.0	N/A	PKI SME
1/2/2013	Updated	Updated to support PKI Steering committee, Microsoft legal and Audit partner recommendations	1.1	1.0	PKI SME
4/2/2013	Updated	Updated to support the practice of "Online" CA Operations.	2.0	1.1	PKI SME
4/30/2014	Revised	Updated to incorporate findings from FY13 WebTrust Audit and internal review.	2.1	2.0	PKI SME

Table of Contents

1. Introduction

The Product Release and Security Services Public Key Infrastructure (PRSS PKI) team, operated by Microsoft Corporation, has been established to provide a variety of digital certificate services to support operations of various Microsoft Product Groups. PRSS PKI functions as the Certification Authority, Registration Authority, and provides directory services to manage keys and certificates, the most common PKI service being the provision of certificates to sign software code files for Microsoft Product Groups offerings. This signing provides consumers with assurance regarding the authenticity and integrity of Microsoft software products.

The Microsoft PRSS PKI service team is responsible for:

- Securing and managing Microsoft's Product Root and it's hierarchy
- Acting as the Certificate Authority (CA) for Microsoft's Product Root and it's hierarchy
- Acting as the Registration Authority (RA) for Microsoft's Product Root and it's hierarchy
- Acting as the CA and fulfillment method for sub-roots in which external customers may be issued certificates with the Product Group acting as the RA or RA and CA.

1.1 Overview

This Certificate Policy (CP) is the principal statement of policy governing the Microsoft PRSS public key infrastructure (PKI) and sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing digital certificates within the PRSS PKI CA hierarchy.

The effective date for implementation of the practices disclosed in this policy document is the date of publication of the CP and will apply to all future CA related activities performed by PRSS PKI and all entities operating within the PRSS PKI CA hierarchy including affiliated Microsoft Product Groups, third party external CAs (hosting subordinate CAs signed by PRSS PKI Root CAs), Certificate Subscribers, and associated Relying Parties.

1.2 Document Name and Identification

This document is formally referred to as the "Microsoft Product Release and Security Services PKI Certificate Policy" (Microsoft PRSS PKI CP). PRSS PKI CAs issue certificates in accordance with the policy and practice requirements of this document. The OID for the PRSS PKI CP is: 1.3.6.1.4.1.311.76.509.1.1

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) collectively refers to all entities authorized to issue public key certificates within the PRSS PKI CA hierarchy.

Obligations of the CAs within the PRSS PKI hierarchy include:

- Generating, issuing and distributing public key certificates in accordance with this CP
- Distributing CA certificates
- Generating and publishing certificate status information (such as CRLs)
- Maintaining the security, availability, and continuity of the certificate issuance and CRL signing functions
- Providing a means for Subscribers to request revocation
- Revoking public-key certificates and distributing certificate status information in the form of Certificate Revocation Lists (CRLs)
- Ensuring that changes in certificate status are reflected in its own repositories and those of authorized certificate validation authorities within the specified time as stated in this CP.
- Periodically demonstrating internal or external audited compliance with this CP.

Within PRSS PKI, there are three general categories of CAs which are the Root CAs, the Intermediate CAs, and the Issuing CAs. The PRSS PKI CA hierarchy structure shall be specified within the Certification Practice Statement (CPS).

1.3.1.1 Root CAs

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

1.3.1.2 Intermediate CAs

These CAs are subordinate to Root CAs and are referred to as Primary Certification Authorities within the PRSS PKI CA hierarchy. Their primary function is to issue Certificates to other CAs. Intermediate CAs may or may not issue some end entity certificates.

1.3.1.3 Issuing CAs

The primary function of these CAs is to issue end-entity Subscriber certificates to internal Microsoft Product Groups or approved 3rd Party entities. Issuing CAs are further classified in the following three categories.

(i) PRSS PKI managed CAs: this category consists of CAs hosted and managed by the PRSS PKI team.

(ii) Product Group managed CAs - this category consists of CAs that are hosted and managed by affiliated Microsoft Product Groups Roots and are subordinate to Root CAs managed by the PRSS PKI team.

(iii) 3rd Party managed CAs - this category consists of CAs that are hosted and managed by 3rd Party Microsoft partners and are subordinate to Root CAs managed by PRSS PKI or CAs managed by PRSS affiliated Microsoft Product Groups.

1.3.2 Registration Authorities

Registration Authorities (RAs) evaluate and either approve or reject Subscriber certificate management transactions (including certificate requests, re-key requests, and revocation requests).

Obligations of the Registration Authorities (RAs) within the PRSS PKI hierarchy include:

- Obtaining a public-key from the Subscriber
- Identifying and authenticating Subscribers in accordance with this CP
- Verifying that the Subscriber possesses the asymmetric private key corresponding to the public key submitted for certification
- Facilitate provisioning of non-Microsoft certificates from external commercial CAs
- Facilitate provisioning of content IDs for mobile to market signing from external commercial CAs
- Receiving, authenticating and processing certificate revocation requests
- Providing suitable training to personnel performing RA functions.

The following RAs operate on behalf of the PRSS PKI CA hierarchy:

(i) PRSS PKI RA: For PRSS PKI Root CAs, Subscribers are Subordinate CAs that are under the control of PRSS PKI. Accordingly, the RA function for these CAs is performed manually by authorized PRSS PKI personnel. For the PRSS PKI managed Issuing CAs, the RA function is also performed by PRSS PKI using a combination of manual processes and defined business rules to approve or reject Subscriber certificate management transactions in accordance with the 'PKI operations guide.'

(ii) Microsoft Product Group RAs – Affiliated Product Groups may operate as an RA and authorize the issuance of certificates to Product Group Subscribers. Additionally, for CA services requested by external customers, i.e., entities that are not full time employees (FTEs) of Microsoft, the RA function is performed by the respective Product Groups engaged in operations with these entities.

Product Group RAs must abide all by all the requirements of the PRSS PKI CP and relevant CPS.

(iii) 3rd Party RAs – external partners that enter into a contractual relationship with Microsoft may operate as an RA and authorize the issuance of certificates issued from 3rd Party hosted CAs that chain to the PRSS PKI managed Root CAs. 3rd Party RAs must abide all by all the requirements of the PRSS PKI CP and relevant CPS.

1.3.3 Subscribers

A Subscriber is the end entity whose name or identifier appears as the subject in a certificate, and

who asserts that it uses its key and certificate in accordance with this CP. Subscribers typically include designated Owners from Microsoft Product Groups or external customers, whose requests for certificates are submitted by Product Groups on behalf of these customers. Subscribers within the PRSS PKI CA hierarchy may be issued certificates for assignment to devices, groups, organizational roles or applications provided that responsibility and accountability is attributable to the organization.

Obligations of Subscribers within the PRSS PKI include:

- Read and agree to the terms of this CP
- Generating or causing to be generated one or more asymmetric key pairs
- 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 in accordance with the terms of the PRSS PKI Subscriber Agreement
- Promptly reporting loss or compromise of private key(s) and inaccuracy of certificate information
- Using its key pair(s) in compliance with this CP.

1.3.4 Relying Parties

A Relying Party is the entity who relies on the validity and binding of the Subscriber with the public key associated with the certificate. Relying Parties typically include entities that may rely upon a Subscriber certificate for purposes of verifying a Subscriber's digital signature to ensure that software products have been developed by Microsoft and have not been modified since they were signed.

