PIXA

Certification Practice Statement

Date: January 02, 2026
Version: 1.0.0

Table of Contents

Document History....1

Acknowledgements....2

1. Introduction....3

1.1. Overview....3

1.2. Document Name and Identification....4

1.3. PKI Participants....5

1.3.1. Certification Authorities....5

1.3.2. Registration Authorities....6

1.3.3. Subscribers....6

1.3.4. Relying Parties....6

1.3.5. Other Participants....6

1.4. Certificate Usage....7

1.4.1. Appropriate Certificate Uses....7

1.4.1.1. PIXA Web Server Certificates....7

1.4.1.2. PIXA Web Server Certificates PKE....7

1.4.1.3. PIXA Client Device Certificates....8

1.4.1.4. PIXA External Client Device Certificates....8

1.4.1.5. PIXA MDM Client Device Certificates....8

1.4.1.6. PIXA Domain Controller KA....8

1.4.1.7. PIXA Exchange Enrollment Agent....9

1.4.1.8. PIXA CEP Encryption....9

1.4.2. Prohibited Certificate Uses....9

1.5. Policy Administration....9

1.5.1. Organization Administering the Document....9

1.5.2. Contact Person....10

1.5.3. Person Determining CPS Suitability for the Policy....10

1.6. Definitions and Acronyms....10

1.6.1. Definitions....11

1.6.2. Acronyms 18
1.6.3. References 18
1.6.4. Conventions 20
2. Publication and Repository Responsibilities 20
2.1. Repositories 20
2.2. Publication of Certification Information 20
2.3. Time or Frequency of Publication 21
2.4. Access Controls on Repositories 21
3. Identification and Authentication 22
3.1. Naming 22
3.1.1. Naming Convention 22
3.1.2. Acceptable Subscriber Names 22
3.1.3. Pseudonyms 22
3.1.4. Registration, Authentication and Role Trademarks 22
3.2. Initial Identity Validation 22
3.2.1. Prove Access to Private Key 23
3.2.2. Authentication of Organization Identity 23
3.2.3. Validation of Authority 23
3.3. Identification and Authentication for Re-Key Requests 23
3.3.1. Identification and Authentication for Routine Re-Key 23
3.3.2. Identification and Authentication for Re-Key After Revocation 23
3.4. Identification and Authentication for Revocation Request 24
4. Certificate Life-cycle Operational Requirements 24
4.1. Certificate Application 24
4.1.1. Who Can Submit a Certificate Application 24
4.1.2. Enrollment Process and Responsibilities 24
4.2. Certificate Application Processing 25
4.2.1. Performing Identification and Authentication Functions 25
4.2.1.1. Entities managed by PIXA 25

4.2.1.2. Un-managed Entities 25
4.2.2. Approval or Rejection of Certificate Applications 26
4.2.3. Time to Process Certificate Applications 27
4.2.4. Verification of DNS Records 27
4.3. Certificate Issuance 27
4.3.1. CA Actions during Certificate Issuance 27
4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate 28
4.4. Certificate Acceptance 28
4.4.1. Conduct Constituting Certificate Acceptance 28
4.4.2. Publication of the Certificate by the CA 28
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 28
4.5. Key Pair and Certificate Usage 29
4.5.1. Subscriber Private Key and Certificate Usage 29
4.5.2. Relying Party Public Key and Certificate Usage 29
4.6. Certificate Renewal 29
4.6.1. Circumstance for Certificate Renewal 29
4.6.2. Who May Request Renewal 29
4.6.3. Processing Certificate Renewal Requests 30
4.6.4. Notification of New Certificate Issuance to Subscriber 30
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate 30
4.6.6. Publication of the Renewal Certificate by the CA 30
4.6.7. Notification of Certificate Issuance by the CA to other Entities 30
4.7. Certificate Re-Key 30
4.8. Certificate Modification 31
4.9. Certificate Revocation and Suspension 31
4.9.1. Circumstances for Revocation 31
4.9.1.1. Reasons for Revoking a Subscriber Certificate 31
4.9.1.2. Reasons for Revoking a Subordinate CA Certificate 33
4.9.2. Who Can Request Revocation 33

4.9.3. Procedure for Revocation Request....33
4.9.3.1. Revocation Reason Codes....33
4.9.3.1.1. Reason Codes....34
4.9.4. Revocation Request Grace Period....35
4.9.5. Time Within Which CA Must Process the Revocation Request....35
4.9.6. Revocation Checking Requirements for Relying Parties....36
4.9.7. CRL Issuance Frequency....36
4.10. Certificate Status Service....36
4.10.1. Certificate Status Service....36
4.10.2. Service Availability....36
4.11. End of Subscription....37
5. Facility, Management and Operational Controls....37
5.1. Physical Security Controls....38
5.1.1. Site Location....38
5.1.2. Physical Access....38
5.1.3. Power and Air Conditioning....39
5.1.4. Water Exposures....39
5.1.5. Fire Prevention and Protection....39
5.1.6. Media StorageT....39
5.1.7. Waste Disposal....39
5.1.8. Off-Site Backup....39
5.2. Procedural Controls....40
5.2.1. Trusted Roles....40
5.2.2. Number of Persons Required per Task....40
5.2.3. Identification and Authentication for Each Role....40
5.2.4. Maximum Latency for CRLs....40
5.2.5. Roles Requiring Separation of Duties....40
5.3. Personnel Controls....41
5.3.1. Qualifications, Experience, and Clearance Requirements....41

5.3.2. Background Check Procedures 41
5.3.3. Training Requirements 41
5.3.4. Retraining Frequency and Requirements 41
5.3.5. Job Rotation Frequency and Sequence 41
5.3.6. Sanctions for Unauthorized Actions 42
5.3.7. Independent Contractor Requirements 42
5.3.8. Documentation Supplied to Personnel 42
5.4. Audit Logging Procedures 42
5.4.1. Types of Events Recorded 42
5.4.2. Frequency of Processing Log 43
5.4.3. Retention Period for Audit Log 43
5.4.4. Protection of Audit Log 44
5.4.5. Audit Log Backup Procedures 44
5.4.6. Audit Collection System 44
5.4.7. Notification to Event-Causing Subject 44
5.4.8. Vulnerability Assessments 44
5.5. Records Archival 44
5.5.1. Types of Records Archived 44
5.5.2. Retention Period for Archive 45
5.5.3. Protection of Archive 45
5.5.4. Archive Backup Procedures 45
5.5.5. Requirements for Time-Stamping of Records 45
5.5.6. Archive Collection System (Internal or External) 45
5.5.7. Procedures to Obtain and Verify Archive Information 45
5.6. Key Changeover 45
5.7. Compromise and Disaster Recovery 46
5.7.1. Incident and Compromise Handling Procedures 46
5.7.2. Computing Resources, Software, and/or Data Are Corrupted 46
5.7.3. Entity Private Key Compromise Procedures 46

5.7.4. Business Continuity Capabilities After a Disaster 46
5.8. CA or RA Termination 46
6. Technical Security Controls 47
6.1. Key Pair Generation and Installation 47
6.1.1. Key Pair Generation 47
6.1.1.1. CA Key Pair Generation 47
6.1.1.2. RA Key Pair Generation 47
6.1.1.3. Subscriber Key Pair Generation 48
6.1.2. Private Key Delivery to Subscriber 48
6.1.3. Public Key Delivery to Certificate Issuer 48
6.1.4. CA Public Key Delivery to Relying Parties 49
6.1.5. Key Sizes 49
6.1.6. Public Key Parameters Generation and Quality Checking 49
6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field) 49
6.2. Private Key Protection and Cryptographic Module Engineering Controls 50
6.2.1. Cryptographic Module Standards and Controls 50
6.2.2. Private Key (n out of m) Multi-Person Control 50
6.2.3. Private Key Escrow 50
6.2.4. Private Key Backup 50
6.2.5. Private Key Archival 51
6.2.6. Private Key Transfer into or from a Cryptographic Module 51
6.2.7. Private Key Storage on Cryptographic Module 51
6.2.8. Method of Activating Private Key 51
6.2.9. Method of Deactivating Private Key 51
6.2.10. Method of Destroying Private Key 51
6.2.11. Cryptographic Module Rating 51
6.3. Other Aspects of Key Pair Management 52
6.3.1. Public Key Archival 52
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 52

6.4. Activation Data 52
6.4.1. Activation Data Generation and Installation 52
6.5. Computer Security Controls 53
6.5.1. Specific Computer Security Technical Requirements 53
6.6. Life Cycle Technical Controls 53
6.7. Network Security Controls 53
6.8. Time Stamping 53
7. Certificate and CRL Profiles 53
7.1. Certificate Profile 53
7.1.1. Version Number(s) 54
7.1.2. Certificate Extensions 54
7.1.2.1. Root CA Certificate Profile 54
7.1.2.2. Subordinate CA Certificate Profile 56
7.1.2.3. Subscriber Certificate Profile 57
7.1.2.3.1. PIXA Web Server 58
7.1.2.3.2. PIXA Web Server PKE 59
7.1.2.3.3. PIXA Client Device 60
7.1.2.3.4. PIXA External Client Device 60
7.1.2.3.5. PIXA MDM Client Device 61
7.1.2.3.6. PIXA Domain Controller KA 61
7.1.3. CRL Distribution Points 61
7.1.3.1. CRL Profile 62
7.1.4. Authority Information Access 62
8. Compliance Audit and Other Assessments 63
8.1. Frequency and Circumstances of Assessment 63
8.2. Identity/Qualifications of Assessor 63
8.3. Assessor's Relationship to Assessed Entity 64
8.4. Topics Covered by Assessment 64
8.5. Actions Taken as a Result of Deficiency 64

