Certificate Policy (CP)

for the

X9 Financial Public Key Infrastructure (PKI)

By: ASC X9 PKI Policy Group

Publication Date: April 3, 2025

Release: 1.0

This page left intentionally blank

CONTENTS

Foreword

Approval of this Certificate Policy that the requirements for due process, consensus, and other criteria for approval have been met.

Consensus is established when, in the judgment of X9, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

CAUTION NOTICE: This Certificate Policy may be revised or withdrawn at any time. The procedures of X9 require that action be taken to reaffirm, revise or withdraw this Certificate Policy no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Disclaimer

Accredited Standards Committee X9, Inc. (X9) is an open standards body and serves as the Governing Body for the X9 Financial PKI. In this role, X9 works in collaboration with financial industry stakeholders to define Public Key Infrastructure (PKI) requirements and best security practices. These are documented in this Certificate Policy (CP), which has been developed by industry experts and is based on established standards and widely accepted best practices.

X9 has partnered with DigiCert to provide PKI solutions that align with this Certificate Policy. This document is published solely to support the implementation of the X9 Financial PKI as provided by DigiCert. Any other use, including the issuance of certificates based on this policy by unauthorized parties, is not endorsed by X9 and is strictly prohibited.

This document and its contents are provided "as is" without any warranties—express, implied, statutory, or otherwise—including, but not limited to, warranties of merchantability, fitness for a particular purpose, non-infringement, or accuracy.

X9 makes no representations or warranties regarding the quality, security, effectiveness, compliance, or fitness for any purpose of any products or services that claim to reference, implement, or conform to this document—except where explicitly endorsed by X9. Users are solely responsible for evaluating such products or services and determining their appropriateness for any particular application.

This document is not an ANSI-approved standard. While X9 has made reasonable efforts to ensure the accuracy and relevance of the content, X9 disclaims any responsibility for errors, omissions, or outcomes resulting from the use or interpretation of this document.

By using any product or service based on this document, users acknowledge and agree that X9 shall not be liable for any direct, indirect, incidental, special, consequential, or exemplary damages—including, without limitation, loss of data, business interruption, or financial loss—arising from the use, implementation, or reliance on such products or services.

Suggestions for the improvement or revision of this Policy are welcome. They should be sent to the X9 Certificate Policy Administrator, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107 Annapolis, MD 21401 USA.

Certificate Policy

1 INTRODUCTION

Accredited Standards Committee X9 (ASC X9 or X9) is an organization created specifically to develop and provide a supporting environment for volunteers to create standards that improve payments and protect financial information both in the US and internationally. This extends to the definition of techniques and tools, where identified, to help secure activity and information exchange in the financial sector. The financial industry relies on the standards and recommendations from X9 to provide trusted and reliable solutions for operations, security, and interoperability.

By extension of this industry trust, X9 is developing a Public Key Infrastructure (PKI) to promote use case-oriented trust, reliance and interoperability. X9 is sensitive to the needs of the industry, particularly as related to existing PKIs that are supporting both general use PKIs and specialized PKIs that serve specific application requirements.

PKI (ISO 21188, X9.79) includes five basic components: the Policy Authority (PA); Registration Authority (RA); a Certificate Authority (CA) hierarchy consisting of a root CA, some number of Subordinate CA, and issuing CA; certificate subjects, and relying parities. Other (X.509) components might be Attribute Authority (AA) or OCSP (RFC 6960) responders.

PKI is a term that describes the sum total of the overarching Root Certificate Authority (RCA), the registration process and Root Registration Authorities (RRA), the subordinate certificate authorities (CAs) computers, software, encryption key storage and processing devices, software, end-users, and communication devices.

New PKIs may operate as subordinate to the X9 PKI by having their CA's certificate signed by an X9 PKI CA for a particular application or "use case."

An X9 Authorized CA is an issuing CA that might be, for example: (i) subordinate to the X9 PKI, (ii) subordinate to a public PKI cross-signed with the X9 PKI, or (iii) private PKI cross-signed with the X9 PKI.

Certificates issued by the X9 branded CA contain the X9 object identifier arc { iso(1) member-organization(3) tc68(133) country(16) x9(840) pki(79) } or simply 1.3.133.16.840.79.

An example of these existing PKIs include cryptographic key establishment and refresh for ATM or POS key encryption keys. The industry requires a continuity of operation of these existing PKIs to service that segment of the financial industry. This CP is not going to preclude the use of the X9 PKI for symmetric encryption keys. Refer to X9.139 and X9.24 Part 2.

But continuity does not exclude the need for those existing PKIs to meet particular security requirements to meet the needs and risk profiles of those applications. Approval of those PKIs' management and environment can be verified through the use of bridge certificates. This kind of evaluation and approval can also be provided to those CAs that choose to "stand alone" rather than being subordinate to an X9 PKI.

This kind operational flexibility provides a wide variety of options to the financial sector and potential support to a wide variety of use cases.

In addition to the above defined entities, this document includes those PKI deployments that are "cross-certified" or "bridged" to the X9 PKI rather than operating as a subordinate to the X9 PKI. These PKIs will operate under the same conditions as the X9 PKI.

This Certificate Policy (CP) document defines the certificate policies for issuance and maintenance of public key certificates by authorized Certificate Authorities (CAs). The development of an X9 Financial Industry Public Key Infrastructure centered on the use of the Internet is established to:

- Improve end-user access to financial services and information.
- Reduce Financial Institution and end-user operating costs (e.g., fraud) through secure implementation of electronic business processes.
- Facilitate secure e-commerce transactions, secured data transmission, cryptographic key exchange and refresh, DLT blockchain, secure remote banking, POS and ATM transaction communication security, and financial aggregator/compilation services. Future applications can also be supported.
- Provide a trust framework to the financial industry that requires a secure environment consistent with the higher risk associated with financial transaction activity.
- Specific use cases may have additional requirements beyond what is presented in this CP.

Realizing these potential benefits will require the use of digital signatures to verify the identity of both senders and receivers of electronic messages, as well as the integrity of the messages themselves. Use of digital signatures requires the use of public key cryptography and public key certificates to bind public key(s) to an identity(ies) and permission(s).

Because public key certificates and the systems that support their use are major prerequisites for creating a more consistent security environment for financial transactions and financial information exchange on the Internet, it is important to begin facilitating their implementation. In support of this goal, X9 has initiated an analysis project aimed at providing commercial public key certificate services to the financial sector. X9 will identify a processing environment that may include the use of third-party service providers for some of their services. X9 may also include provisions for cross-certification with other existing PKIs that meet the X9 requirements to facilitate the establishment of a secure environment for conducting secured and trusted financial information exchange.

Only CAs authorized to operate in accordance with this X9 CP and in an agreement between an X9 approved CA and X9 (agreement) signed with X9, shall assert the X9 CP Object Identifiers (OIDs) in the certificate policies extension of any certificates (Authorized X9 CAs). X9 public key certificates are utilized by individuals, organizations or devices for authentication or submitting digitally signed financial data to other financial institutions or other entities receiving the information (Relying Parties). Any use of or reference to this X9 CP outside of the purview of financial data interchange is completely at the using party’s risk.

X9 assumes no liability for the use of X9 PKI, its Public Keys or any data or transaction secured by, to, or from any relying party. In the absence of any shifting of liabilities based on contracts, relying parties assume all liability and risk.

This X9 Certificate Policy (CP) is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647 Certificate Policy and Certification Practices Framework. The terms and provisions of this X9 CP shall be interpreted under and governed by applicable Federal law.

The X9 PKIs and their relying parties will utilize International Standards Organization and X9 standards and accepted best practices to create and verify digital signatures and exchange encryption keys in a secure manner.

This document is the X9 Certificate Policy, it is neither a standard nor a technical report, nevertheless operative terms used in this Certificate Policy to describe actions are as follows:

- 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.

1.1 Overview

1.1.1 Certificate Policy (CP)

X9 certificates contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to verify an X9 certificate issued from an X9 branded (approved) CA. Within a Bridged CA PKI, a Bridge Certificate will contain the OID of a policy of the Bridged PKI below the Bridged CA. See Section 7.1.6 for OID values.

This X9 CP is consistent with the following Trusted Root Program requirements:

1) AICPA/CICA WebTrust for CA v2.2.1.

2) Intended to be consistent with ASC X9 PKI Operating Rules for Financial Services (to be written).

Relationship Between the X9 CP and the X9 Authorized CAs or X9 Bridged CAs:

The CP states what assurance can be placed in a certificate issued by X9 Authorized CAs or those with bridged CA agreements with an X9 bridged CA certificate. Each X9 Authorized CA or CA bridged to X9 with an X9 bridged certificate shall provide to the X9 Policy Authority a detailed Certification Practice Statement (CPS) that states how the Authorized CA establishes that assurance in accordance with this CP.

1.1.2 Scope

The X9 PKI program exists to facilitate trusted financial transaction and financial data interchange between entities participating in financial services. This exchange may be related to financial transactions, audit data, money transfer, electronic commerce, security management of remote devices, loan management or transfer, other business purposes or other financial or personal data sent or received between entities. This includes financial institutions or applications, and non-financial users. This CP describes the following:

- Roles, responsibilities, and relationships among the CAs, Registration Authorities (RAs), Certificate Manufacturers (CMs), Repositories, Subscribers, Relying Parties, and the Policy Authority (PA) (referred to collectively herein as “PKI Participants”) authorized to participate in the PKI described by this X9 CP.

- The primary obligations and operational responsibilities of the PKI Participants.

- The rules and requirements for the issuance, acquisition, management, and use of X9 certificates or bridge certificates.

- Physical security requirements.

- Auditing requirements.

This X9 CP provides a high-level description of the policies and operation of the X9 Program. Specific detailed requirements for the services outlined in this document may be found in the specific modifications of this CP for each use case specific CP, each X9 Authorized CA’s Memorandum of Agreement (or user agreement) and CPS.

1.2 Document Name and Identification

This Policy is registered with X9. Details to be provided as document and X9 PKI developed and registered. The OID will be provided by the applicable Computer Security Objects Register (CSOR) and included in certificate extensions for certificates issued by the X9 PKI.

A table will be provided listing the policy(ies), their OID(s) and other pertinent information in this section when available. See Section 7.1.6 for OID values.

Version	Date	Summary of Change
1.0	August 22, 2023	Initial Release
1.1	February 12, 2025	Updated legal notices, General Publication

1.3 PKI Participants

This X9 CP describes a bounded public key infrastructure. It describes the rights and obligations of persons and entities authorized under this CP to fulfill any of the following roles:

- Certificate Service Providers (and associated services)
    - Certification Authority (CA) (1.1.1)
    - Registration Authority (RA) (1.1.2)
    - Certificate Manufacturing Authority (CMA) (1.1.5.1)
    - Repository (1.1.5.2)
    - Certificate Status Servers (1.1.1.4)

- End Entities (Subscribers) (1.1.3)
    - Unaffiliated Individual
    - Business Representative
    - Device
    - State and Local Government
    - Subject

- Relying Party (1.1.4)

- X9 Policy Authority (1.1.1.1)

- X9 Program Management Office (1.1.1.2)

Requirements for persons and entities authorized to fulfill any of the above roles are defined below.

Additional obligations are set forth in other provisions of this CP; and include requirements of the CPS, Memorandum of Agreements, and Subscriber Agreements.

1.3.1 Certification Authorities

1.3.1.1 X9 Policy Authority

ASC X9 serves as the Policy Authority and is responsible for organizing and administering the CP. Additionally, the Policy Authority is responsible for managing the X9 Authorized CAs, including bridge

CAs in accordance with the X9 CP and resolving name space collisions within the X9 program. Additional responsibilities of the X9 Policy Authority may include activities related to:

- Examining and evaluating audits of the X9 PKI Service Provider,
- Enforcing compliance,
- Analyzing non-compliance,
- Managing the Certificate Policy,
- Managing the X9 PKI Program Management Office,
- Managing the ASC X9 PKI OID Registry, and
- Managing the ASC X9 PKI Operating Rules for Financial Services.