Obligations of Relying Parties within the PRSS PKI include:

- Confirming the validity of Subscriber public-key certificates
- Verifying that Subscriber possesses the asymmetric private key corresponding to the public-key certificate (e.g., through digital signature verification)
- Using the public-key in the Subscriber's certificate in compliance with this CP.

1.3.5 Other Participants

1.3.5.1 PRSS PKI Steering Committee

The PRSS PKI Steering Committee functions as the PRSS PKI Policy Authority (PA) and consists of representatives from at least, but not limited to, two of the following teams Microsoft Law & Corporate Affairs (LCA), Trustworthy Computing (TWC), Information Security

(InfoSec) and/or PRSS.

Obligations of the PRSS PKI Steering Committee in its role as Policy Authority (PA) include:

- Approving and maintaining this CP
- Interpreting adherence to this CP
- Reviewing/approving, as appropriate, the content of CA certificates
- Reviewing/approving, as appropriate, the overall PKI structure and future growth direction
- Approving the creation of new high assurance CAs
- Reviewing and approving any exceptions to policies and practices defined in this CP
- Resolving or causing resolution of disputes related to this CP
- Remaining current regarding security threats and ensuring that appropriate actions are taken to counteract significant threats
- Ensuring it conducts an efficient and trustworthy service in line with terms agreed with contracting parties or scheme.

1.3.5.2 PRSS PKI Oversight Committee

The PRSS PKI Oversight Committee functions as overseer of the PRSS PKI Policy Authority (PA) and consists of the Corporate Vice Presidents from at least, but not limited to, three of the following teams Internal Information Technology, Trustworthy Computing and Operations.

Obligations of the PRSS PKI Oversight Committee include, as appropriate (appropriateness will be determined by the PKI Steering Committee and any issues of sufficient risk will be sent to the Oversight Committee for final approval):

- Approving major revisions to this CP
- Interpreting adherence to this CP, as appropriate
- Reviewing/approving, as appropriate, the overall PKI structure and future growth direction
- Approving the creation of new high assurance CAs
- Resolving or causing resolution of disputes related to this CP, as appropriate

1.4 Certificate Usage

This document defines the specific communities for which a specific class or type of certificate is applicable, specific PRSS PKI practices and requirements for the issuance and management of such certificates, and the intended purposes and uses of such certificates.

This CP is applicable to all certificates issued by a CA within the PRSS PKI CA hierarchy which include certificates issued by the PRSS PKI team, Microsoft Product Groups, and/or 3rd Party external customers.

1.4.1 Appropriate Certificate Uses

All end-entity certificates issued within the PRSS PKI 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 extension in the issuing CA's certificate. The following are some of the most commonly used EKUs within the PRSS PKI:

- Server Authentication (id-kp-serverAuth) EKU OID=1.3.6.1.5.5.7.3.1
- Client Authentication (id-kp-clientAuth) EKU OID =1.3.6.1.5.5.7.3.2
- Code Signing (id-kp-codeSigning) EKU OID=1.3.6.1.5.5.7.3.3
- Time stamping (id-kp-timeStamping) EKU OID=1.3.6.1.5.5.7.3.8
- OCSP (id-kp-OCSPSigning) EKU OID=1.3.6.1.5.5.7.3.9

The following certificate class options and assurance levels are available to Subscribers in the form of CA and end-entity Certificates issued by the PRSS PKI CAs.

Certificate Class	Assurance Level	Description and Assurance Level
Low Impact	Low Assurance	This class of certificates provides a low level of assurance to publicly available products and services. The CAs support testing scenarios only.
Medium Impact Online	Medium Assurance (Online)	This level is relevant where risks and consequences of compromise are significant. Medium assurance keys are intermediate production CAs (i.e. non-root CAs). CAs operating under this policy are hosted and managed by PRSS PKI and employ pre-defined and approved fulfillment practices to provision CA and end-entity production certificates to Subscribers.
Medium Impact	Medium Assurance	This level is relevant where risks and consequences of compromise are significant. Medium assurance keys are intermediate production CAs (i.e. non-root CAs). CAs operating under this policy are hosted and managed by PRSS PKI and employ pre-defined and approved fulfillment practices to provision CA and end-entity production certificates to Subscribers.
High Impact	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. The PRSS

Certificate Class	Assurance Level	Description and Assurance Level
		PKI Team will assess the risk and apply the appropriate rating. CAs operating under this policy are hosted and managed by PRSS PKI and employ pre-defined and approved fulfillment practices to provision CA production certificates to Subscribers.

1.4.2 Prohibited Certificate Uses

Certificates are currently used for the purposes specified in §1.4.1, but new purposes may be defined as new products and services emerge. 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

This CP is administered by the PRSS PKI Service Manager at Microsoft Corporation.

1.5.2 Contact Person

Contact information is listed below:

PRSS PKI Service Manager

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052-6399

1.5.3 Person Determining CPS Suitability for the Policy

The PRSS PKI Service Manager and PRSS PKI Steering Committee, as defined in section 1.3.5, determine the suitability of a CPS for this policy.

1.5.4 CP Approval Procedures

The following procedures are used to approve this Certificate Policy:

- Microsoft PRSS Certificate Policies are prepared and reviewed by the Microsoft PRSS PKI team.
- Approval of the initial implementation and all modifications to this CP and any subsequent amendments is to be obtained from the PRSS PKI Policy Authority (Steering Committee).
    - At the time of review the Steering Committee will determine if the change is minor or major. This determination is based on an assessment of the change in the amount of risk from the changes.

- Minor modifications are enforced once the Steering Committee and if appropriate LCA review is completed.
- Minor modification versions will be incremented in tenths (i.e. replace v1.0 with v1.1).
- Major modification versions will be incremented in whole number increments (i.e. replace v1.0 with v2.0).
- Major modifications to this CP must be approved by the PRSS PKI Oversight Committee and LCA upon a recommendation from the PRSS PKI Policy Authority (Steering Committee).
- At the time of review the Steering Committee will also determine if the changes require prior notification to users of the CP.
    - If notification, is required the Steering Committee will determine how much notice is to be given (this will usually be approximately 45 calendar days).

The PRSS PKI Service Manager will be responsible for making sure that this CP is reviewed by the PRSS PKI Policy Authority (Steering Committee) at least annually, the clock starts at the time of the most recently approved change.

1.6 Definitions and Acronyms

- **PRSS** – Product Release and Security Services, part of the Operations Services organization
- **Certificate** - digital record that contains information such as the Subscriber's distinguished name and public key, and the signer's signature and data.
- **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)** – see section §1.3.1
- **Compromise** - a loss, theft, disclosure, modification, unauthorized use, or other breach of security related to a Private Key
- **Distinguished Name (DN)** – a globally unique identifier representing a Subscriber
- **Hardware Security Module (HSM)** –a specialized computer hardware system designed to securely store encryption keys
- **Management** – refers to either or all managers involved with PRSS PKI, PRSS and/or Operations Services (OS).
- **Online CA (OCA)** - A certification authority system which signs end entity Subscriber Certificates which 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.
- **Policy Authority (PA)** – the PRSS PKI Steering Committee which creates and maintains the policies related to the PRSS Public Key Infrastructure
- **Private Key** – a confidential encrypted electronic data file that interfaces with a Public Key using the same encryption algorithm, in order to verify Digital Signatures and encrypt files or messages
- **Public Key** – an encrypted electronic data file that is publicly available for interfacing with a Private Key
- **Registration Authority (RA)** – see section §1.3.2
- **Relying Party** – 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
- **Subscriber** – the individual or entity 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 which specifies the stipulations under which a person or organization acts as a Subscriber

2. Publication and Repository Responsibilities

In providing repository services, obligations of the PRSS PKI include:

- Storing and distributing public-key certificates (where relevant)
- Storing and distributing certificate status information (such as CRLs where required)
- Storing and distributing this CP and subsequent updates.
- Storing and distributing the Relying and Subscriber party agreements.