8.6. Communication of Results 64
9. Other Business and Legal Matters 65
9.1. Fees 65
9.2. Financial Responsibility 65
9.2.1. Insurance Coverage 65
9.3. Confidentiality of Business Information 65
9.3.1. Scope of Confidential Information 65
9.3.2. Information Not Within the Scope of Confidential Information 65
9.3.3. Responsibility to Protect Confidential Information 66
9.4. Privacy of Personal Information 66
9.4.1. Privacy Plan 66
9.4.2. Information Treated as Private 66
9.4.3. Information Not Deemed Private 66
9.4.4. Responsibility to Protect Private Information 66
9.4.5. Notice and Consent to use Private Information 66
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 66
9.5. Intellectual Property Rights 67
9.6. Representations and Warranties 67
9.6.1. CA Representations and Warranties 67
9.6.2. RA Representations and Warranties 69
9.6.3. Subscriber Representation and Warranties 69
9.7. Disclaimers of Warranties 71
9.8. Limitations of Liability 71
9.9. Indemnities 72
9.10. Term and Termination 73
9.10.1. Term 73
9.10.2. Termination 73
9.10.3. Effect of Termination and Survival 73
9.11. Individual Notices and Communications with Participants 73

9.12. Amendments 73
9.12.1. Procedure for Amendment 73
9.13. Dispute Resolution Provisions 73
9.14. Governing Law 74
9.15. Compliance With Applicable Law 74
9.16. Miscellaneous Provisions 74
9.16.1. Entire Agreement 74
9.16.2. Assignment 74
9.16.3. Severability 74

Document History

Document Change Control

Version	Release Date	Author	Status & Description
1.0.0	January 5, 2026	Patrick Mercier	Initial CPS for PIXA

Acknowledgements

This PIXA PKI Policy GroupCPS endorses in whole or in part the following industry standards:

• RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)

• RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

• RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile

• The ISO 1-7799 standard on security and infrastructure

This Certificate Policy (CP) incorporates material derived from the *Microsoft PKI Services Certificate Policy (CP)* Version 3.1.9, published April 21, 2025. The Microsoft document is licensed under the Creative Commons Attribution–NoDerivatives 4.0 International License (CC BY-ND 4.0). PIXA retains all intellectual property rights in and to this adapted CP, which is specific to PIXA and includes additional original material.

1. Introduction

This Certification Practice Statement (CPS) of the PIXA PKI Policy Group Certification Authority (hereinafter, PIXA PKI Policy Group) applies to the services of the PIXA PKI Policy Group that are associated with the issuance of and management of digital certificates. This CPS can be found on the PIXA PKI Policy Group repository at: https://www.pixa.ca/pki This CPS may be updated from time to time.

This CPS addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by PIXA PKI Policy Group. PIXA PKI Policy Group is operated and owned by PIXA.

Inquiries on this PIXA PKI Policy Group CPS can be addressed to:

PIXA PKI Policy Group
Patrick Mercier
info@pixa.ca

This CPS is final and binding between PIXA (operating and owning the PIXA PKI Policy Group), a company under public law, with registered office in Canada. (Hereinafter referred to as "PIXA") and the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the PIXA PKI Policy Group.

For subscribers this CPS becomes effective and binding by accepting an appropriate use agreement found at https://www.pixa.ca/documentation. For relying parties this CPS becomes binding by merely addressing a certificate related request on a PIXA certificate to a PIXA directory. The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CPS.

Commented [PM1]: Link to the appropriate use agreement. May want to look at adding an entry in that one regarding certs and directing people to Sections 1.3.3, 1.3.4, 1.4 of this CPS

1.1. Overview

This CPS applies to the specific domain of the PIXA PKI Policy Group. The purpose of this CPS is to present the PIXA practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to PIXA Services' own and industry requirements pursuant to the standards set out above. The certificate types addressed in this CPS are the following :

- Web Server Certificate
- Client Device Certificate

- External Client Device Certificate
- External Client Device Certificate Mobile Device Management
- Kerberos Authentication
- Exchange Enrollment Agent
- CEP Encryption

These Certificates:

- Can be used for the identification of the certificate holder (Client Authentication)
- Can be used to authenticate internal web resources, such as servers and other devices
- Can be used to encrypt communications between internal systems where required by industry or corporate standards.
- Can be assigned to approved Registration Authorities for the purpose of enrollment.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of PIXA certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved including the PIXA PKI Policy Group, PIXA RA, subscribers and relying parties. Certain provisions might also apply to other entities such as the certification service provider, application providers etc.

This CPS describes the requirements to issue, manage and use certificates issued by the PIXA PKI Policy Group under PIXA Root CA which is managed according to practices described in the PIXA Certificate Policy published under https://www.pixa.ca/pki. This CPS relies exclusively on the practices described in the PIXA PKI Policy Group Certificate Policy. A subscriber or relying party of a PIXA PKI Policy Group certificate must refer to the PIXA CPS to establish Trust. It is also essential to establish the trustworthiness of the entire certificate chain of the PIXA certificate hierarchy, including PIXA Root CA.

This CPS is made available on-line under https://www.pixa.ca/pki.

The PIXA PKI Policy Group accepts comments regarding this CPS addressed to the address mentioned above in the Introduction of this document.

1.2. Document Name and Identification

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections

- Changes to contact details

1.3. PKI Participants

The PIXA PKI Policy Group makes its services available to PIXA certificate subscribers. These subscribers include without limitation entities that use the PIXA certificates for the purposes of:

- Authentication (digital signature)
- Encryption

1.3.1. Certification Authorities

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

PIXA PKI Policy Group operates as the Root CA and administers all CA functions within its PKI hierarchy.

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

Obligations of CAs operating within the PIXA PKI Policy Group PKI hierarchy include:

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

1.3.2. Registration Authorities

RA functions at PIXA have been delegated to Microsoft Active Directory Domain Services (ADDS) as well as to the Microsoft Network Device Enrollment Service (NDES) in conjunction with Microsoft Entra ID and Microsoft Intune.

1.3.3. Subscribers

A Subscriber, as defined in Section 1.6, is the end entity whose name or identifier appears as the subject in a certificate, and who uses its key and certificate in accordance with this CPS. Subscribers within the CA's hierarchy MAY be issued certificates for assignment to devices, groups, organizational roles or applications, provided responsibility and accountability are attributable to a role owner within PIXA.

Obligations of Subscribers within the CA's hierarchy include:

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

1.3.4. Relying Parties

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

1.3.5. Other Participants

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

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

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

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

PIXA certificates can be used for **internal** domain transactions that require:

- Authentication and
- Confidentiality

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

1.4.1. PIXA Web Server Certificates

Web Server certificates can be used for web-based transactions. It is meant for entities that wish to participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in secured transactions. See Section 7.1.2.3.1.

1.4.1. PIXA Web Server Certificates PKE

Web Server certificates can be used for web-based transactions. It is meant for entities that wish to participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in secured transactions. This Private Key Exportable (PKE) version of the Web Server Certificate will only be issued on proof of a specific requirement for the functionality.

1.4.1. PIXA Client Device Certificates

Client Device certificates may be used to provide authentication services for provided services such as WIFI, VPN and Device Management. These certificates will also be used to secure remote access capabilities through such protocols as Remote Desktop Services, Terminal Services, to name a few. They may also be used by applications to secure traffic to the device that owns the presented certificate. These certificates will be deployed with the Client Authentication and Remote Desktop Authentication EKUs. These certificates will be issued automatically by ADDS as the RA. See section 7.1.2.3.2.

1.4.1. PIXA External Client Device Certificates

Client Device certificates may be used to provide authentication services for provided services such as WIFI, VPN and Device Management. These certificates will also be used to secure remote access capabilities through such protocols as Remote Desktop Services, Terminal Services and SSH, to name a few. They may also be used by applications to secure traffic to the device that owns the presented certificate. These certificates will be deployed with the Client Authentication and Server Authentication EKU. These certificates will be deployed to non-domain joined Microsoft Windows systems using the Certificate Enrollment Web Service and the Certificate Enrollment Policy Service.

1.4.1. PIXA MDM Client Device Certificates

Client Device certificates may be used to provide authentication services for provided services such as WIFI, VPN and Device Management. These certificates will also be used to secure remote access capabilities through such protocols as Remote Desktop Services, Terminal Services and SSH, to name a few. They may also be used by applications to secure traffic to the device that owns the presented certificate. These certificates will be deployed with the Client Authentication and Server Authentication EKU. These certificates will be issued automatically by Entra ID using NDES and InTune as the RA.

1.4.1. PIXA Domain Controller KA

This certificate will be issued automatically by ADDS as the RA and will include EKU of Client Authentication, Server Authentication and Kerberos Authentication. These certificates will enable PIXA Domain Controllers to provide proof of identity, secure LDAP communications and Windows Hello for Business authentication.