ASC X9 and its Category A members serve as the PA using a balanced representation.

1.3.1.2 X9 PKI Program Management Office

ASC X9 (or the X9 designated management authority) serves as the X9 PKI Program Management Office (PMO) and is responsible for organizing and administering the X9 PKI program and the X9 subordinate CA or bridge CA agreements.

The X9 PMO shall keep the X9 Public Key Infrastructure (PKI) Objects Registration up to date. X9 Authorized CAs requiring new OIDs shall submit a request to the X9 PMO. ASC X9 and its Category A members appoint the PMO using balanced representation.

If new OIDs are required, the X9 PMO shall assign new OIDs to certificate policies as needed and shall maintain control over the numbering sequence of OIDs within the X9 arc.

The X9 PMO is the Policy Authority (PA) for the X9 PKI. Additional responsibilities of the X9 PMO include:

- Verifying qualifications of a subordinate CA or bridged CA to participate in the X9 PKI,
- Signing an agreement with the subordinate CA or bridge CA on behalf of the X9 PKI,
- Sponsoring authorized CAs for cross-certification with the X9 PKI, and
- Ensuring all X9 Authorized CAs are audited and operated in compliance with the X9 CP.

1.3.1.3 X9 Authorized CAs

A CA may issue certificates that assert the policies defined in this X9 CP only if the CA first qualifies as an X9 Authorized CA by:

1. Entering into an appropriate agreement with the X9 PMO.
2. Documenting the specific practices and procedures it will implement to satisfy the requirements of this X9 CP in the appropriate CPS.

The X9 Authorized CA shall assert an X9 Policy OID. See Section 7.1.6 for OID values.

Each X9 Authorized CA shall be responsible where applicable for all aspects of the issuance and management of X9 Certificates, including:

- The application/enrollment process,
- The identification verification and authentication and authorization process,
- The certificate manufacturing process,
- Issuance and dissemination of certificates,
- Publication of certificates,
- Renewal, rekey, suspension, revocation, and replacement of certificates,
- Creation and dissemination of certificate status,
- Generation, storage, processing, and destruction of CA signing keys,
- Ensuring that all aspects of the X9 Authorized CA services and X9 Authorized CA operations and infrastructure related to X9 Certificates issued under this X9 CP are performed in accordance with the requirements, representations, and warranties of this X9 CP,
- Maintaining a PKI compliance audit program of all operational aspects related to this X9 CP including all RA functions whether those functions are performed internally or by a third party,
- Assume responsibility of all CAs that validate to the X9 Authorized CA are compliant with this X9 CP, and
- Assume responsibility of all contracted or subcontracted business operations of the X9 Authorized CA.

The X9 Authorized CA shall be responsible for ensuring that all work is performed under the supervision of the X9 Authorized CA or responsible employees of the X9 Authorized CA, and shall provide assurance of the trustworthiness and competence of employees and their satisfactory performance of duties relating to provision of X9 PKI services.

An Authorized Organization Representative (AOR) shall be assigned for any X9 Authorized CA.

Each X9 Authorized CA or employee of the X9 Authorized CA to whom information may be made available or disclosed shall be notified in writing by the X9 Authorized CA or AOR that information so disclosed to such X9 Authorized CA or employee can be used only for the purposes and to the extent authorized herein.

1.3.1.4 Cross-Certification with the X9 PKI

The cross-signed CA issues CA certificates to other Authorized issuing CAs.

Where the X9 Authorized CA operates a hierarchical PKI, the designated CA may be the hierarchical Root CA or it may be a subordinate CA to a different Root CA (if the CP and CPS of the non-X9 Root CA meet the X9 CP and CPS requirements).

Authorized subordinate CA’s or bridged CA’s may request cross-certification with more than one CA PKI or other PKIs operating to the same X9 PKI CP requirements, and with the same key usage use case.

This cross-certification may be whether or not the X9 Authorized CA employs a hierarchical or other PKI architecture.

1.3.1.5 Certificate Status Servers

X9 Authorized CAs shall provide certificate status services (CSS) such as Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) responders. The OCSP responders may be provided on behalf of the X9 Authorized CA as a CSS, where the CSS is identified in certificates as an authoritative source for revocation information (i.e., Authority Information Access [AIA] certificate extension). The OCSP CSSs identified in certificates issued by X9 Authorized CA CSSs are within the scope of this X9 CP.

1.3.2 Registration Authorities (RAs)

Each X9 Authorized CA shall be responsible for the role and functions of the RA within their hierarchy. An X9 Authorized CA may subcontract RA functions to third party and / or trusted agent RAs who meet trustworthiness requirements (see Section 8) and agree to be bound by and operate within this X9 CP. The X9 Authorized CA CPS shall identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.

The X9 Authorized CA remains responsible for the performance of those services in accordance with this X9 CP and the X9 agreement.

X9 Authorized RA shall only operate with one or more X9 Authorized CA.

The RA is responsible for applicant identity verification and registration, processing and authenticating certificate requests, and authentication of identity functions for Unaffiliated Individuals, Business Representatives, and Servers in compliance with this CP. This includes secure handling of certificate requests, and the specific process for handling of both valid and invalid certificate requests. The RA shall provide services for handling suspension and revocation requests and may provide for aspects of Subscriber education.

The X9 Authorized CA shall ensure audits include all RA functions whether performed internally or by a third party.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate. A subscriber asserts that the key and certificate are used in accordance with the certificate policy and key usage asserted in the certificate. An X9 Authorized CA may issue X9 certificates to the following classes of Subscribers:

- Members of X9. For purposes of the X9 PKI, a Member of X9 (X9 Member) shall be a Board of Directors level member (Category A) with dues paid in full.

- X9 Member Sponsored entities. An entity with a contractual relationship with an X9 Category A Member specifically permitting the Sponsored entity to process one or more activities related to a PKI operating within the X9 PKI. These activities may include, but not limited to public key certificate signing, Registration and Request processing, Revocation or other PKI management-related activities.

- X9 Contracted Entities. Entities with a contractual relationship with X9 to perform one or more activities related to the management and/or operation of the X9 PKI.

- Indirect Subscribers. Entities that subscribe to (or use) a CA that has been associated with the X9 PKI through a cross-signed bridge certificate or a CA certificate signed by the X9 PKI.

An Authorized Organization Representative (AOR) shall act as a point of contact for a subscriber to facilitate direct communication between the X9 Program Management Office, X9 Policy Authority and other PKI management entities.

X9 has the right to add authorized users or new classes of users and the responsibilities associated with such users or classes of users at any time during the term of this CP.

1.3.4 Relying Parties

The Relying Party must verify and use a Subscriber's certificate per the validation process and certificate usage defined in the specific Subscriber License Agreement (SLA) for that use case.

A Relying Party uses a Subscriber's certificate to:

- Verify the integrity of a digitally signed message,
- Facilitate secure exchange of cryptographic data or material,
- Verify a certificate chain,
- Identify or authenticate the signer of a message, or
- Establish confidential communications with the Subscriber.

A Relying Party shall use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

Relying Parties shall validate the certificate and certificate chain including checking the status of each certificate in that chain per ISO 21188 §5.10.3.2 Certificate validation. Exceptions to this policy will be detailed in the Subscriber License Agreement or the appropriate Certificate Policy.

The Relying Party is responsible for deciding how to configure their application for trusted roots and subordinate/issuing CAs.

This CP makes no assumptions or limitations regarding the identity of all Relying Parties. While Relying Parties might be Subscribers, Relying Parties are not required to have an established relationship with X9, the X9 PKI or an X9 Authorized CA. However, X9 Relying Parties are those persons and entities authorized to sponsor, accept and rely upon X9 Certificates for purposes of authentication and verifying digital signatures on electronic records and messages. End users or their applications wishing to accept X9 PKI Certificates agree to be bound by the terms of this Policy.

1.3.5 Other Participants

The X9 Authorized CAs may require the services of other security, community, and application authorities. An X9 Authorized CA CPS shall identify the parties (including third party service providers and cloud providers), define the services, and designate the mechanisms used to support these services.

1.3.5.1 Certificate Manufacturer Authority (CMA)

A CMA is responsible for the functions of manufacturing, issuance, suspension, and revocation of X9 certificates. Each X9 Authorized CA shall perform the role and functions of the CMA. An X9 Authorized CA may subcontract CMA functions to third party CMAs who agrees to be bound by this X9 CP, but the X9 Authorized CA remains responsible for the performance of those services in accordance with this X9 CP and the X9 agreement.

1.3.5.2 Repositories

Each X9 Authorized CA shall perform the role and functions of the Repository, as described in Section 2.1.1, Repository Obligations. An X9 Authorized CA may subcontract performance of the Repository functions to a third-party Repository who agrees to be bound by this X9 CP, but the X9 Authorized CA remains responsible for the performance of those services in accordance with this CP and the requirements stated in its agreement.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The overarching X9 PKI supports a number of different use cases. All current permissible use cases are defined in this Certificate Policy. Some additional or modified requirements may be contained in supplemental Certificate Policy Extensions for certain use cases.

Subscribers and Relying Party Applications may use X9 PKI digital certificates to implement approved use cases within the limitations of this CP.

1.4.2 Prohibited Certificate Uses

Certificates and keys shall not be used for any purposes other than those specifically stated in the certificate. Uses other than those defined in this policy document shall not permitted.

1.5 Policy Administration

1.5.1 Organization Administering this Document

The X9 PKI Policy Authority administers this X9 CP under the authority of the X9 PKI Program Management Office. Contact www.x9.org for further information.

1.5.2 Contact Information

Steve Stevens
X9 Executive Director
steve.stevens@x9.org

www.x9pki.org

X9 PKI Policy Authority (PA)
X9 PKI Program Management Operations (PMO)
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

X9 Administration
admin@x9.org

1.5.3 Person Determining CPS Suitability for the Policy

Suitability to be determined by the X9 PKI PMO.

1.5.4 CPS Approval Procedures

The CPS and the results and recommendations of the independent, trusted third-party shall be submitted to the X9 PKI Program Management Office for approval.

CAs seeking approval to acquire X9 PKI-signed certificates for subordinate or bridge CAs must meet all requirements of an approved CPS. Please contact X9 for updated CPS evaluation procedures and audit requirements.

1.6 Definitions, Terms, and Acronyms

1.6.1 AICPA
American Institute of Certified Public Accountants.

1.6.2 AICPA/CICA WebTrust for CA
American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants WebTrust Principles and Criteria for Certification Authorities. An Audit criteria for assessing compliance with the Certificate Authority Certificate Policy and Certificate Practice along with generally accepted Certificate Authority principles of secure operation. https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services

1.6.3 Authorized Organization Representative (AOR)
An individual or designated group that has been authorized and registered with the X9 PA to represent organizations or functions operating under this CP.

1.6.4 ATM / ABM
Automated Teller Machine or Automated Banking Machine. An unattended terminal that has electronic capability, accepts PINs, disburses currency or checks, and may accept deposits or checks.

1.6.5 ASC X9
Accredited Standards Committee X9 is a standards development organization (SDO) created specifically to develop and provide a supporting environment for volunteers to create consensus standards that improve payments and protect information for the financial services industry both in the US and internationally. ASC X9 is accredited by the American National Standards Institute (ANSI).

1.6.6 Bridging, Bridged CAs, Cross Certificate
Bridging is a process whereby two CAs establish a trust relationship between them by each CA signing a certificate, called a cross certificate, containing a public key of the other CA. When this process has been completed, the two CAs are considered Bridged CAs. In the context of this CP, a bridge is created by the X9 Bridge CA to other CAs / PKIs.

1.6.7 Certificate
See Public Key Certificate.

1.6.8 Certification Authority
An authority trusted by one or more entities to issue and manage public key certificates and CRLs.

1.6.9 Certificate Manufacturer Authority (CMA)
An entity whose function is to receive authenticated requests, format, sign and issue Public Key Certificates. This includes providing certificates included in the chain of certificates that authenticate to the Root CA.