2.1 Repositories

Read and write access to the PRSS PKI repository is restricted to authorized PRSS PKI personnel through the use of appropriate logical access controls.

The PRSS PKI repository shall contain the current and historical versions of this CP, a fingerprint of the PRSS PKI Root CAs, current CRLs for the PRSS PKI CAs, and other information relevant to Subscribers and Relying Parties.

PRSS PKI also maintains a database of issued certificates and CRLs to which access is restricted to authorized PRSS PKI personnel.

2.2 Publication of Certification Information

This CP is published in the Microsoft PRSS PKI repository.

2.3 Time or Frequency of Publication

This CP is published in accordance with §1.5. CRLs are published in accordance with §4.9.6 and §4.9.7.

2.4 Access Controls on Repositories

Read access to the Microsoft Corporation Internet website repository for published CA information is available to all parties worldwide. Appropriate logical access controls are used to restrict access to authorized Microsoft personnel the ability to write to or modify repository content.

3. Identification and Authentication

3.1 Naming

3.1.1 Type of Names

Certificates are issued in accordance with the X.509 standard. All certificate holders require a Distinguished Name. The PRSS PKI Steering Committee approves naming conventions for the creation of distinguished names for certificate applicants.

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

3.1.2 Need for Names to be Meaningful

Distinguished Names shall be meaningful.

3.1.3 Anonymity or Pseudonymity of Subscribers

See § 3.1.2

3.1.4 Rules for Interpreting Various Name Forms

Name forms are interpreted in accordance with §3.1.1 and 3.1.2.

3.1.5 Uniqueness of Names

Uniqueness is achieved through stipulations in §3.1.1 and 3.1.2.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not Applicable.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Where a Microsoft Issuing CA generates key pairs, the Issuing CA must create and submit a certificate request which contains the public key to be certified and is digitally signed with the corresponding private key.

Where the Subscriber generates his/her own key pair(s), the certificate request must contain the public key to be certified and be digitally signed with the corresponding private key. In cases where a key pair is generated by the CA on behalf of a Subscriber, proof of possession of the private key is not required.

3.2.2 Authentication of Organization Identity

All Microsoft employees (full-time and part-time) may submit requests for Certificates/Keys to be issued by CAs managed and hosted by PRSS PKI. Subscriber employment with Microsoft shall be verified with the existence of a valid Microsoft issued smart-card employee badge. A smart-card employee badge is not required in the case automated/systematic request submission using non-user domain accounts, See § 3.2.3.2 Authentication of Non-user domain account. PRSS PKI shall not use any data or document to validate organization identity if the data or document was obtained more than 15 months prior to the Certificate's issuance.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Microsoft Employee

Certificate requests must be digitally signed by Subscribers for the authentication of Microsoft employment status during certificate processing. The certificate associated with the digital signature must be issued by a Microsoft IT Enterprise CA which is provided to individual Microsoft employees on their Smart Card Corporate ID Badges and is protected using an employee selected user pin code. PRSS PKI shall not use any data or document to validate a Microsoft employee's identity if the data or document was obtained more than 15 months prior to the Certificate's issuance.

3.2.3.2 Authentication of Non-user domain account

In the case of automated certificate request submission, Non-User domain accounts may be used. A documented and approved business justification along with risk acceptance is required. In addition to business justification and risk acceptance, the identity and Microsoft employment status of the owner or owners of the non-user domain account must be strongly authenticated. PRSS PKI shall not use any data or document to validate a Microsoft employee's identity if the data or document was obtained more than 15 months prior to the Certificate's issuance.

3.2.3.3 Authentication of 3rd Party Subscriber

In the case of Certificates to be issued from Product Group managed CAs to external customers, only a designated Corporate Contact may be allowed to submit service requests. The Corporate Contacts role shall be assigned by the customer account manager. Subsequent changes to this role shall be verified by Microsoft upon occurrence. PRSS PKI shall not use any data or document to validate the identity of a 3rd party subscriber if the data or document was obtained more than 15 months prior to the Certificate's issuance.

3.2.4 Non-Verified Subscriber Information

Not Applicable.

3.2.5 Validation of Authority

Subscriber authority to request certificates shall be validated by the Certificate owner and the Subscriber's Manager.

3.2.6 Criteria for Interoperation

The following criteria shall be utilized, at a minimum, to determine whether a non-PRSS PKI CA is suitable for interoperation with the PRSS PKI:

- A signed contractual agreement exists between PRSS PKI and the entity operating the non-PRSS CA.
- The entity operating the non-PRSS CA has successfully passed a compliance audit of their CA services.

- The entity operating the non-PRSS CA passes an annual compliance assessment of their CA services to maintain interoperation status.

All interoperation relationships must be reviewed and approved by the PKI Steering Committee prior to commencement. Furthermore, interoperation of the PRSS PKI with a non-PRSS PKI CA may only include cross-certification activities unless specifically allowed otherwise by the PKI Steering Committee.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Certificate re-key, defined as the process whereby a new certificate is issued that is identical to the original but has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period to replace an expiring or expired certificate, is supported by PRSS PKI. A new service request for certificate rekey is required to be submitted and approved.

3.3.2 Identification and Authentication for Re-Key After Revocation

In the event that a CA certificate must be revoked, the CA will be re-keyed in accordance with §3.3.1 or terminated in accordance with §5.8.

The process for re-key after revocation of a Subscriber certificate is complete re-enrollment, which requires the generation of a new Subscriber key pair and the re-performance of the initial Subscriber identification and authentication procedures specified in §3.2.2 and 3.2.3.

3.4 Identification and Authentication for Revocation Request

A Subscriber certificate revocation request is valid if it complies with §4.9 and meets one of the following requirements:

- It is digitally signed with the private key of the Subscriber
- It is digitally signed with the private key of an authorized Issuing CA
- If the Subscriber is unable to digitally sign the revocation request, the CA must perform sufficient procedures to manually authenticate the Subscriber's request.

Revocation service requests for High Assurance CA certificates are required to be approved by the PRSS PKI Steering Committee prior to being processed. Revocation service requests for Medium Assurance and end-entity certificates are required to be approved by the PKI service manager prior to being processed.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Prior to a certificate being issued, the Subscriber must submit a certificate application in the form of a digitally signed service request.

4.1.1 Who Can Submit a Certificate Application?

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

4.1.2 Enrollment Process and Responsibilities

Subscribers of CA certificates are required to assent to and also assert compliance with this CP and the PRSS PKI Certification Practice Statement.

4.2 Certificate Application Processing

Service requests must include all information required by the relevant PRSS PKI certificate application form.