1.4.1. PIXA Exchange Enrollment Agent

This certificate will be issued to the Network Device Enrollment Services servers at PIXA Services. The private key of these certificates will reside on an HSM. These certificates will entitle the NDES server to submit pre-approved certificate subscriptions to the CA based on information provided by Microsoft Entra and Intune.

1.4.1. PIXA CEP Encryption

This certificate will be issued to the Network Device Enrollment Services servers at PIXA Services. These certificates will be used by the Simple Certificate Enrollment Protocol to encrypt sessions between the NDES server and the subscriber.

1.4.1. PIXA Users

This certificate will be issued to subscriber users. This certificate is strictly for authentication to the PIXA Wireless network infrastructure.

1.4.2. Member Server

This certificate will be issued via Active Directory Domain Services as a an RA to member servers that require a Server Authentication certificate issued to their host and DNS names. Enrollment is filtered via computer membership to a specifically designated AD group.

1.4.3. Prohibited Certificate Uses

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not authorized

1.5. Policy Administration

The PIXA PKI Policy Group of the Policy Managing Authority at PIXA manages this CPS. Policy Managing Authority registers, observes the maintenance, and interprets this CPS. The PIXA PKI Policy Group makes available the operational conditions prevailing in the life-cycle management of certificates.

1.5.1. Organization Administering the Document

The PIXA PKI Policy Group is responsible for the maintenance of this CPS.

1.5.2. Contact Person

Contact Information is listed below:

PIXA PKI Policy Group
PIXA
info@pixa.ca

1.5.3. Person Determining CPS Suitability for the Policy

The PIXA PKI Policy Management Group determines the suitability of this CPS to the CP.

PIXA may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CPS.

New versions and publicized updates of PIXA policies are approved by the PIXA Policy Management Authority. The PIXA Policy Management Authority in its present organizational structure comprises of members as indicated below:

- At least one member of the management of PIXA PKI Policy Group.
- At least one authorized agent directly involved in the drafting and development of PIXA practices and policies.

Upon approval of a CPS update by the PIXA Policy Management Authority, that CPS is published in the PIXA online Repository at https://www.pixa.ca/pki. The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CPS is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the PIXA CPS. PIXA PKI Policy Group publishes on its web site at least the two latest versions of its CPS.

The PIXA PKI Policy Management Group reviews and approves any changes to the CPS that is compliant with this CP. Updates to CP or CPS documents SHALL be made available by publishing new versions at https://www.pixa.ca/pki.

1.6. Definitions and Acronyms

Upper Case terms and acronyms, not specified herein, are defined in the CA/B Forum's Baseline Requirements (BR) or the CA/B Forum's Code Signing Baseline Requirements and if not specified in the BR, are defined in the Network and Certificate System Security Requirements (the "NCSSRs").

1.6.1. Definitions

- Affiliate – A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
- Applicant – a natural person or Legal Entity that applies for (or seeks renewal of) a Certificate by a CA.
- Applicant Representative – A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.
- Application Software Supplier – A supplier of Internet browser software or other relying party application software that displays or uses Certificates and incorporates Root Certificates.
- Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
- Audit Report – A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
- Authorization Domain Name – The FQDN used to obtain authorization for certificate issuance for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "'*.*'" from the left-most portion of the Wildcard Domain Name to yield the FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.
- Authorized Port – One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh). • Base Domain Name – The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs

where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

- Baseline Requirements (BR) – An integrated set of technologies, protocols, identity proofing, lifecycle management, and auditing requirements issued by the CA/Browser Forum and available at cabforum.org.
- CAA – From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."
- CA/Browser Forum (CAB Forum) – A consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of digital certificates. Details are available at: cabforum.org. • Certificate - digital record that contains information such as the Subscriber's distinguished name and public key, and the signer's signature and data. • Certificate Application – a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate. • Certificate Management System: A system used by a CA of Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.
- Certificate Policy (CP) – A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements. • Certificate Request – an application for a new Certificate or a renewal of a Certificate. • Certificate Revocation List (CRL) – periodically published listing of all certificates that have been revoked for use by Relying Parties
- Certificate Signing Request (CSR) – a message sent to the certification authority containing the information required to issue a digital certificate • Certificate Systems: The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.
- Certification Authority (CA) – an entity or organization that is responsible for the authorization, issuance, revocation, and management of a certificate. The term equally applies to Roots CAs and Subordinate CAs.
- Certification Practice Statement (CPS) – One of several documents forming the governance framework in which Certificates are created, issued, managed, and

used. • Cross-Certified Subordinate CA Certificate – A certificate that is used to establish a trust relationship between two CAs.

- CSPRNG – A random number generator intended for use in cryptographic system.
- Delegated Third Party - A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
- Domain Authorization Document – Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
- Domain Contact – The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
- Domain Label – From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names. • Domain Name – An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
- Domain Namespace – The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
- Domain Name Registrant – Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
- Domain Name Registrar – A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns). © 2024 Microsoft Corporation Page 19 of 122 Microsoft PKI Services Certification Practice Statement (CPS) v3.2.4
- Distinguished Name (DN) – a globally unique identifier representing a Subject that is used on Certificates and in the Repository

- EV Certificate – A certificate that contains subject information specified and validated in accordance with the EV Guidelines.
- EV Certificate Beneficiaries – Persons to whom the CA and its Root CA make specified EV Certificate Warranties.
- EV Guidelines – Guidelines for the Issuance and Management of Extended Validation Certificates, as defined by the CA/Browser Forum.
- Extended Key Usage (EKU) – An extension in an X.509 certificate to indicate the allowed purpose(s) for the use of the public key. Also referenced or known as "Enhanced Key Usage".
- Fully-Qualified Domain Name (FQDN) – A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
- Government Entity – A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
- High Security Zone: A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.
- High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.
- IP Address – A 43-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
- Issuing CA – The first digital certificate issuing authority who issues certificates signed by the root certificate authority (CA).
- LDH Label – From RFC 5890 (http://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, it's total length must not exceed 63 octets."
- Legal Entity – An association, corporation, partnership, proprietorship, trust, or government entity that has legal standing in a country's legal system.
- PIXA PKI Authority – Combination of PIXA's Steering and Oversight Committees.
- Non-Reserved LDH Label – From RFC 5890 (hhtp://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '- -' in the third and fourth positions."
- Online CA (OCA) - a certification authority system which signs end-entity Subscriber Certificates that are operated and maintained in an online state so as to provide

continually available certificate signing services. Online CAs reside in segmented, secured, and functionally dedicated networks.

- P-Label – A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3942, Section 6.3) from the fifth and subsequent positions.
- Pending Prohibition – The use of a behavior described with this label is highly discouraged, as it is planned to be deprecated and will likely be designated as MUST NOT in the future.
- Private Key – The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- Public Key – The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- Public Key Infrastructure (PKI) – A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
- Random Value – A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
- Registration Authority (RA) – Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- Registration Identifier -- the unique code assigned to an Applicant by the Incorporating or Registration Agency in such entity's Jurisdiction of Incorporation or Registration.
- Reliable Data Source – An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
- Relying Party – a Relying Party is an individual or entity that acts in reliance on a Certificate or digital signature associated with a Certificate.
- Relying Party Agreement – an agreement which specifies the stipulations under which a person or organization acts as a Relying Party

- Repository – an online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- Request Token – A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
- Required Website Content – Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
- Reserved IP Address – An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: o [https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special registry.xhtml](https://www.iana.org/assignments/iana-ipv4-special-registry/iana ipv4-special-registry.xhtml) o [https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special registry.xhtml](https://www.iana.org/assignments/iana-ipv6-special-registry/iana ipv6-special-registry.xhtml)
- Root CA – The top-level CA whose root certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- Secure Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.
- Signing Service – an organization that signs an Object on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.
- Subject – The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- Subject Identity Information – Information that identifies the Certificate Subject. Identity Information does not include a Domain Name listed in the 'subjectAltName' extension or the Subject 'commonName' field.

- Subscriber – an individual or end-entity (person, device, or application) that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate
- Subscriber Agreement – an agreement containing the terms and conditions that the authorized Subscriber consented to for the use of their issued certificate, containing the private key and corresponding public key.
- Suspect Code - code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes.
- Takeover Attack - an attack where a Signing Service or Private Key associated with the Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.
- Technically Constrained Subordinate CA Certificate - a Subordinate CA certificate which uses a combination of Extended Key Usage or Name Constraint extensions, as defined within the relevant Certificate Profiles of this document, to limit the scope within which the Subordinate CA Certificate MAY issue Subscriber or additional Subordinate CA Certificates.
- Terms of Use – Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
- TimeStamp Authority – a service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via secure hashing algorithm) existed at the specific time. If the TimeStamp Authority is delegated to a third party, the CA is responsible that the delegated authority complies with the CAB Code Signing Requirements.
- Transport Layer Security (TLS)/Secure Socket Layer (SSL) – a security protocol that is widely used in the Internet, for the purpose of authentication and establishing secure sessions
- Trusted Role – An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over a Secure Zone or High Security Zone.
- Wildcard Certificate – A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.
- Wildcard Domain Name – A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

- XN-Label – From RFC 5890 (http://tools.ietf.org/html/rfc5890): “The class of labels that begin with the prefix “xn- -“ (case independent), but otherwise conform to the rules for LDH Labels.”