1.6.10 Certificate Policy (CP)
A named set of rules that indicates the applicability of a public-key certificate to a particular community and/or class of application with common security requirements.

1.6.11 Certification Practice Statement (CPS)
A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

1.6.12 Certificate Renewal
Creating a new certificate with the same name, key, and other information as a current certificate, but with a new, validity period and a new serial number. Renewal of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.

1.6.13 Certificate Status Services/ Certificate Status Server
A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status and may also provide additional attribute information for the subject certificate.

1.6.14 CSOR
Computer Security Objects Register. The entity responsible for issuing and recording Object Identifiers and providing lookup services to requesting parties.

1.6.15 Digital Certificate
See Public Key Certificate.

1.6.16 Digital Signature
The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using a private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.

1.6.17 End Entity
A certificate subject which uses its private key for purposes other than signing certificates for relying parties and subscribers. An entity that is identified as the subject of a certificate at the end of a certification path or shares a symmetric key with other entities for communication.

1.6.18 Memorandum of Agreement (MoA)
In the context of this Certificate Policy, this is the legal document between X9 and a Category A member to operate one Certificate Authority supporting a defined use case. The MoA may contain specific conditions of use, operating requirements, period of use, limitations, third-party(ies) assignment, and other aspects of CA, or PKI component operation. Failure to maintain compliance with the Memorandum of Agreement and this CP may result in the revocation of this agreement and all CA certificates issued by the X9 CA under this agreement.

1.6.19 Object Identifier(s), OID(s)
An identifier mechanism standardized by the International Telecommunications Union (ITU), ISO and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name.

1.6.20 Online Certificate Status Protocol (OCSP)
A protocol for determining the current status of a digital certificate.

1.6.21 PKI
See Public Key Infrastructure.

1.6.22 Point-of-Sale device, POS device (or POS terminal)
A device that accepts and forwards bankcard-based credit or debit merchant payment transactions. These devices may or may not accept a PIN.

1.6.23 Policy Authority, PA, Policy Management Authority (PMA), Certificate Policy Authority
The entity responsible for management and oversight of the Certificate Policy (CP). The Policy Authority shall consist of one or more individuals appointed by the Program Management Office.

1.6.24 PKI Program Management Office, PMO

The entity responsible for overall management of the X9 PKI and all of its components. The X9 Program Management Office shall consist of one or more individuals appointed by the Board of Directors to manage the X9 PKI. The Program Management Office will appoint a Policy Authority and perform other duties with the approval of the Board of Directors and X9 Staff. The Program Management Office will prepare a list of activities and responsibilities that will be reviewed and approved by the X9 Staff and Board of Directors. From this list of responsibilities, authority will be extended by the Board of Directors to act on their behalf in managing the X9 PKI.

1.6.25 Public Key Certificate
A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity (e.g., using an X.509 certificate). Additional information in the certificate could specify how the key is used and its validity period.

1.6.26 Public Key Infrastructure
Also known by its acronym PKI as defined in ISO 21188 and X9.79 standards includes five basic components: the Policy Authority (PA); Registration Authority (RA); a Certificate Authority (CA) hierarchy consisting of a root CA, some number of subordinate CAs, and issuing CA; certificate subjects, and relying parities. Other (X.509) components might be Attribute Authority (AA) or OCSP (RFC 6960) responders.

PKI is a term that describes the sum total of the overarching Root Certificate Authority (RCA), the registration process and Root Registration Authorities (RRA), the subordinate certificate authorities (CAs) computers, software, encryption key storage and processing devices, software, end-users, and communication devices.

1.6.27 Registration Authority
An entity responsible for authenticating an entity requesting a certificate and validating the authenticity of the request.

1.6.28 Relying Party
An entity receiving a certificate from a certificate holder for purposes of reliance on the contents of the certificate and use of the public contained therein.

1.6.29 Repository
A storage site of PKI status and related information.

1.6.30 RCA
See Root Certificate Authority.

1.6.31 Root Certificate Authority
In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

1.6.32 Subordinate, Subordinate Certificate Authority, Subordinate CA
A Certification Authority whose Certificate is signed by a Root CA, or another Subordinate CA.

1.6.33 Sponsor
An X9 Category A member that has entered into a Memorandum of Agreement with X9 to authorize the operation of a CA, or some of the CA supporting operations, by a third party. A sponsor assumes responsibility for all third-party operations and compliance with this CP and the conditions stated in the Memorandum of Agreement.

1.6.34 Subscriber
An entity whose name appears as the subject in a certificate.

1.6.35 User Agreement
See Memorandum of Agreement.

1.6.36 X9
See ASC X9.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. Certificates in existence prior to the establishment of this CP are exempt from this requirement.

Optionally, CAs may post subscriber certificates in this repository, except as noted in Section 9.4.2. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The publicly accessible repository system shall be designed and implemented so as to provide high availability overall and limit scheduled down-time. Where applicable, the certificate status server (CSS) shall be designed and implemented so as to provide high availability overall and limit scheduled down-time.

2.2.2 Publication of CA Information

The CP shall be publicly available. The CPS of the CA is not required to be published. However, a summary or redacted CPS shall be available upon request to current or prospective X9 PKI participants.

2.3 Time or Frequency of Publication

An updated version of the CP will be made publicly available within 5 business days of the incorporation of changes.

The CA shall specify in its CPS time limits within which it will publish various types of information.

The CRL is published as specified in Section 4.9.7. All information to be published in the repository shall be published promptly after such information becomes available to the CA.

2.4 Access Controls on Repositories

The CA shall protect information not intended for public dissemination or modification.

CA certificates and CRLs in the repository shall be available to the X9 ecosystem participants. Direct and/or remote access to other information in the CA repositories shall be determined by Policy Authority.

The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under what conditions the restricted information may be made available.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The CA shall assign an X.501 Distinguished Name (DN) to each subscriber. This DN may or may not appear in a certificate field. Subscriber certificates may contain any name type appropriate to the application.

3.1.2 Need for Names to be Meaningful

Names used in certificates must represent an unambiguous identifier for the subject. Names shall be meaningful enough for a human to identify the named entity, irrespective of whether the entity is a person, machine, or process. Interpreting the name semantic may require a reference database (e.g., human resources directory or inventory catalog) external to the PKI.

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. CA certificates that assert this policy shall not include a personal name, but rather shall identify the subject as a CA and include the name-space for which the CA is authoritative. For example:

c= country, o = Issuer Organization Name, cn =OrganizationX CA-3

Refer to the X9 Profiles Document for encoding requirements for distinguished names.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in RFC 2822.

3.1.4 Uniqueness of Names

Each CA must ensure that each of its subscribers is identifiable by a unique name. Each X.500 name assigned to a subscriber by a CA (i.e., in that CA's namespace) must identify that subscriber uniquely. When other name forms are used, they too must be allocated such that each name identifies only one subscriber of that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity. For certificates that assert names that do not identify individual people, an Authorized Organization Representative shall be identified as having responsibility for the certificate subject. The CPS shall identify the method for the assignment of unique subject names.

3.1.5 Recognition, Authentication, and Role of Trademarks

CAs operating under this policy shall not issue a certificate knowing that it infringes on the trademark of another. The PA shall resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

Certificates exist to bind identities to public keys, so it is essential that the identities be appropriately validated. The kind of identity being validated (organization or natural person, etc.), and the degree of rigor required, will vary by use case, so specific identity validation procedures appear in use-case specific CPs.

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request.

In the case where key generation is performed under the CA's or RA's direct control, proof of possession is not required.

(For example, refer to RFC 2986 PKCS#10 CSR.)

3.2.2 Authentication of Organization Identity

Organizational identity shall be established by following the appropriate steps in the use-case specific CP.

Verification shall include checking the certificate requestor has met all audit requirements, Subscriber License Agreement(s), financial responsibility and payments, insurance requirements (if any), sponsorship arrangements, has received X9 PMO approval, and any other requirements established by ASC X9, the PA and/or the sponsoring entity.

3.2.2.1 Identity Authentication for Subordinate CA Certificates

Requests for Subordinate CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing subordinate CA certificates, an authority for the issuing X9 CA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the subordinate CA.

The Subscriber CA issuing subordinate CA certificates shall verify the existence of the organization by verifying the identity and address of the organization and that the address is the subscriber's address of existence or operation.

3.2.2.2 Identity Authentication for End Entity Certificates

For Subscriber organization end entity certificates, the CA shall verify the existence of the organization by verifying the identity and address of the organization and that the address is the subscriber's address of existence or operation.

Use-case specific CPs may contain additional details and/or steps as to how the organization's identity is validated.

3.2.3 Authentication of Individual Identity

Only X9 approved CAs can participate. CAs that use third party RAs must only use approved X9 RAs.

The RA shall use all reasonable means to make sure an organization applying for a certificate has completed all required approvals and agreements, completed and passed the required audit(s), filed the Memorandum of Agreement, paid the necessary fees and completed all other requirements.

The RA shall use reasonable means to ensure the individual identity contained in a certificate request matches the identity of the individual holding the private key corresponding to the public key contained in the certificate request. The RA will verify that all requirements are met before processing a certificate request and signing a certificate for an individual.

Use-case specific CPs may contain additional details and/or steps as to how the individual's identity is validated.

3.2.3.1 Authentication of Human Subscribers

The RA shall ensure that the subscriber's identity information is verified. RAs may accept authentication of a subscriber's identity attested to and documented by a trusted agent or notary to support identity proofing of remote subscribers.

Authentication by a trusted agent or notary does not relieve the RA of its responsibility to perform steps (identified below) 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of records in step 4), below.

At a minimum, authentication procedures for human subscribers must include the following steps:

1. Verify that a request for certificate issuance to the applicant was submitted by the organization identified in the SubjectName and DistinguishedName.

2. Verify Subscriber's organizational membership through use of official organization records.

3. Establish subscriber's identity by appropriate proofing (e.g., in person or secure remote) before the registration authority, based on the following process and commensurate with the desired level of assurance:

    a. The subscriber presents an official form of identification (e.g., a passport or driver's license) as proof of identity,

    b. The RA examines the presented credential that can be linked to the subscriber (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

    c. The credential presented above shall be verified by the RA for currency and legitimacy (e.g., the organization ID is verified as valid).

4. Verify information to be included in the certificate (e.g., e-mail address, subject alternative pseudonymous names).

5. Record and maintain records of the applicant by the RA or CA. This information is archived to help establish an audit trail for dispute resolution.

3.2.3.2 Authentication of Devices

Some computing and communications devices (routers, firewalls, etc.) will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR), or in certain cases the device itself, must provide identifying information for the device. The AOR/device is responsible for providing registration information which may include:

- Equipment identification (e.g., serial number),

- Equipment certificate signing request CSR,

- Equipment authorizations and attributes (if any are to be included in the certificate), or

- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR/device shall be verified. If the device itself provides this information, the identity of the device shall be authenticated. If the information is provided by an AOR for a single device or batch of devices, the AOR shall be authenticated.

3.2.3.3 Authentication of Applications or Services

Some software use cases will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR) must provide identifying information for the device. The AOR is responsible for providing registration information which may include:

- Unique software application or service name (e.g., DNS name),
- Software application or service certificate signing request CSR,
- Software application or service authorizations and attributes (if any are to be included in the certificate), or
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR shall be verified. The CA shall validate that the AOR is authorized to request a certificate for the application or service.

3.2.3.4 Authentication for Roles Certificates

Depending upon use case, Role Certificates may be implemented. Refer to the appropriate use-case specific CP for details on implementation.

A role certificate shall identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name. A role certificate shall not be a substitute for an individual subscriber certificate. Multiple subscribers can be assigned to a role at the same time.

Subscribers issued role certificates shall protect the corresponding role credentials to the same security level as individual credentials.

The procedures for issuing role certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). The AOR may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA shall record the information identified in Section 3.2.3.1 for an AOR associated with 5 the role before issuing a role certificate. The CA or RA shall verify the identity of the AOR using an individual certificate in his or her own name issued by a CA with equivalent assurance as the role 7 certificate, or other commensurate methods.