4.2.1 Performing Identification and Authentication Functions

See § 3

4.2.2 Approval or Rejection of Certificate Applications

Completed Certificate requests, submitted by Subscribers, must be reviewed and approved prior to issuance. The different stages and types of approvals required for each certificate type shall depend upon the certificate level within the CA hierarchy (i.e., high, medium, or low) and the certificate assurance offered (i.e., high, medium, or low). Online or offline status of a CA may add or subtract approval stages and types. Certificate requests from Online CAs may be made, submitted and issued systematically by a CA at any time after successful completion initial subscriber vetting requirements. For certification assurance levels indicated as "Online CA" see section(Assurance levels), continued access to online certificate signing services is subject to the aging and updating requirement in Section 3.2.2, Age of Certificate enrollment data.

4.2.3 Time to Process Certificate Applications

Certificate applications requested from an Offline CA, when possible, shall be processed within ten (10) business days after all required approvals are obtained. Per this CPS there is no time stipulation to complete processing of an application for a certificate made from an "Online CA" unless otherwise indicated in the relevant Subscriber Agreement, a CPS or any other Agreement between PRSS PKI and its participants.

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 RA performs the required identification and authentication steps in accordance with §3.2.2., §3.2.3, §3.3, and §3.4. Certificates shall be checked to ensure that all fields and extensions are properly populated. Exceptions to defined Certificate Policies must be approved by the PKI Steering Committee.

Fulfillment of the High PRSS class of certificates may only be performed by PRSS PKI representatives under multiple user control. A minimum of two PRSS PKI representatives along with members from Microsoft Information Security (InfoSec) and/or Trustworthy Computing (TwC) are required.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Subscribers shall be notified of Certificate creation upon issuance and will be provided access to their Certificates for download and installation.

4.4 Certificate Acceptance

By accepting a certificate, the Subscriber:

- Agrees to be bound by the continuing responsibilities, obligations and duties imposed by this CP,
- Agrees to be bound by the PRSS PKI Subscriber Agreement,
- Represents and warrants that to its knowledge no unauthorized person has had access to the private key associated with the certificate, and
- Represents and warrants that the certificate information it has supplied during the registration process is truthful and has been accurately and fully published within the certificate.

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

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

Certificates will be published in one or both of the following locations (see also §2.1):

- In the PKI tools' database, which makes the certificate searchable and viewable by all users of the client tool (this is the primary location for all certificates), and/or

Posted on the internet at
http://www.microsoft.com/pkiops/Certs/{CA Common Name}.crt

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

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 shall discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6 Certificate Renewal

Certificate renewal, defined as the process whereby a new certificate with an extended validity period is created for an existing key pair, is supported only on an exception basis upon approval from the PKI Service Manager. Certificate renewal is typically implemented via the re-key processes described in §3.3.1 and §3.3.2.

4.7 Certificate Re-Key

See § 3.3

4.8 Certificate Modification

Not applicable.

4.9 Certificate Revocation and Suspension

PRSS PKI supports certificate revocation for all PRSS PKI CAs. PRSS PKI does not currently support certificate suspension. In the case of online CAs, this CP imposes no stipulation on the automated/systematic request and issuance of certificate revocation by the certificate subscriber. The practice of automated or systematic revocation of certificates made by an RA or certificate subscriber may be stipulated by the appropriate CPS or by the PKI operating group.

4.9.1 Circumstances for Revocation

Revocation may take place at the discretion of the PRSS PKI in the event that the security or integrity of the certificate (or information contained within it) or a Subscriber is compromised or threatened. A certificate may be revoked by PRSS PKI under any or all of the following circumstances:

- The Subscriber is terminated or the product group goes out of business.
- The Subscriber requests certificate revocation in accordance with §4.9.3.
- The certificate subject can be shown to have violated the stipulations of this CP, or compromise the security or integrity of the PRSS PKI.
- The Subscriber can be shown to have violated the stipulations of the PRSS PKI Subscriber Agreement.
- Compromise of the Subscriber's private key is known or suspected.
- Compromise of the Root, Intermediate, or Issuing CA's private key is known or suspected.
- Identifying information or attributes in the Subscriber's certificate change before the certificate expires or otherwise reasonably believed to be false, misleading or inaccurate
- As required by applicable law or regulation.

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

Revocation requests are received by the PRSS PKI team and require several steps:

- Prior to the revocation of a Certificate
    - The CA verifies that the revocation has been requested by the Certificate Subscriber or by the Certificate Owner. In cases where the service request pertains to certificate revocation by an affiliated CA, not managed by PRSS, additional approval from the respective 3rd party is also required.
    - Approval by the PKI Steering Committee is required for high assurance CA revocation requests.
- Fulfillment of the revocation is done by marking a certificate as revoked in the PKI tools database and then submitting a CRL service request to the system to generate the appropriate CRLs.

The CRLs are then posted and distributed by the PRSS PKI Team as appropriate.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocation request application shall be initiated within 24 business hours of receiving the request, when possible.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties are required to check certificate status using the applicable CRL before relying upon a certificate.

4.9.7 CRL Issuance Frequency

CRLs for active Microsoft CAs shall be issued with a validity of 6 months or less and upon certificate revocation.

CRLs for non-active CAs (expired and/or retired CAs) shall be issued from the date of expiration/retirement. These CRLs may be valid for up to 30 years and in some cases may have no expiration.

4.9.8 Maximum Latency for CRLs

Not Applicable.

4.9.9 On-Line Revocation/Status Checking Availability

Not Applicable.

4.9.10 On-Line Revocation Checking Requirements

Not Applicable.

4.9.11 Other Forms of Revocation Advertisements Available

Not Applicable.

4.9.12 Special Requirements Regarding Key Compromise

If PRSS PKI discovers, or has reason to believe, that there has been a compromise of a CA private key, PRSS PKI management authority in conjunction with the PKI Steering Committee will immediately convene an emergency Incident Response Team to assess the situation to determine the degree and scope of the incident and take appropriate action, including implementation of PRSS PKI's Incident Response Plan.

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

Not applicable.

4.11 Key Escrow and Recovery

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

4.11.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

PRSS PKI CA and RA operations are conducted within a physically protected environment designed to deter or prevent, and detect unauthorized use of, access to, or discloser of sensitive information and systems. PRSS PKI maintains multiple business resumption facilities for CA and RA operations. PRSS PKI business resumption facilities are protected with equivalent physical and logical security controls. Business Resumption facilities are at geographically disparate locations so that operations may continue if one or more location is disabled.

5.1.2 Physical Access

CA facilities are protected by multi-factor authentication systems, including biometrics. Access is restricted to a limited number of authorized individuals with an approved business need to access PRSS systems and cryptographic materials. Furthermore, access to these facilities is reviewed on a quarterly basis to determine compliance. Access to offline BCDR facilities is reviewed semi-annually.

Offline and Online CA Systems: computing system components, cryptographic hardware, and activation materials are protected through the use of locked equipment racks, locked cabinets, and safes. Access control is implemented in such a way as to require multi person access.

Physical access to cryptographic systems, hardware, and activation materials shall be restricted using multiple access control and shall be logged, monitored, and video recorded by security personal on a 24X7 basis.

5.1.3 Power and Air Conditioning

PRSS PKI CA facilities are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power for CA systems. Also, these secure facilities are equipped with primary and backup climate control system, as appropriate, to maintain optimal levels of temperature and humidity.

5.1.4 Water Exposures

CA systems and cryptographic materials shall be stored in a manner to minimize the risk of water exposure and damage.