1.6.2. Acronyms

Term	Definition
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
DBA	Doing Business As
DNS	Domain Naming System
EKU	Extended Key Usage
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IM	Instant Messaging
ISO	International Organization for Standardization
NIST	(Us Government) National Institute of Standards of Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
TLS	Transport Layer Security
S/MIME	Secure MIME (Multipurpose Internet Mail Extension)
TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol

1.6.3. References

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

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

FIPS 186-4, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, July 2013.

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

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.

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

RFC3912, Request for Comments: 3912, WHOIS Protocol Specification, Daigle, September 2004.

RFC3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, et al. January 2005.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.

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

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

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

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

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

RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013. RFC7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, R. Fielding, J. Reschke. June 2014.

RFC7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect), J. Reschke. April 2015. RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format, Newton, et al, March 2015.

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

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

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

1.6.4. Conventions

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

2. Publication and Repository Responsibilities

2.1. Repositories

A public Repository of CA information and associated policy documents is located at https://www.pixa.ca/pki

2.2. Publication of Certification Information

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

This document SHALL not be used for the issuance and management of Publicly trusted TLS certificates and as such may not adhere to the BRs for public/web trust.

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

A web-based repository is available on a 24x7 basis to all Relying Parties who wish to access this CPS or other information from PIXA PKI Policy Group. The repository SHALL contain the current versions of this CPS and accompanying CP, a fingerprint of the established Root CAs, current CRLs, and other information relevant to Subscribers and Relying Parties.

The CA SHALL host internal test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates, specifically Client or Server Authentication certificates, that chain up to the PIXA PKI Policy Group's root CA. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are

i. valid,
ii. revoked, and
iii. expired.

2.3. Time or Frequency of Publication

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

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

New versions of this CPS and respective CP documents will become effective immediately for all participants listed in Section 1.3. The CA offers CRLs showing the revocation of Microsoft PKI Services Certificates and offers status checking through the online repository. CRLs will be published in accordance with Section 4.9.6 and Section 4.9.7.

2.4. Access Controls on Repositories

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

3. Identification and Authentication

3.1. Naming

3.1.1. Naming Convention

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

3.1.2. Acceptable Subscriber Names

For publication in its certificates PIXA PKI Policy Group accepts subscriber names that are meaningful and can be authenticated as required. Names will commonly be provided by PIXA's approved RAs but when provided manually will be submitted via approved Service Requests. Every approved request must be entered into the service catalog for the PKI service.

3.1.3. Pseudonyms

PIXA PKI Policy Group may allow the use of pseudonyms, reserving its right to disclose the identity of the subscriber as may be required by law or following a reasoned and legitimate request.

3.1.4. Registration, Authentication and Role Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Application or Certificate Request that infringe upon the intellectual property rights of entities outside of their authority.

3.2. Initial Identity Validation

The identification of the applicant for a certificate is carried out according to a documented procedure. This will typically be completed via the approved RAs but may also be completed via an approved Service Request where the approval process verifies identity.

3.2.1. Prove Access to Private Key

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

3.2.2. Authentication of Organization Identity

The Issuing CA SHALL verify the identity of the organization and authority of the Applicant to request Certificates on behalf of the organization, in accordance to procedures set forth in PIXA procedures which will include the use of RAs or the submission of a Service Request.

Requests containing wildcards (*) will be summarily denied.

3.2.3. Validation of Authority

Requests submitted outside of the authorized RA MUST be completed through the submission of a Service Request which will initiate the required authentication processes. Approval of the Service Request will constitute validation of identity and authority.

PIXA PKI Policy Group reserves the right to update registration procedures and subscriber submitted data to improve the identification and registration process.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

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

3.3.2. Identification and Authentication for Re-Key After Revocation

Revoked or Expired Certificates SHALL require a new enrollment. Applicants MUST submit a new Certificate Request and be subject to the same Identification and Authentication requirements as first-time Applicants, as specified in Section 6.1 of this CPS.

3.4. Identification and Authentication for Revocation Request

For the identification and authentication procedures of revocation requests, PIXA PKI Policy Group requires using an online authentication mechanism and/or a request addressed to the PIXA PKI Policy Group.

4. Certificate Life-cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Only employees of PIXA or devices managed by PIXA may submit an application for a Certificate. Contractors for PIXA may be granted special dispensation to submit applications as employees through the existence of user credentials within an approved RA.

Any applications by entities that are not employed by or managed by PIXA must have their application sponsored by an authorized PIXA employee. Approval for the submission will be granted or denied by the PIXA PKI Policy Group

4.1.2. Enrollment Process and Responsibilities

For enrollment not completed automatically via an approved RA, the CA SHALL obtain a Service Request from the applicant.

The applicant can submit an electronic CSR which will include the number of the approved Service Request as the OU field of the DN.

One Service Request is required for each certificate requested.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.1. Entities managed by PIXA

Users and Devices managed via PIXA Active Directory Domain Services or Entra ID as approved Registration Authorities will be identified and authorized based on authoritative information provided by the RA.

4.2.1. Un-managed Entities

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

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

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

Section 3.2 limits the validity period of Subscriber Certificates. PIXA PKI Policy Group MAY use the documents and data provided in Section 3.2.2 to verify certificate information, or may reuse previous validations themselves, provided that PIXA PKI Policy Group obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 10 business days prior to issuing the Certificate.

For validation of Domain Names according to Section 3.2.2.4 any reused data, document, or completed validation MUST be obtained no more than 10 business days prior to issuing the Certificate.

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

After the change to any validation method specified in the Baseline Requirements, PIXA PKI Policy Group may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in CP.

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

PIXA PKI Policy Group does not use Delegated Third Parties to fulfill any of the obligations under this section of the CP.

4.2.2. Approval or Rejection of Certificate Applications

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

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

- Applicant or Subscriber information is unable to be verified;
- The CA deems the certificate issuance MAY negatively impact the CA's business or reputation;
- Failure to consent to the Subscriber Agreement;
- Failure to provide an approved Service Request tracking number;
- Mismatches in submitted values as compared to the Service Request

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

Applications for subordinate CAs are not approved unless the CA in question will be operated by PIXA PKI Policy Group or one of its affiliates and will be governed by the CP and this or its own CPS.

PIXA PKI Policy Group does not issue certificates meant for public trust.

4.2.3. Time to Process Certificate Applications

Certification applications SHALL be processed within a PIXA Service Level Targets defined as:

-

The CA SHALL NOT be responsible for processing delays initiated by the Applicant or from events outside of the CA's control.

Commented [PM2]: Gimme an SLT or SLA this will fall under

4.2.4. Verification of DNS Records

As part of the issuance process, PIXA PKI Policy Group checks for a DNS record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 8659, following the processing instructions set down in RFC 8659 for any records found. This stipulation does not prevent PIXA PKI Policy Group from checking records at any other time.

Requests containing wildcards (*) in the DNS Subject Alternative Name will summarily be declined.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

All automated enrollment requests submitted through an approved RA will automatically be issued to the applicant. The applicant will install the certificate via the built-in mechanism provided by the RA.

For certificate requests not submitted via an approved RA, the following procedure will be followed:

i. The applicant submits or has an authorized individual submit on his behalf the required information in a Service Request. Information provided must include:
    a. e-mail address of applicant
    b. common name (device name)
    c. organizational information
    d. country code
    e. Subject Alternative Name information including all possible DNS names and the IP address of the requesting entity.

ii. The CA Hierarchy Public Key Certificates are installed in the proper stores on the applicant's device.
iii. If the device is a Microsoft Windows Device the applicant follows the steps in section 4.4.1
iv. If the device is not a Microsoft Windows Device:
    a. The applicant generates a certificate request using the appropriate software on the requesting device. The request must include information as described in the content section and the approved Service Ticket number as an OU field. The request must also include CertificationTemplate = "PIXA External Client Device".
    b. The certificate issued will be provided to the applicant after issuance is completed.
v. PIXA PKI Policy Group may positively verify the applicant.
vi. PIXA PKI Policy Group may issue the certificate to the applicant.
vii. Key Based Renewal: allowed.
viii. Revocation: allowed.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

Automatically issued certificates will not generate notification. For all manual issuance, the closure of an approved service ticket will signal issuance or denial of request. The PIXA PKI Policy Group will as part of that closure notify the requester of issuance or rejection.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

A Subscriber's/Applicant's, or Applicant Representative's receipt of a Certificate and subsequent use of the key pair and Certificate constitutes Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

Certificates SHALL be published in a database.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

PIXA has no requirements for this item.

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, or Applicant Representative, has agreed to the Subscriber agreement and accepted the Certificate.

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

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

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

4.5.2. Relying Party Public Key and Certificate Usage

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

4.6. Certificate Renewal

4.6.1. Circumstance for Certificate Renewal

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

4.6.2. Who May Request Renewal

Certificate renewals MAY be requested by the Subscriber or an authorized agent, as long as the renewal request meets the requirements set forth in this CP and the supporting and section 4.6.3 of this CPS.

4.6.3. Processing Certificate Renewal Requests

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

Renewal requests may use an existing valid certificate that has not been revoked and has the extended key use of client authentication.

Certificates issued automatically using authorized RAs will renew automatically using the mechanism provided by their respective RA.