AORs shall be responsible for:

- Authorizing subscribers for a role certificate,
- Recovery of the private decryption key,
- Revocation of subscribers' role certificates,
- Always maintaining a current up-to-date list of subscribers who are assigned the role, and
- Always maintaining a current up-to-date list of subscribers who have been provided the private keys for the role.

3.2.3.5 Authentication for Code Signing Certificates

The procedures for issuing code signing certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). One or more AORs shall be assigned to act on behalf of the code signing certificate subscriber for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA shall record the information identified in Section 3.2.3.1 for an AOR associated with the code signing certificate. The CA or RA shall verify the identity of the AOR using an individual certificate issued by a CA with equivalent assurance as the code signing certificate, or other commensurate methods.

AORs shall be responsible for:

- Authorizing subscribers for a code signing certificate,
- Revocation of subscriber's code signing certificates, and
- Always maintaining a current up-to-date list of subscribers who are authorized to hold code signing certificates and their associated private keys.

3.2.4 Non-verified Subscriber Information

This is the RA process for minimal info verification, if some info cannot be verified to some assurance level, the request must be rejected by the RA.

Information that is not verified shall not be included in certificates. All certificate contents are verified by the CA or RA, either directly or by an attestation from the AOR who is authoritative for the certificate subject.

3.2.5 Validation of Authority

This is the RA process for subject authorization.

We also need X9 process for candidate CA authorization but this might be part of an X9 Audit Program Guide (APG) based on Webtrust for CA but is not part of the CP.

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the subscriber's authority to act in the name of the organization. For role certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

For re-key of any CA certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures per Section 3.2 for initial registration as the initial registration at least once every ten years from the time of original registration.

For re-key of any subscriber certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures per Section 3.2 for initial registration at least once every five years from the time of original registration.

3.3.2 Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.2 above.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The Certificate application process shall provide sufficient information to:

1. Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a certificate. (per Section 3.2.3)

2. Establish and record identity of the applicant. (per Section 3.2.3)

3. Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per Section 3.2.1)

4. Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all must be completed before certificate issuance.

4.1.1 Who Can Submit a Certificate Application

A certificate application shall be submitted to the CA by the Subscriber, AOR, or an RA on behalf of the Subscriber. Multiple certificate requests from one RA or AOR may be submitted as a batch.

4.1.2 Enrollment Process and Responsibilities

All communications among Certification Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification and relevant sensitive data shall be encrypted; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. The confidentiality and integrity of relevant sensitive data shall be protected during out-of-band communications.

Subscribers are responsible for providing accurate information on their certificate applications. CAs are responsible for validating all information before including the information in the certificate.

4.2 Certificate Application Processing

Information in certificate applications shall be verified as accurate before certificates are issued.

Procedures to verify information in certificate applications shall be specified in the CPS.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber shall meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3 of this document. The components of the PKI (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case shall be identified in the CPS.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by a CA under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA shall reject any application for which such validation cannot be completed, or when the CA has cause to lack confidence in the application or certification process.

4.2.3 Time to Process Certificate Applications

After identity and certificate request verification is completed, certificate applications shall be processed and a certificate issued within the time specified in the CPS.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, the CAs/RAs shall:

1. Verify the identity of the requester as specified in Section 3.2 and formal acknowledgement of their obligations as described in Section 9.6.3.

2. Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1.

3. Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).

4. Make the certificate available to the subscriber or requestor, as appropriate.

The certificate request may already contain a to-be-signed certificate built by either the RA or the subscriber. This certificate shall not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective requester shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in the CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance (this may be in batch).

4.4 Certificate Acceptance

Before a subscriber can make effective use of its private key, the CA shall explain to the subscriber its responsibilities and obtain the subscriber's acknowledgement, as defined in Section 9.6.3.

4.4.1 Conduct Constituting Certificate Acceptance

Unless otherwise agreed to by the parties, failure to object to the certificate or its contents shall constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The X9 PA shall be notified whenever a CA operating under this policy issues a CA certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key shall be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. Depending on the specific use case, CAs operating under this policy shall issue CRLs specifying the current status of all revoked, unexpired certificates except for OCSP responder certificates. Depending on the specific use case, OCSP responders will provide a status of all certificates.

It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Any certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the subject name and attributes are unchanged.

In addition, the validity period of the certificate shall not exceed the remaining lifetime of the corresponding private key and the remaining lifetime of the issuing CA's private key, as specified in Section 5.6. The identity proofing requirements listed in Section 3.3.1 shall also be met.

CA Certificates and OCSP responder certificates may be renewed as long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in Section 6.3.2.

The CA may renew previously-issued certificates during recovery from CA key compromise without subject request or approval as long as the CA is confident of the accuracy of information to be included in the certificates.

4.6.2 Who May Request Renewal

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate.

The Subscriber, RA, LRA, or AOR may request the renewal of a Subscriber certificate.

4.6.3 Processing Certificate Renewal Requests

In order to prevent extending the private key lifetime for CA key pairs, renewal of any CA certificate issued under this certificate policy is disallowed.

For renewal of any subscriber certificate issued under this certificate policy, identity may be established through use of a current signature key, except that identity shall be established following the same procedures per Section 3.2 for initial registration at least once every two years from the time of original registration.

Digital signatures on subscriber renewal requests shall be validated before electronic renewal requests are processed per Section 3.3.

Other cryptographic protection over renewal requests include keyed-hash message authentication code (HMAC), authenticated encryption with associated data (AEAD) and signcryption.

For HMAC or AEAD a unique symmetric key per subscriber can establish identity for authorization and the cryptogram can provide authentication.

For signcryption the subscriber signature might be generated using the current signature key or an alternate signature key if the corresponding certificate was issued by the same CA.

4.6.4 Notification of New Certificate Issuance to Subscriber

The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Unless otherwise agreed to by the parties, failure to object to the certificate or its contents shall constitute acceptance of the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

Publication of renewed subscriber certificates is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

An expired certificate may or may not have been revoked, but must not be further re-keyed, renewed, or modified. A certificate may only be re-keyed, renewed once.

Subscribers shall identify themselves for the purpose of re-keying as required in Section 3.3.

4.7.1 Circumstance for Certificate Re-key

No stipulation.

4.7.2 Who May Request Certification of a New Public Key

Requests for certification of a new public key shall be considered as follows:

1. Subscribers with a currently valid certificate may request certification of a new public key.
2. CAs and RAs may request certification of a new public key on behalf of a subscriber.
3. For device, application/service, or role certificates, an AOR that owns or controls the device may request re-key.

4.7.3 Processing Certificate Re-keying Requests

Digital signatures on subscriber re-key requests shall be validated before electronic re-key requests are processed per Section 3.3. Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

The CA shall inform the subscriber of the rekey of his or her certificate and the contents of the certificate.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

All CA certificates must be published as specified in Section 2.

Publication of renewed subscriber certificates is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation.

4.8 Certificate Modification

Certificate modification is allowed.

The replaced certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

A CA may perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage). If the subscriber name has changed, the subscriber shall undergo the initial registration process.

4.8.2 Who May Request Certificate Modification

Requests for certificate modification shall be considered as follows:

1. Subscribers with a currently valid certificate may request certificate modification.
2. CAs and RAs may request certificate modification on behalf of a subscriber.
3. For device, application, and role certificates, an AOR may request certificate modification.

4.8.3 Processing Certificate Modification Requests

A certificate modification shall be achieved using one of the following processes:

1. Initial registration process as described in Section 3.2.
2. Identification & Authentication using a subscriber-signed certificate modification request, as described in Section 4.7.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2.

The RA shall complete all required re-verification prior to issuing the modified certificate.

4.8.4 Notification of New Certificate Issuance to Subscriber

The CA shall inform the subscriber of the modification of his or her certificate and the contents of the certificate.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of the Modified Certificate by the CA

All CA certificates must be published as specified in Section 2.

Publication of renewed subscriber certificates is subject to the requirements in Section 2 and Section 9.4.3 of this policy.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

Revocation requests must be authenticated. See Section 3.4 for more details.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. When this occurs, the associated certificate shall be revoked and placed on the CRL and/or its status changed on the OCSP responder. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation may subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. The AOR of the organization that owns or controls a device can request the revocation of the device's certificate. Other authorized individuals of the organization may request revocation as described in the CPS.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked and allow the request to be authenticated (e.g., digitally or manually signed). The CA may request information sufficient to explain the reason for revocation. The steps involved in the process of requesting a certification revocation are detailed in the CPS.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy.

4.9.5 Time within which CA must Process the Revocation Request

CAs shall revoke certificates as quickly as practical upon receipt of a proper revocation request and after the requested revocation time. Revocation requests shall be processed within as soon as operationally reasonable from the time of receipt.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties shall check the status of certificates when practical depending on the use case associated with the certificate upon which parties are replying. If the certificate is revoked, it will no longer be eligible for use by relying parties.

4.9.7 CRL Issuance Frequency

CRLs, if issued, shall be issued periodically per the CPS, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published no later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote operation.

Online CAs that issue CRLs must issue them at least once every 96 hours, and the *nextUpdate* time in the CRL may be no later than 7 days after issuance time (i.e., the *thisUpdate* time).

Offline CAs that issue CRLs must issue CRLs at least once every 365 days, and the *nextUpdate* time in the CRL may be no later than 365 days after issuance time (i.e., the *thisUpdate* time).

Circumstances related to emergency CRL issuance are specified in Section 4.9.12. The update frequencies may be adjusted for each use case.

4.9.8 Maximum Latency for CRLs

CRLs shall be published as soon as possible after generation. Furthermore, each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for same scope.

4.9.9 On-line Revocation/Status Checking Availability

Where on-line status checking is supported, status information must be updated and available to relying parties as soon as possible after the decision to revoke.

4.9.10 On-line Revocation Checking Requirements

Relying party client software should support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

Specific use cases may allow for our support alternate methods of Revocation Checking or Certificate Status Checking.

4.9.12 Special Requirements Related to Key Compromise

See also Section 4.9.1.

In the case of a compromise of a CA certificate, the CA must immediately notify the X9 PKI PMO that the CA certificate has been compromised. See Section 5.7.1 for incident handling procedures.

4.9.13 Circumstances for Suspension

As specified in the use case specific CP, a certificate can be suspended (temporarily revoked) for a period of time (known as the suspension grace period). During the suspension period, the binding between the subject and the subject's public key defined within the certificate is not considered valid. It will be placed on the CRL and/or the status changed on the OCSP responder. If the grace period has elapsed, the certificate is permanently revoked.

The suspended certificate can be resumed (reactivated) if the certificate has not yet expired and the grace period has not elapsed. Once it is resumed, it will not be placed on the CRL and/or the status changed on the OCSP responder.

The suspended certificate can also be permanently revoked during the grace period if it has not yet expired.

4.9.14 Who Can Request Suspension and Resumption

As described in Section 4.9.2. The suspension and resumption requests shall come from the same organization.

4.9.15 Procedure for Suspension and Resumption Requests

As described in Section 4.9.3.

4.9.16 Suspension Request Grace Period

As described in the CPS.

4.9.17 Time within which CA must Process the Suspension Request

As described in Section 4.9.5.

4.10 Certificate status services

See Section 4.9.9 for OCSP.

If additional certificate status services are supported, they must be described in the CPS.

4.10.1 Operational characteristics

Where applicable this must be described in the CPS.

4.10.2 Service availability

Where applicable this must be described in the CPS.

4.10.3 Optional features

Where applicable this must be described in the CPS.

4.11 End of Subscription

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.12 Key Escrow and Recovery

CA private keys shall never be escrowed.

Under no circumstances shall a subscriber signature key be held in trust by a third party. CAs that support private key escrow for key management keys shall document their specific practices in their CPS and key escrow documentation.

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys shall never be escrowed.