In the event of water damage to CA systems and supporting materials, PRSS PKI shall initiate appropriate recovery steps, determined beforehand, in accordance with the PRSS PKI disaster recovery plan.

5.1.5 Fire Prevention and Protection

- PRSS PKI CA facilities are equipped to prevent, detect, and extinguish outbreaks of fire within the facilities.
- CA systems and cryptographic materials are placed, where appropriate, in fire proof storage containers when not in use to minimize the damage of exposure to flames or smoke.
- PRSS PKI CA facilities meet all local applicable fire code safety regulations.

In the event of heat or smoke damage to CA systems and supporting materials, PRSS PKI shall initiate appropriate recovery steps, determined beforehand, in accordance with the PRSS PKI Disaster Recovery Plan.

5.1.6 Media Storage

All data and content handled by PRSS PKI shall be classified as high business impact (HBI).

Media containing production software and system audit information shall be stored within Corporate Microsoft facilities with appropriate physical and logical access controls in accordance with Microsoft IT Corporate HBI policies.

Media containing production data, i.e., backup of key files etc., shall be stored within PRSS PKI CA hosting facilities that also adhere to appropriate physical and logical access controls in accordance with Microsoft IT Corporate HBI policies.

5.1.7 Waste Disposal

Sensitive waste material shall be disposed of in a secure fashion. Cryptographic devices, smart cards, and other devices that may contain private keys or keying material shall be physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.

5.1.8 Off-Site Backup

Full system backups of the CAs, including backups of system configurations and databases required to reconstitute PKI systems in the event of failure, are made and transported, on a periodic basis, to an offsite backup location with physical security controls commensurate with those at the primary PRSS CA facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

Within the PRSS PKI, the following trusted roles shall be implemented:

- ***PKI team,*** fulfills and supports all PKI services including providing Tier 1 support to customers (i.e., internal business groups) and administration of assets and service requests for PKI services.

- ***Engineering,*** provides PKI system and environment support including building and testing the PKI system and environments in accordance with Microsoft SDLC standard methodology.
- ***PKI Steering Committee,*** provides guidance for PKI policies.
- ***Site Operations,*** provides facilities assistance including installation of new hardware and access management to restricted production management.

5.2.2 Number of Persons Required per Task

Cryptographically sensitive operations within the PRSS PKI such as access to cryptographic materials and systems, CA key generation, CA key recovery, CA key activation and CA system configuration shall require the participation of multiple "trusted" individuals in accordance with §6.2.2. In some cases such as online CA operations where a CA is maintained in an activated state, physical access control must be used to enforce the multi trusted individual requirement.

5.2.3 Identification and Authentication for Each Role

Each person performing a trusted role within the PRSS PKI shall be authorized by management to perform such functions and must satisfy the personnel requirements specified in §5.3.

5.2.4 Roles Requiring Separation of Duties

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

- Handling of CA key and certificate life cycle management activities
- Handling of CA system installation, administration, and maintenance activities

5.3 Personnel Controls

The PRSS PKI operation shall rely on Microsoft Corporate HR policies for personnel management to ensure the trustworthiness of its staff. All project resources must comply with high business impact (HBI) staffing policies. This requirement applies to project FTEs (full time employees) unless otherwise approved.

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

PRSS PKI employees shall undergo background verification checks prior to their commencement of employment at Microsoft. Verification checks shall be performed in accordance with Microsoft Corporate HR new hire policies.

Microsoft PRSS PKI employees shall also be required to sign a nondisclosure agreement

stipulating their understanding and compliance with Microsoft policies and procedures.

5.3.3 Training Requirements

All personnel involved in the PRSS PKI CA hierarchy shall receive the requisite training needed to perform assigned job responsibilities relating to CA or RA operations competently and satisfactorily. Training shall be completed upon hire or as necessary regarding the following areas:

- Basic PKI concepts
- This CP
- Relevant Certification Practice Statements (CPSs')
- Documented PRSS PKI security and operational policies and procedures
- The use and operation of PKI system software.

5.3.4 Retraining Frequency and Requirements

PRSS PKI shall regularly review the state of readiness and awareness of personnel and will renew training on an as needed basis to ensure a consistently high level of awareness and proficiency.

5.3.5 Sanctions for Unauthorized Actions

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

5.3.6 Independent Contractor Requirements

PRSS PKI may employ contractors as necessary.

5.3.7 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

PRSS PKI shall log the following events at a minimum:

- Significant CA key life cycle management events including CA key generation, CA key backup, and other cryptographic device life cycle management information
- CA and Subscriber certificate life cycle management events
    - Requests for certificates, renewal, re-key, and revocation

  - Successful or unsuccessful processing of requests
  - Required certificate request verification activities
  - Generation and issuance of certificates
  - Revocation of certificates
  - Issuance of CRLs
- Logical security-related events including:
  - System crashes, hardware failures and other anomalies
  - Successful and unsuccessful account and service logon
  - Object access
  - Policy changes
  - Account management
- Physical security-related events including:
  - CA facility visitor entry/exit
  - Retrieval of administrator smart cards from off-site secure storage facility
  - All movement of smart cards and hard drives in and out of storage safes

5.4.2 Frequency of Processing Log

Audit logs are reviewed on an as-needed basis.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained as follows:

Log Type	Minimum Retention Period
Logs of CA key management activity	30 years or after 5 years after CA certificate expiration
CA system logs of certificate management activity	30 years or after 5 years after CA certificate expiration
Operating system logs	5 years
Physical access system logs	5 years
Manual logs of physical access	5 years

Log Type	Minimum Retention Period
Video recording of CA facility access	90 days

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

Offline systems Audit logs are backed up on a periodic basis. Online systems events may be forwarded to an internal Microsoft partner of PRSS for review and period backup.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application and operating system level. Manually generated audit data is recorded by PRSS PKI employees. Per section 5.4.5 relative to online CA systems, automatic audit event data which is generated by the system is forwarded to on Microsoft internal PRSS partner team for collection and review.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Vulnerability assessments of the PRSS PKI environment shall be performed as deemed necessary.

5.5 Record Archival

5.5.1 Types of Records Archived

PRSS PKI maintains an archive of logs that include the recorded events specified in §5.4.1.

5.5.2 Retention Period for Archive

See §5.4.3.

5.5.3 Protection of Archive

Archives of relevant records are protected using a combination of physical and logical access controls. PRSS PKI may partner with Microsoft internal teams outside of PRSS to leverage services and subject matter expertise in the area of audit log archive protection services.

5.5.4 Archive Backup Procedures

PRSS PKI archives and retains audit logs at offsite backup locations. PRSS PKI may partner with Microsoft internal teams outside of PRSS to leverage services and subject matter expertise in the area of audit log backup services.

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)

PRSS PKI may partner with Microsoft internal teams outside of PRSS to leverage services and subject matter expertise in the area of audit log archive collection services

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized designated individuals from PRSS PKI are able to obtain access to archive records. The integrity of the information is verified when it is restored.

5.6 Key Changeover

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

See §5.7.4.

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

See §5.7.4.

5.7.3 Entity Private Key Compromise Procedures

If PRSS PKI discovers or has reason to believe that a CA private key has been compromised, the PRSS PKI team will immediately invoke the PRSS PKI Incident Response Plan.