4.6.4. Notification of New Certificate Issuance to Subscriber

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

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6. Publication of the Renewal Certificate by the CA

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

4.6.7. Notification of Certificate Issuance by the CA to other Entities

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

4.7. Certificate Re-Key

Issuing CAs SHALL treat certificate re-key requests identical to applications for new certificates and perform the same identity-proofing processes, as described in Section 3.2, and the same acceptance methods, as described in Section 4.4. Routine re-key of the issuing CA certificates SHALL be performed in accordance with the established Key Generation process of Section 6.1 in this CPS.

4.8. Certificate Modification

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

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

4.9.1. Reasons for Revoking a Subscriber Certificate

PIXA PKI Policy Group SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs (and PIXA PKI Policy Group gains actual knowledge of it):

1. The Subscriber requests in writing, without specifying a CRLreason, that the PIXA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies PIXA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. PIXA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. PIXA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);
5. PIXA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded)

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

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #4, superseded);
7. PIXA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. PIXA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
9. PIXA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
10. PIXA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
11. PIXA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
12. PIXA is made aware that the Certificate was not issued in accordance with PIXA's Certificate Policy or this Certification Practice Statement (CRLReason #4, superseded);
13. PIXA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. PIXA's right to issue Certificates expires or is revoked or terminated, unless PIXA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. Revocation is required by PIXA's Certificate Policy or this Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1. Reasons for Revoking a Subordinate CA Certificate

A Subordinate CA Certificate SHALL be revoked within seven (7) days if one or more of the circumstances in Section 4.9.1.1 occur.

4.9.2. Who Can Request Revocation

Certificate revocations MAY be requested from the authorized Subscribers, RAs,the CA or more of the circumstances in 4.9.1.1 occur that suggests reasonable cause to revoke the certificate.

4.9.3. Procedure for Revocation Request

The CA MAY process revocation requests using at least the following steps:

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

CA SHALL maintain a 24x7 availability to internally respond to any high priority revocation requests. If appropriate, CA MAY forward complaints to law enforcement. Instructions for requesting a revocation:

- PIXA PKI Policy Group provides revocation request instructions directly to subscribers.
- For everyone else please contact via email at info@pixa.ca.

Please refer to Section 1.5.2 for other information on contacting PIXA PKI Policy Group.

4.9.3. Revocation Reason Codes

Subscribers and Relying Parties are required to select the appropriate reason code.

4.9.3.1.1. Reason Codes

- **keyCompromise (RFC 5280, CRLReason #1)** This reason code is used if either of the following applies:
    1. The Subscriber requests revocation for this revocation reason;
    2. PIXA PKI Policy Group obtains verifiable evidence that the certificate subscriber's private key corresponding to the public key in the certificate suffered a key compromise (as outlined in Section 4.9.12).
    3. There is a demonstrated or proven method that exposes the Subscriber's private key to a key compromise;
    4. Anyone requesting revocation for key Compromise has previously demonstrated or can currently demonstrate possession of the private key of the certificate;
    5. There is clear evidence that that the specific method used to generate the private key was flawed; or
    6. There is a demonstrated or proven method that can easily compute the certificate subscriber's private key based on the public key in the certificate (e.g Debian weak key).
- **cessationOfOperation (RFC 5280, CRLReason #5)** This reason code is used if either of the following applies:
    1. The Subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate;
    2. The Subscriber will no longer be using the certificate because they are discontinuing their website; or
    3. There are circumstances indicating that use of a fully qualified domain name in the certificate is no longer legally permitted.
- **affiliationChanged (RFC 5280, CRLReason #3)** This reason code is used if:
    1. The subject's name or other subject identity information in the certificate has changed, but there is no cause to suspect that the certificate's private key has been compromised.
- **Superseded (RFC 5280, CRLReason #4)** This reason code is used if either of the following applies:
    1. The Subscriber requests revocation for this revocation reason;
    2. The Subscriber has requested a new certificate to replace an existing certificate;
    3. There is reasonable evidence that the validation of domain authorization or control for any fully qualified domain name in the certificate should not be relied upon; or

4. The certificate does not comply with a relevant root program policy, the CA/Browsers Forum's Baseline Requirements, or PIXA PKI Policy Group's CP or CPS.

- **No Reason Code** No reason code is included for revocation where none of the reasons in this section apply. If the certificate is revoked for a reason not listed in 4.9.3.1.1 or 4.9.3.1.2 the reasonCode extension MUST NOT be provided in the CRL.
- **Multiple Revocation** If the situation is that multiple revocation reasons apply, the revocation reason of higher priority (as per this priority list) should be indicated.
    1. keyCompromise (RFC 5280, CRLReason #1)
    2. privilegeWithdrawn (RFC 5280, CR Reason #9)
    3. cessationOfOperation (RFC 5280, CRLReason #5)
    4. affiliationChanged (RFC 5280, CRLReason #3)
    5. superseded (RFC 5280, CRLReason #4)

4.9.4. Revocation Request Grace Period

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

4.9.5. Time Within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, PIXA PKI Policy Group SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report. After reviewing the facts and circumstances, PIXA PKI Policy Group SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether the certificate will be revoked, and if so, a date on which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by PIXA PKI Policy Group will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a

complaint from a consumer alleging that they didn't receive the goods they ordered); and

5. Relevant legislation.

4.9.6. Revocation Checking Requirements for Relying Parties

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

4.9.7. CRL Issuance Frequency

The CA SHALL post new CRL entries, as soon as a revocation request is fulfilled.

Subscriber Certificate CRLs SHALL be updated and issued at least once every seven (2) days and record the date and time of the transaction in the CRL's ThisUpdate field. The CRL's NextUpdate field value identifies the point in time when the CRL expires and MUST NOT be more than ten (4) days after the value of the ThisUpdate field. CRLs for Root CA Certificates SHALL be updated and issued at least once every twelve (6) months, within 24 hours after revoking a Subordinate CA Certificate, and the CRL's NextUpdate field value MUST NOT be more than twelve (6) months after the value of the ThisUpdate field. Upon expiration of certain CAs a final CRL MAY be published that has a NextUpdate value that exceeds the time parameters noted elsewhere in this section.

4.10. Certificate Status Service

4.10.1. Certificate Status Service

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

4.10.2. Service Availability

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

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

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

4.11. End of Subscription

Certificate Subscriptions end when the certificate has either been revoked or expires. PIXA PKI Policy Group will not be responsible for the recovery of expired public/private key pairs.

5. Facility, Management and Operational Controls

Commented [PM3]: Major documentation here, and I'm not sure I can complete it as it's very much on premises stuff I can't see or speak to!

PIXA PKI Policy Group SHALL develop, implement, and maintain a comprehensive security program designed to:

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

The Certificate Management Process MUST include:

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

PIXA PKI Policy Group's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Microsoft PKI Services has in place to counter such threats.

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

5.1. Physical Security Controls

5.1.1. Site Location

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

5.1.2. Physical Access

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

Facility security systems electronically log ingress and egress of authorized personnel. Physical access to cryptographic systems, hardware, and activation materials are restricted by multiple access control mechanisms, which are logged, monitored, and video recorded on a 24x7 basis.

5.1.3. Power and Air Conditioning

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

5.1.4. Water Exposures

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

5.1.5. Fire Prevention and Protection

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

5.1.6. Media StorageT

Commented [PM4]: His one is relevant as we are storing the root on external drives

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

5.1.7. Waste Disposal

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

5.1.8. Off-Site Backup

Commented [PM5]: Is one of the external drives going off site?

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

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted Roles consist of vetted and approved employees, contractors, or consultants that require access to or control over the CA's PKI operations. Trusted Role positions are subject to a clearly defined set of responsibilities that maintain a strict multi- person control; such that, no single person is able to perform both validation duties and certificate issuance fulfillment without a secondary review by another "trusted" team member.

The personnel considered for Trusted Role positions MUST successfully pass the screening and training requirements of CPS Section 5.3. Trusted Role positions MAY include, but are not limited to, system administrators, operators, engineers, and certain executives who are designated to oversee CA operations.

5.2.2. Number of Persons Required per Task

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

5.2.3. Identification and Authentication for Each Role

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

5.2.4. Maximum Latency for CRLs

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

5.2.5. Roles Requiring Separation of Duties

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

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

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

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

5.3.2. Background Check Procedures

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

5.3.3. Training Requirements

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

PIXA PKI Policy Group SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

PIXA PKI Policy Group SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the PIXA training regimens.

Personnel in a Trusted Role SHALL comply with PIXA training standards.

5.3.4. Retraining Frequency and Requirements

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

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

5.3.5. Job Rotation Frequency and Sequence

PIXA has no requirements for this item.

5.3.6. Sanctions for Unauthorized Actions

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

5.3.7. Independent Contractor Requirements

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

5.3.8. Documentation Supplied to Personnel

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

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

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

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

PIXA PKI Policy Group SHALL record at least the following events:

1. CA certificate and key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction;
    b. Certificate requests, renewal, and re-key requests, and revocation;
    c. Approval and rejection of certificate requests;
    d. Cryptographic device lifecycle management events;
    e. Generation of Certificate Revocation Lists;
    f. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. PIXA PKI Policy Group Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in the Baseline Requirements and the CA's Certification Practice Statement;
    c. Approval and rejection of certificate requests;
    d. Issuance of Certificates; and
    e. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. Installation, update and removal of software on a Certificate System;
    e. System crashes, hardware failures, and other anomalies;
    f. Firewall and router activities;
    g. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

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

5.4.2. Frequency of Processing Log

Audit logs are reviewed on an as-needed basis.