Under no circumstances shall a subscriber signature key be held in trust by a third party. CAs that support private key escrow for key management keys shall document their specific practices in their CPS and key escrow documentation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation. Specific recovery may be specified in CP use case exceptions or CPS of use cases.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

All CA and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CA and RA equipment is prohibited. CA equipment shall be dedicated to performing CA functions. RA equipment shall be operated to ensure that the equipment meets all physical controls at all times.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive financial information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

Physical access to CA equipment shall be limited to authorized individuals. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

At a minimum, physical access controls for CA equipment and all copies of the CA cryptographic module shall meet the following requirements:

- Controls shall be in place to mitigate unauthorized access to the hardware and sensitive information.
- Be manually or electronically monitored for unauthorized intrusion at all times.
- Ensure an access log is maintained and available for inspection by individuals in Trusted Roles.
- Mandate at least two-person access requirements. Technical or mechanical mechanisms shall be used to enforce the two-person physical access control.
- Other individuals shall be escorted by two authorized persons. This includes maintenance personnel. All individuals shall be recorded in the access log.

When not in use, removable media and sensitive information shall be placed in locked containers sufficient for housing equipment and information commensurate with the sensitivity of the application being protected. Access to the contents of the locked containers shall be restricted to individuals holding CA authorized roles as defined in Section 5.2.1, utilizing dual control and split knowledge while the container is unlocked.

A security check of the room/rack housing CA equipment shall occur prior to leaving the room/rack. The check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation.
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, alarm system, cameras) are functioning properly.
- The area is secured against unauthorized access.

If unattended, the facility housing CA equipment shall be protected by a physical intrusion detection system.

5.1.2.2 Physical Access for RA Equipment

See the appropriate section in the CPS.

5.1.3 Power and Air Conditioning

The facility shall have backup power capability and air conditioning sufficient to support a reliable operating environment. The backup power capabilities shall support the availability requirements in Section 6.7.3.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

The CA shall comply with local commercial building codes for fire prevention and protection.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media not required for daily operation or not required by policy to remain with the CA or RA that contains security audit, archive, or backup information shall be stored securely in a location separate from the CA or RA equipment.

Media containing private key material shall be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or provides access. Storage protection of CA and RA private key material shall be consistent with stipulations in Section 5.1.2.

5.1.7 Waste Disposal

CA and Operations Staff and RA Staff shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information shall be destroyed, such that the information is unrecoverable, prior to disposal. Sensitive media and paper shall be destroyed in accordance with the applicable policy for destruction of such material.

5.1.8 Off-Site Backup

A system backup shall be made when a CA system is initially activated. If the CA system is operational for more than a week, backups shall be made at least once per week. Backups shall be stored offsite. Only the latest backup needs to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

The data backup media shall be stored in a facility approved for storage of information of the same value of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.2.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Trusted roles and associated level of access shall be defined by the CA.

The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for all of those who act in trusted roles.

5.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys,
- Performance of CA administration or maintenance tasks,
- Archiving or deleting CA audit logs; at least one of the participants shall serve in a Security Auditor role, and
- Physical access to CA equipment.

5.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles shall identify themselves and be authenticated by the CA and RA before being permitted to perform any actions set forth above for that role or identity. CA Operations Staff and RA Staff shall authenticate using a credential that is distinct from any credential they use to perform non-trusted role functions.

CA and RA equipment shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication.

Individuals holding trusted roles shall be appointed to the trusted role by an appropriate approving authority. These appointments shall be annually reviewed for continued need, and renewed if appropriate. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

5.3 Personnel Controls

Personnel Security plays a critical role in the CA facility’s overall security system.

5.3.1 Qualifications and Experience, and Related Requirements

Each CA is responsible for determining the candidate's background qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role shall meet the following:

- Be employees of, or a contractor/vendor of, the CA and bound by terms of employment or contract employment in writing.
- Have successfully completed an appropriate training program.
- Have demonstrated the ability to perform their duties.
- Have no conflicting duties that would interfere with their responsibilities as defined in Section 5.2.1 Trusted Roles.

5.3.2 Background Check Procedures

Persons fulfilling Trusted Roles shall pass a comprehensive background check. CAs shall have a process in place to ensure employees undergo background checks.

Prior to commencement of employment in a Trusted Role, the CA shall conduct background checks (in accordance with local privacy laws) which include the following:

- Confirmation of previous employment,
- Check of professional reference,
- Confirmation of the highest or most relevant educational degree obtained,
- Search of criminal records (local, state or provincial, and national),
- Check of credit/financial records,
- Search of driver's license records, and
- Identification verification via National Identity Check (e.g., Social Security Administration records), as applicable.

Factors revealed in a background check that should be considered grounds for rejecting candidates for Trusted Roles or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial or personal responsibility.

Note that the availability and depth of background checks are subject to jurisdictional considerations.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA, CSS or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/CSS/RA security principles and mechanisms,
- All PKI software versions in use on the CA/CSS/RA system,
- All PKI duties they are expected to perform,
- Disaster recovery and business continuity procedures, and
- Stipulations of this policy.

5.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in the CA, CSS, RA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Independent Contractor Requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above shall be permitted access to the CA's secure facilities only to the extent they are escorted and directly supervised by people holding trusted roles at all times.

5.3.7 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs, CSS, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

Security auditing capabilities of CA, CSS, and RA operating system and applications shall be enabled during installation and initial configuration. Below are examples but not an exhaustive list, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,

- Success or failure where appropriate, and

- The identity of the entity and/or operator that caused the event.

The entire list below applies to all CAs and RAs.

Time shall be synchronized with an authoritative time source.

The CA, CSS and RA shall record the events identified in the list below.

1) SECURITY AUDIT:
   - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
   - Any attempt to delete or modify the Audit logs

2) IDENTIFICATION AND AUTHENTICATION:
   - Successful and unsuccessful attempts to authenticate to a system

3) KEY LIFECYCLE EVENTS:
   - Key lifecycle events for CA keys, subscriber keys (if applicable), OCSP signing keys, including
   - Key generation, backup, storage, recovery, archival, and destruction

4) CRYPTOGRAPHIC DEVICE MANAGEMENT:
   - Cryptographic device lifecycle management events
   - Lifecycle events for activation materials

5) PRIVATE AND SECRET KEY EXPORT:
   - The export of private (asymmetric) and secret (symmetric) keys (keys used for a single session or message are excluded)

6) CERTIFICATE REGISTRATION:
   - All certificate requests
   - All verification activities stipulated in Section 3.2 of this policy and the CA's Certification Practice Statement

7) CERTIFICATE REVOCATION:
   - All certificate revocation requests
   - The approval or rejection of a certificate status change request

8) TOKEN MANAGEMENT
   If tokens are used:
   - Loading tokens with certificates
   - Shipment of tokens
   - Zeroizing tokens

9) CA/CSS/RA CONFIGURATION:
   - Installation of the operating system
   - Installation of the CA, CSS or RA
   - Installing hardware cryptographic modules
   - Removing hardware cryptographic modules
   - Re-key of the CA, CSS or RA
   - Destruction of cryptographic modules
   - System startup and shutdown
   - Any security-relevant changes to the configuration of the CA, CSS or RA

10) ACCOUNT ADMINISTRATION:
    - Roles and users are added or deleted
    - The access control privileges of a user account or a role are modified
    - Appointment of an individual to a trusted role
    - Designation of personnel for multi-party control

11) CERTIFICATE PROFILE MANAGEMENT:
    - All changes to any certificate profiles
    - Approvals of changes to certificate profiles

12) PHYSICAL ACCESS / SITE SECURITY:
    - Personnel access to room housing CA
    - Access to the CA server
    - Known or suspected violations of physical security
    - Any removal or addition of equipment to the CA enclosure (equipment sign-out and return)

13) ANOMALIES:
    Including but not limited to:
    - Software error conditions
    - Software check integrity failures
    - Receipt of improper messages
    - Network attacks (suspected or confirmed)
    - Equipment failure
    - Electrical power outages
    - Obvious and significant network service or access failures
    - Violations of certificate policy
    - Violations of certification practice statement
    - Resetting operating system clock

14) MISCELLANEOUS:
    - Cryptographic device lifecycle management events
    - Backing up CA, CSS or RA internal databases
    - Restoring CA, CSS or RA internal databases
    - File manipulation (e.g., creation, renaming, moving)
    - Posting of any material to a repository
    - Access to CA, CSS or RA internal databases
    - All certificate compromise notification requests
    - Configuration changes to the CA, CSS or RA server involving:
        - Hardware
        - Software
        - Operating system
        - Patches

5.4.2 Frequency of Processing Log

Real-time automated analysis tools should be used when applicable. For all logs that cannot be reviewed in real time with the use of an automated tools, logs should be reviewed every 6 months. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Log

Audit log retention shall be defined in the CPS.

5.4.4 Protection of Audit Log

Logs shall be protected to prevent alteration and detect tampering. Specific instructions will be included in the CPS.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up monthly. A copy of the audit log shall be sent off-site every month.

5.4.6 Audit Collection System (Internal and External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

See Section 6.7.7 for requirements on regular penetration testing.

5.5 Records Archival

5.5.1 Types of Events Archived

See Section 5.4.1.

5.5.2 Retention Period for Archive

See Section 5.4.4.

5.5.3 Protection of Archive

See Section 5.4.4.

5.5.4 Archive Backup Procedures

See Section 5.4.5.

5.5.5 Requirements for Time-Stamping of Records

CA/CSS/RA automated archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

Archive data shall be collected in an expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store the CA archive information, shall be published in the CPS or a referenced document.

5.6 Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, only the new key will be used to sign CA and subscriber certificates. If the old private key is

used to sign unexpired OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. When a CA that distributes self-signed certificates updates its private signature key, the CA shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.

If compromise of a CA is suspected, certificate issuance by that CA shall be stopped immediately. An independent, third-party investigation shall be performed in order to determine the nature and the degree of damage. The scope of potential damage shall be assessed in order to determine appropriate remediation procedures. If a CA private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed.

In case of a CSS key compromise, all certificates issued to the CSS shall be revoked and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the CSS shall be re-keyed.

The CA shall notify the X9 Policy Authority in the case of a root CA, or notify the Issuing CA of a subordinate CA, if any of the following occur:

- Suspected or detected compromise of any CA system or subsystem,
- Physical or electronic penetration of any CA system or subsystem,
- Successful denial of service attacks on any CA system or subsystem,
- Any incident preventing a CA from issuing and publishing a CRL or OCSP response prior to the time indicated in the *nextUpdate* field in the currently published CRL or OCSP response, and
- Suspected or detected compromise of a certificate status server (CSS) if:
    - The CSS certificate has a lifetime of more than 72 hours, and
    - The CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the *id-pkix-ocsp-nocheck* extension).

5.7.2 Computing resources, Software, and/or Data are Corrupted

When computing resources, software, and/or data are corrupted, CAs must respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation must be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.

- If the CA signature keys are destroyed, CA operation must be reestablished as quickly as possible, giving priority to the generation of a new CA key pair. The customer Agency Points of Contact (POC) must be notified as soon as possible.

In the event of an incident as described above, the organization operating the CA must post a notice on its web page identifying the incident and provide notification to the X9 PKI PMO. See Section 5.7.1 for contents of the notice.

Otherwise, when systems or data are corrupted and any private key compromise is known or suspected, refer to section 5.7.3 key compromise procedures.

5.7.3 Entity (CA) Private Key Compromise Procedures

5.7.3.1 Root CA Compromise Procedures

In the case of the Root CA compromise, the CA shall:

- Notify the X9 Policy Authority and relying parties via public announcement,
- Notify any cross-certified PKIs of the Root CA compromise so that they can revoke any cross certificates issued to the Root CA or any Subordinate CAs, and
- Notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores.

Further,

- Notifications shall be made in an authenticated and trusted manner.
- Initiation of notification to the X9 Policy Authority and any cross-certified PKIs shall be made at the earliest feasible time and shall not exceed 24 hours beyond determination of compromise or loss unless otherwise required by law enforcement.
- Initiation of notification to relying parties and subscribers may be made after mediations are in place to ensure continued operation of applications and services.