5.7.4 Business Continuity Capabilities After a Disaster

PRSS PKI has established and maintains the following business continuity capabilities to address recovery of the PRSS PKI service and systems in the event of both local and regional level disasters:

- Secure storage of backup cryptographic hardware modules containing copies of the private keys for CAs managed and operated by PRSS PKI at a Microsoft facility more than 1,000 miles away.

- Secure storage of the requisite activation materials at a Microsoft facility more than 1,000 miles away.
- Secure storage of backups of system, data, and configuration information. Backups are made at least every 8-24 hours.
- Secured disaster recovery site at a Microsoft facility more than 1,000 miles away where operations can be restored in the event of a disaster at the primary location
- Business continuity plan for operations that defines the acceptable Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
    - "Offline Operations" The RTO is no more than three days and the RPO is no more than twenty-four hours.
    - "Online Operations" The RTO is no more than one day and the RPO is no more than eight hours.
- Disaster recovery plan (Documented and Tested)
- Disaster recovery testing no less than once per assessment period.

5.8 CA or RA Termination

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

CA key pair generation shall be performed during formal, pre-scripted process ceremonies using hardware cryptographic modules that meet the requirements of §6.2.1. Key generation ceremonies require the participation of multiple trusted employees and are conducted within PRSS PKI facilities, secured according to stipulations defined in §5.

PRSS PKI generates CA key pairs that are (i) within the domain of PRSS PKI and (ii) hosted by PRSS PKI on behalf of Microsoft Product Groups. For CA key pairs generated by PRSS PKI, the process includes members of the Microsoft PRSS PKI team joined by members of the Information Security (InfoSec) group and/or the Trustworthy Computing group (TwC).

CA key pairs, managed and hosted by Microsoft Product Groups and/or external 3rd Party customers, shall be generated in a controlled secure environment and shall comply with key generation and management requirements defined in this CP.

Cryptographic materials, required for the key ceremony, shall be identified and approved prior to the ceremony and retrieved by assigned shareholders under multiple access control at the start of the event. A log shall be maintained of all items removed and replaced from their storage location.

Key ceremonies shall be witnessed by an independent observer not involved in the fulfillment operations.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the Subscriber or by the PRSS PKI team, depending on the application, in accordance with the PRSS PKI 'operations guide'.

6.1.2 Private Key Delivery to Subscriber

Subscribers generate their own key pairs therefore private key delivery is not performed

6.1.3 Public Key Delivery to Certificate Issuer

CA certificate requests are generated and processed by the PRSS PKI team using a controlled process that requires the participation of multiple trusted individuals. CA certificate requests are PKCS #10 requests and accordingly contain the requesting CA's public key and are digitally signed by the requesting CA's private key.

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

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

6.1.4 CA Public Key Delivery to Relying Parties

When the PRSS PKI updates signature key pairs it shall distribute the new public key in a secure fashion. The new Public Key may be distributed in a self-signed Certificate, or in a new CA Certificate (e.g., Cross Certificate) obtained from the issuer(s) of the current CA Certificate(s).

Certificates will be published in one or both of the following locations

- In the PKI tools' database, which makes the certificate searchable and viewable by all users of the client tool (this is the primary location for all certificates), and/or
- PRSS PKI repository (see also §2.1). PRSS PKI Repository information is posted on the internet at: http://www.microsoft.com/pkiops/Docs/Repository.htm

Subscribers of "Online CA" certificates shall have the option to receive the latest CA public key certificate via an automated method such as a callback via the registration authority application interface.

6.1.5 Key Sizes

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

(1) Root CA Certificates

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

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

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

(3) End-Entity (Subscriber Certificates)

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

NOTE: Certificates with smaller public key modulus bit sizes must be approved by the PKI Steering Committee.

6.1.6 Public Key Parameters Generation and Quality Checking

For all new Public keys, Public Key parameters shall be generated in accordance with [FIPS186-3]. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with [FIPS186-3]. RA and CA systems shall enforce the Public Key parameters quality checking requirements of this CP via systematic controls. Certification requests with RSA public key parameters which are in exceptions to FIPS186-3 are specifically noted and are required to be approved by the PKI Steering Committee.

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

Key pairs may be used as follows:

Entity	Permitted Key Usage
Root CA	Signing subordinate CA certificates, CRL signing.
Subordinate CA	Signing subordinate CA certificates, subscriber certificates, and CRLs.
Subscriber	Signing: Keys used for digital signatures shall set the digitalSignature bit. Encryption: Keys used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits.

"Online CA" systems may have systematic controls in place to strongly enforce compliance with this requirement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

CA key pairs managed and hosted by internal PRSS Partners, Microsoft Product Groups and/or external 3rd Party subscribers shall be generated in similarly certified hardware cryptographic modules in compliance with key generation requirements defined in this CP.

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

The participation of multiple trusted individuals is required to perform sensitive CA private key operations (e.g., hardware security module (HSM) activation, signing operations, CA key backup, CA key recovery, etc.). This is enforced through PRSS PKI's allocation among persons or groups with trusted roles of the User or crypto-officer role authentication tokens, required for CA key activation.

The participation of at least two trusted individuals is required to perform sensitive CA private key operations (e.g., signing operations, CA key backup, CA key recovery, etc.) for the Issuing CAs. This is enforced by the physical access controls specified in CP §5.1.2 and physical access controls over the related Crypto officer tokens and user tokens. A threshold (m) number of tokens of the total number (n) of tokens, created and distributed for each hardware cryptographic module security world, is required to activate a CA private key. Token m of n configuration requirements are described in the following table:

Certificate Class	Assurance Level	Minimum Required Quorum of tokens for user or crypto officer token Set (m)	Minimum Required total number of tokens for user or Crypto officer token Set (n)
Low Impact	Low Assurance	1	12
Medium Impact	Medium Assurance	2	12
Medium Impact (Online)	Medium Assurance Online	1	12
High Impact	High Assurance	3	12

Exceptions to these policies require the approval of the PKI Steering Committee. Furthermore, PRSS PKI production security worlds shall not be shared with non-PRSS PKI groups or used to perform signing activities for test CAs.
CA key pairs, managed and hosted by Microsoft Product Groups and/or external 3rd Party customers, shall comply with private key multi-person access control requirements defined in this CP.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

Backup copies of CA private keys shall be stored in encrypted form using cryptographic modules that meet the requirements specified in §6.2.1.

Where copies of Subscriber private keys are stored by PRSS PKI, such keys shall be backed up and stored in encrypted form with physical and logical access restricted to authorized individuals.

6.2.5 Private Key Archival

§6.2.4.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA private keys are generated and used only within hardware cryptographic modules meeting the requirements of §6.2.1. The private key exists outside hardware cryptographic modules only in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

§6.2.6.

6.2.8 Method of Activating a Private Key

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

CA key pairs, managed and hosted by Microsoft Product Groups and/or external 3rd Party customers, shall comply with activation of private key requirements defined in this CP.

"Online CA" key pairs shall remain in an activated state.

6.2.9 Method of Deactivating Private Keys

Cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via removal of activation smart card reader or automatically after a period of inactivity. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of 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, in the presence of multiple trusted personnel after approval from the PKI Steering Committee. When CA key destruction is required, CA private keys shall be completely destroyed through zeroization and/or physical destruction of the device in accordance with manufacturers' guidelines.

CA key pairs, managed and hosted by Microsoft Product Groups and/or external 3rd Party customers, shall comply with private key destruction requirements defined in this CP.