5.4.3. Retention Period for Audit Log

PIXA PKI Policy Group SHALL retain, for the duration defined by PIXA Data Retention Policy or a minimum of 2 years after the following conditions:

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

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

5.4.4. Protection of Audit Log

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

5.4.5. Audit Log Backup Procedures

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

5.4.6. Audit Collection System

PIXA has no requirements for this item.

5.4.7. Notification to Event-Causing Subject

PIXA has no requirements for this item.

5.4.8. Vulnerability Assessments

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

Vulnerability assessments and penetration testing on the CA environment SHALL at least be performed annually.

5.5. Records Archival

5.5.1. Types of Records Archived

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

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

- Systems management and change control activities

5.5.2. Retention Period for Archive

PIXA PKI Policy Group SHALL retain, for the duration defined by PIXA Data Retention Policy or a minimum of 2 years after the certificate ceases to be valid.

5.5.3. Protection of Archive

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

5.5.4. Archive Backup Procedures

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

5.5.5. Requirements for Time-Stamping of Records

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

5.5.6. Archive Collection System (Internal or External)

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

5.5.7. Procedures to Obtain and Verify Archive Information

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

5.6. Key Changeover

PIXA has no requirements for this item.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

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

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

See Section 5.7.4.

5.7.3. Entity Private Key Compromise Procedures

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

5.7.4. Business Continuity Capabilities After a Disaster

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

5.8. CA or RA Termination

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

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1. CA Key Pair Generation

For CA Key Pairs that are either:

1. used as a CA Key Pair for a Root Certificate or
2. used as a CA Key Pair for a Subordinate CA Certificate

PIXA PKI Policy Group SHALL:

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

In all cases, PIXA PKI Policy Group SHALL:

1. generate the CA Key Pair in a physically secured environment as described in this Certification Practice Statement;
2. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
3. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in this Certification Practice Statement;
4. log its CA Key Pair generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this Certification Practice Statement and (if applicable) its Key Generation Script.

6.1.1. RA Key Pair Generation

PIXA PKI Policy Group will generate a key pair for the RA certificate issued to the NDES service on appropriate cryptographic modules.

6.1.1. Subscriber Key Pair Generation

PIXA PKI Policy Group SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. PIXA PKI Policy Group is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. PIXA PKI Policy Group has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
5. PIXA PKI Policy Group is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

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

6.1.2. Private Key Delivery to Subscriber

If a Subscriber generates their own key pairs, Private Key delivery is not performed.

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

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

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

6.1.3. Public Key Delivery to Certificate Issuer

PIXA has PIXA has no requirements for this item.

6.1.4. CA Public Key Delivery to Relying Parties

PIXA has PIXA has no requirements for this item.

6.1.5. Key Sizes

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

Root CA and Subordinate CAs

Key Algorithm	Values
Digest Algorithm	SHA-512
Minimum RSA Modulus Size (bits)	4096
ECC Curve	NIST P-256, P-384, P-521

Subscriber

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

Digital Signature Algorithm (DSA) key lengths (L and N) are described in the Digital Signature Standard, FIPS 186-5 (https://csrc.nist.gov/publications/detail/fips/186/5/final).

6.1.6. Public Key Parameters Generation and Quality Checking

PIXA PKI Policy Group SHALL generate Private Keys using secure algorithms and parameters based on current research and industry standards.

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

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

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

6.2. Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1. Cryptographic Module Standards and Controls

Online CA key pairs are generated and protected by validated FIPS 140-2 level 3 hardware cryptographic modules that meet industry standards for random number and prime number generation. The Timestamp Authority protects its signing key using a process that is at least to FIPS 140-2 Level 3, Common Criteria EAL4+ (ALC, FLR2), or higher.

Offline CA key pairs reside within the CA and SHALL remain air gapped for the duration of its lifetime. Any access to Offline key pairs must adhere to the controls described in section 6.2.2.

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

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

6.2.3. Private Key Escrow

PIXA has no requirements for this item.

6.2.4. Private Key Backup

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

6.2.5. Private Key Archival

PIXA will not participate in private key archival.

6.2.6. Private Key Transfer into or from a Cryptographic Module

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

6.2.7. Private Key Storage on Cryptographic Module

See section 6.2.1

6.2.8. Method of Activating Private Key

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

Commented [PM6]: To be modified once I see the HSM process as we want to ensure that connecting to the private key from another systems isn't too easy!

6.2.9. Method of Deactivating Private Key

PIXA has no requirements for this item.

6.2.10. Method of Destroying Private Key

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

6.2.11. Cryptographic Module Rating

See Section 6.2.1

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

For Certificates issued after the publication of this CPS, the following key and certificate operational periods SHALL be deployed. (See Section 7.1.2.1.1 for additional Root CA Validity restrictions)

Entity Type	Minimum – notBefore	Maximum – NotBefore	Minimum – not after	Maximum – not After
Root Cas	One day prior to the time of signing	The time of signing	4 years	8 years
Online Subordinate Cas	One day prior to the time of signing; or for Cross-Certified the earlier of one day prior to the time of signing or the earliest notBefore date of the existing CA Certificate(s)	The time of signing	The time of signing	4 years
Subscriber	A value within 48 hours of the signing operation.	The time of signing	The time of Signing	1 year

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

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

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

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

6.6. Life Cycle Technical Controls

PIXA has no requirements for this item.

6.7. Network Security Controls

CA systems SHALL reside in highly segmented networks constrained from both the Internet and corporate networks via multiple levels of firewalls.

Interaction with outside entities shall only be performed with servers located in a demilitarized zone (DMZ). All networks associated with CA operations SHALL be monitored by a network intrusion detection system. All systems associated with CA activities shall be hardened with services restricted to only those necessary for CA operations. Changes SHALL be documented and approved via a change management system. Logical and physical access to CA systems and facilities requires two trusted and qualified Microsoft employees.

6.8. Time Stamping

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

7. Certificate and CRL Profiles

7.1. Certificate Profile

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

7.1.1. Version Number(s)

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

7.1.2. Certificate Extensions

PIXA PKI Policy Group asserts compliance with the requirements of PIXA for internal certificate issuance. All certificates issued MUST comply with one of the following certificate profiles, which incorporate, and are derived from RFC 5280 (https://datatracker.ietf.org/doc/html/rfc5280). Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by this document.

- CA Certificates
    - Root CA Certificate Profile
    - Subordinate CA Certificates

7.1.2. Root CA Certificate Profile

Requirements for NL Heath Root CA certificates are as follows:

Version

Must be v3(2)

Serial Number

MUST be non-sequential number greater than zero (0) and less than 2159 containing at least 64 bits of output from a CSPRNG.

Signature

All objects signed by a CA Private Key MUST conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier - derived type in the context of signatures. In particular, it applies to all of the following objects and fields: The signatureAlgorithm field of a Certificate.

Issuer

Encoded value MUST be byte-for-byte identical to the encoded subject (Self-Signed).

Validity

See Section 6.3.2.

Subject

The subject will contain the following:

- countryName – the two-letter ISO 3166-1 country Code representing the Country of Canada (CA).
- organizationName – All variances of the legal entity names of PIXA.
- commonName – An identifier for the certificate such that the certificate's name is unique across all certificates issued and clearly identifiable as belonging to PIXA.

SubjectPublicKeyInfo

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

- RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL. RSASSA-PKCS1-v1_5 with SHA-512: Encoding: 300d06092a864886f70d01010d0500.

The following extensions MUST be PRESENT with the identified values. Any values not identified in the CPS SHALL NOT be PRESENT.

basicConstraints

- The cA field must be set to true.
- The PathLenConstraint MUST be set to 2

keyUsage

- digitalSignature
- keyCertSign
- cRLSign

subjectKeyIdentifier

The subjectKeyIdentifier MUST be set as defined within RFC5280 section 4.2.1.2. The subjectKeyIdenfier SHALL be unique within the scope of all Certificates it has issued for each unique public key (the subjectPublicKeyInfo field of the Root Certificate).

certificatePolicies

1.3.6.1.4.1.64104.2.1

7.1.2. Subordinate CA Certificate Profile

Requirements for NL Heath Subordinate CA certificates are as follows:

Version

Must be v3(2)

Serial Number

MUST be non-sequential number greater than zero (0) and less than 2159 containing at least 64 bits of output from a CSPRNG.

Signature

All objects signed by a CA Private Key MUST conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier - derived type in the context of signatures. In particular, it applies to all of the following objects and fields: The signatureAlgorithm field of a Certificate.

Issuer

Encoded value MUST be byte-for-byte identical to the encoded subject of the Issuing CA.

Validity

See Section 6.3.2.

Subject

The subject will contain the following:

- countryName – the two-letter ISO 3166-1 country Code representing the Country of Canada (CA).
- organizationName – All variances of the legal entity names of PIXA.
- commonName – An identifier for the certificate such that the certificate's name is unique across all certificates issued and clearly identifiable as belonging to PIXA.