If the cause of the compromise can be adequately addressed and it is determined that the PKI can be securely re-established, then the CA shall:

- Generate a new Root CA certificate,
- Solicit requests and issue new Subordinate CA certificates,
- Securely distribute the new Root CA certificate, and
- Re-establish any cross certificates.

5.7.3.2 Subordinate CA Compromise Procedures

In the event of a Subordinate CA key compromise, the following actions shall be performed:

- The CA shall notify the X9 Policy Authority and Issuing CA
- The Issuing CA shall revoke that CA’s certificate,

- And the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 18 hours after the notification.

- The Compromised CA shall also investigate and report to the trust anchor mangers and Issuing CA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA shall be re-established. Upon re-establishment of the CA, new Subscriber certificates shall be requested and issued.

For Subordinate CAs, when a Subscriber certificate is revoked because of compromise, suspected compromise, or loss of the private key, a revocation notice as specified in Section 4.9, shall be published at the earliest feasible time by the supporting CA, but in no case more than 24 hours after notification.

5.7.3.3 CSS Compromise Procedures

In case of a CSS key compromise, the CA that issued the certificate to the CSS shall revoke that certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner. The CSS shall subsequently be re-keyed. If the CSS is self-signed and the CSS certificate expiration is more than 7 days away, the CA shall immediately notify the X9 Policy Authority, relying parties, and any cross-certified PKIs of the CSS compromise so that they can notify all Subscribers and Relying Parties to remove trust in the CSS certificate from each Relying Party application, and install the re-keyed certificate.

It is recommended that the CSS have certificates with shorter lifetimes. A shorter lifetime minimizes the time that a compromised certificate is available.

5.7.3.4 RA Compromise Procedures

In the case that an RA's private key is compromised, the CA that issued the RA certificate shall revoke it, and the revocation information shall be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise shall be investigated by the CA in order to determine the actual or potential date and scope of the RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked.

5.7.4 Business Continuity Capabilities after a Disaster

CAs shall be required to maintain a Disaster Recovery Plan. The CA Disaster Recovery Plan shall be coordinated with any overarching Disaster Recovery Plan that the broader organization may have. The Disaster Recovery Plan shall identify what procedures are in place to mitigate risks to operations. The Disaster Recovery Plan shall include the following:

- Procedures for annual testing of processes to restore service,

- Contact personal for critical operations, and

- The order of restoral of equipment and services.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be re-established as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the CA cannot re-establish revocation capabilities prior to date and time specified in the *nextUpdate* field in the currently published CRL issued by the CA, then the inoperative status of the CA shall be reported to the X9 Policy Authority. The X9 Policy Authority shall decide whether to declare the CA private signing key as compromised and re-establish the CA keys and certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA private key are destroyed as a result the CA shall request that its certificates be revoked.

5.8 CA or RA Termination

When a CA operating under this policy terminates operations before all certificates have expired, entities shall be given as much advance notice as circumstances permit.

Prior to CA termination, notice shall be provided to all cross-certified CAs requesting revocation of all certificates issued to it. In addition:

- The CA shall issue a CRL revoking all unexpired certificates prior to termination; this CRL shall be made available until all certificates issued by the CA expire,
- The CA, CSS, and RA shall archive all audit logs and other records prior to termination,
- The CA, CSS, and RA shall destroy all private keys upon termination,
- The CA, CSS, and RA archive records shall be transferred to an appropriate authority specified in the CPS, and
- If a Root CA is terminated, the Root CA shall use secure means to notify the subscribers to delete all trust anchors representing the terminated CA.

6 TECHNICAL SECURITY CONTROLS

6.1.1 Key Pair Generation and Installation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in cryptographic modules validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher), or some other equivalent standard.

Multi-party control is required for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of CA key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation and video capturing the key pair generation.

6.1.1.2 RA Key Pair Generation

Cryptographic keying material used by RAs to sign request and authenticate to the CA shall be generated in hardware cryptographic modules validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher), or some other equivalent standard.

6.1.1.3 Subscriber Key Pair Generation

Subscriber key pair generation shall be performed by either the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

Hardware cryptographic modules validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher), should be used to generate all subscriber CA and RA key pairs, as well as pseudo-random numbers and parameters used in key pair generation.

6.1.1.4 Certificate Status Server (CSS) Key Pair Generation

Cryptographic keying material used by CSSs to sign status information shall be generated either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher), or equivalent, validated cryptographic modules.

6.1.2 Private Key Delivery to Subscriber

When CAs or RAs generate key pairs on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a subscriber shall not retain any copy of the signing key after delivery of the private signing key to the subscriber,
- The private key(s) must be protected from activation, compromise, or modification during the delivery process,
- The subscriber shall acknowledge receipt of the private key(s),

- Delivery shall be accomplished in a way that ensures that the correct keys and activation data are provided to the correct subscribers,
- For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it, and
- For electronic delivery of private keys, the key material shall be encrypted using a FIPS-approved cryptographic algorithm and key strength at least as strong as the private key.

Activation and any validation data shall be delivered using a separate secure channel.

The CA must maintain a record of the subscriber acknowledgment of receipt of the key.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the subscriber's verified identity to the public key.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a root CA shall be provided to the subscribers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution.

6.1.5 Key Sizes

This CP requires use of RSA, DSA, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed in the certificate profile document. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and validated in accordance with [FIPS 186-4].

Elliptic Curve public key parameters shall always be selected from the set specified in Section 7.1.3 Algorithm Object Identifiers.

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

See Section 7 CERTIFICATE, CRL AND OCSP PROFILES.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CAs shall use a hardware cryptographic module validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher) for signing operations.

RAs shall use a hardware cryptographic module validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher) for signing operations.

CSSs that provide status information shall use a cryptographic module validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher) for signing operations.

6.2.2 Private Key (N of M) Multi-Person Control

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA signing key. CA signing keys shall be backed up only under multi-party control. Access to CA signing keys backed up for disaster recovery shall be under multi-party control. The names of the parties used for multi-party control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

No Stipulation.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-party control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected using the same or stronger controls as the original. Backup procedures shall be included in the CA's CPS.

When using a Stateful Hash-based Signature scheme, such as those described in NIST SP 800-208, the private key material shall be stored in an HSM and shall not be exported or backed up.

6.2.4.2 Backup of CSS Private Key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected using the same or stronger controls as the original.

6.2.5 Private Key Archival

An archived key is an inactive key that is being saved in a secure manner for a non-operational purpose such as a legal requirement for future recovery. [X9.79-1]

This is the key management lifecycle stage when the asymmetric public or private key is retained past its operational period for purposes of post operation (or legal) purposes. For example, public keys used to validate digital signatures might be archived for re-validation or key pairs used for key establishment might be archived to recover the symmetric key. Key archive is recognized in the ANSI X9.24 [2.2] and ISO 11568 [2.7] standards whereas the NIST [2.8, 2.9] publications do not acknowledge termination.

Archived keys are not re-installed into operational environments; rather an archived key is temporary used in a restricted environment for a specific purpose. Once the purpose is completed the temporary key is immediately deleted.

Private signature keys should not be archived as the archived public key is sufficient to verify a digital signature. Other private keys such as those for key establishment or encryption may be archived for session key verification or decryption.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.

Transport keys shall be generated by a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be protected (e.g.,

encrypted) during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

Transport keys used to encrypt private keys shall be handled in the same way as the private key.

6.2.7 Private Key Storage on Cryptographic Module

No Stipulation.

6.2.8 Method of Activating Private Key

Activation of the CA signing key shall be performed under multiparty control, see Section 5.2.2.

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. When not in use, the cryptographic key(s) should be deactivated and stored securely.

6.2.10 Destroying Private Key

Individuals in trusted roles shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys according to manufacturer's instructions which may or may not require physical destruction when they are no longer needed.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key or public key certificate may be archived as part of the activity described in Section 5.5 for Records Archival. Expired or revoked public keys or certificates may be archived for historical signature verification or session key verification. Alternatively, the Subject Key Identifier (SKI) may be archived for public key verification. An archived key is an inactive key that is being saved in a secure manner for a non-operational purpose such as a legal requirement for future recovery. [X9.79-1]

This is the key management lifecycle stage when the asymmetric public or private key is retained past its operational period for purposes of post operation (or legal) purposes. For example, public keys used to validate digital signatures might be archived for re-validation or key pairs used for key establishment might be archived to recover the symmetric key. Key archive is recognized in the ANSI X9.24 [2.2] and ISO 11568 [2.7] standards whereas the NIST [2.8, 2.9] publications do not acknowledge termination.

Archived keys are not re-installed into operational environments; rather an archived key is temporary used in a restricted environment for a specific purpose. Once the purpose is completed the temporary key is immediately deleted.

Private signature keys should not be archived as the archived public key is sufficient to verify a digital signature. Other private keys such as those for key establishment or encryption might be archived for session key verification or decryption.

6.3.2 Certificate Operational Periods and Key Usage Periods

The usage period for CA key pairs shall not exceed the use period stated in the CPS.

All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

For OCSP responders operating under this policy, the maximum private key usage shall not exceed 3 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Mechanisms should comply with X9.24 Part 1 and X9.135 (currently in draft).

6.4.3 Other Aspects of Activation Data

No Stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

6.5.1.1 Access Control

Access to information such as sensitive details about customer accounts, passwords, and ultimately, CA-related private keys should be carefully guarded, along with the machines housing such information.

6.5.1.1.1 Access Control Policy and Procedures

The CA shall create and document roles and responsibilities for each trusted role employee job function in the CPS. The CA shall create and maintain a mapping of these trusted roles and their associated responsibilities to specific employees and their accounts on CA and/or RA systems.

6.5.1.1.2 Account Management

Information system account management features shall ensure that users access only that functionality permitted by their role or function. All account types with access to information systems shall be documented along with the conditions and procedures to follow in creating new accounts. Groups and roles shall have a documented relationship to the business or mission roles involved in operating the CA.

Section 5.2.1 of this document defines roles and job functions for personnel that the CA will use when defining access control mechanisms. The CA shall employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role shall be justified based upon business need. The CA shall take appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. The CA shall review at least quarterly all active accounts to match active authorized users with accounts, and disable or remove any accounts no longer associated with an active authorized user. Systems accessed less than quarterly shall have their accounts reviewed within 30 days of account access.

All account administration activities shall be logged and made available for inspection by appropriate security personnel. Account administration activities that shall be audited include account creation, modification, enabling, disabling, group or role changes, and removal actions. See Section 5.4 for detailed requirements for these logs.

Guest/anonymous accounts for logon to information systems shall be prohibited. Accounts shall be assigned to a single user and shall not be shared.

6.5.1.1.3 Least Privilege

In granting rights to accounts and groups, the CA shall employ the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The CA shall explicitly authorize access to accounts and groups for controlling security functions and security-relevant information. The CA shall authorize access to privileged commands and features of information systems only for specific, organization-defined compelling operational needs and documents the rationale for such access. The CA shall require that users of information systems with access to administrative privileges to utilize non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

6.5.1.1.4 Access Control Best Practices

No Stipulation.

6.5.1.1.5 Authentication: Passwords and Accounts

When the authentication mechanism uses operator selectable passwords, strong passwords shall be employed, as defined in X9.117 Annex B. Passwords for CA authentication shall be different from non-CA systems.

Measures must be in place to identify, to detect and to deter and prevent brute force login attempts.

Refer to X9.117 Annex B for password consideration.

6.5.1.1.6 Permitted Actions without Identification or Authentication

The CA shall document in the CPS a specific list of actions that may be performed on specifically enumerated information systems without identification or authentication, such as retrieving or verifying a published CRL from an Internet-accessible server or accessing a publicly available website. Furthermore, the organization shall document and provide supporting rationale in its security policy and procedures an enumerated list of user actions and systems not requiring identification or authentication (i.e., anonymous access).