6.2.11 Cryptographic Module Rating

See §6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For Certificate issued after the publication of this CP, the following key and certificate usage periods shall be deployed.

Entity Type	Maximum Certificate Validity Period	
Root CA	25 Years	
Subordinate CAs	**Offline CA** 20 Years	**Online CA** 3 Years
Subscribers	15 Months	

Exceptions to the above noted operational and usage periods must be approved by the PKI Steering Committee.

6.4 Activation Data

Hardware cryptographic modules used for CA private key protection shall utilize a share secret token based activation mechanism as described in CP §6.2.2. These token are created during formal "Security World" generation ceremonies, used only when needed, and stored in a secure site when not in use. "Online CA" systems sha1l require that persistent cryptographic module activation is only supported when at least one HSM user share token is present in the module. The activation material left installed into the HSM is protected by physical security access controls.

6.4.1 Activation Data Generation and Installation

See §6.4

6.4.2 Activation Data Protection

See §6.4

6.4.3 Other Aspects of Activation Data

See §6.4

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

PRSS PKI systems use industry standard CA software, PKI applications, cryptographic modules, and smart cards. PRSS PKI systems maintaining CA software and data files shall be secured from unauthorized access. Authorized access to production servers shall be limited to those individuals with a valid business reason for such access.

PKI systems comply with Microsoft Trustworthy Computing (TwC) security policies. The Microsoft corporate network as a whole is protected by industry standard intrusion detection systems and firewalls.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

All CA software shall be developed in accordance with documented Microsoft systems development lifecycle (SDLC) and security development lifecycle (SDL) and processes. Approvals are required at all stages of development by the management. All code is verified, using digital signatures and hashing, before being deployed into the production CA environment.

6.6.2 Security Management Controls

PRSS PKI has tools and processes in place to control and monitor the configurations of the CA systems. PRSS PKI validates the integrity of all software before release into production.

6.7 Network Security Controls

All PRSS PKI CA system functions for assurance levels which are not indicated as "Online CA" are performed in an offline state unattached from any Microsoft internal or external networks.

Online CA functions shall be performed using a Microsoft owned and operated private network, segregated from the Microsoft Corporate network and secured through the use of preventative (properly configured routers and firewalls).

Detective controls (monitoring systems) shall be implemented and maintained. Communications of sensitive information, classified as Microsoft High Business Impact (HBI), shall be encrypted during storage, usage, and transmission across the network.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

CA certificates within the PRSS PKI shall be X.509 Version 3 and shall conform to the RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL profile, dated May 2008.

At a minimum the following basic fields and prescribed field attributes are utilized within the CA certificate profile. Less stringent exceptions to the given basic profile must be approved on a case-by-case basis by the PKI Steering Committee based on a valid documented business case.

Root CA Certificate Profile

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA
Signature Algorithm Identifier	See § 7.1.3
Issuer Distinguished Name	CN = < CA Common Name > OU = < Microsoft Product Group Name > (optional) O = < Organization > L = < Locality > S = < State > C = ISO 3166-1 alpha-2 country code
Valid From	Date and time of certificate issuance. Time is encoded in accordance with RFC 5280.
Valid To	Date and time of certificate expiration. Time is encoded in accordance with RFC 5280. See § 6.3.2
Subject Distinguished Name	Same as Issuer Distinguished Name for self-signed Root CA certificates
Subject Public Key Information	See § 6.1.5

Subordinate CA Certificate Profile

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

End Entity or Out-of-Scope CA Certificate Profile

Field	Description
Version	V3
Serial Number	Positive integer uniquely assigned by CA to include at least 8 random bytes
Signature Algorithm Identifier	See § 7.1.3
Issuer	Subject Distinguished Name of Parent CA
Valid From	Date and time of certificate issuance. Time is synchronized with a reliable time source. . Time is encoded in accordance with RFC 5280.
Valid To	Date and time of certificate expiration. Time is synchronized with a reliable time source. . Time is encoded in accordance with RFC 5280. See § 6.3.2
Subject Distinguished Name: (This attribute is optional unless the Subject Alternative Name is absent.)	All fields are optional unless specified. E = < Email Address > CN = < Subscriber Name > (required) OU = <Subscriber Company Unit Name> i.e., Microsoft Product Group or Partner Name (for certificates issued to external 3rd Party customers) O = <Subscriber Company Name> i.e., Microsoft or Partner Name L = < Locality > S = < State > DC = < Domain Component > C = < ISO 3166-1 alpha-2 code >
Subject Alternative Name: (This attribute is optional unless the Subject Distinguished Name is absent.)	If the Subject Alternative Name is present, one or more of the following fields must be present. UPN = < User Principal Name > DNS = < Domain Name > email = < Email Address >

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

7.1.1 Version Number(s)

PRSS PKI hierarchy certificates are X.509 version 3 certificates.

7.1.2 Certificate Extensions

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

Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 3280 standards and recommendations. The name forms for Subscribers are enforced through PRSS PKI internal policies and the authentication policies described elsewhere in this CP.

7.1.2.1 Key Usage

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

7.1.2.2 Certificate Policies Extension

The CertificatePolicies extension of PRSS PKI X.509 Version 3 Certificates may be present.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of PRSS PKI X.509 Version 3 Certificates may be present.

7.1.2.4 Basic Constraints

PRSS PKI CA Certificates BasicConstraints extension shall have the CA field set to TRUE. End-user Subscriber Certificates BasicConstraints extension, shall be populated with a value of an empty sequence. The criticality field of this extension shall be set to TRUE for CA Certificates, but otherwise set to FALSE.

PRSS PKI CA Certificates shall have a “pathLenConstraint” field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a

certification path. CA Certificates issued to any Product Groups and 3rd Party CA, issuing end-user Subscriber Certificates, shall have a "pathLenConstraint" field set to a value of "0".

7.1.2.5 Extended Key Usage

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

7.1.2.6 CRL Distribution Points

Most PRSS PKI X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

Most PRSS PKI X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the authority key identifier extension to provide a means of identifying the public key corresponding to the private key used to sign the respective certificate. When used, the criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

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

7.1.3 Algorithm Object Identifiers

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

Signature Algorithm	OID ASN.1	Status
md5WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) md5WithRSAEncryption(4)}	*Deprecated from January 27, 2010
Sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}	*Deprecated from January 25th 2013
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}	acceptable
sha256ECDSA	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}	acceptable
sha256ECDSA	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}	acceptable
sha384ECDSA	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}	acceptable
sha512ECDSA	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)}	acceptable

*The use of signature algorithms indicated as deprecated to create new digital signatures on certificates must be approved by the PKI Steering Committee.

Certificates created with deprecated signature algorithms adhere to all the requirements of this CP with the exception that the certificate is generated with deprecated signature algorithm. Additionally legacy CAs which are maintaining certificate status information for valid SHA1 or MD5 certificates may use SHA-1 signatures for generation of CRLs.
Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

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

7.1.4 Name Forms

Root CA, Intermediate CA, Issuing CA and Subscriber certificates are populated in accordance with certificate profiles listed in § 7.1. RA systems and "Online CA" systems shall use systematic controls such as certificate issuance templates to enforce these requirements. Offline CA systems shall use procedural controls to enforce this requirement.

7.1.5 Name Constraints

In lieu of Name Constraints RA systems shall uses systematic controls that enforce that all of the publically resolvable names referenced in a certificate request have had previously been authorized by the name registrant to the subscriber to act on the registrant's behalf in obtaining public key certificate.