SubjectPublicKeyInfo

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

- RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL. RSASSA-PKCS1-v1_5 with SHA-512: Encoding: 300d06092a864886f70d01010d0500.

The following extensions MUST be PRESENT with the identified values. Any values not identified in the CPS SHALL NOT be PRESENT.

basicConstraints

- The cA field must be set to true.
- The PathLenConstraint MUST be set to 1

keyUsage

- digitalSignature
- keyCertSign
- cRLSign

subjectKeyIdentifier

The subjectKeyIdentifier MUST be set as defined within RFC5280 section 4.2.1.2. The subjectKeyIdenfier SHALL be unique within the scope of all Certificates it has issued for each unique public key (the subjectPublicKeyInfo field of the Subordinate CA Certificate).

certificatePolicies

1.3.6.1.4.1.64104.2.1

The following extensions MUST be PRESENT with the identified values. Any values not identified in the CPS SHALL NOT be PRESENT.

authorityKeyIdentifier

MUST be present. MUST be identical to the subjectKeyIdentifier field of the Issuing CA.

crlDistributionPoints

See section 7.1.3

authorityInformationAccess

See section 7.1.4

7.1.2. Subscriber Certificate Profile

Field	Description
Version	MUST be v3(2)
SerialNumber	MUST be non-sequential number greater than zero (0) and less than 2159 containing at least 64 bits of output from a CSPRNG.

Issuer	MUST be identical to the subject field of the Issuing CA.
Validity	See Section 6.3.2
Issuer Unique ID	MUST NOT be present
Subject Unique ID	Must NOT be present
Signature Algorithm Signature	Encoded value MUST be byte-for-byte identical to the Certificate.signature.
crlDistributionPoints	See Section 7.1.3
authorityInformationAccess	See Section 7.1.4

Certificate Naming MUST include in its subject:

Common Name – samAccountName of the device subscribing to a certificate profile.

For manually subscribed certificates, certificate naming MUST also include:

Organizational Unit – Service Request number of the approved service request for certificate enrollment. The Service Request must include all information that will be included in the Certificate Name and Subject Alternative Name of the Certificate.

For manually subscribed certificates, certificate naming MAY include Subject Alternative Names:

DNS - All requested DNS names as approved in the Service Request.

IP Address – The IP address of the subscriber.

7.1.2.3.1. PIXA Web Server

Subscribers must submit a Service Request that includes:

- Common Name: the hostname of the system where the Certificate will be installed
- Subject Alternative Names:
  - IP Address
  - DNS name(s)

The corresponding certificate request can be submitted directly to the OCA or via an REQ file generated on the requesting device. The REQ file must contain the Service Request number as part of the DN under the OU field.

The identity of the certificate-holder is confirmed via the approval process of the Service Request and the request will then be actioned by the PIXA PKI Policy Group. Once the certificate has been issued (or declined), the applicant will be notified by the PIXA PKI Policy Group.

The issuing procedure for a PIXA Web Server certificate is as follows:

i. The device is added to the appropriate Active Directory Domain Services global security group that grants enroll permissions on the template.
ii. The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
iii. The applicant follows the registration procedure.
iv. The applicant submits the required information including technical contact and server information.
v. The applicant accepts the subscriber agreement.
vi. PIXA PKI Policy Group verifies the submitted information by checking service ownership or domain right to use and any other information as it sees fit.
vii. PIXA PKI Policy Group may positively verify the applicant.
viii. PIXA PKI Policy Group may issue the certificate to the applicant.
ix. PIXA PKI Policy Group may publish the issued certificate in an online database
x. Renewal: allowed
xi. Revocation: allowed

PIXA might apply variations of this procedure to meet service, standards or legal requirements.

7.1.2.3.2. PIXA Web Server PKE

This Private Key Exportable (PKE) version of the Web Server Certificate will only be issued on proof of a specific requirement for the functionality.

Subscribers must submit a Service Request that includes:

- Common Name: the hostname of the system where the Certificate will be installed
- Subject Alternative Names:
  - IP Address
  - DNS name(s)

The corresponding certificate request can be submitted directly to the OCA or via an REQ file generated on the requesting device. The REQ file must contain the Service Request number as part of the DN under the OU field.

The identity of the certificate-holder and the requirement for an exportable private key is confirmed via the approval process of the Service Request and the request will then be actioned by the PIXA PKI Policy Group.

Once the certificate has been issued (or declined), the applicant will be notified by the PIXA PKI Policy Group.

The issuing procedure for a PIXA Web Server certificate is as follows:

i. The device is added to the appropriate Active Directory Domain Services global security group that grants enroll permissions on the template.
ii. The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
iii. The applicant follows the registration procedure.
iv. The applicant submits the required information including technical contact and server information.
v. PIXA PKI Policy Group verifies the submitted information by checking service ownership or domain right to use and any other information as it sees fit.
vi. PIXA PKI Policy Group may positively verify the applicant.
vii. PIXA PKI Policy Group may issue the certificate to the applicant.
viii. PIXA PKI Policy Group may publish the issued certificate in an online database
ix. Renewal: allowed
x. Revocation: allowed

PIXA might apply variations of this procedure to meet service, standards or legal requirements.

7.1.2.3.3. PIXA Client Device

This certificate Profile is for all client devices managed by Active Directory Domain Services as the approved Registration Authority. Subscribers will be instructed via Policy to automatically enroll into these certificates.

7.1.2.3.4. PIXA External Client Device

Subscribers must submit a Service Request that includes:

- Common Name: the hostname of the system where the Certificate will be installed
- Subject Alternative Names:
  - IP Address
  - DNS name(s)

The corresponding certificate request will be submitted using the Certificate Enrollment Policy Service. The request must contain the Service Request number as part of the DN under the OU field.

Once the certificate has been issued (or declined), the applicant will be notified by the PIXA PKI Policy Group.

The issuing procedure for a PIXA External Client certificate is as follows:

i. The applicant's user object is added to the appropriate Active Directory Domain Services global security group that grants enroll permissions on the template.
ii. The applicant creates a request containing all required information using the built-in Microsoft console.
iii. PIXA PKI Policy Group verifies the submitted information by checking service ownership or domain right to use and any other information as it sees fit.
iv. PIXA PKI Policy Group may positively verify the applicant.
v. PIXA PKI Policy Group may issue the certificate to the applicant.
vi. PIXA PKI Policy Group may publish the issued certificate in an online database
vii. Key Based Renewal: allowed
viii. Revocation: allowed

PIXA might apply variations of this procedure to meet service, standards or legal requirements.

7.1.2.3.5. PIXA MDM Client Device

This certificate Profile is for all client devices managed by Microsoft InTune and Microsoft Entra as the approved Registration Authority. Subscribers will be instructed via Policy to automatically enroll into these certificates.

7.1.2.3.6. PIXA Domain Controller KA

This certificate Profile is for Domain Controllers managed by Active Directory Domain Services as the approved Registration Authority. Subscribers will be instructed via Policy to automatically enroll into these certificates.

7.1.3. CRL Distribution Points

The CRL Distribution Points extension MUST be present in:

- Subordinate CA Certificates; and
- Subscriber Certificates that

- do not qualify as “Short-lived Subscriber Certificates” and
- do not include an Authority Information Access extension with an id-ad-ocsp accessMethod.

The CRL Distribution Points extension SHOULD NOT be present in:

- Root CA Certificates.

The CRL Distribution Points extension is OPTIONAL in:

- Short-lived Subscriber Certificates.

When present, the CRL Distribution Points extension MUST contain at least two DistributionPointNames. The DistributionPointNames MUST be a fullname formatted as type of uniform Resource Identifier and the scheme MUST be HTTP. The GeneralName of the DistributionPointNames must contain the HTTP URL of the Issuing CA’s CRL service for this certificate.

7.1.3. CRL Profile

All CRLs issued MUST comply with the following CRL profile, which incorporates, and is derived from RFC 5280. A full and complete CRL is a CRL whose scope includes all Certificates issued by the CA. A partitioned CRL (sometimes referred to as a “sharded CRL”) is a CRL with a constrained scope, such as all Certificates issued by the CA during a certain period of time (“temporal sharding”). Aside from the presence of the Issuing Distribution Point extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile. Minimally PIXA PKI Policy Group MUST issue either a “full and complete” CRL or a set of “partitioned” CRLs which cover the complete set of Certificates issued by the CA. In other words, if issuing only partitioned CRLs, the combined scope of those CRLs must be equivalent to that of a full and complete CRL. See section 4.9 for CRL reason codes.

7.1.4. Authority Information Access

If present, the AuthorityInfoAccessSyntax MUST contain one or more AccessDescriptions. Each AccessDescription MUST only contain a permitted accessMethod, as detailed below, and each accessLocation MUST be encoded as the specified GeneralName type.

The AuthorityInfoAccessSyntax MAY contain multiple AccessDescriptions with the same accessMethod, if permitted for that accessMethod. When multiple AccessDescriptions are present with the same accessMethod, each accessLocation MUST be unique, and each AccessDescription MUST be ordered in priority for that accessMethod, with the most

preferred accessLocation being the first AccessDescription. No ordering requirements are given for AccessDescriptions that contain different accessMethods, provided that previous requirement is satisfied.

All Access Methods at PIXA will present an HTTP URL of the Issuing CA's certificate.