6.5.1.2 System Integrity

6.5.1.2.1 System Isolation and Partitioning

All trusted components should be logically separated from each other, and shall be logically separated from any untrusted components of the CA system. The CPS shall document how this logical isolation of components is accomplished.

Security critical processes shall be isolated from processes that have external interfaces. For example, the CA signing processes shall be isolated from registration processes. The CPS shall outline how security critical processes are protected from interference by externally facing processes.

If there are system resources shared amongst trusted and/or untrusted processes, the underlying system(s) shall prevent any unauthorized and unintended information transfer between processes via those shared system resources.

The CA shall develop and document controlled procedures for transferring software updates, configuration files, certificate requests, and other data files between trusted components.

6.5.1.2.2 Malicious Code Protection

The CA system shall employ malicious code protection mechanisms to mitigate the risk of malicious code on CA system components. Malicious code on trusted CA components could allow an attacker to issue fraudulent certificates, create a rogue subordinate or signing CA server, or compromise the availability of the system.

6.5.1.2.3 Software and Firmware Integrity

The CA shall employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on CA systems. Access control mechanisms and configuration management processes (see Section 6.5.1.1 and 6.6.2) shall ensure that only authorized CA Administrators are capable of installing or modifying firmware and software on CA systems.

CA servers shall implement automated or procedural technical controls to prevent and detect unauthorized changes to firmware and software. Example technical controls include signature verification prior to firmware/software installation or execution (such as firmware protections that comply with [SP800-147] or [SP800-147B]), or hash-based white-listing of executables. Unauthorized software or firmware detected by these mechanisms should be blocked from executing. Any instances of unauthorized firmware or software detected by the system shall be logged, and CA Administrators shall be notified of these events.

6.5.1.2.4 Information Protection

The CA shall protect the confidentiality and integrity of sensitive information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer. The CA shall employ technical mechanisms to prevent unauthorized changes or accesses to this information, such as access control mechanisms that limit which users are authorized to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers shall be stored in an encrypted format.

Mechanisms, Policies and Practices should comply with X9.141.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls address various aspects related to the development and change of the CA system through aspects of its life cycle.

The CA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process as defined for the system baseline.

In order to prevent incorrect or improper changes to the CA system, the CA system shall require multi-party control for access to the CA system when changes are made.

For any software developed by the CA, evidence shall be produced relating to the use of a defined software development methodology setting out the various phases of development, as well as implementation techniques intended to avoid common errors to reduce the number of vulnerabilities. Automated software assurance (i.e., static code analysis) tools shall be used to catch common error conditions within developed code. For compiled code, all compiler warnings shall be enabled and

addressed or acknowledged to be acceptable. Input validation shall be performed for all inputs into the system.

Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device). The hardware and software shall be verified as having been supplied from the vendor, with no modifications, and be the version intended for use. Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

All data input to CA system components from users or other system components shall be validated prior to consumption by the receiving entity. Validating the syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match the expected definitions for format and content.

6.6.2 Security Management Controls

A list of acceptable products and their versions for each individual CA system component shall be maintained and kept up-to-date within a configuration management system. Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorized software. Online CA systems shall have automated mechanisms to inventory on at least a daily basis software installed on a system and alert operators if invalid software is found. For offline CA systems, logs shall be checked when systems are accessed at least annually.

To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating. The CA system shall maintain a list of ports, protocols, and services that are necessary for the correct functioning of each component within the CA system. There shall be automated mechanisms to monitor the running processes and open ports against the permitted list.

To validate the integrity of the CA system, automated tools that validate all static files on a component shall be in operation to notify operators when a protected file has changed.

The CA system shall establish and document mandatory configuration settings for all information technology components which compose the CA system. All configuration settings capable of automated assessment shall be validated to be set according to the guidance contained within a documented security configuration checklist on at least daily basis for powered on systems or next power-on for systems which are not left powered-on.

6.6.3 Life Cycle Security Controls

For flaw remediation, the CA shall scan all online CA systems for vulnerabilities using at least one vulnerability scanner at least every quarter. The use of multiple scanners on the most sensitive systems is strongly encouraged.

Each vulnerability found shall be entered into a vulnerability tracking database, along with the date and time of location, and shall be remediated as quickly as operationally possible as per the incident response plan described in Section 5.7.1. Remediation shall be entered into the vulnerability database as well (including date and time).

The CA shall monitor relevant notification channels for updates to packages installed on CA systems (including networking hardware). CAs shall have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. For critical vulnerabilities, the CA shall evaluate and install the update as quickly as operationally possible as per the incident response plan described in section 5.7.1. For less critical vulnerabilities, the CA shall evaluate each package to determine whether an update is required,

and if so, that update shall be applied to all affected CA systems within 48 hours. A log shall be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the CA can discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CA shall correct such errors as quickly as operationally possible as per the incident response plan described in Section 5.7.1 and shall document the reason for the error, and the associated correction.

Remediation activities should not cause unavailability of revocation information.

6.7 Network Security Controls

Many components of a CA are connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care should be taken to ensure those connections do not adversely impact the security of those components. Guidelines for effective CA networking security are discussed in the following sections.

6.7.1 Isolation of Networked Systems

Communication channels between the network-connected CA components and the trusted CA processing components shall be protected against attack. Furthermore, information flowing into these CA components from the network-connected CA components shall not lead to any compromise or disruption of these components.

The components of a CA requiring direct network connections shall be minimized. Those networked components shall be protected from attacks through the use of firewalls to filter unwanted protocols (utilizing access rules, whitelists, blacklists, protocol checkers, etc., as necessary). Data loss prevention tools shall be employed to detect inappropriate leakage of sensitive information.

Root CA systems shall be kept offline.

6.7.2 Availability

CA systems shall be configured, operated, and maintained to maximize uptime and availability. Scheduled downtime shall be announced to Subscribers.

6.7.2.1 Denial of Service Protection

CAs shall state acceptable methods to request revocation in their CPS. At least one of those methods shall be out of band (i.e., network connectivity is not required).

CAs shall take reasonable measures to protect certificate request and issuing services from known DoS attacks. The CA request and issuing availability required by a Subscriber application shall be stated in its CPS.

6.7.2.2 Public Access Protections

Personal Identity Information used in the identity proofing process shall be protected at all times in accordance with local law and shall not be available to public access.

Revocation information and CA certificate information shall be made available in accordance with Section 2 of this CP. However, individual subscriber certificates need not be made available for public access.

6.7.3 Communications Security

6.7.3.1 Transmission Integrity

Source authentication and integrity mechanisms shall be employed to all certificate request, manufacture, and issuance communications, including all related services irrespective of whether those services are hosted on the same or different platform than the CA workstation. Communications between CAs and RAs shall be mutually authenticated to detect changes to information during transmission.

Source authentication for RA to Subscriber communications may employ either online (cryptographic) or offline methods. Offline RA to Subscriber communications shall be protected by traditional means that are legally sufficient (e.g., ink signatures on paper). Initial Subscriber data that has been collected in an unauthenticated or mutable manner shall be verified by the RA before the certificate request is created.

6.7.3.2 Transmission Confidentiality

Intra-CA communications that cross the physical protection barrier of the certificate-signing portion of the CA system shall be confidentiality-protected. Services used by the CA system that are not administered by the CA administrative staff shall provide protection commensurate with the CP.

Confidentiality of Subscriber data shall be maintained. CA to RA communications shall employ encryption to prevent unauthorized disclosure of information during transmission. The level of protection for RA to Subscriber communications shall be determined by the Subscriber (or the Subscriber's organization); in any case, the RA shall be prepared to employ typical techniques for Internet confidentiality (e.g., single-side authenticated TLS).

6.7.3.3 Network Disconnect

Network connection lifetimes between co-located services are driven by the traffic between them. Connections should be terminated after a period of inactivity that is defined in the CA's CPS.

6.7.3.4 Cryptographic Key Establishment and Management

Cryptographic key management for network connections between CAs, RAs and Subscribers includes all aspects of cryptographic key life cycle: key generation, distribution, storage, access and destruction for both symmetric and asymmetric keys.

Key generation and management shall be performed in cryptographic modules that are validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher). Keys that are backed up for business continuity shall have protection comparable to the operational key. All cryptographic key management processes shall be described in the CA's CPS.

RAs shall employ key protection mechanisms implemented in a hardware cryptographic module validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher), or some other equivalent standard (e.g., smart token).

Keys that protect the integrity and confidentiality of an enrollment session shall be generated and managed using cryptographic mechanisms implemented in a cryptographic module validated to either FIPS 140-2 Level 3 (or higher) or FIPS 140-3 Level 3 (or higher), or some other equivalent standard.

6.7.3.5 Application Session Authenticity

For stateless connections between CAs, RAs and Subscribers, a unique, random session identifier for each session shall be generated. The session identifiers shall be validated for each request. Session identifiers shall be invalidated at logout to preserve session authenticity. A logout capability shall be provided with an explicit logout message that indicates the reliable termination of authenticated communications sessions.

6.7.4 Network Monitoring

The CA shall be monitored to detect attacks and indicators of potential attacks. This includes intrusion detection tools.

6.7.4.1 Events and Transactions to be Monitored

The CA shall identify a list of essential information, transaction types and thresholds that indicate potential attacks. These events should include:

- Bandwidth thresholds,
- Inbound and outbound communication events and thresholds,
- Unauthorized network services,
- CPU usage thresholds,
- Certificate request thresholds from a single RA, and
- Access Control thresholds

6.7.4.2 Monitoring devices

A CA shall deploy intrusion detection tools and other monitoring devices with the CA to collect intrusion information and at ad hoc locations within the system to track specific types of transactions of interest to the organization. These monitoring devices shall be configurable to react to specific indications of increased risk or to comply with law enforcement requests. The devices shall alert security personnel when suspected unauthorized activity is occurring. These devices shall be network-based and should be also host-based. Only persons holding trusted roles shall manage the operating state of monitoring devices. The CA should utilize automated tools to support near real-time analysis of events and these tools should be integrated into access control and flow control mechanisms for rapid response to attacks.

6.7.4.3 Monitoring of Security Alerts, Advisories, and Directives

A CA shall monitor information system security alerts, advisories, and directives on an ongoing basis.

The CA shall generate and disseminate internal security alerts, advisories, and directives as deemed necessary. The CA should employ automated mechanisms to make security alert and advisory information available throughout the organization as needed. The CA shall implement security directives in accordance with established time frames, or notifies the compliance auditor of the degree of noncompliance.

6.7.5 Remote Access/External Information Systems

A public RA or CA may be deployed in a private datacenter, hosted in a third-party datacenter, or deployed in a public cloud.

A private RA or CA may be deployed in a private datacenter, hosted in a third-party datacenter, or deployed in a public cloud.

A public cloud provider may operate its own RA and CA within its own public cloud infrastructure.

- Subscriber access to a public RA may be over a public network but access to a private RA may be over a public network or a private network.

- CA Administrator access to a public RA or CA may be over a public network or a private network. (e.g., the CA system operator, system officer, or PKI administrator)
- Auditor access to a public RA or CA may need onsite access.
- Auditor access to a private RA or CA may need onsite access.
- Auditor access to a public cloud may have limited onsite access.

6.7.5.1 Remote Access

If remote access is permitted, access must include multi-factor authentication. Remote access to off-line components is prohibited.

6.7.5.2 Bastion Host

All access to CA signing systems and RA servers shall be mediated by a bastion host (i.e., a machine that presents a limited interface for interaction with the other elements of the CA). No direct access is permitted. The bastion host shall be patched regularly, maintained, and shall only run applications required to perform its duties.

6.7.5.3 Documentation

The CA shall document allowed methods of remote access to CA systems, including usage restrictions and implementation guidance for each allowed remote access method.

6.7.5.4 Logging

See also Section 5.4.

Logging shall be performed on the bastion host for each remote access session with the CA, consistent with Section 5.4. In particular, logs shall include date and time of the connection, the authenticated identity of the requestor, the IP address of the remote system and should also include the commands sent to the bastion host. Logs shall have controls in place to ensure integrity.