7.1.6 Certificate Policy Object Identifier

From the publication of this CP forward, where possible, each certificate issued by a PRSS PKI issuing CA contains the OID of this CP in the Certificate policy extension provided in section 1.2 Document Name and Identification.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.2 Root CA CRL Profile

Field	Description
Version	V2
Signature	*sha1WithRSAEncryption, sha256WithRSAEncryption , or ecdsa-with-SHA256
Issuer	Subject of Issuer
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	6 months (not to exceed)
Revoked Certificates	List of information regarding revoked certificates. CRL entries include:
	• ***Serial Number***, identifying the revoked certificate • ***Revocation Date***, including the date and time of certificate revocation
CRL Entry Extensions	Not used.

*sha1WithRSAEncryption included to represent legacy certificate profiles only.
See §7.1.6.Algorithm Object Identifiers for current signature algorithm status.

7.2.1 Subordinate CA CRL Profile

Field	Description
Version	V2
Signature	*sha1WithRSAEncryption, sha256WithRSAEncryption , or ecdsa-with-SHA256
Issuer	Subject of Issuer
This Update (Effective Date)	Date and time of CRL issuance.
Next Update	6 months (not to exceed)
Revoked Certificates	List of information regarding revoked certificates. CRL entries include:
	• ***Serial Number***, identifying the revoked certificate • ***Revocation Date***, including the date and time of certificate revocation
CRL Entry Extensions	Not used.

*sha1WithRSAEncryption included to represent legacy certificate profiles only.
See §7.1.6 Algorithm Object Identifiers for current signature algorithm status.

7.2.1.1 Version Number(s)

See §7.2.

7.2.2 CRL and CRL Entry Extensions

See §7.2.

7.3 OCSP Profile

Not Applicable.

7.3.1 Version Number(s)

Not Applicable.

7.3.2 OCSP Extensions

Not Applicable.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

Entities comprising the Microsoft PRSS PKI CA hierarchy, including PRSS PKI, participating Microsoft Product Groups, and external 3rd Party customers, are subject to an annual audit that assess compliance with the PRSS PKI CP, CPS, and the WebTrust for Certification Authorities (WebTrust for CAs) audit criteria.

8.2 Identity/Qualifications of Assessor

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

The annual audit shall be performed by auditors demonstrating proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function.

8.3 Assessor's Relationship to Assessed Entity

The entity that performs the annual audit shall be organizationally independent of Microsoft PRSS PKI.

8.4 Topics Covered by Assessment

The scope of the annual audit shall include the requirements of this CP, the PRSS PKI CPS, the PRSS CS CPS, CA environmental controls, CA key management, and certificate life cycle management.

8.5 Actions Taken as a Result of Deficiency

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

Should a severe deficiency be identified that might compromise the integrity of the PRSS PKI, management will consider, with input from the auditor, whether suspension of PKI operations is warranted. Should a severe deficiency be identified that might compromise the integrity of a particular CA, management will assess whether suspension of the particular CA's operations is warranted.

8.6 Communication of Results

Compliance audit results are communicated to PRSS PKI management and others deemed appropriate by management.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

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

9.1.3 Revocation or Status Information Access Fees

PRSS PKI does not charge a fee as a condition of making the CRLs available as required by CP §4.9 and §4.10 available in a repository or otherwise available to Relying Parties. PRSS PKI reserves the right to charge a fee for providing customized CRLs or other value-added revocation and status information services.

9.1.4 Fees for Other Services

PRSS PKI 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

Not Applicable.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Not Applicable.

9.2.2 Other Assets

PRSS PKI customers that maintain CAs outside the realm of the PRSS PKI environment shall have access to sufficient financial resources to support operations and perform duties in accordance with the PRSS PKI CP and to pay damages for potential liability to Subscribers and Relying parties during the operations of these managed CAs.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not Applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

- PRSS PKI policies, procedures and technical documentation supporting this CP
- 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 PRSS PKI CA hierarchy
- Compliance audit results except for WebTrust for CAs audit reports which may be published at the discretion of PRSS PKI Management

9.3.2 Information Not Within the Scope of Confidential Information

This CP and the Certificates and CRLs issued by PRSS PKI are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

See §9.3.1

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.5 Intellectual Property Rights

The following are the property of Microsoft:

- This CP
- Relevant Certification Practice Statements (CPS')
- Microsoft specified Certificate Policy
- Policies and procedures supporting the operation of PRSS PKI
- Microsoft specified Object Identifiers (OIDs)
- Certificates and CRLs issued by PRSS PKI managed CAs
- Distinguished Names (DNs) used to represent entities within the PRSS PKI CA hierarchy
- CA, infrastructure, and Subscriber key pairs

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

9.6 Representations and Warranties

PRSS PKI warrants and promises to provide certification authority services substantially in compliance with this CP and the relevant Microsoft Certificate Policies. PRSS PKI makes no other warranties or promises and has no further obligations to subscribers or relying parties, except as set forth under this CP.

9.7 Disclaimers of Warranties

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

- of 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 PRSS PKI, 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 PRSS PKI; or
- Due to disclosure of personal information contained within certificates or CRLs.

9.8 Limitations of Liability

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

9.9 Indemnities

By their applying for and being issued certificates, or otherwise relying upon such certificates, subscribers, and relying parties, agree to indemnify, defend, and hold harmless the CA, and its personnel, organizations, entities, subcontractors, suppliers, vendors, representatives, and agents from any errors, omissions, acts, failures to act, or negligence resulting in liability, losses, damages, suits, or expenses of any kind, due to or otherwise proximately caused by the use or publication of a certificate that arises from the subscriber's failure to provide the CA with current, accurate, and complete information at the time of certificate application or the subscriber's errors, omissions, acts, failures to act, and negligence. The CA and its RAs are not the agents, fiduciaries, trustees, or other representatives of subscribers or relying parties

9.10 Term and Termination

The CP becomes effective upon publication in the PRSS PKI documentation 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 the PRSS PKI documentation repository.

9.11 Individual Notices and Communications with Participants

Severance or merger may result in changes to the scope, management, and/or operations of this CA. In such an event, this CPS may require modification as well. Changes to the operations will occur consistent with the CA's disclosed CPS management processes.

9.12 Amendments

Amendments to this CP may be made by the PRSS PKI Service Manager and must be approved by the PRSS PKI Steering Committee.

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 PRSS PKI management regarding the dispute. PRSS PKI management will involve the appropriate Microsoft personnel to resolve the dispute.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

See §9.14

9.16 Miscellaneous Provisions

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

If any provision of this CP is found to be unenforceable, the remaining provisions shall be interpreted to best carry out the reasonable intent of the parties. It is expressly agreed that every provision of this CP that provides for a limitation of liability or exclusion of damages, disclaimer or limitation of any warranties, promises or other obligations, is intended to be severable and independent of any other provision and is to be enforced as such.

This CP shall be interpreted consistently with what is commercially reasonable in good faith under the circumstances and considering its international scope and uniform application. Failure by any person to enforce a provision of this CP will not be deemed a waiver of future enforcement of that or any other provision. Any notice, demand, or request pertaining to this CP shall be communicated either using digitally signed messages consistent with this CP, or in writing. Electronic communications shall be effective when received by the intended recipient.