8. Compliance Audit and Other Assessments

PIXA PKI Policy Group SHALL at all times:

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

Commented [PM7]: In the PKI world this means: **It means the CA must be authorized by the organization that operates the PKI.**
In other words, a CA must not simply start issuing certificates on its own. It must be:
- **Formally approved** by the PKI governance body
- **Recognized as a CA** within the trust hierarchy
- **Issued a CA certificate** by a parent CA (or be a self-signed root)
- **Operating under documented policies** (CP/CPS)

This aligns with the RFC's broader theme of ensuring that CAs operate under **controlled, accountable, and auditable** conditions.

8.1. Frequency and Circumstances of Assessment

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with Section 7, as well as audited in line with Section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate. The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4, then no pre-issuance readiness assessment is necessary.

8.2. Identity/Qualifications of Assessor

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

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);

3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;

8.3. Assessor's Relationship to Assessed Entity

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

8.4. Topics Covered by Assessment

TBD (see MS ADCS Assessment ToC)

8.5. Actions Taken as a Result of Deficiency

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

8.6. Communication of Results

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

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

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certified Subordinate CA Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date;

9. Other Business and Legal Matters

9.1. Fees

PIXA does not charge Subscriber fees for internal certificate issuance, renewals, access and or revocation or Status Information.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Any insurance requirements fall under PIXA existing general liability and professional liability insurance and existing policy limits.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

Sensitive PKI Services information shall remain confidential to PIXA PKI Policy Group. The following information is considered confidential to PIXA PKI Policy Group and may not be disclosed:

- PIXA PKI Policy Group policies, procedures and technical documentation supporting this CPS;
- Subscriber registration records, including: Certificate applications, whether approved or rejected, proof of identification documentation and details;
- Certificate information collected as part of the registration records, beyond that which is required to be included in Subscriber Certificates;
- Audit trail records;
- Any Private Key within the PIXA PKI Policy Group CA hierarchy.

9.3.2. Information Not Within the Scope of Confidential Information

This CPS, Certificates and CRLs issued by PIXA PKI Policy Group and any information that the CA has explicitly authorized to disclose are not considered confidential. PIXA may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to PIXA a license to do so, including the right to modify the aggregated Subscriber information

and to permit third parties to perform such functions on its behalf. This Section 9.3.2 is subject to applicable privacy laws.

9.3.3. Responsibility to Protect Confidential Information

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

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

PIXA follows the governing principles established by the PIXA privacy statement located at (https://www.pixa.ca/documentation) when handling personal information.

9.4.2. Information Treated as Private

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

9.4.3. Information Not Deemed Private

See Section 9.3.2

9.4.4. Responsibility to Protect Private Information

See section 9.3.3.

9.4.5. Notice and Consent to use Private Information

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

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

PIXA PKI Policy Group shall be entitled to disclose Confidential/Private Information if, in good faith, PIXA PKI Policy Group 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 PIXA:

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

This Certificate Policy (CP) incorporates material derived from the *Microsoft PKI Services CPS* Version 3.2.4, published July 21, 2024. The Microsoft document is licensed under the Creative Commons Attribution–NoDerivatives 4.0 International License (CC BY-ND 4.0). PIXA retains all intellectual property rights in and to this adapted CP, which is specific to PIXA and includes additional original material.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

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

1. The Subscriber that is a party to the Subscriber Agreement for the Certificate;
2. All Relying Parties who reasonably rely on a Valid Certificate. PIXA PKI Policy Group represents and warrants to the Certificate Beneficiaries, during the period when the Certificate is valid, the CA has complied, in all material aspects and to the best of its knowledge with the CP or CPS in issuing and managing the Certificate.

The certificate warranties specifically include the following:

1. Right to Use Domain Name or IP Address: That, at the time of issuance, PIXA PKI Policy Group

a. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Service Name, Domain, and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
b. followed the procedure when issuing the Certificate; and
c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;

2. Authorization for Certificate: That, at the time of issuance, PIXA PKI Policy Group
a. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
b. followed the procedure when issuing the Certificate; and
c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
3. Accuracy of Information: That, at the time of issuance, PIXA PKI Policy Group
a. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate;
b. followed the procedure when issuing the Certificate; and c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
4. Identity of Applicant: That, if the Certificate contains Subject Identity Information, PIXA PKI Policy Group
a. implemented a procedure to verify the identity of the Applicant in accordance with the CP/CPS Section 3.2 and CP/CPS Section 7.1.4.2.2;
b. followed the procedure when issuing the Certificate; and
c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
5. Subscriber Agreement: That, if PIXA PKI Policy Group and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Subscriber Agreement/Terms of Use;
6. Status: That PIXA PKI Policy Group maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (revoked) of all unexpired Certificates; and

7. Revocation: That the CA will revoke the Certificate for any of the reasons specified in this CP or accompanying CPS, but only to the extent the CA gains actual, undisputed knowledge that one of these reasons has arisen.

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

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

9.6.2. RA Representations and Warranties

PIXA authorizes its on premises Microsoft Active Directory Domain Services and Entra ID (via InTune and NDES) to act as Registration Authorities.

9.6.3. Subscriber Representation and Warranties

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

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

1. The Applicant's agreement to the Subscriber Agreement with the CA, or

2. The Applicant's acknowledgement of the Terms of Use.

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

PIXA PKI Policy Group MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that

the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

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

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. Reporting and Revocation: An obligation and warranty to:
   (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
   (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that

the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.7. Disclaimers of Warranties

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

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

9.8. Limitations of Liability

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

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

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE A CERTIFICATE, INCLUDING AS A RESULT OF (I) ANY TERMINATION OR SUSPENSION OF THIS AGREEMENT OR THE CPS OR REVOCATION OF A CERTIFICATE, (II) OUR DISCONTINUATION OF ANY OR ALL SERVICE OFFERINGS IN CONNECTION WITH THIS AGREEMENT, OR, (III) ANY DOWNTIME OF ALL OR A PORTION OF CERTIFICATE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE CONTENT OF ANY CERTIFICATE (INCLUDING ANY ALLEGEDLY ERRONEOUS CONTENT) OR YOUR RELIANCE ON SUCH CONTENT; (C) THE PROCESS OF ISSUING, REPORTING THE STATUS OF, OR REVOKING ANY CERTIFICATE (INCLUDING ANY ALLEGEDLY FLAWED PROCESS) OR YOUR RELIANCE ON SUCH PROCESS; (D) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (E) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO MICROSOFT'S CERTIFICATE SERVICES; OR (F) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, MICROSOFT AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IN CONNECTION WITH THIS AGREEMENT AND ALL CERTIFICATES ISSUED HEREUNDER, IS LIMITED TO DIRECT DAMAGES INCURRED IN REASONABLE RELIANCE IN AN AMOUNT NOT EXCEEDING THE LESSER OF THE AMOUNT PAID BY YOU FOR THE CERTIFICATE(S) AT ISSUE OR THE AMOUNTS PAID FOR THE CERTIFICATE SERVICES FOR THE CERTIFICATE(S) AT ISSUE IN THE LAST TWELVE (12) MONTHS BEFORE THE CLAIM AROSE (UNLESS THE FOREGOING AMOUNT IS ZERO, IN WHICH CASE SUCH DIRECT DAMAGES LIMIT WILL BE DEEMED TO BE FIVE U.S. DOLLARS).

9.9. Indemnities

Subscribers to PIXA PKI Policy Group PKI do not assume any obligation or potential liability of the CA.

9.10. Term and Termination

9.10.1. Term

This CPS becomes effective upon publication in the Repository.

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

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

9.11. Individual Notices and Communications with Participants

Any notice, demand, or request pertaining to this CPS shall be communicated either using digitally signed messages consistent with this CPS, or in writing. PIXA accepts notices related to this CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from PIXA. If an acknowledgement of receipt is not received within five days, the sender MUST resend the notice in Service Request form. PIXA MAY allow other forms of notice in its Subscriber Agreements.

9.12. Amendments

9.12.1. Procedure for Amendment

Amendments to this CP MAY be made by the PIXA and SHALL be approved by the PIXA PKI Policy Group, as per Section 1.5.4.

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 PIXA PKI Policy Group regarding the dispute.

PIXA PKI Policy Authority will involve the appropriate PIXA personnel to resolve the dispute.

9.14. Governing Law

The Laws of Newfoundland and Labrador govern the interpretation, construction and enforcement of this CPS.

9.15. Compliance With Applicable Law

See section 9.14

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

PIXA has no requirements.

9.16.2. Assignment

PIXA has no requirements.

9.16.3. Severability

In the event of a conflict between this CPS or accompanying CP and a law, regulation, or government order (hereinafter 'Law') of any jurisdiction in which PIXA PKI Policy Group operates or issues certificates, PIXA PKI Policy Group MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law.

In such an event, PIXA PKI Policy Group SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of PIXA PKI Policy Group's CPS or CP a detailed reference to the Law requiring a modification of CP or CPS implemented by PIXA PKI Policy Group.

PIXA PKI Policy Group MUST also (prior to issuing a certificate under the modified requirement) PIXA of the relevant information newly added to its CPS or CP by sending a message to the PIXA governing body.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to PIXA PKI Policy Group's CPS or CP, and a notice to the PIXA governing body must be made within 90 days.