6.7.5.5 Automated Monitoring

Automated monitoring shall be performed on all remote sessions with the bastion host, and on all interactions between the bastion host and other CA systems. Upon detection of unauthorized access, the CA shall terminate the connection and log the event.

6.7.5.6 Authentication

Any machine used to access CA systems remotely shall require two or more factors of authentication. In particular, a hardware token shall be required. Authentication shall occur between the remote machine and the bastion host.

6.7.5.7 Communications Security for Remote Access

All communications between the remote access host and the CA system shall be protected by [FIPS 140], or some other equivalent standard, validated cryptography, as required for CA to RA communications in Section 6.7.4.5. Session identifiers shall be invalidated at logout to preserve session authenticity, as described in Section 6.7.4.6, Session Authentication.

6.7.6 Penetration Testing

The CA System shall annually, or whenever major system changes occur, conduct external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems. Penetration testing shall occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

A standard method for penetration testing consists of:

- Pretest analysis based on full knowledge of the target system,
- Pretest identification of potential vulnerabilities based on pretest analysis, and
- Testing designed to determine exploitability of identified vulnerabilities.

Detailed rules of engagement shall be agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Vulnerabilities uncovered during penetration testing shall be incorporated into the vulnerability remediation process.

Refer to X9.111 for specific information related to Penetration Testing.

6.8 Time-Stamping

Asserted times shall be accurate to within three minutes of Coordinated Universal Time. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

Certificates issued by a CA under this policy shall conform to the X9 Profiles Document. Any deviations from this profile must be approved by the X9 Policy Authority and documented within the CA's CPS.

Each certificate issued by a CA shall be given a serial number consisting of a unique (within the scope of the issuing CA), positive integer, not longer than 20 octets.

See the X9 Profiles Document for additional Certificate Profile information.

7.1.1 Version Number(s)

The CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

For CA certificates, the following extension values shall be set:

- The keyUsage extension shall be marked critical and assert at least the keyCertSign and cRLSign usages.
- The extended key usage extension may assert the extended key usages that will be asserted in certificates issued by the CA. If the extended key usage extension is present, then the anyExtendedKeyUsage key purpose shall not be asserted.
- The basicConstraints extension shall be marked critical and assert the CA value. Subordinate CA certificates shall specify a pathLenConstraint consistent with their intended use case.

For end-entity certificates, the following extension values shall be set:

- The keyUsage extension shall be marked as critical and shall assert the minimum number of key usages required for functionality.
- The extendedKeyUage extension shall assert the minimum number of extended key usages (extKeyUsage) required for functionality in alignment with their use case. The anyExtendedKeyUsage key purpose shall not be asserted.
- If included, the basicConstraints extension shall not have the cA field asserted.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use a signature algorithm approved for use in the X9 SD-34 Registry, defined in an X9 standard, or one of the following OIDs:

id-EdDSA25519	{iso(1) identified-organization(3) thawte(101) id-Ed25519(112)}
id-EdDSA448	{iso(1) identified-organization(3) thawte(101) id-Ed448(113)}

Where certificates are signed using RSA with Probabilistic Signature Scheme (PSS) padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. If RSA signatures with PSS padding are used, then the hash algorithms and OIDs specified below shall be used:

id-sha256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use a signature algorithm approved for use in the X9 SD-34 Registry, defined in an X9 standard, or one of the following OIDs:

id-EdDSA25519	{iso(1) identified-organization(3) thawte(101) id-Ed25519(112)}
id-EdDSA448	{iso(1) identified-organization(3) thawte(101) id-Ed448(113)}

7.1.4 Name Forms

The subject field in certificates issued under this policy shall be populated with an X.500 Distinguished Name as specified in Section 3.1.1.

The issuer field of certificates issued under this policy shall be populated with a non-empty X.500 Distinguished Name as specified in Section 3.1.1.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Refer to section A.6 of the X9 Profiles Document.

7.1.7 Usage of Policy Constraints Extension

The CAs must not assert policy constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this policy shall not contain a critical certificate policies extension. Certificate policy extension must be non-critical.

7.2 CRL Profile

CRLs issued by a CA under this policy shall conform to the CRL profile specified in the X9 Profiles Document.

7.2.1 Version Number(s)

CRLs issued by a CA shall be X.509 Version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in the X9 Profiles Document.

7.3 OCSP Profile

OCSP Responses issued by a CA under this policy shall conform to the OCSP profile specified in the X9 Profiles Document.

Certificate status servers (CSSs) operated under this policy shall sign responses using algorithms designated for CRL signing.

7.3.1 Version Number(s)

CSSs operated under this policy shall use OCSP version 1.

7.3.2 OCSP Extensions

Detailed OCSP profiles addressing the use of each extension are specified in the X9 Profiles Document.

8 COMPLIANCE AND OTHER ASSESSMENTS

The CA organization shall at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates; including being licensed or registered, if required, as a CA in each legal jurisdiction in which it operates.

2. Be authorized by X9 to issue Certificates and operate its PKI to support those use case(s) listed in their user agreement(s).

3. Comply with the Requirements in this CP.

4. Complete initial and periodic assessments based on the current version of the WebTrust Principles and Criteria for Certification Authorities.

8.1 Frequency or Circumstances of Assessment

CA and RA entities shall be subject to a periodic compliance assessment at least once per year. CA entities that do not meet compliance may be subject to more frequent assessment requirements. The periods covered by the WebTrust assessment must remain unbroken from the date of being trusted by X9.

8.2 Qualifications of Assessor

The assessor must demonstrate competence in the field of compliance assessments, and must be thoroughly familiar with the CA's CPS and this CP. The WebTrust Assessor must perform such compliance assessor as a regular ongoing business activity. In addition to the previous requirements, the assessor must be included on the list of approved WebTrust practitioners maintained by the Chartered Professional Accounts Canada.

8.3 Assessor's Independence

The WebTrust Assessor firm shall be independent from the entities (CA and RAs) being assessed, based on applicable professional standards. To ensure independence and objectivity, the WebTrust Assessor must not have served the entity in developing or maintaining the CA entity's operation or certificate practices statement. The X9 Policy Authority shall determine whether a WebTrust Assessor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance assessment is to verify that a CA and its recognized RAs comply with all the requirements of the current versions of the CA's CPS and the X9 Certificate Policy for Financial Services. The scope of the WebTrust engagement shall include all root and subordinate CAs, including any bridge CAs, trusted by the X9 hierarchy.

8.5 Communication of Results

WebTrust report and identification of corrective measures shall be provided to the X9 Policy Authority one week from the completion and within three months of the end of the assessment period.

8.6 Actions Taken as a Result of Deficiency

When the WebTrust Assessor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI, the following actions shall be performed:

- The WebTrust Assessor shall document the discrepancy in the WebTrust Assessment Report.
- The CA shall provide a management assertion accompanying the WebTrust Assessment Report.
- The CA shall be responsible for providing additional details, as required, as to the nature of the discrepancy to the X9 Policy Authority.
- The CA will propose a remedy, including expected time for completion, to the appropriate X9 Policy Authority.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the X9 Policy Authority may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The X9 Policy Authority shall provide to the CA its procedures for making and implementing such determinations. The X9 Policy Authority has the right to require periodic status updates on outstanding remediation activities. A special compliance assessment may be required to confirm the implementation and effectiveness of any remedy.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Issuing CA's, at their discretion, may charge fees for issuance or renewal of certificates.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

This CP contains no financial limits on the use of certificates issued by CAs under the policy. Rather, entities, acting as relying parties, may determine what financial limits, if any, they wish to impose for consummating a transaction using such certificates.

9.2.1 Insurance Coverage

If applicable insurance coverage exists, the amount of coverage or nonexistence of coverage will be documented in the CPS.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

If insurance or warranty coverage exists the amount of coverage or nonexistence of coverage will be documented in the CPS.

9.3 Confidentiality of Business Information

The CA shall protect the confidentiality of sensitive business information stored or processed on CA systems that could lead to abuse or fraud. The CPS shall specify what constitutes sensitive business information for that CA.

Public access to CA organizational information shall be determined by the CA.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The CA shall develop, implement, and maintain a privacy plan. The privacy plan shall document what personal information or personal data is collected as defined under the applicable legal regimes, how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2 Information Treated as Private

CAs shall protect all personal information or personal data from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of any archives containing personal information or personal data that are maintained by CAs operating under this policy shall not be released except as allowed by the privacy plan.

9.4.3 Information not Deemed Private

This is defined in the use case specific CP.

9.4.4 Responsibility to Protect Private Information

Personal information or personal data must be stored securely and may be released only in accordance with the privacy statement of the CA.

9.4.5 Notice and Consent to Use Private Information

The CA may not provide any notice or obtain the consent of the subscriber in order to release private information unless in accordance with other stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Policy, or Judicial or Administrative Process

The CA shall not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The CA shall not knowingly violate intellectual property rights owned by others.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CAs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the requirements of this policy.

A CA that issues certificates that assert a policy defined in this document shall conform to the requirements of this document, including, if applicable:

- Providing a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance with the requirements of the CPS.

- If the CA uses RA(s), the CA must ensure that registration information is accepted only from approved RAs operating under an approved CPS.

- Use of only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.

- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with Section 9.6.3.

- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the requirements of this policy, and comply with a CPS approved by the Policy Authority for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. A compliant RA shall:

- Maintain its operations in conformance to the stipulations of the approved CPS.

- Include only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.

- Ensure that obligations are imposed on subscribers in accordance with section 9.6.3, and that subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

A subscriber shall be required to acknowledge acceptance of the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For device certificates, at least one subscriber from the subscriber organization shall acknowledge acceptance of the requirements the organization shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers shall:

- Accurately represent themselves in all communications with Certificate Service Providers.

- Protect associated private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.

- Promptly notify the appropriate CA (or its agent) upon suspicion of loss or compromise of any applicable private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.

- Abide by all the terms, conditions, and restrictions levied on the use of associated private key(s) and certificate(s).

9.6.4 Relying Parties Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

An entity that has a device certificate issued to it shall be responsible for all actions taken or assertions made under that device certificate.

9.7 Disclaimers of Warranties

Any stakeholders operating under this policy shall not disclaim any representations or warranties described in this CP.

9.8 Limitations of Liability

CAs may limit their liability to any extent not otherwise prohibited by this CP, provided that the CA remains responsible for complying with this CP and the CA's CPS. Such limitations, for example, may be set forth in applicable agreements between any Certificate Service Provider and its affiliates/customers/etc.

9.9 Indemnities

CAs may establish indemnities including, for example, in applicable agreements between the PKI/CA and its affiliates/customers/etc.

9.10 Term and Termination

9.10.1 Term

This CP and any amendments to it shall be effective upon publication and remain in effect until replaced with an updated version or terminated by the policy authority.

9.10.2 Termination

This CP, any CAs under this CP, and the associated PKI shall remain in effect until terminated by the Policy Authority.

9.10.3 Effect of Termination and Survival

The requirements of this CP shall remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

The Policy Authority shall establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

The Policy Authority shall review this CP at least once every year. Corrections, updates, or changes to this CP may be made publicly available at the discretion of the Policy Authority. Suggested changes to this CP shall be communicated to the contact in Section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the entity requesting the change.

9.12.2 Notification Mechanism and Period

Any amendment to the CP approved by the Policy Authority shall become effective 30 days following the publication of the amended CP and all known concerned stakeholders (PA staff, relying parties, subscribers, etc.) shall be notified.

9.12.3 Circumstances Under Which OID Must be Changed

At the discretion of the Policy Authority, the OID may be changed based on any change of circumstances.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the state of Utah shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions.

9.15 Compliance with Applicable Law

All CAs operating under this policy shall comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by contract, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of X9 (such consent not to be unreasonably withheld), except that X9 may assign and delegate this CP to any party of its choosing.

The CPS must enumerate all duties and operations that may be delegated to other organizations or parties. The PA and PMO will review and determine what may or may not be delegated.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in Section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

End of Document